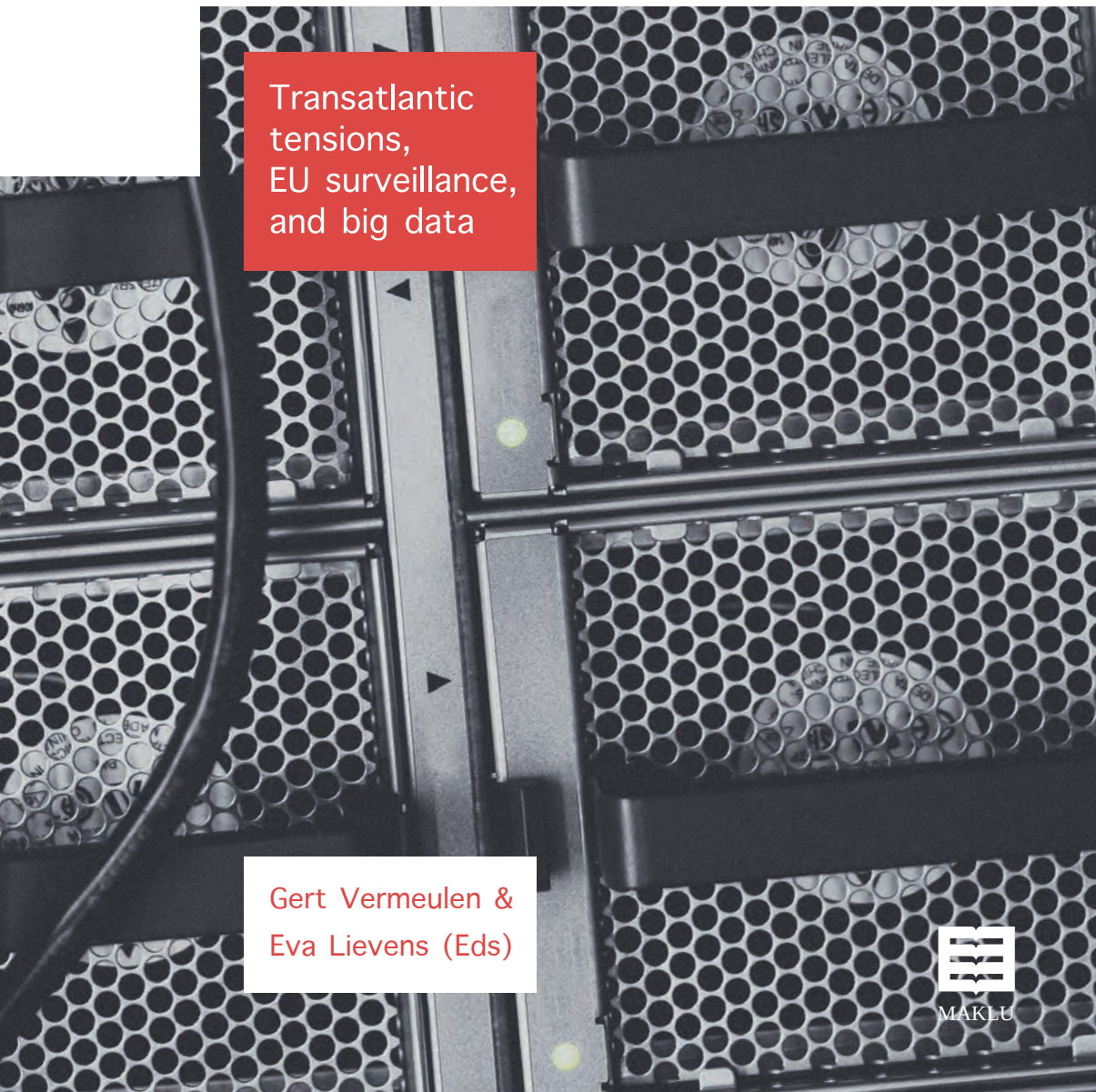
Data Protection and Privacy under Pressure



Transatlantic tensions, EU surveillance, and big data

Gert Vermeulen &
Eva Lievens (Eds)

MAKLU

Data Protection and Privacy under Pressure

Data Protection and Privacy under Pressure

Transatlantic tensions, EU surveillance, and big data

Gert Vermeulen
Eva Lievens
(Eds)

Maklu

Antwerp | Apeldoorn | Portland

Data Protection and Privacy under Pressure
Transatlantic tensions, EU surveillance, and big data
Gert Vermeulen and Eva Lievens (Eds)
Antwerp | Apeldoorn | Portland
Maklu
2017

341 p. – 24 x 16 cm
ISBN 978-90-466-0910-1
D/2017/1997/89
NUR 824

Maklu-Publishers
Somersstraat 13/15, 2018 Antwerp, Belgium, info@maklu.be
Koninginnelaan 96, 7315 EB Apeldoorn, The Netherlands, info@maklu.nl
www.maklu.eu

USA & Canada
International Specialized Book Services
920 NE 58th Ave., Suite 300, Portland, OR 97213-3786, orders@isbs.com,
www.isbs.com

TABLE OF CONTENTS

Preface

GERT VERMEULEN & EVA LIEVENS

Since the Snowden revelations, the adoption in May 2016 of the General Data Protection Regulation and several ground-breaking judgments of the Court of Justice of the European Union (CJEU), data protection and privacy have been at the top of the agenda of policymakers, industries and the legal research community.

Against this backdrop, it is the aim of this book to shed light on a number of key developments where individuals' rights to data protection and privacy are at stake or 'under pressure', by giving the floor to a variety of authors with different backgrounds and expertise.

We are honoured that, in an introductory chapter, Joe Cannataci was willing to reflect on his mission and experiences as the UN Special Rapporteur on the right to Privacy. His contribution provides a behind-the-scenes look at his activities and puts forward a number of thought-provoking ideas and proposals.

A first section, "Transatlantic tensions", pertains to the persistent transatlantic tensions around various EU-US data transfer mechanisms and EU jurisdiction claims over non-EU-based companies, sparked by milestone court cases. Since the early 2000s, the (in)adequacy of the US data protection regime has been a continuous point of discussion and concern in EU-US relations, both commercial and in the sphere of national security, public interest and law enforcement. This notwithstanding, the post 9/11 climate gave rise to the conclusion of several EU-US agreements for exchange of personal data. For 15 years, commercial data transfers from the EU to the US were legitimised if corporate US recipients were self-certified under the Safe Harbour principles, until invalidated in late 2015 by the CJEU in the Schrems case following the Snowden revelations in the Summer of 2013. Three chapters, respectively by Gert Vermeulen, Stefano Saluzzo and Elif Mendos Kuşkonmaz, discuss the EU-US Privacy Shield – successor of the Safe Harbour agreement – and the EU-US PNR agreement, critically assessing their potential and flaws. In their respective chapters, Brendan Van Alsenoy and Alberto Miglio delve into jurisdictional issues around the competence of EU DPA's and courts to urge US companies to comply with EU data protection law, before and after entry into force of the GDPR.

A second section, "EU Surveillance", scrutinises the expanding control or surveillance mechanisms and interconnection of databases in the areas of migration control, internal security and law enforcement, and oversight thereon.

Initially in the aftermath of 9/11, and more recently with the migration crisis and renewed problems with terrorism, radicalism and extremism, the EU has continued to step up internal security, by putting in place and further enhancing control or surveillance mechanisms and databases, and making them interoperable for multiple purposes. Niovi Vavoula sketches the evolution of pan-European immigration databases and highlights key privacy concerns prompted by their establishment, operation and reconfiguration over time. Wojciech Wiewiórowski respectively Mario Oetheimer and Ioannis Kouvakas discuss standards and proper oversight mechanisms in the domain of surveillance for both public security purposes and national intelligence.

In a third section, "Big data", current and future legal challenges related to big data and automated decision-making are explored in different contexts. The processing and combining of enormous amounts of information and the analysis of that data to inform decisions, facilitated by sophisticated algorithms, is fast becoming a standard practice in many different sectors. Industry, healthcare organisations and law enforcement authorities are only a few actors that increasingly rely on big data to take decisions that, on the one hand, could benefit society in general (eg economic growth, prediction of epidemics or crime), but, on the other hand, may have a significant impact on individuals (eg invasion of the right to privacy, the 'right to not to know' in healthcare, or far-reaching profiling for commercial purposes). The section explores the potential of big data and reflects on its possible impact on the right to privacy and data protection in three fairly different contexts. Anneleen Rummens, Wim Hardyns and Lieven Pauwels provide a comparative overview of predictive policing methods reported in criminological literature, focusing on their characteristics, strengths, weaknessess, methodological parameters, predictive ability and effectiveness. Claudia Seitz reflects on the use and possible privacy impacts of big data for healthcare and pharmaceutical purposes, such as for 'personalised medicine'. Finally, Valerie Verdoodt and Eva Lievens explore the use of big data for personalised advertising targeting children and consider how the interests of children and advertisers can be reconciled.

We are indebted to Ligeia Quackelbeen, Stéphanie De Coensel, Yente Neelen, Ingrida Milkaite and Argyro Chatzinikolaou for their invaluable assistance in the copy-editing and proofreading process.

25 November 2017

Games people play

Unvarnished insights about privacy at the global level

JOSEPH A. CANNATACI[1]

1. PROLOGUE

Why does Country P appear unconcerned that its legal systems does not adequately protect a woman whose genitalia were photographed without permission by a health care worker during a gynaecological procedure? Why does country M appear to be permitting extremely intrusive surveillance by its security apparatus on journalists? Does country M appear to be permitting extremely intrusive surveillance by its security apparatus on journalists and human rights activists? Is country X being honest or cynical when it attempts to persuade me that its system of safeguards for surveillance is a truly rigorous and effective one? Are the Embassy staff of country Y bluffing or being dead serious when they threaten me with *serious consequences* if I were to follow a course of action which they find displeasing? Was that a death threat that just came at me over the phone or is this job making me paranoid? What are we going to do about that country whose government published on-line 30 years' worth of sensitive medical data for 10% of its citizens and failed to de-identify the data subjects in a robust manner? Country Z is, most surprisingly, questioning my very right to receive and consider complaints about privacy infringements from individuals yet it presents itself as a champion of human rights? Country W backs me in some areas yet pulls the rug out from under my feet by introducing questionable legislation which patently does *not* uphold privacy as a universal right.

These are only some of the questions and issues arising during a random working day of the UN Special Rapporteur on the right to Privacy (SRP). Not only national governments seem to be constantly playing games. Also some

[1] United Nations Special Rapporteur on the right to Privacy; Head of the Department of Information Policy & Governance and Deputy Dean, Faculty of Media & Knowledge Sciences, University of Malta; Full Professor, Chair of European Information Policy & Technology Law, Co-Founder and Co-Director of the Security, Technology & e-Privacy (STeP) Research Group, Faculty of Law, University of Groningen; Full Professor (adjunct), Security Research Institute, School of Computer and Security Science, Edith Cowan University Australia. Email: jcannataci@sec.research.um.edu.mt.

international NGOs have been playing the diplomacy game and trying to move with the diplomatic currents so much that they seem incapable of realising that now is the time to swim against the current, because otherwise it will sweep them to the inevitable destruction of their goals. Needless to say, commercial corporations are also playing games, between themselves, with governments and some of them with the me too.

2. GUIDE FOR THE READER

When invited to write this contribution, I thought about doing something unusual rather than the usual spiel about privacy and how important it is as a right - though of course it is. So I chose for a think-piece which is partially based on an approach such as *a day in the life of, or a year in the life of...* - a piece which can be occasionally playful as well as dead serious. After decades of trying to explain technology to lawyers, and law to techies, I have found out that using the dry language of scholarship does not necessarily work when going across disciplines and that a conversational style sometimes gets the job done much better.

It is most unusual for me to write in the first person or to rely on my personal experiences and archives as the main source for a contribution in a scholarly book. For more than three decades I have analysed and commented on the behaviour of, and the results achieved by, other actors. When appointed the UN's first SRP on the 3rd July 2015 I had absolutely no idea that two years down the line I would abandon or suspend my usual style of writing in order to draw more on personal experience. Perhaps it is important to break the silence about certain matters, even if it were only to examine and challenge the expectations that people worldwide may have from the machinery of the UN. For surely it is a key function of legal and other scholars to understand the rule-making process in order to be able to better interpret the results of that process. This contribution therefore attempts to capture the unvarnished story behind the scene, unveiling the omissions and lacunae, and offering an insight into the successes and the failures of the office of the SRP in developing privacy protection. Understanding that games are being played, and when, how, why and by whom, is essential to the development of the subdiscipline we today identify as technology law.

I should perhaps also open with a slight apology to Eric Berne, the author of the best-selling non-fiction work of the 1960s *Games People Play* for the title of this contribution is an intentional pun, in multiple ways[2], based on some of his ideas and their subsequent development. Berne was a Canadian psychiatrist who gave birth to that field of psychoanalytic theory called *Transactional Analysis* (TA). Now, my apology is one born out of academic etiquette for Berne died in 1970, almost ten years before I read his popular work and then started following some of the literature that came out of TA. I was quickly fascinated by the possibility that my own field of specialisation, privacy, could add a further dimension to the development of Transactional Analysis or at least Transactional Analysis to mine.[3] This thought was sparked off in 1985 by a comment by the eminent Italian jurist, Rodolfo Pagano:

> Several commercial applications such as the use of magnetic cards, remote supervision services and the electronic transfer of funds are more and more frequently being put into operation. They represent a more serious threat of the invasion of privacy than that deriving from the traditional collection of data as we understand it. For example, the system utilized in the electronic transfer of funds keeps the records of the transactions of an individual for a certain period of time. These data may be used to construct a set profile of the individual's life style, his activities and movements. The possibility of constructing a profile of the individual, of drawing attention to his behaviour (e.g. through the use of his credit card) would appear to be more insidious than the collection of certain 'sensitive' data. Perhaps it is necessary to revise the list, and even the concept of 'sensitive' data.[4]

This paragraph reads as fresh today as it did when it was written and when I read it thirty two years ago. In 1985, Pagano wisely foresaw the problems of profiling of individuals that transactional data could lead to, though he might

---

[2] If you wish to really understand in just how many ways, please read more about Transactional Analysis and what it can tell us about the hows and whys of human behaviour, and then apply that to the way various people behave around you and me, especially in diplomatic, inter-governmental, surveillance and NGO circles.

[3] Transactional Analysis, both as a sub-discipline and perhaps especially as a method of psychoanalysis, has had its ups and down since the 1960s. More recently, within the literature, one sees emerging different and overlapping theories of transactional analysis: cognitive, behavioural, relational, re-decision, integrative, constructivist, narrative, body-work, positive psychological, personality adaptational, self-reparenting, psychodynamic and neuro-constructivist.

[4] Rodolfo Pagano, 'Data Protection: The Challenge Ahead' (1985) 8 TDR 45.

not have foreseen how right he was or the actual scale of the mountain of transactional data that each of us generates every day in 2017 as we go around life carrying and clicking or tapping on our smartphone, swiping our cards, leaving digital footprints all over the place including every web-site we visit, every 'Like' we oblige a data harvester with. Rather unfortunately, thirty two years down the line, we have not yet revised either the list or the concept of 'sensitive' data. Regretfully, in some countries at least, we seem to be heading for a situation where the collection of such data and the profiling of individuals is the rule, and every effort to subject it to special safeguards such as those presupposed for sensitive data is fought tooth and nail.

The profiling of individuals based on their multiple transactions has, thanks to the Internet, in less than a quarter-century, become a dominant business model worth hundreds of billions, soon trillions, of dollars or euro every year. Moreover, law enforcement agencies and intelligence services wish to take advantage of this phenomenon too. Like Eric Berne, they think that they can learn more about individuals from an intimate knowledge of their transactions, in their case without ever having to physically approach or follow the individuals in question.

3. 'CROWN JEWEL' OF THE UN'S HUMAN RIGHTS COUNCIL: UNDER-RESOURCED SPECIAL RAPPORTEURS

Kofi Anan, in 2006, described the Special Procedures of which Special Rapporteurs (SRs) form part, as *the crown jewel* of the UN's human rights protection system: '[…] it is crucial that the [Human Rights] Council preserves and strengthens what he called its *crown jewel* – the system of Special Procedures, or rapporteurs, independent experts and working groups tasked with examining a specific area of human rights.'[5] The *crown jewel* description has become something of a mantra and I would not be the first to invite some critical analysis as to whether the work of a SRs is or can be really effective or successful.[6]

[5] X, 'Annan calls on Human Rights Council to strive for unity, avoid familiar fault lines' *UN News Centre* (29 November 2006) <http://www.un.org/apps/news/story.asp?NewsID=20770#.VjO8cbQT1H8>.

[6] See for example Catarina de Albuquerque, 'Special Procedures of the HRC: Devalued 'crown jewel' or powerful tool for the powerless?' *ISHR* (New York, 24 May 2016) <http://www.ishr.ch/news/special-procedures-hrc-devalued-crown-jewel-or-powerful-tool-powerless>.

One can normally tell as to whether somebody is serious about doing something by measuring the resources that have been allocated to the task. Indeed, one of the key things that a project management consultant looks for is the answer to the question whether enough resources have been allocated to ensure that the objectives set for the project can be reasonably met. If not, and if it would seem that starving the project of resources was deliberate, it would be reasonable to ask whether the project has been deliberately set up to fail. This is why the question 'does the Data Protection Authority in Country XYZ have adequate resources … and does it have teeth at law' was always such an important one. At one point, I was trying to understand why so many people seemed so excited about the appointment of an SRP who was being allocated next to no resources: '[…] the UN's human rights portfolio only receives 3 per cent of the organisation's regular budget, the Special Procedures Branch within the OHCHR is allocated 12.6 per cent of overall human rights funding. The increase in mandates puts an additional strain on OHCHR as an increase in funding has not accompanied the increase in the number of Special Procedures mandates. This means Special Rapporteurs regularly seek additional support outside the UN, which might raise independence issues.'[7] If countries really wished the UN SRs to succeed then one would normally reason that they would accord them enough resources instead of approximately one non-domain specialist located in Geneva and a very limited budget for travel. SRs, while being terrific value for money, as *pro bono* experts generate considerable output for the UN to consider. In 2015 'they submitted 134 reports to the Human Rights Council and 38 reports to the General Assembly; they transmitted a total of 532 communications (urgent appeals and letters of allegation) to 123 States and 13 non-State actors; and they issued 450 media products, comprising 323 press releases, 53 media statements and 75 media advisories.'[8] Many examples may be provided of how the UN permanent machinery treats the SRs in a poor manner, sometimes almost giving the impression that they behave badly towards SRs and render them scant support in a deliberate effort to discourage them. When I confronted a senior UN official about the matter, he replied: 'Do you really want to know why we treat SRs like sh...? That's because we know that if any SR were to resign, then another ten or twenty would rush forward to fill his place.' Any more games of this sort will tip the balance given the disappointment generated by the cynicism of states.

[7] ibid.

[8] ibid.

4. THE SRP AS A 'CRITICAL FRIEND' AND 'DEVELOPER OF A COMMON SUBSTANTIVE INTERPRETATION OF THE RIGHT TO PRIVACY IN A VARIETY OF SETTINGS'

In his 2006 address to the Human Rights Council, Mr. Anan went on to explain the 'peer review' or external auditor function of an SR: 'It has long since been recognized in theory, and increasingly also in practice, that the rule of law cannot be left to the discretion of governments, no matter how democratically elected they may be.'[9] Hence, when taking on the mandate of SRP, I interpreted its role to be that of a 'critical friend'.

I also welcomed, less than a week after being appointed, the articulation of my role as an SRP by Katitza Rodgriguez from the Electronic Frontier Foundation (EFF): 'He will play a crucial role in developing a common substantive interpretation of the right to privacy in a variety of settings and will be responsible for carrying out systematic analyses and research, and monitoring on the right across the world. Mr. Cannataci will also play a role in providing much-needed guidance to states and companies on the interpretation of the right to privacy.'[10] I said to myself: 'at least one other person out there is applying the right metric, at least one other person out there is understanding the limits and also the opportunities available to an unpaid volunteer SRP, an under-resourced and over-worked individual whose role it is to speak the inconvenient truth to countries which may not wish to listen, to diplomats whose cosy life may have to become a bit more complicated and tiring, to governments which may not be at all keen to put human rights first, to NGOs whose understanding of the role may be altogether imperfect'.

'Developing a common substantive interpretation of the right to privacy in a variety of settings' matched *my* expectations as to what I could reasonably hope to achieve in the job as well as what all the evidence I could muster in thirty years of research on the subject revealed about privacy. That evidence, for example, very clearly suggests that there exist cultural differences in attitudes to and interpretation of privacy. Yet, that is precisely where I was to witness the very first set of games that people played and expected me to play when it came to my approach to privacy, ie the response to the questions 'Does everybody world-wide have a right to privacy?', 'Does everybody world-wide have an identical understanding of what is meant by privacy or

[9] ibid.

[10] Katitza Rodriguez, 'EFF welcomes the United Nations new Privacy watchdog' EFF (San Francisco, 8 July 2016) <https://www.eff.org/deeplinks/2015/07/eff-welcomes-united-nations-new-privacy-watchdog>.

the right to privacy?', 'Does everybody world-wide value privacy in the same way?' It was clear to me that some people confused these questions or at least the answers to them. It only eventually became clear to me that some of this confusion was deliberate, part of multiple games many people chose to play in parallel.

5. SURVEILLANCE, PRIVACY AND INTERNATIONAL LAW

5.1. Context

The increased tempo of terrorist attacks in Belgium, France, Germany and the United Kingdom have created national and sometimes international moods which give priority to security and which put privacy somewhere on the back burner if not off the hob or cooking range and out of the kitchen altogether. Terrorist attacks are always highly regrettable and deplorable. But they also have impacts in public policy and political terms and for a mandate such as this one. When it comes to surveillance it is always difficult if not impossible to avoid the impression that some countries are very cynical or downright hypocritical in their approach to privacy but in an atmosphere of heightened tension due to terrorism, legitimate concerns about security sometimes tend to be increased unduly by an emotive and/or calculatingly political approach which prevents governments from dealing with threats and risks in a proportionate manner as befits any measures interfering with privacy in a democratic society. Moreover, in their wish to be seen to be doing something about terrorism or other threats, some governments, happily not all, have displayed a tendency to introduce privacy-intrusive measures in their laws and operational procedures which do not appear to be effective nor proportionate nor necessary. During 2016-2017 the Governments of Belgium, Germany, the Netherlands and the UK, to mention but a handful of examples, have introduced legislation the effectiveness, proportionality and scope of which varies considerably.

The situation is complicated further by the elephants (plural) in the room. Privacy and surveillance continue to be particularly hot subjects which few countries appear to be keen to discuss since well over a hundred individual UN member states appear to be receiving and exchanging intelligence on a bilateral basis with at least one and sometimes more than one of the five permanent members of the Security Council of the UN. While few are prepared to admit this openly, doing anything which would appear to openly support international initiatives aimed at reducing the extent to which privacy is interfered with by surveillance, is not a particularly attractive prospect for those countries big or small which wish to continue to receive intelligence on a bilateral basis. None of these countries wish to upset the power(s) which

is/are feeding them with intelligence and sometimes even with material assistance including hardware and software which can be used for surveillance. This then is the context in which the SRP is expected to work and achieve progress in protecting privacy from undue interference from surveillance.

The attitude of some major powers known to be carrying out bulk interception, bulk hacking and other aggressive forms of surveillance in cyberspace has been particularly disappointing though perhaps not at all surprising. Their reaction to any approaches regarding the extent to which state behaviour in cyberspace can be considered to be appropriate and respectful of privacy ranges from polite discussion to lack of engagement to near-hysterical accusations which one could hopefully be forgiven for translating as 'This has nothing to do with your mandate and mind your own business'. In the face of such hostility or indifference when it comes to the priority of surveillance and privacy, it is difficult to detect formal sources of encouragement to do much about the subject in the behaviour of a number of important and powerful UN member states. For the reasons given previously, the number of other less powerful states willing to openly hold the larger states to account in matters of surveillance and privacy is *prima facie* at first very small. Not wishing to upset one or more of the 5Ps means that the stage set for the SRP to take action in this priority area is fraught with unseen obstacles and difficulties such that one risks running against an unholy alliance intent on blocking any initiatives which may reduce the ability of the state to carry out surveillance.

On the other hand, some members of civil society, academia and a whole range of other stakeholders – including a growing number of governments – have expressed genuine interest in the efforts of the SRP to get a proper, constructive, international discussion on privacy and surveillance. The number of countries not engaging in mass surveillance or bulk interception on the internet far outweighs the number of countries that do possess and deploy such capabilities. There is also a number of emerging economies keen to put their fledgling democracies on the right path when it comes to human rights. Many of these regularly ask the SRP to provide them with a model law which they can use when it comes to surveillance and privacy. The SRP is unable to, hand on heart, refer such questions to any state which has set a gold standard through its own legislation on surveillance, since, in his opinion, while there are some states which have recently made huge progress, there is no one single shining example of national surveillance legislation which is perfectly in compliance with and respectful of the universal right to privacy. Instead, it is clearly time to define and refine such a standard in such a way that it would be useful at both national and international level.

5.2. Towards an international legal instrument on government-led surveillance and privacy in cyberspace?

It is by now public knowledge that, in my capacity as SRP, I am exploring the creation of a new international legal instrument on surveillance and privacy in cyberspace. Many countries keep asking me for a model law to regulate the issues apart from advice on how best to settle problems like jurisdiction and transfer of personal data across borders.

In order to remain zen in the unforgiving confines of the privacy world, it is often useful to seek inspiration from famous philosophers from centuries and millennia gone by, who had never dreamt of the Internet but who had nevertheless learned a lot about life and about humanity. Sometime between the 6th and 4th centuries BC, Lao Tzu or Laozi as he is often known, is believed to have been one of the authors, if not the primary author, of the *Tao Te Ching* or *Daodejing*, one of the most significant works in Chinese cosmogony. In Chapter 64 one reads 'A journey of a thousand li starts beneath one's feet' which today is commonly rendered as 'A journey of a thousand miles begins with a single step'. This was the spirit which encouraged me to welcome the creation of the post of and accept the role of SRP and indeed it is a source of encouragement in taking the next important steps, one of which is the creation of a draft international legal instrument on surveillance and privacy.

The mention of international law here is deliberate. Another obstacle to the protection of the right to privacy that I have identified is the vacuum that exists in international law when it comes to surveillance and privacy in cyberspace. To be fair, there are many areas of cyberlaw which are currently unregulated in a satisfactory manner, bedevilled as the subject is by problems of definition, jurisdiction and attempts to impose notions of national sovereignty ill-suited to an internet without borders. At this stage however the primary concern of the SRP is not to cure all the problems readily apparent in the regulation of a cyberspace where currently the only piece of specific international law applicable is the Cybercrime Convention. The primary focus is surveillance in cyberspace, the very set of issues brought to public attention by the Snowden revelations and which fuelled much of the discussion which led to the creation of the SRP's mandate. Moreover it is not only the *lack of substantive rules* which have been identified as an obstacle to privacy promotion and protection but also the lock of *adequate mechanisms*. For example, the March 2017 report of the SRP to the UN Human Rights Council points out that:

> [the Cybercrime Convention] has not yet managed to make the transfer of personal data across borders and access to data required for investigations as fast and as problem-free as some would have hoped for.

> One of the main reasons for this relative failure is that it has continued to rely too much on the 19th century mind-set of the sovereign nation state rather than cater for the reality of the borderless internet of the 21st century. … the Cybercrime Convention has not delivered on timely transborder flows of personal data which are suitable for detection, investigation and prevention of crime in the Internet age. One of the main reasons for not doing so is possibly that it did not go that extra step of creating a mechanism such as an international body tasked with – and granted the authority to authorise - international access to data, internationally.[11]

Almost needless to point out is that what applies above to transborder flows in the area of crime, largely also applies to privacy and personal data in the field of national security where most countries remain reliant on bilateral arrangements based on mutual trust or a lack of trust. The lack of transparency or at least adequate oversight in such flows of personal data does nothing to generate trust or confidence in the individual citizen, the general public or amongst nations.

When briefly examining the issue of mechanisms, in my report to the UN Human Rights Council on 7th March 2017, I indicated that

> the Cybercrime Convention, in tandem with other multilateral treaties, including new ones created for the purpose, has the potential to be expanded in such a way so as to create an international authority which would be able to grant the equivalent of an international surveillance warrant or international data access warrant (IDAW) that would be enforceable in cyberspace. Countries signing up to such a new treaty or additional protocol could be contributing their own specialised independent judges to a pool who would, sitting as a panel, conceivably act as a one-stop shop for relevant judicial warrants enforceable world-wide – naturally in those countries which would become party to the treaty. In this way, to return to our previous example of the July 2015 decision, companies like Microsoft, Google, Facebook, Amazon, Apple and other tech giants operating data centres internationally would not need to worry about any state overstepping its boundaries but rather would be faced with an international data access warrant issued on grounds of reasonable suspicion under clear international law. Likewise, citizens world-wide would be assured that their right to

[11] Joseph A Cannataci, 'Report of the special rapporteur on the right to privacy' (UN-HRC, A/HRC/34/60, 7 March 2017) <http://www.ohchr.org/Documents/Issues/Privacy/A_HRC_34_60_EN.docx>.

> privacy, not to mention other rights such as freedom of expression and freedom of association, is being protected with appropriate safeguards, even-handedly and universally.

The mandate given to the SRP in 2015 states very clearly that I have the duty:

> (c) To identify possible obstacles to the promotion and protection of the right to privacy, to identify, exchange and promote principles and best practices at the national, regional and international levels, and to submit proposals and recommendations to the Human Rights Council in that regard, including with a view to particular challenges arising in the digital age.[12]

In keeping with this mandate I have identified obstacles, some of which I have outlined above in this contribution, but likewise in keeping with the mandate, one may ask what are my proposals and recommendations to the Human Rights Council about this subject going to be? At this stage, it is growingly apparent that one of the things that would be most meaningful for my mandate would be to recommend to the Human Rights Council that it move to support the adoption of a legal instrument within the UN that could simultaneously achieve two main purposes:

- provide the governments of states with a set of principles and model provisions that could be integrated into their national legislation embodying and enforcing the highest principles of human rights law and especially privacy when it comes to surveillance;
- provide the governments of states with a number of options to be considered to help plug the gaps and fill the vacuum in international law and particularly those relating to surveillance and privacy in cyberspace.

While the need for such a legal instrument is clear, its precise scope and form are as yet unclear. Whereas the substance of its contents is emerging clearly from ongoing research and stakeholder consultations[13], the best vehicle to achieve these purposes is yet to be determined especially given the mood in some countries and the preoccupation with other priorities at the international level. The project of embarking on a new piece of international law is not something to be undertaken lightly and it is very important to get the timing right. While many stakeholders in civil society and corporations make no

---

[12] See section on mandate Special Rapporteur on the right to privacy: <http://www.ohchr.org/EN/Issues/Privacy/SR/Pages/SRPrivacyIndex.aspx>.

[13] For some details of the ongoing consultations and discussions please visit <www.mappingtheinternet.eu>.

secret of having a preference to develop safeguards and remedies through a piece of hard law such as a multilateral treaty, others advocate a more gradual approach through a piece of soft law such as a set of Guidelines or Recommendations.

There are many more paragraphs with more detailed reasoning which one may wish to read in the SRP report to the Human Rights Council of the 7th March 2017 but my interim conclusions were and remain:

> In summary therefore, a legal instrument regulating surveillance in cyberspace would be another step, complementary to other pieces of existing cyberlaw such as the Cybercrime Convention, one which could do much to provide concrete safeguards to privacy on the Internet. Happily for the SRP's mandate, a pre-existing initiative, the EU-supported MAPPING project is actually exploring options for a legal instrument regulating surveillance in cyberspace. A draft text exists, is being debated by experts from civil society and some of the larger international corporations and it is expected that this text will get a public airing some time in 2017 and certainly before the spring of 2018. It would be premature for anybody including the SRP to take a position on such a text or a similar one at this early stage of exploring options but it is possible that this could eventually prove to be a useful spring-board for discussion by governments within inter-governmental organisations including and perhaps especially the UN.[14]

Having identified the problems within international law, the role of the SRP remains to try and find practical solutions. Unlike an NGO, whose advocacy is most often done publicly, an SRP is best advised not to automatically seek to conduct the mandate in the public arena but to use all channels open to him, including diplomatic channels, in order to try and get things done, especially the right things done, in the right way, in the right time for the right reason. Very often, doing things away from the spotlight, means being careful not to embarrass or indeed humiliate people or countries, however inane or unacceptable their initial attitudes or positions may be. If the end objective is to persuade a country and its diplomats to do the right thing and agree to the right text, then not only should embarrassment and humiliation not be on the agenda, but to recall the effectiveness of Ghandi's approach and to muster mounds of patience and the ability to smile gently are also essential require-

[14] Joseph A Cannataci, 'Report of the special rapporteur on the right to privacy' (UN-HRC, A/HRC/34/60, 7 March 2017) <http://www.ohchr.org/Documents/Issues/Privacy/A_HRC_34_60_EN.docx>.

ments. In other words, however much my preference may be to pursue a policy of complete transparency, in practice that would be self-defeating and counter-productive: some of the individuals or countries talking to me in private don't wish to be seen talking to me at all or until the very last minute when they are prepared to go public with their position, especially if their position in public is going to be radically or even slightly different to the position they may have espoused previously. The only tool or weapon available to the SRP is the power of persuasion and if persuasion needs to be undertaken in private then what happens in public may possibly be more productive. While watching the countries play games between themselves the SRP must walk a delicate tightrope being very cautious not to be drawn into complicity with somebody else's inappropriate and possibly unethical agenda. For the countries are not only playing games between themselves but many of them have diplomats playing games with the mandate as well.

In private, in a fit of honesty, away from cameras and microphones, some diplomats will admit that there is a reluctance to embark on new international legal instruments with binding clauses because they are sick and tired of the efforts by some other countries to usurp them. In other words, since some countries will try to hijack an international legal instrument and then use the very terms of something intended to promote rights to instead suppress these rights, the diplomatic corps of some democratic states become reluctant to participate in something that may be used later by some states to justify and legitimise their actions however much these actions may be manifestly against the very spirit of such an international agreement whether the latter is simply consensus around a report or more especially a treaty or other legal instrument. This is a genuine concern. Whenever they embark on drafting anything new, the lives of diplomats and technical experts will become much harder and proportionately less comfortable.

This concern has a terrible chilling effect on the development of new international law. Diplomats, international lawyers and other technical experts have no answer to my oft-repeated contentions especially that one of the fundamental issues of dealing with privacy in cyberspace is that there is no international law which, for example settles issues of jurisdiction in cyberspace or deals with surveillance in cyberspace. Yet some of their countries present inane and patently wrong statements to the contrary, sometimes publicly. It's hard to decide whether this is simply the result of *battle-fatigue* especially after recent futile and particularly frustrating negotiations in 2017 or yet another form of tactical bid to win some time. Let's take one of the most recent and pertinent set of incidents, using as many examples as we can take from the public domain and particularly from the US, whose commitment to democracy and open government often means that, whether one agrees with

them or not, the workings of its Government and the thinking of some of its officials are more immediately accessible.

5.3. Group of Governmental Experts on Information Security

5.3.1. Applicability in principle of international law to cyberspace

The SRP mandate's work on a draft legal instrument on surveillance and privacy is not the only international discussion touching on international law in cyberspace. There have been running, in parallel, the annual sessions of the UN's Group of Governmental Experts on Information Security (GGE). The focus of the latter has been primarily on cybersecurity and indeed on cyberwar but there are many areas of overlap with the SRP mandate since a lot of the state behaviour in cyberspace inevitably has an impact on the privacy of hundreds of millions of netizens who may find themselves unwittingly under surveillance by one or more countries for one or more reasons at any given moment in time. So it has been very natural for me to watch very closely the outcomes of the GGE.

In 2013 and 2015 some progress was registered by the GGEs of those years arriving at a consensus holding that 'international law, and in particular the Charter of the United Nations', were applicable to cyberspace. This is more or less in line with the philosophy of, but nuanced from, the June 2014 resolution of the Human Rights Council in Geneva which affirms 'that the same rights that people have offline must also be protected online, in particular freedom of expression, which is applicable regardless of frontiers and through any media of one's choice.' This is all very well insofar as having a general statement of principle is concerned but is of little use in practice unless more detailed rules are available. It is necessary to here drill down a bit into what this really means and what it can compare to.

Let's assume that the current state of international law[15], also partially thanks to the efforts of past GGEs and the 2014 HRC resolution, is that Art 17 of the ICCPR, ie the universal right to privacy, is applicable to cyberspace. This is roughly the high level equivalent of saying that Art 8 of the European Convention on Human Rights shall also apply in cyberspace. The devil is in the detail, though, and at UN level there has been no codification of detailed privacy norms internationally applicable in cyberspace and particularly not in the case of surveillance arising out of espionage activities. If we were to contrast global with regional developments, unlike the UN, the Europeans did not stop

[15] Some would actually shed doubt on the strict accuracy of this assertion.

at Article 8 of the ECHR. Instead, over the past 40 years they developed several other layers, each one more detailed than the one above. So the Article 8 of the ECHR gave rise to Convention 108 – the European Data Protection Convention of 1981 which developed more detailed rules for the application of privacy rules in the computer world and this was later amplified and developed further quite considerably through several sectoral recommendations as well as the EU's Directive 46/95 and, more recently, by the EU's 2016 General Data Protection Regulation and its accompanying Directive covering the police and criminal justice sector. When you compare the UN privacy rules system and the European privacy eco-system you quickly understand why, after forty years of steady evolution, although quite imperfect, the level of development of European rules around privacy, computers and the internet massively outstrips those of the UN rules, which are nowhere near detailed enough to make them really useful in practice. In the same way, while the 2013 and 2015 GGEs were welcome insofar as they agreed that the high level principles of international law shall apply in cyberspace, how they shall apply and specifically where they may be enforced and by whom are just some of the many gaps still extant in international cyberlaw.

5.3.2. Failure to move beyond high-level principles

Timeliness is also an area of concern 'Given that it took the GGE nearly a decade to agree that international law applied to state use of ICTs, it is hard to see this process easily overcoming the legal, technological, and political problems inherent in assessing *how* international law applies.'[16]

Notwithstanding the paucity of current UN rules, the undoubted value of the outcomes of previous GGEs and the need for further progress, the 2016-2017 GGE failed quite spectacularly. Arun Moran Sakumar summarises the position at end June 2017 quite succinctly:

> For lack of consensus, the GGE will not submit a report of its recommendations to the UN General Assembly. The GGE failed because it could not agree on draft paragraph 34, detailing how international law applies to the use of Information and Communication Technologies (ICTs) by states. Some states that refused to endorse this paragraph offered the untenable—and frankly, facetious—rationale that affirming the application of the UN charter principles on the use of force and

[16] X, 'The UN GGE on Cybersecurity: How International Law Applies to Cyberspace' CFR (New York, 14 April 2015) <https://www.cfr.org/blog/un-gge-cybersecurity-how-international-law-applies-cyberspace> (emphasis added).

> international humanitarian law would result in the *militarisation* of cyberspace. Others doggedly insisted on including the right to apply *countermeasures* in scenarios that fell below the threshold of the 'use of force' in cyberspace, which risks opening the door further for destabilizing conduct. In the end, both sides missed the forest for the trees. The 2016-17 UN GGE had made measurable progress in clarifying certain norms of behavior for state and non-state actors. In the fracas over the paragraph, the participants failed to appreciate that the codification of norms and principles does more for a cyberspace regime than any endorsement of international legal principles.

The reasons for failure are typical of the '*games people play'* at the GGE. An informal *compte rendu* of what happened and why in June 2017 in New York leaves one with the distinct impression of a number of countries jockeying for position in cyberspace.

In an explanation of its GGE position, Cuba declared that it opposed the equivalence [made] between the malicious use of ICTs and the concept of 'armed attack'. In reality, Cuba and others are concerned that an endorsement of the 'right to self-defense' will undermine asymmetric advantages which states that do not enjoy conventional superiority over their adversaries may have in cyberspace. So, Russia, which may be concerned that the United States will retaliate conventionally in response to a cyber operation that it deems to be an armed attack, would have concerns about including the phrase. On the other hand, India, which would want the option to respond to Pakistan's cyber operations through conventional means, may welcome the express affirmation of a right to self-defense. Other commentators have noted that it is unlikely most cyber operations would cross the high legal threshold of an armed attack. However, it is the sovereign prerogative of states to define what qualifies, and a validation of their right to self-defense in the UN GGE serves as a deterrent against conventionally inferior adversaries.[17]

As a prelude of what it would like to try and discuss the applicability of international human rights law (IHRL) such as privacy, it is particularly interesting to read an assessment of what would be the applicability of international humanitarian law (IHL) to cyber operations by states:

> In the past, states like China have argued that applying IHL to cyberspace legitimizes military activities in it, which they claim to oppose. This argument, however, is really about military objectives. Countries that are rapidly scaling up their offensive cyber capabilities are buying

[17] Arun Moran Sakumar, 'The UN GGE Failed. Is International Law in Cyberspace Doomed As Well?' *Lawfare* (04 July 2017) <https://lawfareblog.com/un-gge-failed-international-law-cyberspace-doomed-well >.

> time to test the effects of new weapons on civilian networks and critical infrastructure. To commit to the applicability of IHL, they fear, would be to foreclose the development and testing of some cyber weapons that may have unintended consequences. One such area of risk is the international legal obligation to distinguish between civilians and combatants. Can cyber weapons, aimed at a combatant's network, effectively distinguish between its targets and the civilian infrastructure it may have to cross to reach them?[18]

So where do these latest developments of 2017 leave us? In a situation where, while we may not be at out-and-out war, nobody can claim that cyberspace is in a state of peace. Citizens on the net are being very frequently caught in the electronic cross-fire and reconnaissance probes. The lack of true cyberpeace means that for one reason or another the personal data, including the private correspondence, of hundreds of millions of citizens has been hacked into or monitored by states or state-sponsored entities between 2010 and 2017. Where, in international law, are the remedies for these privacy infringements? My reading of the situation, from private discussions with many diplomats and from publicly available sources, would suggest that I am not the only person who is quite fed up with the games people play when it comes to applying international law to cyberspace. For example, it is rare to see a seasoned diplomat break cover and publicly express the deep frustration palpable in the public statement released by the top US person leading that country's efforts at the 2017 GGE.

In her address to the chair of 23rd June 2017, US Deputy Coordinator for Cyber Issues, Ms. Michele Markoff publicly agreed with my long-held contention that one of the real problems with the GGE is its failure to 'fulfil the mandate given to this Group by the UN General Assembly to study *how* international legal rules and principles apply to the use of ICTs.'[19] She then goes on to lambast those states which she considers are holding up progress. Her statement oozes disappointment and frustration: 'Despite years of discussion and study, some participants continue to contend that is it premature to make such a determination and, in fact, seem to want to walk back progress made in previous GGE reports. I am coming to the unfortunate conclusion that those who are unwilling to affirm the applicability of these international legal rules and

---

[18] ibid.

[19] Michele G. Markoff, 'Explanation of Position at the Conclusion of the 2016-2017 UN Group of Governmental Experts (GGE) on Developments in the Field of Information and Telecommunications in the Context of International Security' US Department of State (New York, 23 June 2017) <https://www.state.gov/s/cyberissues/releasesandremarks/272175.htm>.

principles believe their States are free to act in or through cyberspace to achieve their political ends with no limits or constraints on their actions.'[20]

Apart from the obvious fact that some other countries would also accuse – and its own allies have accused - the US of acting as if it is 'free to act in or through cyberspace to achieve their political ends with no limits or constraints on their actions', it is difficult to disagree with Ms. Markoff's assessment of the situation especially as it tends to be quasi-identical to the one I expressed in my report to the UN Human Rights Council, just over three months earlier, on 7th March 2017:

> At this moment in time, the evidence available to the SRP would suggest that a number of states, even some leading democracies, regrettably treat the Internet in an opportunistic manner, as somewhere where their LEAs and especially their SIS can operate relatively unfettered, intercepting data and hacking millions of devices, (smartphones, tablets and laptops as much as servers) world-wide. In doing so, approximately 15-25 states treat the Internet as their own playground over which they can squabble for spoils, ever seeking to gain the upper hand whether in terms of cyber-war, or espionage or counter-espionage, or industrial espionage. The list of motivations goes on while the other 175-odd states look on powerless, unable to do much about it except hope that somehow cyber-peace will prevail… It's no use beating round the bush: the only way this clarity can be achieved, the only way that these safeguards and remedies can be introduced in a way where their enforcement becomes more timely, more even-handed and expedient is through multilateral agreement enshrined in international law. What the world needs is not more state-sponsored shenanigans on the Internet but rational, civilised agreement about appropriate state behaviour in cyberspace.[21]

5.3.3. Failure to even agree on voluntary, non-binding norms

In June 2017 Ms. Markoff however left no doubt as on to whom she pinned the blame for the GGE's failure: 'It is unfortunate that the reluctance of a few participants to seriously engage on the mandate on international legal issues has prevented the Group from reaching consensus on a report that would further the goal of common understandings among UN Member States on these

---

[20] ibid.

[21] Joseph A Cannataci, 'Report of the special rapporteur on the right to privacy' (UN-HRC, A/HRC/34/60, 7 March 2017) <http://www.ohchr.org/Documents/Issues/Privacy/A_HRC_34_60_EN.docx>.

important issues. This is particularly disappointing given the work this Group has done in this session to reach common understandings on the implementation of stabilizing measures, including voluntary, non-binding norms of responsible State behavior in cyberspace and confidence-building measures'. It is however the last sentence of her official statement that conveys the finality of the failure of the GGE 'our work has been in vain, despite extraordinary efforts from the chair, and I look forward to continuing to work with others on these efforts that are so important to international peace and security. I call on all member states to take this seriously in the future and focus on international law.'

Now coming from Ms. Markoff this is exasperated talk indeed. Easily the most senior US diplomat in the sphere of cybersecurity, she has personally contributed to considerable progress in consensus-creation and confidence-building measures in cyberspace over the years. Yet her message, if implicit in places, is quite clear: 'We cannot hope to reach a consensus with some (few) countries at GGE so let's work with *others*'. I tend to agree with her that it's time to focus on international law and on what can be achieved by working with 'others' but would advise that it may be now also be time to grasp the opportunity to change tactics too.

5.4. Need to also consider a hard law codification

Perhaps due to the fact that she has, for more than two decades, worked so intensively with issues related to Russia and China, Ms Markoff is the chief architect of the US policy advocating 'voluntary, non-binding norms of responsible State behavior in cyberspace and confidence-building measures'. The latter are of course hugely useful and an important soft law prelude to hard law outcomes but they cannot substitute some of the solutions that can only be provided by hard law. Sooner or later the world needs to transition from 'voluntary, non-binding norms of responsible State behavior in cyberspace and confidence-building measures' to 'binding norms of responsible state behaviour in cyberspace'. If the US were to focus its efforts by working with *others* whom it can trust it should find this transition to be much easier to make.

The games played by certain countries led to the failure of the 2017 GGE. As a result of this failure, I detect a deep sense of international frustration to the point that future meetings of the GGE may be in doubt. It is not unlikely that, given the position taken by the 'few', the US and other leading democracies may not unreasonably conclude that the GGEs have outlived their usefulness, that at this moment in time the possibilities for further progress in that forum are now temporarily or permanently exhausted. This does not mean that all hope of developments for international law in cyberspace are dead. It simply

means that for the time being, discussions about cyberlaw, cybersecurity and privacy will have to take place in another forum, possibly with a more restricted set of actors who will work out an international *modus vivendi* that they may enjoy and which would eventually be extended to other states, especially when the latter would sincerely embrace the same strict values to be applied to state behaviour in cyberspace inter alia regarding privacy and other human rights. That different forum may very well be the discussion of a legal instrument, binding or non-binding, in part or in whole, on surveillance in cyberspace.

Hopefully the games played at GGE should persuade the US and other major democracies that:

> [t]o expend much political capital on a difficult exercise to explain how international law applies, rather than building norms that enable states to perform their legal obligations diligently, was a strategic mistake by the major GGE powers. For those opposing the inclusion of specific legal principles, it should be clear that the tide is turning. Governments today increasingly desire rules that predict state behaviour. The GGE's failure will likely spur states to articulate their own national cyber doctrines and push for bilateral or regional initiatives to 'legalize' cyber norms.[22]

As I recognise the intrinsic difficulties and the strategic mistakes, my call as SRP is clear: we should focus much effort on 'building the norms that enable states to perform their legal obligations diligently'. Some of those detailed norms, clearly not all, may be eventually established through an international legal instrument on surveillance and privacy. Which of those norms can immediately be made binding and those which should for the time being be non-binding remains to be seen.

The predominance of the mantra of 'voluntary, non-binding norms of responsible State behavior in cyberspace' has had its day and should not stand in the way of other forms of true progress. The true wisdom of 'voluntary, non-binding norms of responsible State behavior in cyberspace' should be appreciated as being part of the formula for going forward, but not to the exclusion of other solutions. There is a time and a place for everything. The failure of GGE 2017 reinforces the lesson that now is the time to develop and build those detailed norms that Arun Mohan Sukumar so very correctly identified. He also articulated the point that 'the codification of norms and principles does more for a cyberspace regime than any endorsement of international legal

[22] ibid.

principles'. The discussion of a new legal instrument detailing norms regulating surveillance and privacy in cyberspace should be an excellent opportunity for the codification of norms and existing higher-level principles. As explained explicitly to the UN General Assembly on 20th October 2017, a legal instrument could be soft law such as that afforded by a non-binding recommendation or hard law such as a multilateral treaty or even a mixture of both depending on consensus on the timing of the measures to be adopted. The US needs to participate fully in the discussion about the codification and further detailed development of norms for it to influence what may become binding now and what it would be premature to expect to be binding. As for 'voluntary' that goes without saying. Nothing can force a country to adopt a recommendation or sign and ratify a treaty but if it does sign then that constitutes a contract which it must honour, a contract which it must respect. The many benefits for privacy of that international contract are there to be reaped.

5.5. Need to respect the privacy of citizens and non-citizens, both domestically and abroad

A next point is that of trust. Can US diplomacy afford to remain insensitive to the not-so-hidden outrage that its behaviour causes? 'The (2015) GGE recommendation did not fare better where international law has rules. Since the release of the 2013 GGE report, the United States has refused to discuss many activities Snowden disclosed, such as offensive cyber operations against foreign nations, let alone explain how they complied with international law. The United States has argued its international legal obligations to protect privacy did not apply to its foreign surveillance activities, which angered allies.'[23] This latter stance has not only outraged many US allies but is totally and explicitly rejected by the mandate of the SRP. In my report to the HRC of 7th March 2017 I stated in no uncertain terms that 'it is of utmost importance that states respect the right to privacy, which is based on human dignity, on a global level. Surveillance activities, regardless of whether they are directed towards foreigners or citizens, must only be carried out in compliance with fundamental human rights such as privacy. Any national laws or international agreements disregarding this fact, must be considered outdated and incompatible with the universal nature of privacy and fundamental rights in the digital age.'[24] My clear recommendation is that 'States should prepare them-

[23] ibid.

[24] Joseph A Cannataci, 'Report of the special rapporteur on the right to privacy' (UN-HRC, A/HRC/34/60, 7 March 2017) <http://www.ohchr.org/Documents/Issues/Privacy/A_HRC_34_60_EN.docx>.

selves to ensure that both domestically and internationally, privacy be respected as a truly universal right – and, especially when it comes to surveillance carried out on the internet, privacy should not be a right that depends on the passport in your pocket'.[25] While the previous recommendations applied to all states, that same report also included recommendations aimed specifically at the US: 'If privacy, like freedom from torture or so many other rights, is a fundamental human right it is also a universal right which means that everybody all over the world has the right to privacy, irrespective of where he or she may be, irrespective of whatever passport he or she may hold and likewise irrespective of colour, creed, ethnic origin, political philosophy or sexual orientation. This is the truth to which the SRP calls the US Senate to give witness too. On so many occasions, US Governments have sought to punish human rights violations in other countries, often leading the way in drawing red-lines and creating sanctions to improve the chances of their observance. In removing distinctions between US citizens and other citizens, by extending privacy safeguards afforded to US citizens to all the citizens of the world, the Senate would be striking a sensible blow for the universality of the fundamental human right to privacy and one against xenophobic trends in law-making. In so doing it will also match European privacy and data protection law which makes no distinction between the privacy rights of citizens and non-citizens'.[26]

When making such observations and recommendations, I do not take a more lenient approach with one country than with another. For example, in my recent official country visit to France, I made it a point to directly quiz the safeguards introduced in France when it comes to authorising surveillance outside French territory including surveillance of non- French citizens. I was delighted to confirm that the French oversight authority was, in an experimental fashion, *de facto* applying the same pre-authorisation regime for foreign surveillance that it applies for domestic surveillance. In other words, each and every request for a foreign surveillance operation goes to the same oversight authority, CNCTR, that is responsible for prior authorisation of domestic intelligence activities. This means that while not obliged to do so by law, *de facto* and at the request of the French Government itself, since March 2017, the CNCTR meets three times a week to discharge its various oversight duties, provides independent oversight of the espionage activities, domestic and foreign, against relatively strict criteria spelt out by the relative laws of 2015.

[25] ibid para 44.

[26] ibid para 45.

While the system in practice appears to be working well, I will still be recommending to the French Government to transition this important safeguard of prior authorisation of foreign surveillance from *de facto* to *de jure* at the earliest possible instance, thus setting a good example in the meantime. I intend to make similar recommendations to the US Government where both practice and law do not provide the same standards of protection to the privacy of non-US persons than the current practices in France. I also intend to press for the strict adoption of similar standards across Europe and in every single country I visit.

I stress this example about safeguards for privacy in the case of foreign surveillance since the US knows that is has lost the trust of many of its allies when it comes to surveillance in cyberspace. Knowing is one thing, caring is another. I cannot count how many ambassadors have privately confided to me 'So what precisely has the US changed in its international behaviour regarding surveillance since the Snowden revelations? Has it not continued very much as before, expecting us to put up with its intrusive behaviour while it 'gets away with it?' I very respectfully suggest that it is precisely this trust that the US needs to regain in order to help the world transition from the welcome novelty of 'voluntary, non-binding norms of responsible State behavior in cyberspace and confidence-building measures' to the legal certainty that is the central requirement of the rule of law and which can only be delivered through 'binding norms of responsible state behaviour in cyberspace'.

5.6. **Insufficiency of existing international law**

Yet another point relates to the false argument that existing international law is sufficient and appropriate. I have openly, respectfully but very firmly rejected the US position expressed by its representative on the 20th October 2017 at the Third Committee of the General Assembly of the United Nations meeting in New York: 'we, and many other countries, do not favour pursuing a binding legal instrument at this stage, *as existing international instruments provide a sufficient and appropriate framework for these issues*'.[27] This is utter baloney. There is no sufficient and appropriate framework for these issues. The problem is that, when those words are uttered in a diplomatic forum they also become part of the 'games people play'. The country making that patently false statement could count on the fact that many other influential countries

[27] X, 'Intervention by US national delegation during the interactive dialogue with the Special Rapporteur on Privacy' (Third Committee of the 72nd session of the General Assembly of the United Nations, 20 October 2017) < http://eu-un.europa.eu/eu-intervention-united-nations-3rd-committee-interactive-dialogue-protection-migrant-workers-families/>.

would not contradict it. Not because the statement *per se* is right but because many countries, some of which may have been actively lobbied by the US on the issue, do not wish to be seen to be openly contradicting the US. Also because a number of leading democratic states do not think that some other powerful countries are acting in good faith and that the current token efforts are enough to be seen to be doing something or else what could currently be achieved at this point in time in the current fora has been achieved and that the possibilities for further achievement are exhausted. To put it more bluntly, the failure of GGE in achieving concrete progress on appropriate state behaviour in cyberspace does not put other democracies into the mood to expend the effort to publicly disagree with the US however much the US statement may be wrong. On the contrary, it possibly also marks possible resignation that such a statement is simply self-serving and further serves to erode trust in the US - which is a true pity since this is an opportunity to show leadership in such matters.

The US statement is also fundamentally misleading in other ways since 'international law does not prohibit or regulate espionage. So at the moment the GGE agreed international law applies to state use of ICTs, international law did not (and still doesn't) apply to one of the most important state uses of ICTs that cause international security problems.'[28] In other words, the infringements of privacy caused by surveillance on the internet which is the outcome of espionage activities, ie the very activities by states which led to the creation of the mandate of SRP remain outside the ambit of international law. Does the US have credibility with its allies when it comes to the privacy of the citizens and leaders of those very allies? As an SRP I have the duty to be neutral and objective about such matters so my clear answer to that last question is: No.

6. PRIVACY AS A UNIVERSAL ENABLING RIGHT TO DEVELOP ONE'S PERSONALITY

The Universal Declaration of Human Rights of December 1948 was innovative in many ways. 'Nevertheless, some still argue that the declaration represents a neo-colonialist attempt by the West to control the lives of those in the developing world. Such arguments have been used by authoritarian leaders and states to violate human rights (particularly those of women and children)

[28] X, 'The UN GGE on Cybersecurity: How International Law Applies to Cyberspace' CFR (New York, 14 April 2015) <https://www.cfr.org/blog/un-gge-cybersecurity-how-international-law-applies-cyberspace>.

under the guise of enforcing tradition.'[29] When countries voted in 1948, the tiny minority of states which abstained included Saudi Arabia which argued that 'Articles 16 and 18 (the rights for men and women to marry who they choose, and the right to freedom of religion) were in opposition to Islamic faith and teachings which emphasise patriarchal authority'.[30] So certainly, some rights in UDHR have been controversial from the beginning, pitting a more individualist approach against one more concerned with preserving certain elements of their cultural past and present.

There is an entire body of literature as to why human rights are universal or not, but there is little space here to play the arguments out here in a comprehensive manner. Authors like O'Connor have drawn attention to the fact that 'the universality of the document has been criticised by some, not least by members of the American Anthropological Association (AAA). They argue that by claiming human rights are universal, we ignore and undermine the cultural differences that exist between societies in different parts of the world. How can one single document claim to represent every single person in the world, when our experiences are so different?'[31] On examining more closely the AAA's two major declarations on anthropology and human rights it is clear that things are much more nuanced and that 'As a professional organization of anthropologists, the AAA has long been, and should continue to be, concerned whenever human difference is made the basis for a denial of basic human rights, where *human* is understood in its full range of cultural, social, linguistic, psychological, and biological senses.'[32]

The reason why I am referring to the anthropological approach is that I then adopted it myself to test for evidence that privacy exists. This has, to date, provided the evidence that privacy is indeed universal as a value thought it may appear in different forms in some societies.

---

[29] Tin O'Connor, 'Debating Human Rights – universal or relative to culture?' *DevelopmentEducation.ie* (11 February 2014) <http://developmenteducation.ie/blog/2014/02/debating-human-rights-universal-or-relative-to-culture/>.

[30] ibid.

[31] ibid.

[32] X, 'Statement on Human Rights' *Anthropology and Human Rights Committee for Human Rights American Anthropological Association* <http://humanrights.americananthro.org/1999-statement-on-human-rights/>.

Long before becoming SRP, indeed more than three decades before the UN even created its role in March 2015, I had personally become fascinated with the *raison d'être* of privacy, why it existed, where it existed? My interest in the subject was sparked while researching my doctoral thesis on Privacy and Data Protection in 1984 when I read a paper written by an anthropologist and based on field-work with the Inuit in the early 1970s, exploring the realities of privacy in small restricted spaces including one-roomed igloos in the very cold north of Canada. This combined with my reflections about the *Census* case,[33] then just decided by the German Constitutional Court in 1983, which held that privacy and informational self-determination were essential for a person to fulfil his or her right to freely develop his or her own personality. By 1985 therefore I was asking myself questions like 'Was there an evolutionary advantage to privacy?' and 'When, where and why did man develop privacy-seeking behaviour over time?'

As is normal when researching a thesis, I had to temporarily abandon the deeper pursuit of these questions in order to answer many more mundane ones… but the fundamental curiosity in me had been permanently piqued. So by 2002 I was back trying to study links between privacy and the development of personality. I then developed plans for an on-going research project which became a labour of love ultimately planned to be published in a book entitled 'The right that never [quite] was: privacy and personality across cultures'. It was clear to me that the fascinating research about privacy in different cultural settings, published by Irwin Allen in 1975, needed to be taken further. In order to discover the truth about privacy I set myself the goal to carry out research with cross-section of the oldest surviving indigenous tribes on the planet and carry out a comparative analysis of what they thought and felt about privacy-related behaviour. Organised as the inCONNECT project and starting with desk research and ethnographic work on different tribes in the Amazon, I moved on to field work with the oldest hunter-gatherer tribes in the forests of Kenya in 2009-2010, the aboriginals in Australia from 2009 onwards and eventually different indigenous peoples in peninsular Malaysia and in the jungles of northern Borneo as of 2012. To do so I assembled an international inter-disciplinary team including anthropologists, a cognitive psychologist, liaison officers and gender officers from the relative tribes and other specialists. Together we devised a research instrument which was used in hundreds of interviews with indigenous peoples in these countries, trying to explore their perceptions of privacy even if they

[33] *Census act case* [1983] BCVerfGE 65, 1.

lived in the remotest places in the forest or jungle and even if their language did not even have a word for privacy.

My very intensive duties as SRP have, since 2015, compelled me to temporarily suspend further field-work for the inCONNECT project, but I came to my role as SRP in August 2015 completely convinced that privacy exists everywhere and anywhere where man may live, even in the most primitive conditions. In some places it may manifest itself in slightly different forms but privacy-related behaviour remains a universal characteristic of human kind. The evidence I had been gathering for several years suggested that not only is privacy alive and well but that privacy-related behaviour may have a common core across most societies with some 'local differences'. This made it even easier for me to recognise privacy as a universal right, with everybody having a right to privacy anywhere and everywhere, though their concept of privacy and their expectations of the privacy right may differ in some aspects from place to place. There is no contradiction in this approach. The core values of privacy remain the same everywhere but at the periphery of value-systems there may be some variations which may have developed locally for one or more reasons including geography, climate and certain aspects of culture including religious beliefs. Thus I came to the role of SRP with the evidence that privacy is one of the essential pre-requisites which help a person develop their personality in a free, unhindered manner, in a way which helps one ask oneself the questions and find some of the answers such as 'Who am I now, today and who do I want to become, to develop into, by tomorrow or next year or in five years' time?'. Thus privacy is also very close to, but should not be confused with, concepts like autonomy and self-determination.

This is also what prompted me to specifically and explicitly identify the need to develop a better understanding of privacy within the global discourse facilitated by the mandate of the SRP. Thus, the first point in my ten-point plan first discussed at the ICDPPC in Amsterdam at end October 2015, read as follows:

> Going beyond the existing legal framework to a deeper understanding of what it is that we have pledged to protect: There is a need to work on developing a better, more detailed and more universal understanding of what is meant by the *right to privacy*. What does it mean and what should it mean in the 21st century? How can it be better protected in the digital age? Activities will be organised and research will be supported to examine possible answers to these key questions which will help provide essential foundations for other parts of the SRP's action plan.

This was articulated further, a few months later, in my March report 2016 to the UN Human Rights Council in Geneva. In asking the question 'Why privacy?' and positing privacy as an enabling right as opposed to being an end in itself, I openly declared that I was pursuing an analysis of privacy as an essential right which enables the achievement of an over-arching fundamental right to the free, unhindered development of one's personality.

In order to help focus a fresh, structured debate on fundamentals I then stated my intention:

> to provocatively posit privacy as being an enabling right as opposed to being an end in itself. Several countries around the world have identified an over-arching fundamental right to dignity and the free, unhindered development of one's personality. Countries as geographically far apart as Brazil and Germany have this right written into their constitution and it is the SRP's contention that a) such a right to dignity and the free, unhindered development of one's personality should be considered to be universally applicable and b) that already-recognised rights such as privacy, freedom of expression and freedom of access to information constitute a tripod of enabling rights which are best considered in the context of their usefulness in enabling a human being to develop his or her personality in the freest of manners.

This initiative kicked off with a capacity-filling event (90 participants registered) entitled 'Privacy, Personality and Flows of Information' (PPFI) held in New York in July 2016. The participation in this event by experts and stakeholders, especially civil society from around five continents was very encouraging and confirmed the need to hold a series of PPFI events around the world.

Within less than nine months however we also were to witness an important new development at the UN which would further reflect and reinforce the work of my mandate on privacy and personality. In March 2017, a year since my appeal about the subject in March 2016, a little bit of history was made when the following was articulated and recognised in a resolution (*(UN A/HRC/L.17/Rev – March 2017))* of the Human Rights Council in March 2017:

> Recognizing the right to privacy also as an enabling right to the free development of personality and, in this regard, noting with concern that any violation to the right to privacy might affect other human rights, including the right to freedom of expression and to hold opinions without interference, the right to freedom of peaceful assembly and association.

The second edition of PPFI, the one for MENA – the Middle East and North African region - was held in Tunis on 25-26 May 2017 and was a resounding success with some 65-70 participants from Algeria, Egypt, Lebanon, Morocco, Syria, Tunisia and Qatar actively contributing to the discussion.

The third edition of PPFI was held in Hong Kong, China on September 29-30 2017 back-to back with ICDPPC 2017. It had in excess of seventy (70) participants registered and was declared by many participants to be an unqualified success.

The UN SRP mandate built up this PPFI initiative with scientific rigour, matching what we had learned from an anthropological approach to privacy, yet some people worked behind the scenes to discredit the approach and the pushback of some individuals and a tiny minority of NGOs was quite noticeable, especially in the early stages. As people got used to the idea of the value of actually talking about privacy in different cultural settings and with an acutely more focused gender perspective, then pushback lessened but never disappeared altogether. Some people clearly disagreed with and/or felt menaced by the activities of the UN SRP mandate and chose to obstruct rather than assist. Their games were noticed but not allowed to hamper the generally successful thrust of this mandate.

7. IS PRIVACY LIKE COKE? THE CULTURAL FLAVOUR OF PRIVACY AS A UNIVERSAL RIGHT

One of the games people have played throughout my term as UN SRP has been to pit what science tells us regarding the truth about cultural differences and privacy with the 'risks' taken by my open approach to 'a better of understanding of privacy'. Instead of taking a cue from Katitza Rodriguez's view that the SRP is dedicated to 'developing a common substantive interpretation of the right to privacy in a variety of settings', any move from my end to engender a decent discussion about the subject of cultural differences and privacy has been met by open or hidden accusations that this would put at risk the international and universal nature of privacy. So I sought to get my thinking straight in a number of ways, hence the Coke analogy.

Coming from a generation brought up with advertisements extolling the virtues of 'ice-cold Coke on the back of my throat', in many years of continuous travelling I formed the impression that Coke does not taste the same everywhere. Recently, curiosity got the better of me and I spent half an hour relaxing while following search engine responses to the query 'Does Coke taste the same everywhere?' What I found was quite interesting, though since it would

probably fill a couple of hefty volumes I'll only give you a flavour (no puns intended) here.

The official explanation from the Coca-Cola company reads as if it was possibly written by a lawyer with several years' experience in diplomatic circles: 'The basic ingredients and process used to make Coca-Cola are the same in all countries, although people perceive taste in very different ways. It is possible for the same soft drink to vary slightly in taste due to other factors such as the temperature at which it is consumed, the foods with which it is consumed, or the conditions in which it is stored prior to consumption'.[34] The key fudge here is the adjective 'basic' in 'basic ingredients'. For, in a closely-guarded recipe such as the one for Coke, just what is basic and what is local flavour or 'non-basic' if you prefer to put it that way? In other words, apart from age (when it was bottled), temperature and packaging what are the other variables that could make Coke taste differently if not something different in the ingredients? If water is an ingredient that is not considered basic then that could explain at least some of the difference in taste: water, obtained from different sources all perfectly safe to drink, tastes so differently and can have so many different mineral properties that one could easily believe that it would impact the taste of Coke.

Dan Stifter, former Brand Director at Coca-Cola between 1994-2000, probably came much closer to the truth when explaining that 'Coke taste changes over time as the ingredients blend and soften, it is not a completely stable flavor profile. Like wine, it evolves over time and should be drank as fresh as possible. Other than that, there is absolutely no difference in the Coke formula anywhere in the world, and Coke spends unbelievable amounts of money on quality control to make sure that's true. the only change that is allowed is the type of sugar - cane sugar, sugar or high fructose corn syrup are the only options, and those cause some different mouth feels which changes the experience for sure.'[35] Well, it would seem that it's not only the water – which would certainly be different everywhere - but also the type of sweetener which could be a second different ingredient or variable - accounting for the variations in taste in Coke around the world. Is that all? Apparently not.

---

[34] X, 'Does Coca-Cola taste different in different countries?' *Coca Cola* <http://www.coca-cola.co.uk/faq/does-coca-cola-taste-different-in-different-countries >.

[35] Dan Stifter, 'Why does Coke taste different from one country to another?' *Quora* (17 September 2016) <https://www.quora.com/Why-does-Coke-taste-different-from-one-country-to-another>.

Take two neighbouring countries. 'Mexican Coke has a small, but devoted slice of the Coke-drinkers market (a majority love Coca-Cola Classic, there are tons of Diet Coke admirers, and then there are the cherry and vanilla lovers). Mexican Coke uses real cane sugar (instead of the Coke in the U.S. which uses high-fructose corn syrup), and is bottled in small glass bottles—this for some people is all the difference. So much so that when the Mexican bottler of Coca-Cola let it slip that it was considering switching to high-fructose corn syrup to save money, fans of Mexican Coke expressed enough outrage to get the Mexican bottler to stick with cane sugar.'[36] Is that all? Well, not really. Type of sweetener is one factor but quantity is another. While admitting that 'the principal factor is one ingredient, Mexican coke is made with Cane Sugar and US coke is made with Corn Syrup, the result, a very different taste in the sweetness of the coke.' Luis Fernando Mata Licón suggests that: 'The biggest difference are the level of sugars, Mexican coke has 53 grams of sugar while the one of the US has 39 grams.'[37] This is borne out by insider knowledge. Denna Neff, former Senior Analyst at The Coca-Cola Company (1997-2003) affirms that 'The mixture, water, and taste preference of the country's culture is taken into consideration for a finished product.'[38] Which is explained by Fozan Zh as being 'Since different cultures have different preference of level sugar it is sweeter in some then the others depending on which market Coke is targeting. For example coke in some Asian countries is sweeter than coke in western countries.'[39]

So, in a nutshell, it boils down to cultural differences and cultural tastes. Roughly the same conclusions can be arrived at when examining other 'universal products' such as Big Macs. The brand, the concept, is global but the

---

[36] Mike Dang, 'Does Mexican Coke Really Taste Different From Coke Produced in the US?' *The Billfold* (11 November 2013) <https://www.thebillfold.com/2013/11/does-mexican-coke-really-taste-different-from-coke-produced-in-the-u-s/>.

[37] Luis Fernando Mata Licón, 'Why does Coke taste different from one country to another?' *Quora* (17 February 2015) <https://www.quora.com/Why-does-Coke-taste-different-from-one-country-to-another>.

[38] Denna Neff, 'Why does Coke taste different from one country to another?' *Quora* (05 November 2017) <https://www.quora.com/Why-does-Coke-taste-different-from-one-country-to-another>.

[39] Fozan Zh, 'Why does Coke taste different from one country to another? (15 February 2015) *Quora* <https://www.quora.com/Why-does-Coke-taste-different-from-one-country-to-another>.

flavour, sometimes, may be somewhat local.[40] I am not being flippant or frivolous when using universal brands to try and help explain what can be properly understood by a universal fundamental human right such as privacy.

Exactly what is global and what is local about privacy is one of the key questions that any privacy scholar has to face. What *IS* the truth about privacy? Is it the same everywhere? Or is it the same in core values while allowing for cultural differences at the periphery? Can a right like privacy be universal while retaining elements of diversity in its universality? While the concept of privacy is known in all human societies and cultures at all stages of development and throughout all of the known history of humankind it has to be pointed out that there is no binding and universally accepted definition of privacy.[41] To understand the right better it is necessary to think of it from two perspectives. First, it should be considered what the positive core of the right encompasses. Secondly, the question arises how to delimit the right in the form of a negative definition eg 'This or that is *not* privacy-related'. It would appear that we are some distance from having completed these two tasks.

The absence of a universally agreed and accepted definition of privacy is not the only major handicap faced by the SRP. Even had the drafters of all the existing legal instruments, UN and otherwise, included a universally agreed definition of privacy in those instruments, we would still have had to deal with what can be conveniently summed up as the Time, Place, Economy and Technology (TPET) dimensions. For the passage of time and the impact of technology, taken together with the different rate of economic development

---

[40] To begin to understand just how different the ratios of ingredients and nutritional value can be – a well as the sourcing of the ingredients in a Big Mac can be, see below:

Calories (kCal) 480 Australia to 600 Mexico. US 540.
Carbohydrate (g) 35g New Zealand to 57g Chile. US 45g.
Dietary Fiber (g) 2.5g Argentina to 5g Greece US 3g.
Fat (g) 24g UK to 33g Mexico. US 29g
Sodium (mg) 730 Malaysia to 2300 Sweden and Switzerland. US 1040.

Analysed by Denem using consolidated sources: <https://www.democraticunderground.com/discuss/duboard.php?az=view_all&address=389x6898507>.

[41] For a much more detailed insight into the SRP's assessment of the existence and time, place and space dimensions of privacy across the millennia see Joseph A Cannataci, (ed) *The library of essays on law and privacy. The Individual and Privacy. Volume I* (Routledge 2015) <https://www.routledge.com/The-Individual-and-Privacy-Volume-I/Cannataci/p/book/9781409447177 >.

and technology deployment in different geographical locations means that legal principles established fifty years ago (ICCPR) or even thirty-five years ago (eg the European Convention on Data Protection) let alone seventy years ago (UDHR) may need to be re-visited, further developed and possibly supplemented and complemented to make them more relevant and useful to the realities of 2016.

The time dimension is perhaps particularly significant since it may help explain that both individual and communal privacy in a given society may vary greatly from one historical period to another and that different societies in different geographical locations may develop differently. When one would compare one society to another therefore, its development in terms of privacy must not only be measured objectively on certain criteria but also on the reasons why one society may have progressed faster than another in the time dimension. Thus economics and climate would generally influence as to whether a home has several separate rooms or one big communal room. In most societies we have witnessed the evolution of homes to multi-room spaces generally increasing the privacy of spaces as the number of spaces grew. So privacy here is not static: when time passes, privacy perspectives in a given family or society may change.

A way of extending the usefulness of the Coke analogy would be to understand things as follows: 'Anybody and everybody has the right to drink Coke anywhere and everywhere around the planet, even if it tastes a bit – or a lot - different and comes in different cans or bottles with different labels.' Or 'anybody and everybody has the right to privacy anywhere and everywhere around the world, even if that right might pertain to a concept of privacy which is constructed a bit differently in different places and which may be packaged and labelled in different ways.'

8. **EPILOGUE**

One would have thought that certain states would be very keen to take advantage of the existence of a critical friend in the person of the SRP, but that is really not the case. The reason why I won't go now into the cases I mentioned in the very first paragraph of this contribution is because most of them are still *sub judice* so I'll only be able to publish details in or after 2018 since the completion of replies from states to my letters are still awaited…and amongst the games states play in this case is that they 'work the system' like mad. If they are allowed 60 days' time to respond to a question, one country systematically times its responses to arrive on Day 59 or 60. So in answer to the question 'Why does Country P appear unconcerned that its legal systems do not adequately protect a woman whose genitalia were photographed

without permission by a health care worker during a gynaecological procedure?' the proceedings in that case are still ongoing. As are those in response to question like 'What are we going to do about that country whose Government published on-line 30 years' worth of sensitive medical data for 10% of its citizens and failed to de-identify the data subjects in a robust manner?'

As for the behaviour of embassy staff of country Y is concerned and whether they were bluffing or being dead serious when they threatened me with 'serious consequences' if I were to follow a course of action which they find displeasing. I'd rather not discuss that matter in order not to make things worse. And Yes, that was a death threat that just came at me over the phone and No, I'm not paranoid. Yes, country Z was elected to the Human Rights Council and is, most surprisingly, questioning my very right to receive and consider complaints about privacy infringements from individuals.

Games people play? Perhaps we should liken the game to football. The SRP's role is like that of the manager or coach. Except that it's worse. At least in football one's critics ostensibly all wish the team to win. That's football. As an SRP you are dealing with a whole load of vested interests including those of countries/people who don't wish to see the SRP's team win and others who don't wish to be outshone.

Being the UN SRP could be all about people and the games they play, if you let it. In other words, you have to keep saying there's more at stake than a game and in so doing, say the inconvenient truths that others do not wish to hear. With practice, one gets good at that game too.

9. SELECTED LITERATURE

Cannataci J A (ed), *The library of essays on law and privacy. The Individual and Privacy. Volume I* (Routledge 2015) <https://www.routledge.com/The-Individual-and-Privacy-Volume-I/Cannataci/p/book/9781409447177 >

Cannataci J A, 'Report of the special rapporteur on the right to privacy' (UN-HRC, A/HRC/34/60, 7 March 2017) <http://www.ohchr.org/Documents/Issues/Privacy/A_HRC_34_60_EN.docx>

Dang M, 'Does Mexican Coke Really Taste Different From Coke Produced in the U.S.?' *The Billfold* (11 November 2013) <https://www.thebillfold.com/2013/11/does-mexican-coke-really-taste-different-from-coke-produced-in-the-u-s/>

de Albuquerque C, 'Special Procedures of the HRC: Devalued 'crown jewel' or powerful tool for the powerless?' *ISHR* (New York, 24 May 2016) http://www

.ishr.ch/news/special-procedures-hrc-devalued-crown-jewel-or-powerful-tool-powerless>

Markoff M G, 'Explanation of Position at the Conclusion of the 2016-2017 UN Group of Governmental Experts (GGE) on Developments in the Field of Information and Telecommunications in the Context of International Security' *US Department of State* (New York, 23 June 2017) <https://www.state.gov/s/cyberissues/releasesandremarks/272175.htm>

Neff D, 'Why does Coke taste different from one country to another?' *Quora* (05 November 2017) <https://www.quora.com/Why-does-Coke-taste-different-from-one-country-to-another>

Licón L F M, 'Why does Coke taste different from one country to another?' *Quora* (17 February 2015) https://www.quora.com/Why-does-Coke-taste-different-from-one-country-to-another>

O'Connor T, 'Debating Human Rights – universal or relative to culture?' *DevelopmentEducation.ie* (11 February 2014) <http://developmenteducation.ie/blog/2014/02/debating-human-rights-universal-or-relative-to-culture/>

Pagano R, 'Data Protection: The Challenge Ahead' (1985) 8 TDR 45

Rodriguez K, 'EFF welcomes the United Nations new Privacy watchdog' *EFF* (San Francisco, 8 July 2016) <https://www.eff.org/deeplinks/2015/07/eff-welcomes-united-nations-new-privacy-watchdog>

Sakumar A M, 'The UN GGE Failed. Is International Law in Cyberspace Doomed As Well?' *Lawfare* (04 July 2017) <https://lawfareblog.com/un-gge-failed-international-law-cyberspace-doomed-well>

Stifter D, 'Why does Coke taste different from one country to another?' *Quora* (17 September 2016) <https://www.quora.com/Why-does-Coke-taste-different-from-one-country-to-another>

X, 'Annan calls on Human Rights Council to strive for unity, avoid familiar fault lines' *UN News Centre* (29 November 2006) <http://www.un.org/apps/news/story.asp?NewsID=20770#.VjO8cbQT1H>

X, 'The UN GGE on Cybersecurity: How International Law Applies to Cyberspace' *CFR* (New York, 14 April 2015) <https://www.cfr.org/blog/un-gge-cybersecurity-how-international-law-applies-cyberspace>

X, 'Intervention by US national delegation during the interactive dialogue with the Special Rapporteur on Privacy' (Third Committee of the 72nd session of the General Assembly of the United Nations, 20 October 2017)

<http://eu-un.europa.eu/eu-intervention-united-nations-3rd-committee-interactive-dialogue-protection-migrant-workers-families/>

X, 'Statement on Human Rights' *Anthropology and Human Rights Committee for Human Rights American Anthropological Association* <http://human-rights.americananthro.org/1999-statement-on-human-rights/>

X, 'Does Coca-Cola taste different in different countries?' *Coca Cola* <http://www.coca-cola.co.uk/faq/does-coca-cola-taste-different-in-different-countries >

Zh F, 'Why does Coke taste different from one country to another? (15 February 2015) *Quora* https://www.quora.com/Why-does-Coke-taste-different-from-one-country-to-another>

Eyes wide shut

The Privacy Shield's blunt denial of continued bulk, mass or indiscriminate collection or processing and unnecessary or disproportionate access and use by US intelligence and law enforcement authorities

GERT VERMEULEN[1]

1. INADEQUACY OF THE US DATA PROTECTION REGIME: CLEAR SINCE 9/11, CLEARER SINCE SNOWDEN

The Europol-US agreement of 20 December 2002[2] and the EU-US mutual assistance treaty in criminal matters of 25 June 2003[3], both concluded in the immediate aftermath of 9/11, soon set the tone, in that US non-compliance with key EU data protection standards was set aside in favour of enabling EU-US data flows after all.

[1] Full Professor of International and European Criminal Law, Director Institute for International Research on Criminal Policy (IRCP), Department Chair Criminology, Criminal Law and Social Law, Faculty of Law, Ghent University; Privacy Commissioner, Commission for the Protection of Privacy (Belgium). Email: gert.vermeulen@ugent.be. This text is an updated and elaborate version of Gert Vermeulen, 'The Paper Shield. On the degree of protection of the EU-US privacy shield against unnecessary or disproportionate data collection by the US intelligence and law enforcement services' in Dan JB Svantesson and Dariusz Kloza (eds), *Trans-Atlantic Data Privacy Relations as a Challenge for Democracy* (European Integration and Democracy Series, vol 4, Intersentia 2017).

[2] Supplemental agreement on the exchange of personal data and related information (Europol Police Office-United States of America) (20 December 2002) <https://www.europol.europa.eu/content/supplemental-agreement-between-europol-police-office-and-united-states-america>

[3] Agreement on mutual legal assistance (European Union-United States of America) (25 June 2003) OJ L 181/34.

Neither in terms of police or judicial cooperation the adequacy of the US data protection level could be established, whilst both the (then) Europol-Agreement and Directive 95/46[4] required so. Purpose limitation (specialty)[5] in the use of data provided by Europol or EU Member States proved an almost nugatory concept, where the US was allowed to freely make use of information that was procured in criminal cases for purely administrative or intelligence purposes.[6] Later, in 2006, it was revealed that the US Treasury had procured access to worldwide scriptural bank transactions by means of administrative subpoenas *vis-à-vis* the US hub of the (Belgium-based) *Society for Worldwide Interbank Financial Telecommunication* (SWIFT) in the context of combating the financing of terrorism, but surely alluding to other (including economic) goals as well.[7] Moreover, SWIFT itself defected herein, as its US hub did not endorse the so-called *Safe Harbour* principles.[8] These had been developed in 2000 by the European Commission[9] to ensure that, given that the US data

[4] Directive 95/46/EC of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1995] OJ L 281/31.

[5] Els De Busser, 'Purpose limitation in EU-US data exchange in criminal matters: the remains of the day' in Marc Cools and others (eds), *Readings on criminal justice, criminal law and policing* (Vol 2, Maklu 2009) 163.

[6] Steve Peers, 'The exchange of personal data between Europol and the USA' (2003) Statewatch Analysis no 15 <www.statewatch.org>; Gert Vermeulen, 'Transatlantisch monsterverbond of verstandshuwelijk? Over het verschil tussen oorlog en juridische strijd tegen terreur en de versterkte politie- en justitiesamenwerking tussen EU en VS' (2004) 25(1) Panopticon 90; Paul De Hert and Bart De Schutter, 'International Transfers of Data in the Field of JHA: The Lessons of Europol, PNR and Swift' in Bernd Martenczuk and Servaas Van Thiel (eds), *Justice, Liberty, Security: New Challenges for EU External Relations* (I.E.S. series nr. 11, VUB Press 2008) 326-327 and 329-333.

[7] See Belgian Privacy Commission, 'Opinion on the Transfer of Personal Data by the CSLR SWIFT by Virtue of UST (OFAC)' 37/2006 <https://www.privacycommission.be/sites/privacycommission/files/documents/advies_37_2006_1.pdf>; Also: Patrick M Connorton, 'Tracking Terrorist Financing through SWIFT: When U.S. subpoenas and foreign privacy law collide' (2007) 76(1) Fordham L Rev 283.

[8] Gloria González Fuster, Paul De Hert and Serge Gutwirth, 'SWIFT and the vulnerability of transatlantic data transfers' (2008) 22(1-2) Intl Rev of L Computers & Technology 191.

[9] Commission Decision 2000/520/EC of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce [2000] OJ L 215/7.

protection regime in itself could not be qualified as adequate, commercial EU-US data transfers would nonetheless be enabled.[10] Companies that indicated (and self-certified) their compliance with the principles laid down in the Commission's Safe Harbour Decision, were to be considered as – from a data protection perspective – 'safe harbours' within US territory, to which EU companies were allowed to transfer data. This, however, was not the case for the SWIFT hub in the US, so that the Belgian company should have refrained from localizing (backup) data in it. The EU's response to this scandal was far from convincing. While intra-European payment transactions were admittedly no longer sent to the US hub (albeit that in the meantime SWIFT had registered it as a 'safe harbour'), the Commission negotiated on behalf of the EU an agreement with the US, allowing the latter, via a Europol 'filter' (which painfully lacks proper filtering capacity) to obtain *bulk*-access on a case-by-case basis to these intra-European payment transactions. This 2010 TFTP-agreement (*Terrorist Financing Tracking Program*[11]) furthermore contains an article in which the US Treasury is axiomatically deemed adequate in terms of data protection.[12] Notwithstanding this, and given the known practice of wide data-sharing between US government administrations and bodies contrary to the European purpose-limitation principle, the *in*adequacy of the US data protection regime was at the time beyond doubt. That the Foreign Intelligence Surveillance Act (FISA)[13], amended post-9/11 with the Patriot Act[14] and further expanded in 2008[15] (FISA Amendments Act), allowed the US to monitor – either with or without a court order – electronic communication in

---

[10] See William J Long and Marc Pang Quek, 'Personal data privacy protection in an age of globalization: the US-EU safe harbor compromise' (2002) 9(3) JEPP 325.

[11]Agreement on the processing and transfer of Financial Messaging Data from the European Union to the United States for purposes of the Terrorist Finance Tracking Program (European Union–United States of America) (30 November 2009) OJ L 008/11.

[12] Article 6 of the TFTP Agreement (n 11) reads: " […] the U.S. Treasury Department is deemed to ensure an adequate level of data protection for the processing of financial payment messaging and related data transferred from the European Union to the United States for purposes of this Agreement."

[13] Foreign Intelligence Surveillance Act of 1978 50 USC §§ 1801-11, 1821-29, 1841-46, 1861-62, 1871.

[14] Uniting and Strengthening America by providing appropriate tools required to intercept and obstruct terrorism (USA Patriot Act) Act of 2001; Paul T Jaeger, John Carlo Bertot and Charles R McClure, 'The impact of the USA Patriot Act on collection and analysis of personal information under the Foreign Intelligence Surveillance Act' (2003) 20 Government Information Quarterly 295.

[15] Foreign Intelligence Surveillance Act of 1978 Amendments Act of 2008.

a way that was disproportionate, worldwide and in bulk, was clear as well.[16] This and more was confirmed in the summer of 2013 with the revelations of whistleblower *Edward Snowden.* [17] These revelations were particularly shocking because of the revealed extent of the interception practices of the NSA (National Security Agency) – *inter alia* through the PRISM and Upstream programmes – and the British intelligence service GCHQ's (Government Communications Headquarters)[18] – which for years had spied on *Belgacom International Carrier Service* (Bics). As a subsidiary of Belgium-based (tele)communications provider *Proximus*, Bics provides worldwide hardware through which telecom companies and government agencies run their electronic communication (internet-, telephony-, mobile- and texting-traffic). Moreover, the intense mutual cooperation between the NSA and GCHQ, and within the so-called Five Eyes Community (comprising the intelligence services of Canada, Australia and New Zealand), was confirmed by the revelations, although many were well aware that these five, within the context of Echelon, had been monitoring worldwide satellite communications for decades, including for commercial purposes. Already in 2000, the European Parliament had instigated an investigative commission against these practices.[19] From the US

---

[16] Els De Busser, 'Purpose limitation in EU-US data exchange in criminal matters: the remains of the day' in Marc Cools and others (eds), *Readings on criminal justice, criminal law and policing* (Vol 2, Maklu 2009) 163; Els De Busser, *Data Protection in EU and US Criminal Cooperation* (Maklu 2009).

[17] The outrage broke in June 2013, when *the Guardian* first reported that the US National Security Agency (NSA) was collecting the telephone records of tens of millions of Americans, see: Glenn Greenwald, 'NSA collecting phone records of millions of Verizon customers daily' *The Guardian* (London, 6 June 2013) <http://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order>; Also: Mary-Rose Papandrea, 'Leaker Traitor Whistleblower Spy: National Security Leaks and the First Amendment' (2014) 94(2) Boston U L Rev 449.

[18] The involvement of the British GCHQ was revealed by *the Guardian* on the 21st of June, 2013. See: Ewen MacAskill and others, 'GCHQ taps fibre-optic cables for secret access to world's communications' *The Guardian*, (London, 21 June 2013) <http://www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa>.

[19] See European Parliament decision setting up a temporary committee on the ECHELON interception system, 29 June 2000 <http://www.europarl.europa.eu/sides/getDoc.do?type=MOTION&reference=B5-2000-0593&language=EN> and the final report that was published in 2001: Temporary Committee on the ECHELON Interception System, 'Report on the existence of a global system for the interception of private and commercial communications (ECHELON interception system) (2001/2098(INI))' FINAL A5-0264/2001 PAR1, 11 July 2001. See also: Franco Piodi and Lolanda Mombelli, 'The ECHELON Affair. The European Parliament and the Global Interception System

side, the publication of NSA-newsletters in the summer of 2015 as a result of the *Snowden* revelations, plainly confirmed these allegations.[20]

2. SAFE HARBOUR DEAD

Using the leverage handed to her under the Lisbon Treaty[21], the then Commissioner of Justice *Reding* launched an ambitious legislative data protection package at the outset of 2012.[22] A proposed regulation was initiated to replace Directive 95/46[23] , and aimed *inter alia* to bind (US) service providers on EU territory by European rules on data protection. In parallel, a proposed directive had to upgrade the 2008 Framework Decision on data protection in the sphere of police and judicial cooperation in criminal matters.[24] In Decem-

1998 – 2002' (2014) European Parliament History Series <http://www.europarl.europa.eu/EPRS/EPRS_STUDY_538877_AffaireEchelon-EN.pdf>.

[20] See Henry Farrell and Abraham Newman, 'Transatlantic Data War. Europe fights back against the NSA' (2016) 95(1) Foreign Affairs 124.

[21] Treaty of Lisbon Amending the Treaty on European Union and the Treaty establishing the European Community (adopted 17 December 2007) OJ 2007/C 306/01.

[22] Viviane Reding, 'The European data protection framework for the twenty-first century' (2012) 2(3) International Data Privacy Law 119; Commission, 'Safeguarding Privacy in a Connected World -A European Data Protection Framework for the 21st Century' (Communication) COM (2012) 9 final.

[23] Colin J Bennet and Charles D Raab, 'The Adequacy of Privacy: the European Union Data Protection Directive and the North American Response' (1997) 13 The Information Society 245, 252.

[24] Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters [2008] OJ L 350/60; See also: Els De Busser and Gert Vermeulen, 'Towards a coherent EU policy on outgoing data transfers for use in criminal matters? The adequacy requirement and the framework decision on data protection in criminal matters. A transatlantic exercise in adequacy' in Marc Cools and others (eds), *EU and International Crime Control* (vol 4, Maklu 2010).

ber 2015 political agreement was reached on the new Regulation and the Directive.[25] Both of them were formally adopted in April 2016[26] and EU Member States are due to apply them from 25 respectively 6 May 2018 onwards. The adequacy requirement for data transfers to third states moreover remains intact. *Reding* also took up the defense for EU citizens for what concerns US access to their personal data.[27] Just a few months after the *Snowden* revelations, she came up with two parallel communications at the end of November 2013: 'Rebuilding Trust in EU-US Data Flows' (COM(2013) 846 final)[28] and 'communication on the functioning of the Safe Harbour from the perspective of EU citizens and companies established in the EU' (COM(2013) 847 final)[29] (hereafter: Safe Harbour communication). The first communication was accompanied by a report containing the 'findings on the ad-hoc workgroup data protection of the EU and the US'[30], which, among others, stipulated that the improvements in the Safe Harbour Decision should address the 'structural deficiencies in relation to the transparency and enforcement, the material safe harbour principles and the functioning of the *exception for*

---

[25] For an overview of the route leading up to these instruments, see the (then: 2004-2014) European Data Protection Supervisor's overview: Peter Hustinx, 'EU Data Protection Law: The Review of Directive 95/46/EC and the Proposed General Data Protection Regulation' (2015) <https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Speeches/2014/14-09-15_Article_EUI_EN.pdf>.

[26] Regulation (EU) 2016/679 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L 119/1; Directive (EU) 2016/680 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA [2016] OJ L 119/89.

[27] See Els De Busser, 'Privatization of Information and the Data Protection Reform' in Serge Gutwirth and others (eds), *Reloading Data Protection* (Springer 2014).

[28] Commission, 'Rebuilding Trust in EU-US Data Flows' (Communication) COM(2013) 846 final.

[29] Commission, 'Communication on the Functioning of the Safe Harbour from the Perspective of EU Citizens and Companies Established in the EU' (Communication) COM(2013) 847 final.

[30] Report of 27 November 2013 on the Findings by the EU Co-Chairs of the Ad Hoc EU-US Working Group on Data Protection [2013] <http://ec.europa.eu/justice/data-protection/files/report-findings-of-the-ad-hoc-eu-us-working-group-on-data-protection.pdf>.

national security'.[31] After all, the Safe Harbour Decision explicitly determined that the demands of 'national security, public interest and law enforcement' of the US supersede the Safe Harbour principles.[32] As it turned out, these exceptions rendered the safe harbours unsafe. In its 2013 Safe Harbour communication, the Commission established that 'all companies involved in the PRISM-programme, and which grant access to US authorities to data stored and processed in the US, appear to be Safe Harbour certified.' As such, '[t]his has made the Safe Harbour scheme one of the conduits through which access is given to US intelligence authorities to collecting personal data initially processed in the EU' (point 7). This was indeed the case: *Microsoft, Google, Facebook, Apple, Yahoo!, Skype, YouTube* … all of them were self-certified under Safe Harbour and simultaneously involved in the PRISM-programme. The Commission concluded that '[t]he large scale nature of these programmes may [have] result[ed] in [*more*] data transferred under Safe Harbour being accessed and further processed by US authorities *beyond what is strictly necessary and proportionate to the protection of national security* as foreseen under the exception provided in the Safe Harbour Decision'.[33]

Real urgency in the negotiations with the US only (re)surfaced following the ruling of the CJEU on 6 October 2015 in response to the appeal of *Max Schrems* against the Irish Data Protection Commissioner (in proceedings against *Facebook*[34], that has its European headquarters in Dublin) before the Irish High Court.[35] The latter had requested a preliminary ruling by the CJEU, namely as to whether the Irish privacy commissioner (as it had itself upheld) was bound by the Safe Harbour Decision of the Commission to the extent that it could no longer be questioned whether the US data protection regime was adequate, as such leading the Irish privacy commissioner to conclude that it could not investigate the complaint filed by *Schrems*. The latter had argued the contrary, based on the post-*Snowden* ascertainment that *Facebook* was active in the PRISM-programme, regardless of its self-certification under the Safe Harbour principles.[36] The CJEU concluded *inter alia* that '[t]he right to respect for

---

[31] Emphasis added.

[32] See Annex I, para 4.

[33] Safe Harbour Communication (n 29) point 7.1. (emphasis added).

[34] Natasha Simmons, 'Facebook and the Privacy Frontier' (2012) 33(3) JBL 58.

[35] Case C-362/14 *Maximillian Schrems v Data Protection Commissioner* EU:C:2015: 650.

[36] Andreas Kirchner, 'Reflections on privacy in the age of global electronic data processing with a focus on data processing practices of facebook' (2012) 6(1) Masaryk University Journal of Law and Technology 73; Mireille Hildebrandt, 'The rule of law in

private life, guaranteed by article 7 of the Charter and by the core values common to the traditions of the Member States, would be rendered meaningless if the State authorities were authorised to access electronic communications on a casual and generalised basis without any objective justification based on *considerations of national security or the prevention of crime that are specific to the individual concerned and without those practices being accompanied by appropriate and verifiable safeguards*'.[37] The CJEU furthermore recalled, with explicit reference to its Data Retention judgment of 8 April 2014[38] (in which it had declared the Data Retention Directive invalid) and its earlier judgments as cited under points 54 & 55 of its Data Retention judgment, its consistent case-law that 'EU legislation involving interference with the fundamental rights guaranteed by articles 7 and 8 of the Charter [regarding the respect for private and family life and the protection of personal data respectively] must, according to the Court's settled case-law, lay down *clear and precise* rules governing the scope and application of a measure […]'.[39] Still with reference to the Data Retention judgment (and the case-law cited under point 52 hereof), the CJEU jointly stated that 'furthermore and above all, protection of the fundamental right to respect for private life at EU level requires derogations and limitations in relation to the protection of personal data to apply *only in so far as is strictly necessary*'[40], whereby of course '[l]egislation *is not*

cyberspace?' (Inaugural Lecture at Radboud University Nijmegen, 2013) <http://works.bepress.com/mireille_hildebrandt/48/>; Bert-Jaap Koops, 'The trouble with European data protection law' (2014) Tilburg Law School Legal Studies Research Paper Series 04/2015 <http://m.isaca. org/Groups/Professional-English/privacy-data-protection/GroupDocuments/2014-08-24%20%20The%20Trouble%20with%20European%20Data%20Protection%20 Law.pdf>; Fanny Coudert, 'Schrems vs. Data Protection Commissioner: a slap on the wrist for the Commission and new powers for data protection authorities' (*European Law Blog* 2015) <https://lirias.kuleuven.be/bitstream/123456789/511500/1/FannyCoudert_Post+CJEU+Schrems_final.pdf>; Reid Day, 'Let the magistrates revolt: A review of search warrant applications for electronic in-formation possessed by online services' (2015) 64(2) U Kan L Rev 491; Shane Darcy, 'Battling for the Rights to Privacy and Data Protection in the Irish Courts' (2015) 31(80) Utrecht J of Intl and Eur L 131; David Flint, 'Computers and internet: Sunk without a trace – the demise of safe harbor' (2015) 36(6) JBL 236; Hannah Crowther, 'Invalidity of the US Safe Harbor framework: what does it mean?' (2016) 11(2) JIPLP 88; Nora Ni Loideain, 'The End of Safe Harbor: Implications for EU Digital Privacy and Data Protection Law' (2016) 19(8) J Internet L 7.

[37] *Maximillian Schrems* (n 34) para 34 (emphasis added).

[38] Joined Cases C 293/12 and C 594/12 *Digital Rights Ireland a.o.* EU:C:2014:238.

[39] *Maximillian Schrems* (n 34) para 91 (emphasis added).

[40] ibid, para 92 (emphasis added).

limited to what is strictly necessary where it authorises, on a generalised basis, *storage* of all the personal data of all the persons whose data has been transferred from the European Union to the United States without any differentiation, limitation or exception being made in the light of the objective pursued and without an objective criterion being laid down by which to determine the limits of the access of the public authorities to the data, and of its subsequent use, *for purposes which are specific, strictly restricted* and capable of justifying the interference which both *access to* that data and its *use* entail'.[41] In other words: collection (storage), access and use for reasons of national security, public interest or law enforcement require *specific and precise* criteria and are but allowed when *strictly necessary for specific purposes that are strictly restricted*. Given the fact that the Commission had omitted to implement such an assessment in its Safe Harbour Decision, the CJEU decided on the invalidity of the latter. Hence, with the *Schrems* case, the CJEU firmly put the finger on the following issue: engagements by US companies through self-certification under the Safe Harbour principles do not provide (adequate) protection as long as it remains unclear whether, despite large-scale interception programmes like PRISM, the US privacy regime may be considered adequate. With the sudden invalidity of the Safe Harbour Decision, a replacement instrument became an urgent necessity. The European Commission (since November 2014 the *Juncker* Commission, with *Věra Jourová* as the Commissioner for justice, fundamental rights and citizenship competent *inter alia* for data protection, under custody of super-commissioner (vice-president of the Commission) *Frans Timmermans* was quick to temper emotions. In a communication on the very day of the CJEU's decision, *Timmermans* recognized the Court's confirmation of the necessity 'of having robust data protection safeguards in place before transferring citizens' data'. He furthermore added that, following its Safe Harbour communication, the Commission was working with the US authorities 'to make data transfers *safer* for European citizens' and that, in light of the *Schrems* judgment, it would continue to work 'towards a renewed and *safe* framework for the transfer of personal data across the Atlantic'.[42]

---

[41] ibid, para 93 (emphasis added).

[42] Commission, 'Communication on the transfer of personal data from the EU to the United States of America under Directive 95/46/EC following the Judgment by the Court of Justice in Case C-362/14 (Schrems)' (Communication) COM(2015) 566 final; First Vice-President Timmermans and Commissioner Jourová, 'Press conference on Safe Harbour following the Court ruling in case C-362/14 (Schrems)' (Statement European Commission, 6 October 2015) (emphasis added).

3. LONG LIVE THE PRIVACY SHIELD? *TELE2 SVERIGE AB* AND DIGITAL RIGHTS IRELAND RESPECTIVELY *LA QUADRATURE DU NET* AND OTHERS V COMMISSION

On 29 February 2016, the Commission presented its eagerly awaited 'solution'. It launched a new communication, 'Transatlantic Data Flows: Restoring Trust through Strong Safeguards'[43], and immediately attached hereto – in replacement of the invalidated Safe Harbour Decision – its draft adequacy decision[44] of the US data protection regime (with 7 annexes) for data transfers under the protection of the so-called 'EU-US Privacy Shield'. On the JHA Council the day after, Jourovà hooted: 'Written assurances regarding the limitations on access to data by US public authorities on national security grounds'. Following a negative initial opinion about the initial draft decision, issued by the Article 29 Data Protection Working Party on 13 April 2016,[45] the Commission had no viable choice but to initiate summary renegotiations with the US, leading to just marginal adjustments of the Privacy Shield. The Article 29 Working Party (having nothing but mere advisory power in the first place) gave in,[46] as did the Article 31 Committee[47] (which did have veto power over the draft decision). The revised version of the Privacy Shield adequacy decision was adopted by the European Commission on 12 July 2016.

Un-surprisingly, the Privacy Shield is already facing legal challenges before the CJEU, following two actions for annulment filed on 16 September and 25 October 2016 in cases brought by Digital Rights Ireland[48] respectively *La Quadrature du Net* and Others[49] against the Commission, which the below

---

[43] Commission, 'Transatlantic Data Flows: Restoring Trust through Strong Safeguards' (Communication) COM(2016) 117 final.

[44] Commission Implementing Decision of xxx pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-U.S. Privacy Shield.

[45] Article 29 Working Party, 'Press release' (13 April 2016); Article 29 Working Party, 'Opinion 01/2016 on the draft EU-U.S. Privacy Shield adequacy decision' WP 238 (13 April 2016).

[46] Article 29 Working Party, 'Press release' (1 July 2016).

[47] On 8 July 2016, following its non-decision of 19 May on the initial version of the Privacy Shield.

[48] Case T-670/16 *Digital Rights Ireland v Commission* [2016] action brought on September 16, 2016.

[49] Case T-738/16 *La Quadrature du Net and Others v Commission* [2016] action brought on October 25, 2016.

analysis will refer to where relevant.[50] This will equally be the case for the Irish High Court judgment of 3 October 2017 in the case between *the Irish Data Protection Commissioner v Facebook Ireland Ltd.* and *Maximillian Schrems*, referring the issue of the validity of the Standard Contractual Clauses underlying personal data transfers from Facebook Ireland to Facebook Inc. (US) to the CJEU for a preliminary ruling.[51] At least indirectly, the case surely adds to the pressure on the Privacy Shield as well. Even with over 2,500 companies[52] self-certified under the new scheme, it will likely not survive infancy.

This is especially true since the CJEU has issued yet another judgment, on 21 December 2016, after a request for a preliminary ruling in the case *Tele2 Sverige AB*,[53] on data retention under the ePrivacy Directive. As will be explained in the analysis below, the findings of the CJEU at least indirectly place a bomb under the Privacy Shield as well, where it holds that 'general and indiscriminate retention of traffic data and location data' is inacceptable, leaving Member States the possibility for only 'targeted'[54] retention of traffic and location data, meaning that such retention must then be defined also in terms of the 'public […] that may potentially be affected'[55] and on the basis of 'objective evidence which makes it possible to identify a public whose data is likely to reveal a link, at least an indirect one, with serious criminal offences, and to contribute in one way or another to fighting serious crime or to preventing a serious risk to public security'[56]. Indiscriminate data collection, irrespective of later access or use restrictions, has been formally invalidated by the CJEU,

---

[50] Leaving out pleas and arguments relating to a lack of effective remedy or provision of independent monitoring under the Privacy Shield or US law, since these are not the focuses of the current contribution.

[51] *The Data Protection Commissioner v Facebook Ireland Limited And Maximillian Schrems* (2016) No. 4809 P. (The Hight Court Commercial) <http://www.europe-v-facebook.org/sh2/HCJ.pdf>. Reference to this judgment will also remain limited, ie by not dealing with the core issue of lack of effective remedy under the Standard Contractual Clauses transfer mechanism.

[52] The International Trade Administration (ITA) US Department of Commerce, 'Privacy Shield List' <https://www.privacyshield.gov/list>.

[53] Joined Cases C–203/15 and C–698/15, *Tele2 Sverige AB v Post-och telestyrelsen and Secretary of State for the Home Department v Tom Watson* EU:C:2016:970.

[54] ibid, para 108.

[55] ibid, paras 110-111.

[56] ibid, para 111.

even in a clearer fashion than in its 2014 Data Retention judgment. Interestingly, it has moreover explicitly ruled that data concerned must be retained within the European Union, which indirectly raises fresh doubts about the legitimacy of transferring (electronic communications) data under the Privacy Shield, and even under the Umbrella Agreement or the TFTP.

Before evaluating the Privacy Shield on its merits, it pays to bear in mind that, conceptually, it bears a very strong resemblance with the Safe Harbour regime. The *Safe Harbour* principles have now been renamed as *privacy* principles, which should serve as the new basis for data transfers coming from the EU to organizations – essentially: corporations – in the US who endorse these principles through the act of self-certification. Mirroring the Safe Harbour Decision, there is furthermore a general exception hereto should national security, public interest or law enforcement require so. Hence, the central question is whether the 'limitations' and 'safeguards' that are presented by the Privacy Shield – the Safe Harbour regime did not foresee any of these – are convincing enough. The way in which the European Commission desperately tried to convince everyone, through the means of its communication and the attached (draft) adequacy decision, of the satisfactory nature of the new regime, and that the US will effectively display an adequate data protection level under the Privacy Shield, is painful to witness. The heydays of former European justice commissioner *Reding* seem long gone. Apparently, demanding a genuine commitment of the US to refrain from collecting in bulk personal data of EU citizens or coming from the EU, and to only intercept communications and other personal data when strictly necessary and proportionate, was a political bridge too far. It seems that Commissioner *Jourová* (and super-commissioner *Timmermans*) have succumbed to the dominant importance of maintaining benevolent trans-Atlantic trade relations. Allowing trans-Atlantic transfers of personal data from companies or their subsidiaries in the EU to companies based in the US is after all the primordial goal of the Privacy Shield. Tough negotiating was apparently not considered an option, not even in the renegotiation stage. Nonetheless, one fails to see why such a commercial transfer of personal data *without* the option to do so in bulk, or without resorting to a capturing of such data that is disproportionate for intelligence or law enforcement purposes, would have been too high of a stake during negotiations. Companies - including the major US players like *Google, Apple, Facebook and Microsoft* - will *in the long run* not benefit from the fact that they will not be able to protect the data of their European or other users against government access. It is regrettable that they themselves seem insufficiently aware of this, leaving aside scarce counter-examples like the Apple-FBI

clash.[57] In the meantime, the very minimum is to burst the bubble of the European Commission's discourse in the privacy shield communication and its (draft) adequacy decision. The 'limitations' and 'safeguards' that the shield - according to the Commission - offers against US data collection in the interest of national security (by the intelligence services), public interest or law enforcement (by the police) are by absolutely no means sufficient. A simple focused reading and concise analysis hereof suffice to demonstrate this.

4. DATA COLLECTION FOR NATIONAL SECURITY PURPOSES

4.1. Amalgamation of collection and access v access and use

The Commission's analysis is misleading because it repeatedly posits that the 'limitations' to which the US will commit and that are applicable on the parts concerning 'access' and 'use'[58] for the purpose of national security, public interest or law enforcement, will be sufficient in light of EU law to amount to an adequate level of data protection. According to EU law, however, processing of personal data takes place as soon as 'collection' takes place, regardless of any future 'access' to this data or the 'use' thereof. By systematically wielding the term 'access' instead of 'collection', or by posing as if the limitations regarding 'access' will - with the proverbial single stroke of a brush - also include sufficient limitations in terms of 'collection', the Commission is wilfully pulling one's leg. To the extent still necessary, it suffices to recall the previously mentioned 2014 Data Retention judgment of the CJEU. In the latter, the Court abundantly made clear that limitations are necessary both in the phase of the 'collection' of personal data (*in casu* retention or conservation by suppliers of electronic communication services of traffic data in fixed and mobile telephony, internet access, internet e-mail and internet telephony) as in the phases of 'accessing' this data or its later 'use' (*in casu* by the competent police and judicial authorities). As such, the Commission skips a step, or at least tries to maintain the illusion that the Privacy Shield's limitations in terms of 'access' and 'use' will suffice to speak of an adequate data protection. This, however, is a flagrantly false rhetoric. Just the same, also the part that concerns the initial 'collection' of personal data by the competent authorities (*in*

[57] See, eg X, 'Taking a bite at the Apple. The FBI's legal battle with the maker of iPhones is an escalation of a long-simmering conflict about encryption and security' *The Economist* (London, 27 February 2016) <http://www.economist.com/news/science-and-technology/21693564-fbis-legal-battle-maker-iphones-escalation>.

[58] Commission Implementing Decision of 12 July 2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-US Privacy Shield [2016] C(2016) 4176 final (revised decision) para 67.

casu the US intelligence or law enforcement services) is bound by strict requirements. After all, one of the reasons why the CJEU dismissed the Data Retention Directive as invalid[59] was because 'in particular, it is not restricted to a retention in relation (i) to data pertaining to a particular time period and/or a particular geographical zone and/or to a circle of particular persons likely to be involved, in one way or another, in a serious crime, or (ii) to persons who could, for other reasons, contribute, by the retention of their data, to the prevention, detection or prosecution of serious offences'. It is important to bear in mind that back then, the debate was only on the conservation (and as such 'collection') by service providers of electronic communications, and not even on the direct 'collection' by intelligence and law enforcement services themselves, as is currently the case with the Privacy Shield.

With the CJEU judgment in *Tele2 Sverige AB* of December 2016, there is no doubt left that any preventative data retention must be 'limited […] to what is strictly necessary', 'with respect to the categories of data to be retained, the means of communication affected, *the persons concerned* and the retention period adopted',[60] these limitation criteria being explicitly cumulative, whilst the initial Data Retention judgment of 2014 (by the use of 'and/or') still left the door open for data retention which would not be targeted in terms of the 'persons concerned' or the 'public affected'.

Apart from this, the CJEU, in its 2014 Data Retention judgment, argued that in the Data Retention Directive '[there is] not only […] a general absence of limits', and that '[it] also fails to lay down any objective criterion by which to determine the limits of the *access* of the competent national authorities to the data and their subsequent *use* for the purposes of prevention, detection or criminal prosecutions concerning offences that, in view of the extent and seriousness of the interference with the fundamental rights enshrined in articles 7 and 8 of the Charter, may be considered to be sufficiently serious to justify such an interference'.[61] The Court continued that the 'Directive does not contain substantive and procedural conditions relating to the *access* of the competent national authorities to the data and to their subsequent *use*. Article 4 of the directive, which governs the *access* of those authorities to the data retained, does not expressly provide that that *access* and the subsequent *use* of the data in question must be *strictly restricted* to the purpose of preventing and detecting *precisely defined* serious offences or of conducting

[59] Joined Cases C-293/12 and C 594/12 *Digital Rights Ireland a.o.* EU:C: 2014:238, para 59.

[60] *Tele2* (n 52) para 108 (emphasis added).

[61] *Digital Rights Ireland* (n 59) para 60.

criminal prosecutions relating thereto; it merely provides that each Member State is to define the procedures to be followed and the conditions to be fulfilled in order to gain access to the retained data in accordance with necessity and proportionality requirements'.[62] Ultimately, and still with reference to 'access' and 'use', the Court lamented that the Directive 'does not lay down any objective criterion by which the number of persons authorised to *access* and *subsequently use* the data retained is limited to what is strictly necessary in the light of the objective pursued' and that '[a]bove all, the access by the competent national authorities to the data retained is not made dependent on a prior review carried out by a court or by an independent administrative body whose decision seeks to limit *access* to the data and their *use* to what is strictly necessary for the purpose of attaining the objective pursued and which intervenes following a reasoned request of those authorities submitted within the framework of procedures of prevention, detection or criminal prosecutions. Nor does it lay down a specific obligation on Member States designed to establish such limits'.[63] *Mutatus mutandis*[64] both the necessity and proportionality requirements can be firmly derived from the Data Retention judgment, and this with regards to the 'collection' of data on the one hand, and the 'access' to and 'use' of this data on the other. It was (as a minimum) to be expected from the Commission's Privacy Shield-communication that it would, for the discerned phases of 'collection' and 'access and use' respectively, carefully and systematically inquire into the US-proposed 'limitations' to its processing of and interference with EU personal data, drawing on the EU privacy requirements like these had been operationalized by the CJEU in its 2014 Data Retention judgment. Unfortunately, The privacy Shield Communications does not do so. From a substantive perspective, it is moreover the case that the guarantees in terms of 'collection' are clearly insufficient, since eg bulk collection of data remains perfectly possible under certain scenario's. Not only - and contrary to how it is presented by the Commission - does the Privacy Shield fail to solve this with the limitations it contains in terms of 'access and use', these limitations are inherently flawed as well, as they do not comply with nor mirror the (EU) requirements of strict necessity and proportionality.

---

[62] ibid, para 61 (emphasis added).

[63] ibid, para 62 (emphasis added).

[64] In the context of the Privacy Shield it is not just about the collection of, access to and use of personal data by police and judicial authorities in the framework of serious criminal offences, but also by intelligence and law enforcement services in the context of national security, public interest and law enforcement.

4.2. **Continued bulk or indiscriminate collection and processing**

In itself[65] it is gratifying that under PPD-28 (the *Presidential Policy Directive* 28 of 17 January 2014)[66] intelligence operations concerning sigint (signals intelligence, or the interception of electronic communication) will from now on only be allowed for purposes of foreign or counter-*intelligence* in support of *government* missions, and no longer with a view to benefit US companies' commercial interests. Sigint for industrial espionage, or to allow US companies to poach orders from European counterparts - which, as it turned out, happened *inter alia* with Echelon - has now been prohibited.

As far as diversions go, this is a big one. Following the *Schrems* judgment, this is evidently no longer the issue. The real question is whether the limitations on data collection for government purposes in the fields of national security, public interest (other than for economic motives or to gain a competitive advantage) or law enforcement are convincing enough. The reality is they are not, regardless of the Commission's attempts to mask this. Yet, on the other hand, what we do get is an abundance of vague engagements on behalf of the US. The following is an anthology:

Data collection under PPD-28 shall always be 'as tailored as feasible'[67], and members of the intelligence community '*should* require that, *wherever practicable*, collection *should* be focused on specific foreign intelligence targets or topics *through the use of discriminants* (eg specific facilities, selection terms and identifiers') [68]. There is a little too much of 'should' in this sentence for it to be genuinely convincing. Also, '*wherever practicable*' is both very conditional and open-ended, and the mere use of 'discriminants' evidently does not guarantee compliance with strict necessity and proportionality requirements. At the very most, they imply that bulk collection will not take place without at least some form of selection. Furthermore, the US engagements coming from the Office of the Director of National Intelligence (ODNI) recognise without much ado that bulk-sigint under 'certain' circumstances (that

[65] Commission Implementing Decision (draft decision) (n 43) para 70.

[66] Presidential Policy Directive, 'Signals Intelligence Activities' Presidential policy directive/PPD-28, 17 January 2014 <https://www.whitehouse.gov/the-press-office/2014/01/17/presidential-policy-directive-signals-intelligence-activities>.

[67] Commission Implementing Decision of 12 July 2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-US Privacy Shield [2016] C(2016) 4176 final (revised decision) para 71.

[68] ibid, para 70 (emphasis added).

are not very 'certain' to begin with, 'for instance in order to identify and assess new or emerging threats')[69] will still take place. The Commission on its part apparently considers it sufficiently reassuring that this may only take place when targeted collection through the use of discriminants is not deemed feasible 'due to technical or operational reasons'. The recognition by the Commission (dexterously stashed away in footnote 71) that the feasibility report, which was supposed to be presented to former President Obama by the Director of National Intelligence with reference to the possibility of developing software that would make it easier for the intelligence community to '*rather* conduct targeted instead of bulk-collection' [emphasis added], concluded that there is *no* software-based alternative to replace bulk-collection entirely, apparently does not contradict this reasoning. On the contrary, the Commission smoothly falls in with the ODNI's own estimation that bulk collection will not be the rule (rather than the exception)[70] - as if that would be sufficient in light of the EU requirements in terms of collection. Similarly comforting to the Commission is that the assessment of when a more targeted collection would be deemed technically or operationally 'not feasible', is not left to the individual discretion of individual staff of the intelligence community.[71] Now that really would have been quite wrong. In addition, the Commission sees an extra 'safeguard' in the fact that the potential 'discriminants' shall be determined by high-level policy makers, and that they will be (re)evaluated on a regular basis.[72] Ultimately, the Commission seems fully convinced when the ODNI-engagements make it clear that bulk-sigint *use* will - in any case - remain 'limited' to a list of six 'specific' national security purposes (cf. below, under c.). Limitations to the phase of 'use' do not, however, imply safeguards to the phase of 'collection'. This is rather *basic* in EU privacy law. To sum it up in the Commission's own view, the conclusion is that '*although not phrased in those legal terms'*, there is compliance with the EU requirements of necessity and proportionality[73]: bulk-collection needs to remain the exception rather than the rule, and should it nevertheless take place, the six 'strict' limitations for *use* are applicable. Rephrased in non-misleading terms: bulk-collection remains possible, so that it is by no means compliant with the tight restrictions of EU privacy law in terms of data collection.

---

[69] ibid, para 72.

[70] ibid, para 71.

[71] Commission Implementing Decision (draft decision) (n 43) para 60; more broadly phrased in Commission Implementing Decision (revised decision) para 70.

[72] Commission Implementing Decision (revised decision) (n 64) para 70.

[73] ibid, para 76.

The above argumentation is also prominently featuring in the actions for annulment of the Commission's Privacy Shield adequacy decision brought in the fall of 2016 by Digital Rights Ireland respectively *La Quadrature du Net* and Others. The 4th plea in law relied on by Digital Rights Ireland alleges that the provisions of the FISA Amendments Act 'constitute legislation permitting public authorities to have *access on a generalised basis* to the content of electronic communications and consequently are not concordant with Article 7 of the Charter […]'[74]. The generalised nature of collections allowed under the US regulatory regime is also the core element underlying the 1st plea in law put forward by *La Quadrature du Net* and Others,[75] leading them to conclude that the adequacy decision infringes article 7 of the Charter by not drawing the conclusion that such 'access on a generalised basis to the content of electronic communications' compromises the essence of the fundamental right to respect for private life. The plea in law draws on several paragraphs of the revised decision itself: '[…] PPD-28 explains that Intelligence Community elements *must sometimes collect bulk signals intelligence* in certain circumstances, for instance in order to identify and assess new or emerging threats […]'[76]; 'According to the representations from the ODNI, even *where the Intelligence Community cannot use specific identifiers to target collection*, it will seek to narrow the collection 'as much as possible' […]'[77]; '[…] Targeted collection is clearly prioritised, while *bulk collection is limited to (exceptional) situations* where targeted collection is not possible for technical or operational reasons. […]'[78].

To the extent necessary, also the Irish High Court, in its judgment of 3 October 2017[79], unambiguously established that '[o]n the basis of [the] definition [in Directive 95/46] and the evidence in relation to the operation of the PRISM and Upstream programmes authorised under s. 702 of FISA, it is clear that there is *mass indiscriminate processing* of data by the Unites States government agencies, whether this is described as mass or targeted surveillance'.

---

[74] Case T-670/16 *Digital Rights Ireland v Commission* [2016] action brought on September 16, 2016 (emphasis added).

[75] Case T-738/16 *La Quadrature du Net and Others v Commission* [2016] action brought on October 25, 2016.

[76] Commission Implementing Decision (revised decision) (n 64) para 72 (emphasis added).

[77] ibid, para 73 (emphasis added).

[78] ibid, para 76 (emphasis added).

[79] *The Data Protection Commissioner v Facebook Ireland Limited And Maximillian Schrems* (n 50) para 193 (emphasis added).

Even if, for Upstream, it may well be the case that 'mass *searching* […] is for targeted communications and […] in that sense not indiscriminate, […] it involves the *collection* of non-relevant data […]', so the Court held, thereby confirming the essential difference between 'bulk *searching*' v 'bulk *acquisition, collection or retention*'[80].

4.3. Access and use beyond strict necessity and proportionality

The six 'specific' national security purposes (mentioned above) to which the bulk-sigint *use* will be 'limited' according to the ODNI-engagements are the following[81]: 'detecting and countering certain activities of foreign powers, counterterrorism, counter-proliferation, cybersecurity, detecting and countering threats to US or allied armed forces, and combating transnational criminal threats, including sanctions evasion'. Downright optimistic is he who can discern the specificity hereof. No wonder that *La Quadrature du Net* and Others, in their action of 25 October 2016 for annulment of the Commission's adequacy decision, build their 2nd plea in law on it, alleging that the 'six national security purposes […] cannot be considered as [an] objective criterion allowing a limitation to "purposes which are specific, strictly restricted and capable of justifying the interference"'.

Moreover, it remains an arduous task to assess these purposes *überhaupt* in the sense of 'restrictions', let alone that they would be convincing in light of the EU requirements in this field as operationalised in the CJEU's Data Retention judgment. Nevertheless, the Commission appears to see such considerations as nit-picking. In its adequacy decision, the Commission even attempts to embellish all of this[82] by *not* mentioning the six vague purposes by name, but by adducing their potential to detect and counter threats stemming from espionage, terrorism, weapons of mass destruction, threats to cyber-security, to the armed forces or military personnel, or in the context of transnational criminal threats to any of the other purposes. Such a misrepresentation is without honour. What we should be able to expect from the European Commission is that it protects the privacy of the European citizen and that it will inform the latter (via its communication and (draft) adequacy decision) in a clear and correct way, not that the Commission contemptuously approaches EU citizens with hollow and US-friendly rhetoric whilst continuing to give away their privacy via bulk-collection in order to facilitate almost any US-in-

[80] ibid, para 192 (emphasis added).

[81] Original letter annexed to the initial draft decision, p 4 para 3; Annex VI to the revised decision p 93 para 4.

[82] Commission Implementing Decision (revised decision) (n 64) para 74.

telligence purpose. As if all of this weren't enough already, the above mentioned *use* - 'limitations' will also be applicable to the *collection* of personal data that runs through trans-Atlantic submarine cables – located outside of US territory – and this – at least according to the Commission – is the icing on the cake in terms of reassurance.[83] Just for completion, for this specific type of data, collection is not liable for a request conformant to FISA-legislation or through a so-called *National Security Letter* of the FBI. Such a request - accentuated by the Commission - *will* be mandatory when the intelligence community wishes to retrieve information from companies *on* US territory that are 'self-certified' under the new Privacy Shield.[84]

This type of 'access' - and for that matter, a relief that for once this term is utilised in its proper, genuine meaning - would continuously need to be specific and limited, as it would require specific terms of selection or criteria. The fact that this would (even) be applicable to the PRISM-programme is considered a real windfall, at least by the Commission: this information is after all selected on the basis of individual selection criteria such as e-mail addresses and telephone numbers, and not through keywords or names of individuals.[85] As the Commission itself cannot resist emphasising, according to the *Civil Liberties Oversight Board* this would mean that in the US, when necessary, it would exclusively concern 'targeting specific [non-U.S.] persons about whom an individualised determination has been made'. Footnote 87 clarifies that the continuation of unleashing PRISM on US companies under the Privacy Shield will therefore *not* entail the undirected (unspecific) collection of data on a large scale. As you like it. PRISM apparently is *not* a programme for the collection of data on a large scale, or it is (at least) sufficiently selective to pass the test of European privacy law. It seems the Commission itself was mistaken when, at the end of November 2013, it claimed in its Safe Harbour communication that 'the large scale character of these programmes [...] [could] have as a consequence that, of all the data that was transferred in the framework of the safe harbour, more than was strictly necessary for, or proportionate to, the protection of national security, was consulted and further processed by the American authorities, as was determined by the exception foreseen in the Safe Harbour decision.' Moreover, as the Commission is so eager to allege, there is *empirical evidence* that the number of *targets* affected through PRISM on a yearly basis is 'relatively small *compared to the overall flow of data on*

[83] ibid, para 75.

[84] ibid, para 78.

[85] ibid, para 81 (sic).

the internet'.[86] The source for this statement is the 2014 annual report of the ODSI itself, hence it indeed appears that the PRISM-authorisation under FISA was applicable 'only' to 93.000 targets. Thus, nothing too large-scale for the Commission. Add to this the ODSI-warranty (in annex VI to the adequacy decision) that the bulk-collection only takes place on a 'small proportion of the internet', this including the capturing of data on the trans-Atlantic cables[87], and finally, everyone is convinced. Finally, what is added are a number of nugatory *additional* guarantees in the following paragraphs[88] such as, for instance, that it is insufficient that sigint was collected over the course of the 'routine activities of a foreign person' to spread it or to retain it permanently without there being other intelligence-based reasons for this.[89] EU citizens may rest assured: electronic communication regarding their day-to-day routines will not be retained permanently when there are no well-founded reasons to do so. All of this leads the Commission to conclude[90] that, in the US, there are ample rules in place specifically designed to ensure that 'any interference for purposes of national security with the fundamental rights of the persons whose personal data are transferred [...] under the EU-US Privacy Shield [is limited] to what is *strictly necessary* to achieve the legitimate objective in question' [emphasis added]. And with this alone the European citizen will have to make do. Those who thought that, following the *Schrems* judgment, there would be a real *issue* with the commercial transfers of personal data to the US simply because the companies on its territory had to run this data through the PRISM-filter were sorely mistaken. The CJEU based the invalidity of the Safe Harbour decision of the Commission on the techno-legal establishment that the latter had omitted to include in its decision that 'it must find, duly stating reasons, that the third country concerned in fact ensures, by reason of its domestic law or its international commitments, a level of protection of fundamental rights essentially equivalent to that guaranteed in the EU legal order, a level that is apparent in particular from the preceding paragraphs of the present judgment'.[91] In essence, the CJEU herewith refers to the substantive criteria of the Data Retention judgment. The European Commission's failure to mention 'that the United States in fact 'ensures' an adequate level of protection by reason of its domestic law or its international

[86] ibid, para 82.

[87] ibid.

[88] ibid, para 83-87.

[89] ibid, para 87.

[90] ibid, para 88.

[91] ibid, para 96.

commitments'[92] was enough for the Court to decide on a techno-legal breakpoint, 'without there being any need to examine the content of the safe harbour principles'.[93] Unfortunately, this (and only this) seems to be precisely what the European Commission remembers from the *Schrems* judgment, and is the (sole) reason why the Commission seems convinced that its reasoned ascertainment of the adequate safeguards in the US' privacy regime will suffice. While the *reasoning* aspect of this ascertainment is not open to question, the adequacy hereof is very equivocal - yet this was surely one of the *Schrems* judgment's demands. In brief, the presented argumentation is selective, often misleading, sometimes plain bogus. And last but not least, any effort to introduce a profound scrutiny based on the criteria established in the Data Retention judgment was omitted by the Commission, contrary to the CJEU *Schrems* judgment that specifically referred hereto.

5. DATA COLLECTION FOR LAW ENFORCEMENT OR PUBLIC INTEREST PURPOSES

In its adequacy decision, the Commission also evaluates the data protection-relevant limitations and safeguards afforded by US law within the *law enforcement* sphere. At the risk of sounding redundant, very much like all of the foregoing, the Commission's conclusion, un-surprisingly, is that the US data protection level is to be considered adequate.[94] Search and seizure by law enforcement authorities principally requires, according to the 4th amendment, a prior court order based on *'probable cause'*. In certain circumstances, however, the 4th amendment is not applicable because for some forms of electronic communication there are no legitimate privacy expectations. In such an event, a court order is not mandatory, and law enforcement may revert to a 'reasonability test'. The latter simply implies that a consideration is made between the level of infringement of an investigative measure with respect to an individual's privacy and the extent to which that measure is deemed necessary in function of legitimate government purposes like law enforcement (or another public interest). For the European Commission, this suffices to conclude that this *'captures the idea'* of necessity and proportionality under EU law.[95] The cold fact that the 4th amendment is quite simply not applicable to non-US citizens outside of US territory does not change the Commission's

[92] ibid, para 97.

[93] ibid, para 98.

[94] ibid, para 125.

[95] ibid, para 126.

viewpoint. The reasoning is that EU citizens would receive and enjoy the indirect protection that US companies - where their data is being stored - enjoy. The establishment that such a protection can be bypassed fairly easily via a simple reasonability test, and that the privacy of a company is not automatically at stake when law enforcement is after the private data of a user (only), is conveniently not addressed. According to the Commission, there are furthermore additional protective mechanisms, such as directives of the ministry of justice that allow law enforcement access to private data only on grounds that are labelled by the Commission as 'equivalent' to the necessity and proportionality requirement: these directives after all stipulate that the FBI must take recourse to the *least intrusive measure*.[96] That such a principle only addresses the *subsidiarity* of applying certain investigative measures, instead of dealing with their *necessity* or *proportionality* will probably be considered as nit-picking again. Finally, the Commission deals with the practice of administrative subpoenas (as issued at the time against the SWIFT US-hub). These are, as can be read, allowed only in particular circumstances and are subject to an independent judicial appraisal. What remains underemphasized - perhaps not to spoil the fun - is that the latter is only a possibility when a company refuses to spontaneously give effect to an administrative subpoena, thus forcing the government to have recourse to a judge for effecting said subpoena.

Likewise, when administrative subpoenas are issued in the *public interest*, similar limitations[97] are applicable. After all, administrations are only allowed to order access to data that is deemed relevant for matters under their competence - who would have thought any different? - and of course need to pass through the aforementioned reasonability test. All the more reason for the Commission, without wasting any more words on the matter, to promptly come to a conclusion[98] similar to the one on the collection of data in view of national security. As it is seemingly evidently stated, the US has rules in place that are specifically designed so that 'any interference for law enforcement or other public interest purposes with the fundamental rights of the persons whose personal data are transferred [will be limited] to what is *strictly necessary* to achieve the legitimate purpose in question' and that ensure 'effective legal protection against such interference'.

---

[96] ibid, para 127.

[97] ibid, para 129.

[98] ibid, para 135 (emphasis added).

The failure to safeguard against indiscriminate access to electronic communications by US law enforcement authorities has also been picked up by Digital Rights Ireland in its action of 16 September 2016 for annulment of the Privacy Shield adequacy decision. Its 8th plea in law alleges that, based on this very argument, the decision is invalid as a breach of the rights of privacy, data protection, freedom of expression and freedom of assembly and association, as provided for under the Charter and by the general principles of EU Law.

6. **CONCLUSION**

The Privacy Shield is all the added value of a scrap of paper – insufficient, lacking credibility, misleading – and nothing but a new jackstraw for the previous *Safe Harbour* approach. None of the US harbours have become safer, PRISM and the likes remain on track. The Commission has nevertheless gone through great lengths to set forth why all of us *should* believe that the 'limitations' and 'safeguards' available under US law are in line with the EU requirements of strict necessity and proportionality. The 2015 *Schrems* judgment, apparently, hasn't changed anything.

Luckily, it seems a matter of time only before the CJEU, in line with the latter decision, building on its 2014 Data Retention and 2016 *Tele2 Sverige AB* judgments, and following the actions for annulment brought in the fall 2016 by *Digital Rights Ireland* respectively *La Quadrature du Net* and Others, reinforced by the Irish High Court's recent judgment in *Data Protection Commissioner v Facebook Ireland Ltd. and Maximillian Schrems*, invalidates the Privacy Shield and annuls the Commission's corresponding adequacy decision.

In doing so, it will show that EU data protection standards are not up for grabs, neither in the trans-Atlantic relations nor in the EU's future relations with key trading partners in East and South-East Asia and with countries in Latin America and the European neighbourhood, which the Commission will negotiate or is negotiating similar 'shields' with,[99] like Japan.[100]

Likewise, the EU and data protection authorities, intelligence and law enforcement oversight bodies and courts throughout the EU should draw lessons on the internal level. They must in particular see to it that, irrespective of later access or use restrictions, preventative data retention or collection

[99] Commission (EC), 'Exchanging and Protecting Personal Data in a Globalised World' (Communication) COM(2017) 7 final, 10 January 2017.

[100] Commission (EC), 'Joint statement by Commissioner Věra Jourová and Haruhi Kumazawa, Commissioner of the Personal Information Protection Commission of Japan on the state of play of the dialogue on data protection' (Joint Statement), 4 July 2017.

for protecting internal security or crime fighting is sufficiently selective, not only with respect to the categories of data to be retained, the means of communication affected and the retention period adopted, but also with respect to the persons concerned and the public affected.

7. SELECTED LITERATURE

Bennet CJ and Raab CD, 'The Adequacy of Privacy: the European Union Data Protection Directive and the North American Response' (1997) 13 The Information Society 245

Connorton PM, 'Tracking Terrorist Financing through SWIFT: When U.S. subpoenas and foreign privacy law collide' (2007) 76(1) Fordham L Rev 283

Coudert F, 'Schrems vs. Data Protection Commissioner: a slap on the wrist for the Commission and new powers for data protection authorities' (*European Law Blog* 2015) <https://lirias.kuleuven.be/bitstream/123456789/511500/1/FannyCoudert_Post+CJEU+Schrems_final.pdf>

Crowther H, 'Invalidity of the US Safe Harbor framework: what does it mean?' (2016) 11(2) JIPLP 88

Day R, 'Let the magistrates revolt: A review of search warrant applications for electronic in-formation possessed by online services' (2015) 64(2) U Kan L Rev 491

Darcy S, 'Battling for the Rights to Privacy and Data Protection in the Irish Courts' (2015) 31(80) Utrecht J of Intl and Eur L 131

De Busser E, *Data Protection in EU and US Criminal Cooperation* (Maklu 2009)

De Busser E, 'Purpose limitation in EU-US data exchange in criminal matters: the remains of the day' in Cools M and others (eds), *Readings on criminal justice, criminal law and policing* (vol 2, Maklu 2009)

De Busser E and Vermeulen G, 'Towards a coherent EU policy on outgoing data transfers for use in criminal matters? The adequacy requirement and the framework decision on data protection in criminal matters. A transatlantic exercise in adequacy' in Cools M and others (eds), *EU and International Crime Control* (vol 4, Maklu 2010)

De Busser E, 'Privatization of Information and the Data Protection Reform' in Gutwirth S and others (eds), *Reloading Data Protection* (Springer 2014)

De Hert P and De Schutter B, 'International Transfers of Data in the Field of JHA: The Lessons of Europol, PNR and Swift' in Martenczuk B and Van Thiel S (eds), *Justice, Liberty, Security: New Challenges for EU External Relations* (I.E.S. series nr. 11, VUB Press 2008)

Farrell H and Newman A, 'Transatlantic Data War. Europe fights back against the NSA' (2016) 95(1) Foreign Affairs 124

Flint D, 'Computers and internet: Sunk without a trace – the demise of safe harbor' (2015) 36(6) JBL 236

Gonzalez Fuster G, De Hert P and Gutwirth S, 'SWIFT and the vulnerability of transatlantic data transfers' (2008) 22(1-2) Intl Rev of L Computers & Technology 191

Greenwald G, 'NSA collecting phone records of millions of Verizon customers daily' *The Guardian* (London, 6 June 2013) <http://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order>

Hildebrandt M, 'The rule of law in cyberspace?' (Inaugural Lecture at Radboud University Nijmegen, 2013) <http://works.bepress.com/mireille_ hildebrandt/48/>

Hustinx P, 'EU Data Protection Law: The Review of Directive 95/46/EC and the Proposed General Data Protection Regulation' (2015) <https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Speeches/2014/14-09-15_Article_EUI_EN.pdf>

Jaeger PT, Bertot JC and McClure CR, 'The impact of the USA Patriot Act on collection and analysis of personal information under the Foreign Intelligence Surveillance Act' (2003) 20 Government Information Quarterly 295

Kirchner A, 'Reflections on privacy in the age of global electronic data processing with a focus on data processing practices of facebook' (2012) 6(1) Masaryk University Journal of Law and Technology 73

Koops BJ, 'The trouble with European data protection law' (2014) Tilburg Law School Legal Studies Research Paper Series 04/2015 <http://m.isaca.org/Groups/Professional-English/privacy-data-protection/GroupDocuments/2014-08-24%20%20The%20Trouble%20with%20European%20Data%20Protection%20 Law.pdf>

Long WJ and Quek MP, 'Personal data privacy protection in an age of globalization: the US-EU safe harbor compromise' (2002) 9(3) JEPP 325

MacAskill E and others, 'GCHQ taps fibre-optic cables for secret access to world's communications' *The Guardian*, (London, 21 June 2013) <http://www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications -nsa>

Ni Loideain N, 'The End of Safe Harbor: Implications for EU Digital Privacy and Data Protection Law' (2016) 19(8) J Internet L 7

Papandrea MR, 'Leaker Traitor Whistleblower Spy: National Security Leaks and the First Amendment' (2014) 94(2) Boston U L Rev 449

Peers S, 'The exchange of personal data between Europol and the USA' (2003) Statewatch Analysis no 15 <www.statewatch.org>

Piodi F and Mombelli I, 'The ECHELON Affair. The European Parlia-ment and the Global Interception System 1998 – 2002' (2014) European Parliament History Series <http://www.europarl.europa.eu/EPRS/EPRS_STUDY_538877_AffaireEchelon-EN.pdf>.

Reding V, 'The European data protection framework for the twenty-first century' (2012) 2(3) International Data Privacy Law 119

Simmons N, 'Facebook and the Privacy Frontier' (2012) 33(3) JBL 58

Vermeulen G, 'Transatlantisch monsterverbond of verstandshuwelijk? Over het verschil tussen oorlog en juridische strijd tegen terreur en de versterkte politie- en justitiesamenwerking tussen EU en VS' (2004) 25(1) Panopticon 90

Vermeulen G, 'The Paper Shield. On the degree of protection of the EU-US privacy shield against unnecessary or disproportionate data collection by the US intelligence and law enforcement services' in Svantesson DJB & Kloza D (eds), *Trans-Atlantic Data Privacy Relations as a Challenge for Democracy, European Integration and Democracy Series* (vol 4, Intersentia 2017)

X, 'Taking a bite at the Apple. The FBI's legal battle with the maker of iPhones is an escalation of a long-simmering conflict about encryption and security' *The Economist* (London, 27 February 2016) <http://www.economist.com/news/science-and-technology/21693564-fbis-legal-battle-maker-iphones-escalation>

Reconciling the (extra)territorial reach of the GDPR with public international law

BRENDAN VAN ALSENOY[1]

1. INTRODUCTION

Extraterritoriality and data protection make for a controversial mix. Different attitudes towards privacy, coupled with a lack of global consensus on jurisdictional boundaries, fuel an intense debate among those advocating jurisdictional restraint and those emphasizing the need to ensure effective protection.[2] With the adoption of the General Data Protection Regulation (GDPR),[3] the EU legislature has revised the territorial scope of EU data protection law. In part, the GDPR confirms choices made by policymakers and the Court of Justice of the European Union (CJEU) in the context of Directive 95/46/EC.[4] In other respects, important new elements have been introduced.

During the preparation of the GDPR, commentators warned that the EU was in danger of overstepping its jurisdictional boundaries.[5] As a member of the

---

[1] Legal advisor, Commission for the Protection of Privacy, Belgium; senior affiliated postdoc researcher, KU Leuven Centre for IT & IP law (imec). I would to thank Joelle Jouret and Michal Czerniawski for their useful input and feedback during the writing process. Any errors or mistakes are my own. Email: Brendan.VanAlsenoy@privacycommission.be.

[2] See Dan Jerker B. Svantesson, *Extraterritoriality in Data Privacy Law* (Ex Tuto Publishing 2013) 20, 21; Chistopher Kuner, 'Extraterritoriality and regulation of international data transfers in EU data protection law' (2015) 5 IDPL 235; Paul de Hert and Michal Czerniawski, 'Expanding the European data protection scope beyond territory: Article 3 of the General Data Protection Regulation in its wider context' (2016) 6 IDPL 230 and Merlin Gömann, 'The new territorial scope of EU data protection law: deconstructing a revolutionary achievement' (2017) 54 CM L Rev 567.

[3] Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), [2016] OJ L 119/1-88.

[4] Regulation Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data, [1995] OJ L 281/31-50.

[5] See eg Omer Tene and Christopher Wolf, *Overextended: Jurisdiction and Applicable Law under the EU General Data Protection Regulation* (White Paper, The Future of Privacy Forum, 2013) 1,10.

international community, the European Union is bound to observe the general principles of customary international law of jurisdiction.[6] According to customary international law, there should be a *bona fide* connection between the subject matter of a dispute and the State asserting jurisdiction over it.[7] The aim of this contribution is to scrutinize the triggers'[8] that render EU data protection law applicable to conduct which takes place, either in whole or in part, outside of Union territory. The analysis shall be limited to the EU's exercise of prescriptive jurisdiction, leaving questions of adjudicative or enforcement jurisdiction for future work. I will begin by analyzing the territorial scope of the GDPR, in particular its potential for extra-territorial reach.[9] Similarities and differences between the GDPR and Directive 95/46 will be highlighted, looking back at relevant case law and guidance to clarify key concepts. Next, the legitimacy of EU's assertion of prescriptive jurisdiction will be assessed from the perspective of public international law. The main question this contribution seeks to answer is: can the (extra-)territorial scope of the GDPR be reconciled with the principles of public international law? Or has it in fact 'overextended' itself?

2. THE EXTRA-TERRITORIAL REACH OF THE GDPR

The territorial scope of the GDPR is determined by article 3. For purposes of this contribution, the two most important triggers are (a) the presence of a relevant establishment of a controller or processor on EU territory and (b)

---

[6] Mistale Taylor, 'Permissions and prohibitions in data protection jurisprudence' (2016) 2 Brussels Privacy Hub Working Paper 3, 5, with reference to Case C-366/10 *Air Transport Association of America and Others v Secretary of State for Energy and Climate Change* EU:C:2011:864, paras 101 and 123.

[7] See Cedric Ryngaert, *Jurisdiction in International Law* (Oxford University Press 2008) 21 et seq. See also Bernhard Maier, 'How Has the Law Attempted to Tackle the Borderless Nature of the Internet' (2010) 18 IJLIT 142, 155.

[8] A "trigger" is a mechanism that launches the application of EU law and delimits its personal and territorial scope of application (Joanne Scott, 'The New EU 'Extraterritoriality'' (2014) 51 CM L Rev 1343, 1344).

[9] For a discussion of the concept of "extra-territoriality" see Dan Jerker B. Svantesson 'The Extraterritoriality of EU Data Privacy Law – Its Theoretical Justification and Its Practical Effect on U.S. Businesses' (2014) 50 Stan J intl L 60. See also Joanne Scott, 'Extraterritoriality and Territorial Extension in EU Law' (2014) 62 Am J Comp L 87, 90.

the monitoring or targeting of EU data subjects.[10] Whilst the first ground governs the situation in which the controller or processor has an establishment on EU territory, the second ground governs the situation where there is no such establishment. It is already clear, however, that both triggers have an extra-territorial dimension.

2.1. Article 3(1) GDPR

Article 3(1) provides that the GDPR shall apply

> to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not.

Determining the territorial scope of the GDPR pursuant to article 3(1) implies prior identification of the entity which is acting as a 'controller' or 'processor' of the processing, as well as the location of its 'establishment(s)'. Equally important, however, is the reference to the 'context of activities': this criterion implies that the establishment must be involved in activities implying the processing of personal data in question.[11] Or rather, the establishment must be involved in a 'real and effective exercise of activities in the context of which the personal data are being processed'.[12]

Article 3(1) GDPR is the successor of article 4(1)(a) of Directive 95/46, with two notable changes. First, article 3(1) GDPR makes reference not only to an establishment of a controller, but also to an establishment of a processor. As a result, the processing of personal data might also be subjected to EU law by virtue of a *processor* having an establishment located within the EU.[13] Second, article 3(1) explicitly indicates that it is not necessary for the processing of

---

[10] In addition to these 'main criteria', the GDPR also specifies in article 3(3) that the GDPR applies to the processing of personal data by a controller not established in the Union, but in a place where Member State law applies by virtue of public international law. Recital (25) indicates that this might be the case, for example, as regards the processing of personal data carried out in a Member State's diplomatic mission or consular post.

[11] Article 29 Data Protection Working Party, 'Opinion 8/2010 on applicable law' WP 179 (16 December 2010).

[12] ibid 11.

[13] For a discussion of implications of this addition see Els J. Kindt, 'Why research may no longer be the same: About the territorial scope of the New Data Protection Regulation' (2016) 32 CLS Rev 729, 741 and Lokke Moerel, 'The data transfer regime for processors does not make sense and requires clarification' (*GDPR Conundrums: Data Transfer*, 9 June 2016) <https://iapp.org/news/a/gdpr-conundrums-data-transfer>.

personal data to take place within the EU in order for the GDPR to apply. As a result, article 3(1) GDPR has the potential for extra-territorial reach: EU data protection law shall apply to processing taking place outside EU territory if it is being carried out 'in the context of the activities of an establishment of the controller or processor' located within the EU.[14] To properly delineate the extra-territorial reach of the GDPR, it is necessary to analyze the words 'establishment' and 'in the context of the activities'.

2.1.1. 'Establishment'

The term 'establishment' is not formally defined by the GDPR, but according to recital (22) implies 'the effective and real exercise of activity through stable arrangements.' The legal form of such 'arrangements', whether it be simply a branch or a subsidiary with a legal personality, is not a determining factor in that respect.[15]

The term 'establishment' is not always given a uniform meaning or interpretation in EU law.[16] In relation to the freedom of establishment under article 50 TFEU, the Court of Justice of the European Union has considered that a stable establishment requires that 'both human and technical resources necessary for the provision of particular services are permanently available'.[17] In the context of data protection law, the concept of establishment has received a particularly broad interpretation. In its *Weltimmo* ruling, the Court of Justice of the European Union (CJEU) stated that the concept should be interpreted in a flexible rather than a formalistic manner.[18] It extends to any real and effective activity — even a minimal one — exercised through stable

---

[14] See also Brendan Van Alsenoy and Marieke Koekkoek, 'Internet and jurisdiction after Google Spain: the extraterritorial reach of the 'right to be delisted''(2015) 5 IDPL 105, 107.

[15] This portion of recital (22) GDPR is almost identical to the corresponding text of recital (19) of Directive 95/46.

[16] Scott (n 8) 1352.

[17] Article 29 Data Protection Working Party, 'Opinion 8/2010 on applicable law' WP 179 (16 December 2010). See also Lokke Moerel, 'The long arm of EU data protection law: Does the Data Protection Directive apply to processing of personal data of EU citizens by websites worldwide?' (2011) 1 IDPL 28, 35 (concluding that all subsidiaries and most branch offices will qualify as 'establishments').

[18] Case C-230/14 *Weltimmo sro v Nemzeti Adatvédelmi és Információszabadság Hatóság* EU:C:2015:639, para 29 (hereafter "*Weltimmo*"). Article 29 Data Protection Working Party, 'Update of Opinion 8/2010 on applicable law in light of the CJEU judgement in Google Spain' WP 179 (16 December 2015).

arrangements.[19] According to the CJEU, both the degree of stability of the arrangements and the effective exercise of activities should be assessed in the light of the specific nature of the economic activities and the provision of services concerned. This is particularly true for undertakings offering services exclusively over the Internet.[20] As a result, in some circumstances, the presence of *one single representative* can suffice to constitute a stable arrangement if that representative acts with a sufficient degree of stability 'through the presence of the necessary equipment for provision of the specific services concerned in the Member State in question'.[21]

Although it has received a broad interpretation, the concept of establishment is not without limits. Mere accessibility of a website, for example, would not suffice to constitute an 'establishment' for purposes of article 3(1).[22] A stable presence of at least some human and technical resources appears necessary to conclude that an 'establishment' exists within the EU.[23]

2.1.2. 'In the context of the activities'

Mere physical presence of a controller or processor on Union territory is not sufficient to render the GDPR applicable pursuant to article 3(1). To render the GDPR applicable, it is necessary that the processing at issue is undertaken "in the context of the activities" of an establishment on EU territory. The CJEU has clarified the meaning of the words 'in the context of the activities' in three rulings: *Google Spain*, *Weltimmo* and *Verein für Konsumenteninformation*.

In *Google Spain*, the CJEU was asked to determine whether Google's search engine activities (ie, the crawling of web pages, indexation, storage, etc) may be viewed as taking place 'in the context of the activities' of one of its local subsidiaries, *Google Spain SL. Google Spain's* activities consisted in the promotion and sale of advertising space, as a commercial representative of Google. The CJEU began by confirming that the notion of 'in the context of the activities' does not require that the establishment in question itself is actively

[19] *Weltimmo* (n 18).

[20] *Weltimmo* (n 18).

[21] *Weltimmo* (n 18) para 30. See also the Opinion of Advocate General Cruz Villalón on *Weltimmo* (n 18) para 34.

[22] Case C-191/15 *Verein für Konsumenteninformation v Amazon EU Sàrl* EU:C:2016:388, para 76 (hereafter "*Verein für Konsumenteninformation*").

[23] See also Article 29 Data Protection Working Party, 'Opinion 8/2010 on applicable law' WP 179 (16 December 2010).

engaged in the processing.[24] It also considered that those words cannot be interpreted restrictively, in the light of the objective of ensuring effective and complete protection.[25] The CJEU went on to consider that the activities of the search engine operator and those of its establishment are 'inextricably linked', as Google's search engine service is closely related to the activity of selling advertising space.[26] Specifically, the Court reasoned that

> the activities relating to the advertising space constitute the means of rendering the search engine at issue economically profitable and that engine is, at the same time, the means enabling those activities to be performed.[27]

Based on these considerations, the CJEU concluded that the processing of personal data is carried out 'in the context of the activities' of an establishment of the controller

> when the operator of a search engine sets up in a Member State a branch or subsidiary which is intended to promote and sell advertising space offered by that engine and which *orientates its activity towards the inhabitants of that Member State*.[28]

Weltimmo concerned the processing of personal data by a company running a property dealing website. Although the company was formally registered in Slovakia, it published adverts concerning Hungarian properties.[29] For that purpose, it processed the personal data of the advertisers, several of whom had Hungarian nationality. When the Hungarian Data Protection Authority decided to investigate, *Weltimmo* countered that the authority was not competent and could not apply Hungarian law in respect of a supplier of services established in another Member State.[30] In its assessment, the CJEU reiterated

---

[24] Case C-131/12 *Google Spain SL, Google Inc. v Agencia Española de Protección de Datos (AEPD), Mario Costeja González* EU:C:2014:317, para 52 (hereafter: "*Google Spain*").

[25] *Google Spain* (n 24) para 53.

[26] *Google Spain* (n 24) para 56.

[27] *Google Spain* (n 24) para 56.

[28] *Google Spain* (n 24) para 60 (emphasis added).

[29] *Weltimmo* (n 18) para 9.

[30] *Weltimmo* (n 18) para 12.

that the wording 'in the context of the activities' cannot be interpreted restrictively, with reference to its earlier *Google Spain* ruling.[31] To ascertain whether the establishment was involved in the exercise of activities 'in the context of which' the processing is carried out, the referring court was invited to take into account the fact that the activity of the controller in respect of the processing is 'mainly or entirely directed at that Member State'.[32] In addition, the referring court was invited to consider the presence of a representative in that Member State, who is responsible for *recovering the debts resulting from that activity* and for *representing* the controller in the administrative and judicial proceedings relating to the processing of data concerned.[33] The nationality of the persons concerned by the data processing was, however, deemed irrelevant.[34]

In *Verein für Konsumenteninformation*, the CJEU was asked to clarify whether or not the processing of personal data by *Amazon EU* must comply with the data protection rules of each Member State to which its commercial activities are directed.[35] While indicating that mere accessibility of a website does not suffice to constitute a relevant 'establishment', the Court clearly hinted that there may be an establishment other than *Amazons EU*'s Luxembourg headquarters in the context of which the processing of personal data is being carried out.[36] If the referring court found that to be the case, the processing of personal data by *Amazon EU* would be governed by the law of the Member State to which it directs its activities.[37] The CJEU left it to the referring court, however, to determine whether there is indeed an establishment on the territory of a Member State other than Luxembourg in the context of which the processing of personal data is taking place.[38]

---

[31] *Weltimmo* (n 18) para 25.

[32] *Weltimmo* (n 18) para 41. To establish whether the activities of the controller were in fact 'mainly or entirely' directed at Hungary, the referring court was invited to consider whether the advertisements on the property dealing website concerned properties situated in Hungary and whether they were written in the Hungarian language.

[33] *Weltimmo* (n 18) para 41.

[34] *Weltimmo* (n 18) para 41.

[35] *Verein für Konsumenteninformation* (n 22) para 72.

[36] *Verein für Konsumenteninformation* (n 22) para 80.

[37] *Verein für Konsumenteninformation* (n 22) para 81.

[38] *Verein für Konsumenteninformation* (n 22) paras 81 and 79.

2.1.3. Evaluation

The case law of the CJEU concerning Directive 95/46 clearly favors a broad interpretation of the notions of 'establishment' and 'in the context of the activities'. With the adoption of article 3(1) GDPR, the EU legislator has chosen to confirm the CJEU's broad interpretation of these concepts.[39] While fa stable presence of at least some human and technical resources appears necessary in order to qualify as an 'establishment', the permanent presence of a single agent equipped with little more than a laptop may be enough, at least in some circumstances.[40] The notion of 'in the context of activities' has similarly received a broad interpretation. It is not required that the personal data are processed 'by' the establishment in question or that the controller itself resides on EU territory. There must, however, exist a clear link between the processing at issue and the activities of the establishment. The link can be direct (eg a customer support activity) or indirect (eg monetization activities which enable and cause the processing to be performed).[41] It is interesting to note, however, that the CJEU has repeatedly referred to the *orientation of activities* when determining applicable law. In each of the aforementioned cases, the CJEU considered whether the establishment in question 'orientates' or 'directs' its activities to the Member State in question. Such orientation seemingly takes precedence over 'degree of involvement': while it has been

[39] See also Paul de Hert and Michal Czerniawski, 'Expanding the European data protection scope beyond territory: Article 3 of the General Data Protection Regulation in its wider context' (2016) 6 IDPL 230, 237; Mistale Taylor, 'Permissions and prohibitions in data protection jurisprudence' (2016) 2 Brussels Privacy Hub Working Paper 3,13 and Merlin Gömann, 'The new territorial scope of EU data protection law: deconstructing a revolutionary achievement' (2017) 54 CM L Rev 567, 575.

[40] The Opinion of Advocate General Cruz Villalón on *Weltimmo* (n 18) para 34.

[41] The statement that the link may be indirect does not imply that the link may be attenuated. Indeed, while the link between the processing activity and the activities of the establishment may be considered as 'indirect', the CJEU took care in *Google Spain* to emphasize that the activities of the establishment and the processing at issue were 'inextricably' linked. See also Article 29 Data Protection Working Party, 'Update of Opinion 8/2010 on applicable law in light of the CJEU judgement in *Google Spain'* WP 179 (16 December 2015). Gömann, on the other hand, considers that the *Google Spain* ruling has effectively interpreted article 4(1)a so extensively that it is enough if there is "*a somewhat tangible physical establishment on EU territory whose supporting activity shows at least a tiny (online) link to the actual processing activity of the third country processor*") (Merlin Gömann, 'The new territorial scope of EU data protection law: deconstructing a revolutionary achievement' (2017) 54 CM L Rev 567, 574). See also Maja Brkan, *Data Protection and European Private International Law* (EUI Working Papers, RSCAS 2015/40, 2015) 33.

suggested that the territorial scope of Directive 95/46 should be determined by looking at which establishment has a 'closer connection' to the processing,[42] the CJEU has so far only had regard to (a) the relationship between the processing at issue and the activities of the establishment and (b) whether the establishments directs those activities to the territory of an EU Member State.[43]

2.2. **Article 3(2) GDPR**

Article 3(2) explicitly addresses the territorial scope of the GDPR in case of processing of personal data by a controller or processor not established in the Union. It provides that the GDPR shall be applicable to

> the processing of personal data *of data subjects who are in the Union* by a controller or processor not established in the Union, where the processing activities are related to:
>
> (a) the *offering of goods or services*, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or
>
> (b) the *monitoring of their behaviour* as far as their behaviour takes place within the Union.

2.2.1. 'Data subjects in the Union'

While article 3(2) only applies in case the controller or processor is not established in the Union, the processing of personal data must concern data subjects located in the Union. De Hert and Czerniawski offer the example of a European tourist shopping on Fifth Avenue in New York as a situation where article 3(2) GDPR clearly would not apply.[44] The requirement that the data subject be located in the Union must be assessed at the moment when the relevant trigger activity takes place, ie at the moment of offering of goods or

---

[42] Opinion of Advocate General Saugmandsgaard Øe on *Verein* (n 22) para 127.

[43] See also Opinion of Advocate General Bot, Case C-2010/16, 24 October 2017, para 100 (considering that every establishment may be relevant, regardless of whether there is a European 'head office', which within the group's internal division of tasks is considered "exclusively responsible" for collecting and processing personal data throughout the entire territory of the European Union). The judgment of the CJEU in this procedure is still pending.

[44] Paul de Hert and Michal Czerniawski, 'Expanding the European data protection scope beyond territory: Article 3 of the General Data Protection Regulation in its wider context' (2016) 6 IDPL 230, 238.

services or the moment when the behavior which is being monitored. Processing activities which are 'related' to the activity which triggered application of article 3(2) also falls within the territorial scope of the GDPR.

2.2.2. 'Offering of goods or services'

The first activity triggering the application of article 3(2) is the 'offering of goods or services'. Recital (23) clarifies that article 3(2)(a) requires conduct on the part of the controller or processor which demonstrates its *intention* to offer goods or services to data subjects located in the Union:

> In order to determine whether such a controller or processor is offering goods or services to data subjects who are in the Union, it should be ascertained whether it is *apparent* that the controller or processor *envisages* offering services to data subjects in one or more Member States in the Union [emphasis added].

As a result, mere accessibility of a website is considered insufficient to ascertain such an intention.[45] Conversely, use of a currency or language generally used in one or more EU Member States, in particular where that language is not generally used in the third country where the controller or processor is established, or the mentioning of customers or users who are in the Union, may make it apparent that the controller envisages offering goods or services to data subjects in the Union.[46]

The criteria identified in recital (23) echo the CJEU's reasoning in the joined *Pammer* and *Hotel Alpenhof* cases.[47] Here, the CJEU was called upon to clarify what it means to 'direct activity' within the meaning of article 15(1) of the Rome I Regulation.[48] While the notions of 'directing activity' and 'offering of goods and services' are not identical[49], the CJEU's case law on this point is likely to be influential in shaping the further interpretation of article

---

[45] Recital 23.

[46] ibid (n 45).

[47] Joined cases C-585/08 and C-144/09 *Peter Pammer v Reederei Karl Schlüter GmbH & Co KG and Hotel Alpenhof GesmbH v Oliver Heller* EU:C:2010:740 [2010] ECR I-2527, paras 84 and 94.

[48] Regulation No 593/2008 on the law applicable to contractual obligations (Rome I), [2008] OJ L-177/6-16.

[49] Mistale Taylor, 'Permissions and prohibitions in data protection jurisprudence' (2016) 2 Brussels Privacy Hub Working Paper 3, 17.

3(2)(a).[50] In the *Pammer* and *Hotel Alpenhof* ruling, the CJEU also identified other factors as being relevant, such as: the payment of money to a search engine to facilitate access by consumers domiciled in various Member States; the mention of telephone numbers with the international code; the top-level domain name used; and the description of itineraries from one or more other Member States to the place where the service is provided.[51]

2.2.3. 'Monitoring of behavior'

The second activity triggering the application of article 3(2) is 'monitoring of behaviour'. Recital (24) indicates that article 3(2)(b) is first and foremost concerned with online tracking and profiling activities:

> In order to determine whether a processing activity can be considered to monitor the behaviour of data subjects, it should be ascertained whether natural persons are *tracked on the internet* including potential subsequent use of personal data processing techniques which consist of *profiling* a natural person, particularly in order to take decisions concerning her or him or for analysing or predicting her or his personal preferences, behaviours and attitudes.

Article 3(2)(b) GDPR is the successor of article 4(1)(c) of Directive 95/46, that provides that Member States must apply their national data protection laws if the controller who is not established in the EU 'makes use of equipment' situated on its territory. While the term 'equipment' in first instance refers to physical objects,[52] the Article 29 Working Party has given the term

---

[50] See also Merlin Gömann, 'The new territorial scope of EU data protection law: deconstructing a revolutionary achievement' (2017) 54 CM L Rev 567, 585.

[51] *Pammer* (n 47) paras 81 and 83. See also Omer Tene and Christopher Wolf, *Overextended: Jurisdiction and Applicable Law under the EU General Data Protection Regulation* (White Paper, The Future of Privacy Forum, 2013) 1,7 and Ruth Boardman, James Mullock and Ariane Mole, *Bird & Bird guide to the General Data Protection Regulation* (april 2016) 2.

[52] Michal Czerniawski, 'Do We Need the 'Use of Equipment' as a factor for the territorial applicability of the EU Data Protection Regime?' in Dan Jerker B. Svantesson and Dariusz Kloza (eds), *Trans-atlantic data privacy as a challenge for democracy* (Intersentia 2017) 221, 227. The legislative history of Directive 95/46 suggests that its drafters only had physical objects in mind when using the word 'equipment'. See also Lokke Moerel, 'The long arm of EU data protection law: Does the Data Protection Directive apply to processing of personal data of EU citizens by websites worldwide?' (2011) 1 IDPL 28, 33 and 36.

a broad interpretation, which comprises both human and technical resources.[53] More specifically, the Working Party understands the term 'equipment' to have the same meaning as the term 'means' used in article 2(d) of the Directive (ie the definition of controller).[54] On the basis of this broad interpretation, the Working Party has considered that the use of JavaScript banners or cookies might also be considered as 'means' within the meaning of article 4(1)(c).[55] As a result, the use of cookies by non-EU controllers to track data subjects located in the EU is considered to fall within the territorial scope of Directive 95/46. While this interpretation has been the subject of considerable criticism, the EU legislator has apparently chosen to embrace it by providing it with a more explicit legal footing.

Interestingly, neither article 3(2)b nor recital (24) make any reference to the intention of the controller or processor to monitor the behavior of data subjects in the Union. As a result, it would appear that cookie-based tracking of EU data subjects would trigger the territorial scope of the GDPR, regardless of whether the cookie was placed via a website actively targeting EU residents. The only requirement stipulated by article 3(2)(b) is that the monitoring of behavior concerns behavior which takes place in the Union.[56]

Finally, it should be noted that even though recital (24) only refers to 'tracking on the internet', the wording of article 3(2)(b) is sufficiently broad to cover other techniques of behavioral monitoring (eg through wearables or other smart devices).[57]

---

[53] Article 29 Data Protection Working Party, 'Opinion 8/2010 on applicable law' WP 179 (16 December 2010).

[54] ibid (n 53).

[55] ibid 21-22.

[56] See also Anni-Maria Taka, 'Cross-Border Application of EU's General Data Protection Regulation (GDPR) – A private international law study on third state implications' (Master's Thesis in Private International Law and EU Law, Uppsala Universitet 2017) 83 <http://www.diva-portal.org/smash/get/diva2:1127596/FULLTEXT01.pdf> and Paul Voigt and Axel von dem Bussche, *The EU General Data Protection Regulation (GDPR) - A Practical Guide* (Springer 2017) 28.

[57] Taka (n 56) 78; Merlin Gömann, 'The new territorial scope of EU data protection law: deconstructing a revolutionary achievement' (2017) 54 CM L Rev 567, 588 and Liane Colonna, 'Article 4 of the EU Data Protection Directive and the irrelevance of the EU–US Safe Harbor Program?' (2014) 4 IDPL 203, 215.

2.2.4. Evaluation

Article 3(2)(a) extends the territorial scope of the GDPR to non-EU controllers and processors which 'target' EU data subjects.[58] The targeting approach subjects the application of EU law to entities located outside its territory to the requirement that those entities reveal the intention to reach ('actively target') individuals located within their territory.[59]

While asserting jurisdiction solely on the basis of targeting is arguably new to EU data protection law[60], the target and direction of offering goods and services has been an important factor in the case law of the CJEU analyzing the territorial scope of EU data protection law.[61] In doing so, article 3(2)(a) incorporates a trigger familiar to other areas of EU legislation, namely the trigger of 'market access' or 'conduct that consists of a step in the direction of gaining access to the EU market'.[62]

Interestingly, article 3(2)(b) does not, at least on the face of it, involve a market access trigger. While the monitoring of behavior may by itself be viewed as involving a form of 'targeting', it does not necessarily involve 'purposeful' targeting of data subjects who are in the Union. For example, websites often place (or enable the placement of) cookies without discriminating on the basis of the geographic origin of the website visitor, ie regardless of whether the

---

[58] Dan Jerker B. Svantesson, 'Extraterritoriality and targeting in EU data privacy law: the weak spot undermining the regulation' (2015) 5 IDPL 226; Paul de Hert and Michal Czerniawski, 'Expanding the European data protection scope beyond territory: Article 3 of the General Data Protection Regulation in its wider context' (2016) 6 IDPL 238; Mistale Taylor, 'Permissions and prohibitions in data protection jurisprudence' (2016) 2 Brussels Privacy Hub Working Paper 3,17 and Michal Czerniawski, 'Do We Need the 'Use of Equipment' as a factor for the territorial applicability of the EU Data Protection Regime?' in Dan Jerker B. Svantesson and Dariusz Kloza (eds), *Trans-atlantic data privacy as a challenge for democracy* (Intersentia 2017) 221, 235.

[59] Thomas Schultz, 'Carving Up the Internet: Jurisdiction, Legal Orders, and the Private/Public International Law Interface' (2008) 19 EJIL 799, 817.

[60] De Hert and Czerniawski (n 58) 238.

[61] Cf *supra*; section II.1.c. See also Els J. Kindt, 'Why research may no longer be the same: About the territorial scope of the New Data Protection Regulation' (2016) 32 CLS Rev 729, 735.

[62] See Joanne Scott, 'The New EU 'Extraterritoriality'' (2014) 51 CM L Rev 1343, 1348 and Michal Czerniawski, 'Do We Need the 'Use of Equipment' as a factor for the territorial applicability of the EU Data Protection Regime?' in Dan Jerker B. Svantesson and Dariusz Kloza (eds), *Trans-atlantic data privacy as a challenge for democracy* (Intersentia 2017) 221, 230.

visitor's query originates from the EU or not. Such cookies may be used to track individuals' online activities across websites, often with a view to enable online behavioral advertising. If that is the case, are those processing activities covered by article 3(2)(b)? This question will be revisited later on.

In any event, commentators are still divided as to whether the GDPR's increased emphasis on targeting is a good or bad thing. Svantesson considers that targeting has great theoretical appeal, but is often difficult to apply in practice.[63] Both Taylor and Czerniawski consider the overt emphasis on targeting a step forward in comparison to article 4(1)(c) of Directive 95/46, providing a stronger connection to trigger jurisdiction.[64] Kindt, on the other hand, considers the targeting approach as too restrictive and warns that significant gaps in protection may arise in the future.[65]

3. ASSESSMENT UNDER PUBLIC INTERNATIONAL LAW

Under public international law, there must be a 'sufficient connection' before a state can assert either prescriptive or adjudicative jurisdiction.[66] There are approximately five general principles upon which a jurisdictional claim might be based, namely (1) the territoriality principle (objective and subjective); (2) the nationality principle (active or passive); (3) the effects principle; (4) the protective principle; or (5) the universality principle.[67] For purposes of public international law, it is the territoriality principle which is the primary - but not the sole - basis of jurisdiction.[68] The principle of territoriality entails

---

[63] Dan Jerker B. Svantesson, 'Extraterritoriality and targeting in EU data privacy law: the weak spot undermining the regulation' (2015) 5 IDPL 226.

[64] Mistale Taylor, 'Permissions and prohibitions in data protection jurisprudence' (2016) 2 Brussels Privacy Hub Working Paper 3, 18 and Michal Czerniawski, 'Do We Need the 'Use of Equipment' as a factor for the territorial applicability of the EU Data Protection Regime?' in Dan Jerker B. Svantesson and Dariusz Kloza (eds), *Trans-atlantic data privacy as a challenge for democracy* (Intersentia 2017) 221, 232.

[65] Els J. Kindt, 'Why research may no longer be the same: About the territorial scope of the New Data Protection Regulation' (2016) 32 CM L Rev 729, 738-739.

[66] Christopher Kuner, 'Data Protection Law and International Jurisdiction on the Internet (Part 1)' (2010) 18 IJLT 176.

[67] See Dan Jerker B. Svantesson 'The Extraterritoriality of EU Data Privacy Law – Its Theoretical Justification and Its Practical Effect on U.S. Businesses' (2014) 50 Stan J intl L 80; Bernhard Maier, 'How Has the Law Attempted to Tackle the Borderless Nature of the Internet' (2010) 18 IJLIT 142, 143.

[68] Uta Kohl, *Jurisdiction and the Internet – Regulatory Competence of Online Activity* (Cambridge University Press 2007) 20; Cedric Ryngaert, *Jurisdiction in International*

that each state has the right to regulate persons, matters and events within its own territory.[69] It is based on the principle of sovereign equality of States and the principle of non-intervention.[70] A corollary of the territoriality principle is that states should exercise some restraint before asserting jurisdiction extra-territorially: if a state wishes to be recognized as sovereign within its own borders, it must respect the sovereignty of other states within their borders.[71] Nevertheless, states increasingly undertake to regulate conduct taking place abroad, using a variety of justifications for doing so.[72] The EU is no exception in this regard.[73] The aim of this section is to scrutinize the extraterritorial reach of the GDPR from the perspective of public international law.

3.1. Establishment: A physical or virtual connection with EU territory?

Article 3(1) of the GDPR advances the 'establishment' of a controller or processor on EU territory as a trigger for the application of EU data protection law. 'Establishment' is normally a strong connecting factor. In theory, all this concept does is provide for a straightforward application of the territoriality principle.[74] If you are established and operate within a state's territory, you

Law (Oxford University Press 2008) 27 et seq. See also Section 402 of the *Third Restatement of the Law of the Foreign Relations Law of the United States*.

[69] Kohl (n 68) 89.

[70] Ryngaert (n 68) 29.

[71] Brendan Van Alsenoy and Marieke Koekkoek, 'Internet and jurisdiction after Google Spain: the extraterritorial reach of the 'right to be delisted''(2015) 5 IDPL105, 108. Other arguments advocating against extra-territorial assertions of jurisdiction include unforeseeability, limited enforceability, liability under multiple jurisdiction, etc. See eg Bernhard Maier, 'How Has the Law Attempted to Tackle the Borderless Nature of the Internet' (2010) 18 IJLIT 142, 161-162.

[72] Dan Jerker B. Svantesson 'The Extraterritoriality of EU Data Privacy Law – Its Theoretical Justification and Its Practical Effect on U.S. Businesses' (2014) 50 Stan J intl L 61; Uta Kohl, *Jurisdiction and the Internet – Regulatory Competence of Online Activity* 89-108; Joanne Scott, 'The New EU 'Extraterritoriality'' (2014) 51 CM L Rev 1343, 1344; Robert Dover and Justin Frosini, *The extraterritorial effects of legislation and policies in the EU and US* (Study for the European Parliament's Committee on Foreign Affairs 2012) 48.

[73] See in particular Joanne Scott, 'The New EU 'Extraterritoriality'' (2014) 51 CM L Rev 1343, 1344.

[74] Bernhard Maier, 'How Has the Law Attempted to Tackle the Borderless Nature of the Internet?' (2010) 18 IJLIT 142, 174.

have to play by its rules. This makes sense. However, things may get trickier when the territorial nexus of establishment is used as a means to regulate conduct abroad. Moerel has already pointed out that in the case of article 4(1)(a) of Directive 95/46, the principle of territoriality has a 'more or less virtual nature'.[75]

> The formal place of establishment of the controller is not relevant […] The controller of the data itself may be established outside of the EU. […] [T]he territoriality principle is in fact adhered to by Article 4(1)(a) as *the data processing is virtually connected to the territory of the EU* (ie takes place in the context of the activities of the establishment in the Member State).[76]

So the use of 'establishment' to link the processing with EU territory may not be entirely straightforward. There are, however, additional justifications that might solidify the EU's assertion of jurisdiction vis-à-vis non-EU entities. The effects principle, which is an extension of the territoriality principle, stipulates that states may regulate behavior which takes place outside its territory insofar as it produces substantial effects within its territory.[77] This principle is frequently applied in competition matters, whereby states use it to assert jurisdiction over foreign practices which restrict competition in national markets.[78] Even though the effects principle has been developed in the context of antitrust law,[79] its logic can be extended to other areas of law, including data

---

[75] Lokke Moerel, 'The long arm of EU data protection law: Does the Data Protection Directive apply to processing of personal data of EU citizens by websites worldwide?' (2011) 1 IDPL 28, 29.

[76] Moerel (n 75) 29-30 (emphasis added). See also Paul De Hert and Michal Czerniawski, 'Expanding the European data protection scope beyond territory: Article 3 of the General Data Protection Regulation in its wider context' (2016) 6 IDPL 234.

[77] Section 402 of the Third Restatement of the Law of the Foreign Relations Law of the United States. See also Dan Jerker B. Svantesson 'The Extraterritoriality of EU Data Privacy Law – Its Theoretical Justification and Its Practical Effect on U.S. Businesses' (2014) 50 Stan J intl L 82; Cedric Ryngaert, *Jurisdiction in International Law, United States and European perspectives* (PhD Thesis, Leuven 2007) 198. See also Max Huffman, 'A Retrospective of Twenty-Five Years on the Foreign Trade Antitrust Improvements Act' (2007) 44 Hous LR 285.

[78] Dan Jerker B. Svantesson 'The Extraterritoriality of EU Data Privacy Law – Its Theoretical Justification and Its Practical Effect on U.S. Businesses' (2014) 50 Stan J intl L 82.

[79] See also Deepa Rishikesh, 'Extraterritoriality Versus Sovereignty in International Antitrust Jurisdiction' (1990) 14 World Competition 33, 49; Cf A Retrospective of Twenty-Five Years (43).

protection law.[80] Similar to antitrust law, data protection cannot be fully effective when applied strictly territorially.[81] Moreover, international human rights law offers direct support for the proposition that states should consider the effects of foreign conduct on their citizens' privacy.[82]

In its *Google Spain* ruling, the CJEU made repeated references to the need to ensure 'effective and complete' protection of individuals. It also noted, at several occasions, that the processing of personal data by search engines may bring about a serious interference with the rights which Directive 95/46 was designed to protect.[83] This language suggests that the CJEU's conclusion was motivated in no small part by the recognition that Google's search engine activities may have a real impact (ie 'substantial effect') on data subjects in the EU. In the words of the CJEU:

> […] it cannot be accepted that the processing of personal data carried out for the purposes of the operation of the search engine should escape the obligations and guarantees laid down by Directive 95/46, which would compromise the directive's effectiveness and the effective and complete protection of the fundamental rights and freedoms of natural persons which the directive seeks to ensure […].[84]

The effects principle is considered a controversial basis of jurisdiction, particularly in relation to internet content regulation.[85] Due to the global nature of the internet, any state might claim to be affected by online content or activity originating from anywhere in the world.[86] The jurisdictional principle of *reasonableness* requires states to balance the need for effectiveness against

---

[80] Brendan Van Alsenoy and Marieke Koekkoek, 'Internet and jurisdiction after Google Spain: the extraterritorial reach of the 'right to be delisted''(2015) 5 IDPL 105, 109.

[81] See more generally John H. Currie, *Public International Law* (Irwin Law 2001) 300.

[82] See Dan Jerker B. Svantesson 'The Extraterritoriality of EU Data Privacy Law – Its Theoretical Justification and Its Practical Effect on U.S. Businesses' (2014) 50 Stan J intl L 78 and Mistale Taylor, 'The EU's human rights obligations in relation to its data protection laws with extraterritorial effect' (2015) 5 IDPL 246.

[83] *Google Spain* (n 24) paras 80-81.

[84] *Google Spain* (n 24) para 58.

[85] See generally Daniel Castro and Robert Atkinson, 'Beyond Internet Universalism: A Framework for Addressing Cross-border Internet Policy' (2014) The Internet Technology & Innovation Foundation 1, 7.

[86] See also Jonathan Zittrain, 'Be Careful What You Ask For: Reconciling a Global Internet and Local Law' Harvard Law School Public Law Research Paper No. 03/2003.

the principle of non-intervention.[87] The CJEU's interpretation of article 4(1)(a) is quite 'reasonable' if one considers the alternative. If the CJEU had ruled otherwise, this would, in the long run, create an unfair competitive advantage for non-EU based companies (who only have subsidiaries in the EU) over EU companies (who are fully established in the EU). The advantage would be particularly significant in markets where personal data processing is an important aspect. In other words: holding article 4(1)(a) inapplicable would be the equivalent of extending 'special guest status' to foreign data controllers who offer their (data-intensive) services on the EU market.[88] The suggestion that the CJEU is mindful of the potential implications for the EU market is all the more compelling if one considers that the CJEU's holding explicitly refers to whether the establishment in question 'orientates' its activities to the Member State in question.

3.2. Is it 'targeting' or 'being targeted' that matters?

Earlier it was pointed out that article 3(2) GDPR employs 'targeting' as a trigger to render the GDPR applicable to controllers and processors not established in the EU. In such a scenario, the primary nexus with EU territory is not the presence of a controller or processor within the EU, but rather the location of the data subjects to which the relevant activities are targeted.[89] Article 3(2) GDPR identifies two such 'relevant activities': the offering of goods or services and the monitoring of behavior. In case of the former, it is clear that the GDPR will only apply if it is apparent that the controller or processor 'purposefully targeted' data subjects within the EU. In case of the latter, the situation is not so clear-cut.

---

[87] Brendan Van Alsenoy and Marieke Koekkoek, 'Internet and jurisdiction after Google Spain: the extraterritorial reach of the 'right to be delisted''(2015) 5 IDPL 105, 116. See Restatement (Third) of the Law of the Foreign Relations. The principle of reasonableness is closely linked (but not identical to) the principle of 'comity'. For more information see Jurisdiction in International Law (n 43) 42 et seq. See also Christopher Kuner, 'Data Protection Law and International Jurisdiction on the Internet (Part 2)', (2010) 18 IJLT 244.

[88] Brendan Van Alsenoy and Marieke Koekkoek, 'Internet and jurisdiction after Google Spain: the extraterritorial reach of the 'right to be delisted''(2015) 5 IDPL 105, 110.

[89] Clearly Gottlieb, *The General Data Protection Regulation: Key Changes and Implications* (Alert Memorandum 2016) 3 <https://www.clearymawatch.com/wp-content/uploads/sites/106/2016/10/Alert-memo-PDF-Version-2016-50.pdf>.

Asserting jurisdiction in case of purposeful targeting is often viewed as legitimate.[90] While the precise meaning of what constitutes 'targeting' (and what does not) may vary[91], the purposeful targeting arguably does enhance the legitimacy of a state's decision to regulate.[92] If a foreign entity deliberately targets its activity towards residents of another country, it may reasonably foresee that the government of that country might impose certain rules. Moreover, the use of targeting criteria can help to minimize the potential impact on other states' interests in so far as the assertion of prescriptive jurisdiction is limited to activity which are targeted to its own inhabitants.[93]

While the requirement of 'purposeful targeting' is absent from article 3(2)(b) GDPR, one could argue that such a requirement should be 'read into' this provision. First, it has been suggested that some degree of intentionality is in fact implicit in the concept of 'monitoring' itself.[94] Second, the legislative history of article 3(2) GDPR suggests that the EU legislature precisely sought to soften the potential for global applicability of the GDPR.[95] On the other hand, one could argue if the EU legislature had wanted to subject the monitoring trigger of article 3(2)(b) GDPR to the requirement of 'purposeful targeting', it would have done so. Moreover, if article 3(2)(b) GDPR were to require "purposeful" targeting of people in the EU, its practical importance would be significantly

---

[90] See eg Omer Tene and Christopher Wolf, *Overextended: Jurisdiction and Applicable Law under the EU General Data Protection Regulation* (White Paper, The Future of Privacy Forum, 2013) 1, 6-8.

[91] Thomas Schultz, 'Carving Up the Internet: Jurisdiction, Legal Orders, and the Private/Public International Law Interface' (2008) 19 EJIL 799, 816.

[92] Also Paul De Hert and Michal Czerniawski, 'Expanding the European data protection scope beyond territory: Article 3 of the General Data Protection Regulation in its wider context' (2016) 6 IDPL 238-239.

[93] This is not to say that States may never undertake to regulate behavior which is not specifically targeted at their jurisdiction or its inhabitants, it merely serves underscore that the potential with other States interests will be considerably smaller the scope of the jurisdictional assertion is limited to activities targeted at the State's own territory.

[94] See also Anni-Maria Taka, 'Cross-Border Application of EU's General Data Protection Regulation (GDPR) – A private international law study on third state implications', citing R. Jay, Guide to the General Data Protection Regulation: A Companion to Data Protection Law and Practice, 75-76.

[95] See Dan Jerker B. Svantesson 'The Extraterritoriality of EU Data Privacy Law – Its Theoretical Justification and Its Practical Effect on U.S. Businesses' (2014) 50 Stan J intl L 107-110.

reduced: such processing activities would often be covered by article 3(2)(a) GDPR.

The two opposing viewpoints are likely to lead to the same conclusion in relation to companies who specialize in online tracking. These companies amass vast amounts of data on people located within the EU, which is often specifically intended to facilitate personalized (ie 'targeted') advertising of people located in the EU. As such, there is a clear intention to 'target' people located in the EU. But what about the individual websites who enable third parties to track cookies? According to the Article 29 Working Party, website operators ('publishers') bear some responsibility when enabling of targeted advertising.[96] However, these website operators do not necessarily themselves monitor the behavior of data subjects across websites. While they do perform processing activities 'related' to the monitoring of data subjects in the Union (by enabling third parties to track visits to their website), some might argue that the connection with EU territory becomes too attenuated.

Perhaps a balanced outcome might be reached applying a systematic reading of article 3(2) GDPR and its corresponding recitals. Recital (24) explicitly refers to internet tracking and profiling techniques, suggesting either that an element of intentional or active tracking is required,[97] or that the monitoring must reach a certain level of intrusiveness. The benefit of such an approach would be that it still enables some form of case-by-case assessment. Moreover, such an approach would be more readily justifiable under the effects principle, which stipulates that a State may regulate behavior what takes place outside its territory insofar as it produces 'substantial effects' within its territory.

[96] Article 29 Data Protection Working Party, 'Opinion 2/2010 on online behavioural advertising' WP 171 (22 June 2010). The distribution of responsibility between publishers and ad network providers may be clarified in the context of CJEU Request for a preliminary ruling from the Oberlandesgericht Düsseldorf (Germany) lodged on 26 January 2017 - Case C-40/17 *Fashion ID GmbH & Co.KG v Verbraucherzentrale NRW eV* [2017] action brought on January 26, 2017.

[97] Rob Sumroy and others, 'New rules, wider reach: the extra-territorial scope of the GDPR' (*Slaughter and May*, June 2016) <https://www.slaughterandmay.com/media/2535540/new-rules-wider-reach-the-extraterritorial-scope-of-the-gdpr.pdf>.

4. CONCLUSION

When reviewing the extraterritorial reach of the GDPR, it is clear that article 3 reflects a combination of jurisdictional principles.[98] Where its applicability is triggered by virtue of an establishment of the controller or processor, the extraterritorial reach can be justified by a combination of the territoriality principle and the effects principle. As the case law of the CJEU indicates that the 'orientation' of activities is significant, the need to ensure a level playing field within the EU market helps to argue that the EU's exercise of prescriptive jurisdiction is in fact reasonable.

The targeting approach of article 3(2) GPDR can also be justified by reference to the objective territoriality and/or effects principle.[99] As far as the offering of goods or services is concerned, the additional criteria set forth by the GDPR help to protect against jurisdictional overreach. Where the monitoring of data subjects in the EU is concerned, however, no specific safety valves are provided for. In my opinion, applicability of the GDPR can be readily justified once the monitoring activity reaches a certain level of intrusiveness. In the absence of further clarification, however, considerable uncertainty remains as to when exactly article 3(2)(b) will be triggered. It is therefore desirable that that this matter be clarified either in future regulatory guidance or by the EU legislature as part of its review of the ePrivacy Directive. The pending reference before the CJEU regarding the geographical scope of delisting may also provide further insight.[100] In any event, it will be interesting to see to what extent principles of public international law will effectively be taken into account when determining the extra-territorial scope of EU data protection law.

---

[98] See also Liane Colonna, 'Article 4 of the EU Data Protection Directive and the irrelevance of the EU–US Safe Harbor Program?' (2014) 4 IDPL 203, 213-215.

[99] See also Mistale Taylor, 'Permissions and prohibitions in data protection jurisprudence' (2016) 2 Brussels Privacy Hub Working Paper 3, 18-24, who additionally cites the personality principle as a principle of jurisdiction underlying the GDPR's approach.

[100] Request for a preliminary ruling from the Conseil d'État (France) lodged on 21 August 2017, Case C-507/17 *Google Inc. v Commission nationale de l'informatique et des libertés (CNIL)*.

5. SELECTED LITERATURE

Article 29 Data Protection Working Party, 'Opinion 2/2010 on online behavioural advertising' WP 171 (22 June 2010)

Article 29 Data Protection Working Party, 'Opinion 8/2010 on applicable law' WP 179 (16 December 2010)

Article 29 Data Protection Working Party, 'Update of Opinion 8/2010 on applicable law in light of the CJEU judgement in Google Spain' WP 179 (16 December 2015)

Boardman R, Mullock J and Mole A, *Bird & Bird guide to the General Data Protection Regulation*, (april 2016)

Brkan M, *Data Protection and European Private International Law* (EUI Working Papers, RSCAS 2015/40, 2015) 33

Castro D and Atkinson R, 'Beyond Internet Universalism: A Framework for Addressing Cross-border Internet Policy' (2014) The Internet Technology & Innovation Foundation 1

Colonna L, 'Article 4 of the EU Data Protection Directive and the irrelevance of the EU–US Safe Harbor Program?' (2014) 4 IDPL 203

Currie JH, *Public International Law* (Irwin Law 2001)

Czerniawski M, 'Do We Need the 'Use of Equipment' as a factor for the territorial applicability of the EU Data Protection Regime?' in Dan Jerker B. Svantesson and Dariusz Kloza (eds), *Trans-atlantic data privacy as a challenge for democracy* (Intersentia 2017) 221, 227.

De Hert P and Czerniawski M, 'Expanding the European data protection scope beyond territory: Article 3 of the General Data Protection Regulation in its wider context' (2016) 6 IDPL 230

Dover R and Frosini J, *The extraterritorial effects of legislation and policies in the EU and US* (Study for the European Parliament's Committee on Foreign Affairs 2012)

Gömann M, 'The new territorial scope of EU data protection law: deconstructing a revolutionary achievement' (2017) 54 CML Rev 567

Gottlieb C, *The General Data Protection Regulation: Key Changes and Implications* (Alert Memorandum 2016) 3 <https://www.clearymawatch.com/wp-content/uploads/sites/106/2016/10/Alert-memo-PDF-Version-2016-50.pdf>

Huffman M, 'A Retrospective of Twenty-Five Years on the Foreign Trade Antitrust Improvements Act' (2007) 44 Hous LR 285.

Kindt EJ, 'Why research may no longer be the same: About the territorial scope of the New Data Protection Regulation' (2016) 32 CLS Rev 729

Kohl U, *Jurisdiction and the Internet – Regulatory Competence of Online Activity* (Cambridge University Press 2007)

Kuner C, 'Data Protection Law and International Jurisdiction on the Internet (Part 1)' (2010) 18 IJLT 176

Kuner C, 'Data Protection Law and International Jurisdiction on the Internet (Part 2)' (2010) 18 IJLT 244

Kuner C, 'Extraterritoriality and regulation of international data transfers in EU data protection law' (2015) 5 IDPL 235

Maier B, 'How Has the Law Attempted to Tackle the Borderless Nature of the Internet' (2010) 18 IJLIT 142

Moerel L, 'The long arm of EU data protection law: Does the Data Protection Directive apply to processing of personal data of EU citizens by websites worldwide?' (2011) 1 IDPL 28

Moerel L, 'The data transfer regime for processors does not make sense and requires clarification' (*GDPR Conundrums: Data Transfer*, 9 June 2016) <https://iapp.org/news/a/gdpr-conundrums-data-transfer>

Rishikesh D, 'Extraterritoriality Versus Sovereignty in International Antitrust Jurisdiction' (1990) 14 World Competition 33

Ryngaert C, *Jurisdiction in International Law* (Oxford University Press 2008)

Ryngaert C, *Jurisdiction in International Law, United States and European perspectives* (PhD Thesis, Leuven 2007)

Schultz T, 'Carving Up the Internet: Jurisdiction, Legal Orders, and the Private /Public International Law Interface' (2008) 19 EJIL 799

Scott J, 'The New EU 'Extraterritoriality'' (2014) 51 CML Rev 1343

Scott J, 'Extraterritoriality and Territorial Extension in EU Law' (2014) 62 Am J Comp L 87

Sumroy R, 'New rules, wider reach: the extra-territorial scope of the GDPR' (*Slaughter and May*, June 2016) <https://www.slaughterandmay.com/media/2535540/new-rules-wider-reach-the-extraterritorial-scope-of-the-gdpr.pdf>

Svantesson DJB, *Extraterritoriality in Data Privacy Law* (Ex Tuto Publishing 2013)

Svantesson DJB, 'The Extraterritoriality of EU Data Privacy Law – Its Theoretical Justification and Its Practical Effect on U.S. Businesses' (2014) 50 Stan J intl L 60

Svantesson DJB, 'Extraterritoriality and targeting in EU data privacy law: the weak spot undermining the regulation' (2015) 5 IDPL 226

Taka A-M, 'Cross-Border Application of EU's General Data Protection Regulation (GDPR) – A private international law study on third state implications' (Master's Thesis in Private International Law and EU Law, Uppsala Universitet 2017)

Taylor M, 'Permissions and prohibitions in data protection jurisprudence' (2016) 2 Brussels Privacy Hub Working Paper 3

Tene O and Wolf C, *Overextended: Jurisdiction and Applicable Law under the EU General Data Protection Regulation* (White Paper, The Future of Privacy Forum, 2013)

Van Alsenoy B and Koekkoek M, 'Internet and jurisdiction after Google Spain: the extraterritorial reach of the 'right to be delisted''(2015) 5 IDPL 105

Voigt P and von dem Bussche A, *The EU General Data Protection Regulation (GDPR) - A Practical Guide* (Springer 2017)

Zittrain J, 'Be Careful What You Ask For: Reconciling a Global Internet and Local Law', Harvard Law School Public Law Research Paper No. 03/2003

Back to Yahoo!?

Regulatory clashes in cyberspace in the light of EU data protection law

ALBERTO MIGLIO[1]

The implementation of the *Google Spain* judgment of the Court of Justice of the European Union raises issues largely similar to those prevailing in the debate on the regulation of Internet content in the late 1990s and 2000s. By looking at the most famous case from that period, this contribution discusses what lessons, if any, can be learnt from that debate. It argues that while geographic filtering, which the 2000 *Yahoo!* case endorsed as a technique for the regulation of online activities, represents a valid model for dealing with delisting of online search results, in this context any one-size-fits-all approach would have serious shortcomings. However, in turn, the quest for more flexible approaches raises concerns that regulators, courts and businesses will have to address.

1. INTRODUCTION

Controversial as it was, the judgment of the Court of Justice of the European Union in *Google Spain,*[2] which rather imprecisely dubbed 'the judgment on the right to be forgotten',[3] was widely and immediately perceived as a landmark case that would shape how we deal with the Internet.[4]

Requiring search engines to take down URLs containing personal data of which the processing does not (or no longer) comply with EU data protection law is undoubtedly of significant practical importance for individuals seeking

[1] Postdoc fellow, Law Department, University of Turin. Email: alberto.miglio@unito.it.

[2] Case C-131/12 *Google Spain SL and Google Inc v Agencia Española de Protección de Datos* (AEPD) *and Mario Costeja González* EU:C:2014:317.

[3] For criticism see Orla Lynskey, 'Control over Personal Data in a Digital Age: *Google Spain v AEPD and Mario Costeja Gonzalez*' (2015) 78 Modern Law Review 522, 528.

[4] See Eleni Frantziou, 'Further Developments in the Right to be Forgotten: The European Court of Justice's Judgment in Case C-131/12, *Google Spain SL, Google Inc v Agencia Espanola de Proteccion de Datos*' (2014) 14 Human Rights Law Review 761; Christopher Rees and Debbie Heywood, 'The 'right to be forgotten' or the 'principle that has been remembered'' (2014) 30 Computer Law and Security Review 574, 577.

to keep control over the spread of personal data across the web. This is demonstrated by the high number of requests for delisting addressed to Google, that in May 2017 reported having evaluated 720,000 applications in three years, removing around 43 percent of the more than 2 million links submitted. [5]

Perhaps even more important, the judgment's significance is demonstrated by the ongoing lively debate that it has generated on the protection of fundamental rights online and on the application of EU data protection law. Aside from the controversial character of some of the Court's findings – such as the qualification of search engines as data controllers [6] or the conclusion that Google Inc.'s data processing fell within the scope of the EU data protection law despite being carried out in a third country – and the widespread criticism it received especially from the US,[7] it is the questions the judgment left open that have continued to provide food for thought for academics, practitioners and citizens alike.

Indeed, considering it represented a first step in a new direction, the judgment has raised a number of questions that are complicating its implementation and are calling for further judicial clarification.[8] Some of those questions relate to the actual process of sorting information that has to be delisted. Who should decide and under which supervisory mechanisms? How should this process be conducted? When should information be considered inadequate, irrelevant or no longer relevant or excessive and therefore be removed? How should search engines balance the protection of privacy and freedom of expression?[9]

Arguably the most contentious issue that has surfaced in the implementation of delisting, however, is the geographic scope of the obligation to remove

---

[5] Peter Fleischer (Google's Global Privacy Counsel), 'Three years of striking the right (to be forgotten) balance' (*Google in Europe*, 15 May 2017) <https://www.blog.google/topics/google-europe/three-years-right-to-be-forgotten-balance/>.

[6] For a critical appraisal see Giovanni Sartor, 'Search Engines as Controllers. Inconvenient Implications of a Questionable Classification' (2014) 21 MJ 564.

[7] See, for instance, John W. Kropf, 'Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD). Case C-131/1' (2014) 108 AJIL 502.

[8] Indra Spiecker, 'A New Framework for Information Markets: *Google Spain*' (2015) 52 Common Market Law Review 1033, 1039.

[9] The Court of Justice will soon have to deal with some of these questions in the context of a reference from a preliminary ruling proposed in February 2017 by the French Council of State: Conseil d'Etat, order of 24 February 2017, Mme C, M. F, M. H, M. D., applications Nos 391000, 393769, 399999, 401258.

search results. This is a different question than the one relating to the personal scope of application of the Data Protection Directive. The Court of Justice made clear in *Google Spain* that the Directive applies to data controllers established in third countries as long as they have an establishment on EU territory for the promotion and sale of advertising space. Although this statement is certainly a source of tensions in transatlantic relations and is viewed – improperly perhaps – as a claim to extraterritorial jurisdiction, the key question relating to the geographic scope of the 'right to be forgotten' is another one, namely whether a search engine operator should delist results on a local or global scale.

Whereas its application to search engines for purposes of data protection may be a novelty triggered by the CJEU's finding that search engine operators are data controllers within the meaning of the Data Protection Directive, the underlying problem is a classic one and is well-know to anyone having even a limited familiarity with jurisdictional claims in cyberspace.[10] It is the question of determining the scope of application of local laws in the online environment and the ways of their enforcement.

Indeed, the rise of the Internet made the quest for jurisdictional criteria applicable to online activities a major problem of cyber law. While the borderless structure of the web made content published online ubiquitous and in principle accessible from anywhere in the world, States have attempted to regulate online activities by enforcing local laws, which often considerably diverge from one another. This phenomenon has generated jurisdictional conflicts and powerfully revived the academic debate on international law limits to jurisdiction.

Against this background, the contribution addresses the following question: What lessons, if any, can be learnt for EU data protection law from the scholarly debate and the case law that developed in the late 1990s and in the 2000s in the context of the regulation of web-based content? The contribution attempts to answer this question by exploring the similarities between the implementation of delisting under the EU Data Protection Directive and the *Yahoo!* Case,[11] which is by far the most famous example of litigation concerning the enforcement of local laws against global Internet service providers (ISPs).

---

[10] Orla Lynskey, 'Control over Personal Data in a Digital Age: *Google Spain v AEPD and Mario Costeja Gonzalez*' (2015) 78 Modern Law Review 522, 531.

[11] Tribunal de Grande Instance de Paris, order of 22 May 2000, *UEJF and Licra v Yahoo! Inc and Yahoo! France*. For an interesting account of the case see Jack Goldsmith and Tim Wu, *Who Controls the Internet? Illusions of a Borderless World* (Oxford University Press 2006).

2. JURISDICTIONAL CONFLICTS IN CYBERSPACE: YAHOO!

When in May 2000 a French court enjoined *Yahoo!*, a US-based ISPs, to enforce restrictions on the access to web content that infringed French law, the decision provoked an outcry overseas and started a complex jurisdictional conflict.

The case originated from a lawsuit two French NGOs filed against *Yahoo! Inc*. in the *Paris Tribunal de Grande Instance*. The plaintiffs complained that Nazi memorabilia, of which the display is prohibited by French law, were offered for sale on an auction web page operated by *Yahoo!,* and sought an injunction prohibiting the defendant from offering such items for sale in France. In its defence, *Yahoo!* challenged the jurisdiction of the French court and argued that compliance with French law would require the worldwide removal of the contentious web page, thereby infringing the right to free speech *Yahoo!* and its users enjoyed under the First Amendment to the US Constitution. After finding that it had jurisdiction to hear the claim since the harm was produced in France, the *Tribunal de Grande Instance* requested an opinion from an international team of experts as to whether it was technically feasible to block users based in France from accessing the contentious web page. The experts concluded that the then current state of technology would allow *Yahoo!* to implement a geographically selective blocking with an estimated success rate of approximately 90 percent. Based on this finding, the court ordered *Yahoo!* to block access from France to the content which infringed French law. Despite suing the plaintiffs in California seeking a declaratory judgment preventing the French order from being enforced in the US, faced with the prospect of substantial fines in case of non-compliance, *Yahoo!* eventually relented and even banned Nazi memorabilia from its auction sites altogether.

Yahoo! is undoubtedly the most widely discussed case on Internet jurisdiction, as it is cited in virtually every publication on the subject as the foremost example of the interplay of conflicting public policies in the online world.[12] In *Yahoo!*, the conflict involved the constitutional protection of free speech and

[12] See Paul Schiff Berman, 'The Globalization of Jurisdiction' (2002) 151 Pennsylvania Law Review 311, 327; Jack Goldsmith and Tim Wu, *Who Controls the Internet? Illusions of a Borderless World* (Oxford University Press 2006), 1; Bernard Maier, 'How Has the Law Attempted to Tackle the Borderless Nature of the Internet?' (2010) 18 IJLIT 142; Andreas Manopoulos, 'Raising 'Cyber-Borders': The Interaction Between Law and Technology' (2003) IJLIT 40; Joel Reidenberg, 'Technology and Internet Jurisdiction' (2005) 153 University of Pennsylvania Law Review 1951; Mathias Reimann, 'Introduction: The Yahoo! Case and Conflict of Laws in the Cyberage' (2002-2003) 24 Michigan Journal of International Law 663, 665; Georgios I Zekos, 'State Cyberspace Jurisdiction and Personal Cyberspace Jurisdiction' (2007) 15 IJLIT 1.

the safeguard of democratic values underpinning the prohibition of Nazi apology. As the same activity was illegal under French law but enjoyed constitutional protection in the US, the case exemplified the potential of the web to give rise to regulatory clashes. Justifying the assertion of prescriptive jurisdiction by multiple States, the borderless nature of the Internet made such clashes all the more likely.

Therefore, it is not surprising that the French court's decision in the *Yahoo!* case was highly controversial and met with considerable criticism especially in the US.[13] Some authors feared that imposing an obligation on ISPs to comply with local laws would force Internet service providers to adapt to the most restrictive standard imposed by any national law in order to avoid liability.[14] Freedom of expression and the then popular idea of the Internet as a global free space would suffer as a result.

In fact, this reading of the case omits to consider one key aspect of the order issued by the French court. While finding that *Yahoo!* had to comply with French law, the court did not impose worldwide compliance by banning Nazi-related items from its auction website altogether. By contrast, it merely requested *Yahoo!* to filter access to the relevant content based on the physical location of surfers. This could be done through geographic filtering technology, which by identifying the physical location of devices accessing the network would allow a 'zoning'[15] of the web.

Far from representing an instance of exorbitant jurisdiction – a view many held even on this side of the Atlantic[16] – the Paris court's decision in fact exemplified a pluralistic approach to the regulation of the Internet. As Professor Muir-Watt noted in a commentary on the *Yahoo!* case, the possibility offered by technology to filter content based on the location of Internet-connected terminals provided for a legitimate and practical solution for regulatory conflicts in cyberspace.[17] 'Zoning' through geolocation and geographic filtering

---

[13] See, for instance, Ben Laurie, 'An Expert's Apology' (21 November 2000) <http://apache-ssl.securehost.com/apology.html>.

[14] Thomas Schultz, ''Carving up' the Internet: Jurisdiction, Legal Orders, and the Private/Public International Law Interface' (2008) 19 EJIL 799, 812-813.

[15] For this expression see L. Lessig, A. Resnick, 'Zoning Speech on the Internet: A Legal and Technical Model', (1999) 98 Michigan Law Review 395.

[16] See Daniel Arthur Laprès, 'L'exorbitante affaire Yahoo' (2002) Journal de droit international 975.

[17] Horatia Muir Watt, 'Yahoo! Cybercollision of Cultures: Who Regulates?' (2002-2003) 24 Michigan Journal of International Law 273, esp 379-289; cf also Joel

would allow for the coexistence of a plurality of regulatory spaces within the web, each of which could reflect different policy choices. On the one hand, this would prevent the circumvention of local laws. On the other hand, it would still be possible for transnational ISPs to offer their services across different jurisdictions without having to comply with the requirements of all local laws *simultaneously*: they would *merely* have to differentiate the content that would be accessible to surfers in different countries by resorting to filtering.

3. TERRITORIAL SCOPE OF DELISTING SEARCH RESULTS UNDER EUROPEAN DATA PROTECTION LAW: THREE ALTERNATIVES

Almost two decades after the *Paris Tribunal de Grande Instance* issued its order in the *Yahoo!* case, the *Google Spain* judgment has marked the emergence of a similar clash between competing views on the balancing of constitutional values on the Internet[18] and the debate on the extension of the obligation to delist search results under EU law closely resembles discussions on Internet jurisdictions that were popular in the early-mid 2000s.

When it has been established that a request for delisting personal data made by a data subject should be granted, there are three possible ways for a search engine operator to implement it.

a) The first option consists of applying the delisting only to the national domain(s) of the search engine website corresponding to the Member State concerned or to all Member States of the European Union. In the case of Google, if a request for delisting is made, say, from Belgium, this means that Google would delist the data on google.be and possibly also on other EU domains such as google.fr, google.de, google.it etc. By contrast, users would still be able to access the original information by typing the same query on google.com or any non-European country domain of the Google search engine.

Not surprisingly, this has been the solution preferred and originally implemented by Google when dealing with delisting requests in the aftermath of the *Google Spain* ruling. It has also been endorsed by the the Advisory Council to Google on the right to be forgotten.[19]

Reidenberg, 'Yahoo and Democracy on the Internet' (2002) 42 Jurimetrics 261, 271-275.

[18] Christopher Kuner, 'Google Spain in the EU and International Context' (2015) MJ 158, 159.

[19] See Advisory Council to Google on the Right to be Forgotten, Final Report (6 February 2015) 20.

In order to justify its choice, Google provided statistical data showing that more than 95% of all queries originating in Europe are made through local versions of the search engine, with onlyvery few EU-based users resorting to google.com for their searches. The problem with those data, however, is that these are aggregated data that cover all Google searches. By contrast, Google has not provided any data showing that this pattern is also true for *name* queries – the only searches to which delisting applies.

In any event, whether or not searchers are more likely to switch to google.com for personal name searches than for other queries, the problem with delisting limited to some national domains of the search engine is that this approach is open to easy circumvention.[20] Most Internet users are aware that it suffices a click at the bottom of the page to switch from, say, google.be to google.com. In addition, when a request for delisting has been granted a notice at the bottom of the page informs users that 'some results may have been removed under data protection law in Europe', possibly prompting curious surfers to look for the missing information on other versions of the search engine. In light of these circumstances, delisting search results only on some national domain of Google Search without any additional measure can hardly be considered an adequate safeguard for the right of data protection.

b) Global delisting. Alternatively, the search engine operator could be required to de-index search results globally, removing the relevant personal data from all versions of its engine and making it effectively impossible to access from anywhere in the world. Proponents of this approach include notably the French data protection authority (CNIL) and the Article 29 Working Party. They argue that global delisting is necessary to ensure effective protection of the data subject's right to privacy.

In its 2014 Guidelines on the implementation of the *Google Spain* judgment, the Article 29 Working Party emphasised that limiting de-listing to EU domains on the grounds that users tend to access search engines via their national domains does not satisfactorily guarantee the rights of data subjects and therefore does not amount to a correct implementation of the Court of Justice's ruling. It added that in order to provide effective and complete protection of the data subject's rights, delisting would have to be 'effective on all relevant domains, including .com'.[21] While this statement leaves open two

[20] See Emmanouil Bougiakiotis, 'The Implementation of the Google Spain Ruling' (2016) 24 IJLIT 311, 325.

[21] Article 29 Data Protection Working Party, Guidelines on the implementation of the Court of Justice of the European Union judgment on 'Google Spain and Inc v Agencia

important questions – namely what is needed to make delisting *effective* and whether third county national domains also qualify as 'relevant domains' in addition to .com[22] – the dominant view is that the Working Party advocates global delisting.[23] The French data protection authority in particular has been a vocal proponent of this approach[24] and has challenged Google's policy on several occasions.[25]

Global delisting, however, is often criticised as implying a disproportionate expansion of the EU's jurisdiction and possibly a breach of international law.[26] In addition, it is often viewed as a highly unpractical solution that could trigger an international clash.[27]

c) Finally, a third option is 'zoning' by geographic filtering. According to this model, while delisting does not affect non-European domains of the search

Española de Protección de Datos (AEPD) and Mario Costeja González' C-131/12 (adopted on 26 November 2014) 14/EN WP 225, 3.

[22] On the uncertainty regarding this question see Dan Svantesson, 'Limitless Borderless Forgetfulness? Limiting the Geographical Reach of the Right to be Forgotten' (2015) Oslo Law Review 116, 120.

[23] See Emmanouil Bougiakiotis, 'The Implementation of the Google Spain Ruling' (2016) 24 International Journal of Law and Information Technology 311, 330. See also Christopher Kuner, 'Google Spain in the EU and International Context' (2015) 22 MJ 158, 160, noting that the DPAs approach 'seems to represent a departure from their former view that the territorial application of EU data protection law should be limited by factors such as proportionality and enforceability'.

[24] In an article published on the French newspaper Le Monde, the president of the CNIL and of the Article 29 Working Party presented several arguments in favour of worldwide delisting: see Isabelle Falque-Pierrotin, 'Pour un droit au déréférencement mondial' (29 December 2016) Le Monde.

[25] See 'CNIL orders Google to apply delisting on all domain names of the search engine' (12 June 2015) <https://www.cnil.fr/fr/node/15790>. For a brief overview of the case law of both civil and administrative courts in France on the right to delisting, see Olivia Tambou, 'Le droit à l'oubli numérique' (2017) 606 Revue de l'Union européenne 156, 160-162.

[26] For a discussion on the EU data protection law in light of international law limits to jurisdiction see Dan Svantesson, 'The Extraterritoriality of EU Data Privacy Law – Its Theoretical Justification and Its Practical Effect on U.S. Business' (2014) 53 Stan J intl L 53; see also the contribution by Brendan Van Alsenoy in this volume.

[27] See Paul De Hert and Vagelis Papakonstantinou, 'Google Spain. Addressing Critiques and Misunderstandings One Year Later' (2015) 22 Maastricht Journal of European and Comparative Law 624, 637.

engine, surfers accessing the Internet from the EU/EFTA territory are prevented from viewing the filtered content whatever version of the engine they are using.

Despite scholarly suggestions that this approach, which corresponds to the solution imposed by the French court in the *Yahoo!* case, could represent a viable option for dealing with delisting,[28] surprisingly it was not initially considered by the major actors involved in the implementation of the *Google Spain* ruling, namely Google and national data protection authorities. On the one hand, Google first only deleted search results on the country domains corresponding to the EU Member States, on the implicit assumption that geographic filtering was not necessary to ensure an effective protection of the data subjects' rights. On the other hand, the Article 29 Working Party did not even discuss whether geographic filtering could constitute an adequate remedy and insisted on delisting on all relevant domains without specifying how it should be implemented.[29]

Eventually, following indications by several national DPAs, in March 2016 Google modified its approach to delisting. In addition to removing search results on all European versions of the search engine, it resorted to geographic filtering by restricting access to the delisted URL on all domains, including google.com, 'when accessed from the country of the person requesting the removal'.[30] Geographic filtering has thus become the practice since.

4. REFERENCE FOR PRELIMINARY RULING FROM THE FRENCH COUNCIL OF STATE

The new approach adopted by Google in dealing with requests and the abandonment of a selection criterion based solely on country domains has not put an end to disputes over the territorial scope of delisting.

Only a few days after Google announced that it would block access to search results based on geolocation, the CNIL adopted a decision sanctioning it for

---

[28] Orla Lynskey, 'Control over Personal Data in a Digital Age: Google Spain v AEPD and Mario Costeja Gonzalez' (2015) 78 Modern Law Review 522, 531-532.

[29] Article 29 Data Protection Working Party, Guidelines on the implementation of the Court of Justice of the European Union judgment on 'Google Spain and Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González' C-131/12 (adopted on 26 November 2014) 14/EN WP 225, 3.

[30] Peter Fleischer 'Adapting our approach to the European right to be forgotten' <https://www.blog.google/topics/google-europe/adapting-our-approach-to-european-rig/>.

failure to comply with its delisting obligations.[31] The CNIL rejected the approach followed by the search engine operator, pointing at two major shortcomings. First, geographic filtering does not prevent users located in third countries, including individuals having personal or business relationships with the data subject, from viewing the contentious search results. Second, blocking based on surfers location can be circumvented by altering the geographic location of an IP address through a proxy server. Therefore, according to the CNIL geographic filtering does not sufficiently protect the data subject's right to privacy.

Google challenged the CNIL decision before the Council of State, which after hearing the parties stayed the proceedings and request a preliminary ruling from the Court of Justice.[32] The three questions submitted by the referring court all deal with the territorial scope of the delisting obligation and essentially reflect the options outlined in the previous paragraphs.

The first question poses the alternative between global and geographically selective delisting. In other words, the Council of State asked whether the Directive obliges a search engine provider to delist search results on every national domain of the engine, in order to prevent access to the relevant results from any country in the world.

Only in the case of a negative answer to the first question, the second and the third question become relevant. With the second question, the referring court requested clarification as to whether delisting should only target the search engine's domain name corresponding to the country the research is assumed to have been launched from or whether it should extend to the domain names of all 28 European versions of the engine (eg google.be, google.nl, google.fr. etc).

Finally, the third question deals with geographic filtering. If the Directive does not impose global delisting, does it require from search engine operators, in addition to the removal of search results from the European domains, filter-

[31] CNIL 'Droit au déréférencement : la formation restreinte de la CNIL prononce une sanction de 100.000 € à l'encontre de Google' (decision of 10 March 2017) <https://www.cnil.fr/fr/droit-au-dereferencement-la-formation-restreinte-de-la-cnil-prononce-une-sanction-de-100000-eu>.

[32] Conseil d'Etat 'Google Inc., application No. 399922' (19 July 2017) <http://www.conseil-etat.fr/Decisions-Avis-Publications/Decisions/Selection-des-decisions-faisant-l-objet-d-une-communication-particuliere/CE-19-juillet-2017-GOOGLE-INC>.

ing based on the location of hardware in order to prevent access to the relevant content from users based in the EU, whichever version of the search engine they use?

5. GEOGRAPHIC FILTERING: THE WAY FORWARD?

Looking at the discussion on the geographic scope of delisting and at the questions referred to the Court of Justice in light of the *Yahoo!* case, suggests that geographic filtering could represent the optimal solution. In *Yahoo!*, geolocation and filtering allowed for the coexistence of different regulatory regimes on a territorial basis, preserving the effectiveness of local law while avoiding unnecessary overreach. Since the implementation of the right to delisting poses a similar problem, this approach could be seen as offering an equal satisfactory solution.

Yet, two major dissimilarities between the *Yahoo!* type of cases and the *Google Spain* type of situations seem to undermine the analogy. The first is the different nature of the underlying policy conflicts. The second is the difference in complexity of the assessment that their required for enforcement.

a) The judgment in *Google Spain* must be read against the background of the strong emphasis the Court has placed on the effective protection of fundamental rights especially after the entry into force of the Lisbon Treaty which transformed the Charter of Fundamental Rights into a binding instrument of primary law. This tendency has been particularly pronounced with respect to data protection,[33] as it is recognised in the Charter as an autonomous right,[34]

[33] See Maja Brkan, 'The Unstoppable Expansion of the EU Fundamental Right to Data Protection. Little Shop of Horrors?' (2016) 23 MJ 812; Maja Brkan, 'The Court of Justice of the EU, Privacy and Data Protection: Judge-made Law as a Leitmotiv in Fundamental Rights Protection' in Maja Brkan, Evangelia Psychogiopoulou (eds), *Courts, Privacy and Data Protection in the Digital Environment* (10 et seq, Elgar, 2017), Selena Crespi, 'Diritti fondamentali, Corte di giustizia e riforma del sistema UE di protezione dei dati' (2015) Rivista italiana di diritto pubblico comunitario 819; Hielke Hijmans, 'Right to Have Links Removed. Evidence of Effective Data Protection' (2014) 21 MJ 555, 556.

[34] Art 8 of the Charter.

and clearly discernible in the case law both prior[35] and subsequent to *Google Spain.*[36]

The judgment itself is based on a teleological reasoning.[37] The Court's analysis and main findings are clearly driven by the concern to ensure that the data subjects' rights are effectively protected and that the safeguards put in place by the legislature are not circumvented.[38]

Defintely other arguments will also play a role when the Court answers the questions raised by the Council of State. Among them is certainly the issue of what limits international law poses to the reach of unilateral regulation of the Internet – a defence that Google has already raised in the domestic proceedings. Yet the Court has so far been cautious in drawing international law limits to the territorial reach of EU measures, and has done so not only in the field of competition law where extraterritoriality has longer been accepted.[39] In the light of precedents, effective protection of the data subject's rights can be expected to play a more prominent role in the Court's analysis. The decisive question is thus likely to be whether filtering, despite its intrinsic geographic limitation and the risk of circumvention through a proxy, offers sufficient safeguards for the data subject's privacy.

Whatever the Court's answer will be, it seems clear that the *Yahoo!* precedent is only of limited use when dealing with data protection issues. Not, however, because it is outdated or no longer offers a valid paradigm for dealing with regulatory conflicts in cyberspace; rather because of the different nature of

---

[35] See eg Joined Cases C-92/09 & C-93/09 *Volker und Markus Schecke GbR and Hartmut Eifert v Land Hessen* EU:C:2010:662 [2010] ECR I-11063; Joined cases C-293/12 é C-594/12 *Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others* [2014] EU:C:2014:238.

[36] See Case C-362/14 *Maximillian Schrems v Data Protection Commissioner* EU:C:2015:650; Joined Cases C–203/15 and C–698/15, *Tele2 Sverige AB v Post-och telestyrelsen and Secretary of State for the Home Department v Tom Watson* EU:C:2016:970.

[37] Paul De Hert and Vagelis Papakonstantinou 'Google Spain. Addressing Critiques and Misunderstandings One Year Later' (2015) 22 MJ 624, 629.

[38] *Google Spain*, (n 2) para 54.

[39] To date, the judgment that most comprehensively deals with the extraterritorial application of EU law is Case C-366/10 *American Transport Association of America and Others v Secretary of State for Energy and Climate Change* [2011] EU:C:2011:864 where the Court of Justice upheld the validity of a directive establishing a greenhouse gas emissions trading scheme for the aviation sector.

conflicts that arise in the implementation of data protection law. In other words, it might be easier and more obvious to accept the territorially limited application of a State's public policy choice – such as the prohibition of Nazi apology – than the geographically selective application of a fundamental right.

b) The second problem is that while all relevant actors – Google, the DPAs and the Council of State – assume that one of the three approaches outlined above – territorially selective delisting based on national domains, territorially selective delisting based on geographic filtering or global delisting – must apply to all instances, this is not necessarily the case.

From the viewpoint of search engine operators, the demand for criteria applicable to the generality of cases is perfectly understandable. As any other data controllers under a duty to comply with EU data protection law, they have a strong interest in implementing standards, ideally even automated or semi-automated procedures that would reduce costs. From the perspective of national DPAs, the concern for the maximisation of fundamental rights protection is an equally powerful incentive to advocate global delisting.

Such a one-size-fits-all approach, however, might not be the best way of dealing with requests for de-indexing of web search results. In this respect, the enforcement of a right to data privacy significantly differs from a *Yahoo!* type of situation. In the case of a state policy forbidding, as in *Yahoo!*, the sale of certain items considered illegal under the local law, the prohibition is meant to apply without regard to competing interests and its enforcement usually does not require a great deal of balancing. In addition, once geographic filtering is in place, it does not frustrate the purpose of the French policy that people engage in the commerce of Nazi-related items in the US.

By contrast, when it comes to implementing a right to deleting – or delisting – personal data, the picture is much more complex. As the Court of Justice recognised in *Google Spain*, processing requests for delisting requires a 'fair balance' to be struck between the data subject's fundamental rights to privacy and data protection under Articles 7 and 8 of the Charter of Fundamental Rights and the interest of users in having access to information.[40] Although the Court failed to explicitly recognise it – a failure that has attracted major criticism[41] – the users' 'interest' may also enjoy fundamental right status as

---

[40] Case C-131/12 *Google Spain SL and Google Inc vc Agencia Española de Protección de Datos (AEPD) and Mario Costeja González* [2014] EU:C:2014:317, para 81.

[41] See Eleni Frantziou, 'Further Developments in the Right to be Forgotten: The European Court of Justice's Judgment in Case C-131/12, *Google Spain SL, Google Inc v Agencia Espanola de Proteccion de Datos*' (2014) 14 Human Rights Law Review 761, 769.

its preservation is instrumental to guaranteeing the freedom of expression and information. It can be safely assumed that striking a 'fair balance' requires a careful case-by-case assessment and that the relative weight of privacy and competing rights or interests is not always the same. In practice, the outcome of the balancing test could depend on a number of variables, such as the nature of the data (sensitive/non sensitive), whether the information published is false or defamatory, the status and personal condition of the data subject (minors might deserved enhanced protection), whether the data were processed illegally, etc.

It is true that those concerns are already addressed at a different stage, namely when a decision has to be taken on granting a request for delisting in the first place. Nevertheless, they could also affect the desirable geographic scope of delisting.

On the one hand, in certain cases public interest in the availability of information may be strong or even stronger in a third country than within the EU.[42] This problem can be significant in the light of the relatively ill-defined protective scope of the EU data protection rules. Although the Article 29 Working Party has stated that DPAs will deal with claims presenting 'a clear link between the data subject and the EU, for instance where the data subject is a citizen or resident of an EU Member State',[43] neither the application of Data Protection Directive nor that of the General Data Protection Regulation (GDPR) that will replace it as of May 2018 are dependent on the nationality or residence of the data subject.[44] As a consequence, at least in theory, EU

[42] Brendan Van Alsenoy and Marieke Koekkoek mention the Mosley case as a good example where there might be a strong interest of users based in third countries in the availability of information (Brendan Van Alsenoy and Marieke Kokkoek, 'Internet and Jurisdiction after Google Spain: The Extraterritorial Reach of the 'Right to be Delisted'' (2015) 5 IDPL 105, 113.

[43] Article 29 Data Protection Working Party, Guidelines on the implementation of the Court of Justice of the European Union judgment on '*Google Spain and Inc v Agencia Española de Protección de Datos* (AEPD) and *Mario Costeja González*' C-131/12, (26 November 2014) WP 225, 3.

[44] The application of the GDPR is conditional on the data subject being 'in the Union' if the data controller or processor is not established in the Union (Art 4(2)). However, as in the directive this is not a requirement for processing of personal data carried out in the context of an establishment of the data controller or processor on the EU territory (Art 4(1)). In addition, both the Directive and the Regulation contain a recital indicating that the right to the protection of personal data applies 'whatever [the] nationality or residence' of the data subject (recital 2).

data protection law 'could apply to requests for suppression from individuals anywhere in the world'.[45]

On the other hand, the data subject's privacy may will be threathened by physical or legal persons located in third countries. In those cases, geographic filtering can hardly offer an effective remedy. Although not related to personal data, a recent Canadian case offers an interesting illustration of the problem.[46] A Canadian company (Equustek) sued a former distributor, that re-labeled a product and solded it as its own, for breach of intellectual property rights. Equustek won the case, but the infringer relocated its premises to an unknown place and continued to sell its products online. Based on a court order prohibiting the infringer from carrying on business on the Internet, Google de-indexed its web pages, but limited the delisting to google.ca. Equustek then brought court proceedings seeking an injunction requiring Google to delist the infringer's websites from all its search results worldwide. Hearing the case on appeal from Google which had lost before the first instance court, the Supreme Court of Canada delivered a judgment upholding Equustek' right to obtain a global injunction. It noted that the injunction against Google could only attain its purpose if it applied where Google operates, namely globally, and that delisting limited to certain national domains would not prevent harm to the petitioner. Aside from concerns that relate specifically to IP rights – notably in the light of their traditionally territorial character – the judgment illustrates some of the challenges that territorially selective enforcement poses to the effectiveness of rights in the online environment. It is not difficult to imagine cases – as a way of example, one might think of revenge porn of cyberstalking of minors – where the data subject might suffer serious harm from the failure to de-indexing search results on a worldwide basis.

In conclusion, none of the possible approaches to the implementation of delisting seems suitable to apply to all cases. While a selection based on national domains is obviously ineffective and easy to circumvent, global delisting risks being disproportionate and triggering unnecessary jurisdictional conflicts. The 'third way' offered by geographic filtering, although it *generates*

---

[45] Christopher Kuner, 'The Court of Justice of the EU Judgment on Data Protection and Internet Search Engines: Current Issues and Future Challenges' In Hess B and Mariottini C (eds), *Protecting Privacy in Private International and Procedural Law and by Data Protection* (Nomos, 2015) 19, 29; see also Dan Svantesson 'Limitless Borderless Forgetfulness? Limiting the Geographical Reach of the Right to be Forgotten' (2015) Oslo Law Review 116, 130.

[46] Supreme Court of Canada *Google Inc v Equustek Solutions Inc* [2017] SCC 34.

no interference with the jurisdiction of third countries, may in certain cases be insufficient to effectively protect the rights of the data subject.

6. STRENGTHS AND WEAKNESSES OF A MORE FLEXIBLE APPROACH

In the light of such difficulties, some authors have argued that the territorial scope of delisting under EU data protection law should not necessarily be the same in all circumstances and could vary depending on the nature of data[47] or on a set of substantive factors such as the state interests involved, the likelihood of adverse impact on the data subject in case of territorially selective delisting, the degree of normative convergence between the States involved and the existence of connections with the territory of the forum State.[48] In order to reduce the complexity of a balancing text based on such a variety of substantive factors, other scholars, while still rejecting the assumption that one mode of implementation would work in every case, have suggested adopting geographic filtering as the default approach, while assessing the need for global implementation on a case-by-case basis.[49]

All such attempts at elaborating a nuanced approach to the implementation of the right to delisting are certainly meritorious and would arguably permit a more careful balancing of the rights and interests and stake, in addition to reducing the risk of jurisdictional clashes. However, they also raise two problems that should not be neglected.

a) The first is the need to find a legal basis for any test aimed at determining the scope of delisting on a case-by-case basis. Unfortunately, both the Directive and the GDPR, despite the latter containing specific provisions on the 'right to be forgotten', are completely silent on the territorial scope of application of the duty to delete data that is inadequate, irrelevant or no longer relevant or excessive. As they do not offer any guidance at all as to the scope

[47] Dan Svantesson 'Limitless Borderless Forgetfulness? Limiting the Geographical Reach of the Right to be Forgotten' (2015) Oslo Law Review 116, 131-134.

[48] Brendan Van Alsenoy and Marieke Koekkoek 'Internet and Jurisdiction after Google Spain: The Extraterritorial Reach of the 'Right to be Delisted'' (2015) 5 IDPL 105, 116-119.

[49] See Emmanouil Bougiakiotis 'The Implementation of the Google Spain Ruling' (2016) 24 IJLIT 311, 330.

of delisting, *a fortiori* they do not suggest that delisting should have a different scope depending on the kind of information or the interests involved.[50]

The absence of express guidance in the legislative text could certainly be overcome through judicial interpretation. After all, the Court will have to interpret provisions that rely on vague and flexible notions such as 'appropriateness' or 'excessiveness'. In particular, article 12(b) of the Directive mandates rectification or erasure of data 'as appropriate', a criterion that could perhaps be relied upon to legitimise selective delisting.[51] Yet, filling the gap in the legislation through judicial interpretation will require time and create, at least temporarily, legal uncertainty, adding to the many complex questions that already surround the personal and material scope of the 'right to be forgotten' and its implementation.[52] In the meantime, practices developed by data controllers required to enforce request for delisting and the supervision by national DPAs could help devise criteria for determining the territorial requests scope of delisting. In particular, the article 29 Working Party in its advisory function could offer a crucial contribution in this respect.

b) The second problem would be inherent to the rejection of a one-size-fits-all approach and to the search for more flexible solutions. Inevitably, making the scope of delisting dependent on a balancing test would add one further level of complexity to a normative framework that is already highly complex and burdensome to the point of being often perceived as dysfunctional.[53]

Seen from this perspective, the debate on the territorial scope of delisting highlights a dilemma that is not limited to the implementation of the *Google*

---

[50] Against this background, the request for preliminary ruling by the Council of State does not hint at criteria that may suggest different outcomes in different cases and appears to rest on the assumption that the same formula should apply under all circumstances. It remains to be seen whether the Advocate General and the Court will discuss the possible benefits of a more flexible approach or instead stick to an abstract assessment of the alternatives raised by the referred questions.

[51] Daphne Keller, 'The Right Tools: Europe's Intermediary Liability Laws and the 2016 General Data Protection Regulation' forthcoming in Berkeley Technology Law Journal <https://law.stanford.edu/publications/the-right-tools-europes-intermediary-liability-laws-and-the-2016-general-data-protection-regulation/>.

[52] For an overview of some of these problems within the wider context of EU data protection law see Maja Brkan, 'The Unstoppable Expansion of the EU Fundamental Right to Data Protection. Little Shop of Horrors?' (2016) 23 MJ 812.

[53] Dan Svantesson, 'A 'Layered Approach' to the Extraterritoriality of Data Privacy Laws" (2013) 3 IDPL 278; Dan Svantesson 'The Extraterritoriality of EU Data Privacy Law – Its Theoretical Justification and Its Practical Effect on U.S. Business' (2014) 53 Stan J intl Law 53, 67.

Spain ruling but arguably underlies EU data protection law more generally. On the one hand, calling for unrestrained global reach might on paper offer better protection of individual rights and support the EU's ambition to act as a global trendsetter in the field by stimulating spontaneous convergence towards its stricter regulatory standard – a sort of 'Brussels effect'[54] for privacy and data protection. Inherent risks of this approach would be its possible limited effectiveness outside the EU borders and adverse effects on transatlantic relations.[55] On the other hand, any alternative approach that could do justice-better to the complexities of individual cases would also make it harder for online operators and data subjects alike to cope with the intricacies of EU data protection law. It would thereby increase barriers to entry in online markets[56] and possibly wide the gap between the law in books and the law in action.[57]

Interestingly, both approaches are likely to contribute to a process of fragmentation of the Internet that has been ongoing further for quite some time. This process whereby, in the wake of *Yahoo!* and similar cases, the web has been increasingly 'carved up' into discrete legal spheres by the exercise of sovereign regulatory power.[58]

The alternative between global and territorially selective delisting points, however, to two different models of fragmentation. In the territorially selective model, geographic filtering allows global undertakings to offer online services across a number of jurisdictions and permits the coexistence of a plurality of divergent local laws each in its own territorial sphere. By contrast, claims for the global application of local data protection laws (or any other

---

[54] Anu Bradford, 'The Brussels Effect' (2012) 107 Northwestern University Law Review 1.

[55] On the possible measures that third countries could adopt as a reaction ('blocking legislation') see Dan Svantesson, 'The Extraterritoriality of EU Data Privacy Law – Its Theoretical Justification and Its Practical Effect on U.S. Business' (2014) 53 Stan J intl Law 53, 94-95.

[56] See Emmanouil Bougiakiotis, 'The Implementation of the Google Spain Ruling' (2016) 24 IJLIT 311, 319; David Stute, 'Privacy Almighty? Tge CJEU's Judgment in Google Spain SL v AEPD' (2015) 36 Michigan Journal of International Law 649, 676-677.

[57] On the gap between the expectations raised by EU data protection law and its actual prospects of enforcement see Bert-Jaap Koops, 'The Trouble with European Data Protection Law' (2014) 4 IDPL 250, 251-253.

[58] Thomas Schultz, ''Carving up' the Internet: Jurisdiction, Legal Orders, and the Private/Public International Law Interface' (2008) 19 EJIL 799.

local laws) coupled with the threat of 'market destroying measures'[59] could potentially undermine the ability of companies to offer their services in different jurisdiction. Yet, that risk could arguably materialise only in the presence of much stronger policy divergences than the current different understandings of freedom of expression across the Atlantic. The actual impact of the scope of search engines' delisting obligations on tensions in transatlantic relations should therefore not be overestimated.

7. SELECTED LITERATURE

Bradford A, 'The Brussels Effect' (2012) 107 Northwestern University Law Review

Berman P S, 'The Globalization of Jurisdiction' (2002) 151 Pennsylvania Law Review

Bougiakiotis E, 'The Implementation of the Google Spain Ruling' (2016) 24 IJILT

Brkan M, 'The Unstoppable Expansion of the EU Fundamental Right to Data Protection. Little Shop of Horrors?' (2016) 23 MJ

Brkan M, 'The Court of Justice of the EU, Privacy and Data Protection: Judge-made Law as a Leitmotiv in Fundamental Rights Protection' In Brkan M and Psychogiopoulou E, (eds) *Courts, Privacy and Data Protection in the Digital Environment* (10 et seq, Elgar, 2017)

CNIL orders Google to apply delisting on all domain names of the search engine' (12 June 2015) <https://www.cnil.fr/fr/node/15790>

CNIL 'Droit au déréférencement : la formation restreinte de la CNIL prononce une sanction de 100.000 € à l'encontre de Google' (decision of 10 March 2017) <https://www.cnil.fr/fr/droit-au-dereferencement-la-formation-restreinte-de-la-cnil-prononce-une-sanction-de-100000-eu>

[59] Namely measures that could penalise a foreign party for failure to comply with the forum law. For this notion see Dan Svantesson, 'The Extraterritoriality of EU Data Privacy Law – Its Theoretical Justification and Its Practical Effect on U.S. Business' (2014) 53 Stan J intl Law 53, 98. As examples of market destroying measures the Author mentions the prohibition for the foreign party to trade in the forum jurisdiction, the unenforceability of credits within that same jurisdiction and the exclusion from government contracts.

Conseil d'Etat 'Google Inc., application No. 399922' (19 July 2017) <http://www.conseil-etat.fr/Decisions-Avis-Publications/Decisions/Selection-des-decisions-faisant-l-objet-d-une-communication-particuliere/CE-19-juillet-2017-GOOGLE-INC>

Crespi S, 'Diritti fondamentali, Corte di giustizia e riforma del sistema UE di protezione dei dati' (2015) Rivista italiana di diritto pubblico comunitario 819

De Hert P and Papakonstantinou V, 'Google Spain. Addressing Critiques and Misunderstandings One Year Later' (2015) 22 MJ

Falque-Pierrotin I, 'Pour un droit au déréférencement mondial' (29 December 2016) Le Monde

Fleischer P, 'Three years of striking the right (to be forgotten) balance' <https://www.blog.google/topics/google-europe/three-years-right-to-be-forgotten-balance/>

Fleischer P, 'Adapting our approach to the European right to be forgotten' (*Google in Europe*, 15 May 2017) <https://www.blog.google/topics/google-europe/adapting-our-approach-to-european-rig/>

Frantziou E, 'Further Developments in the Right to be Forgotten: The European Court of Justice's Judgment in Case C-131/12, Google Spain, SL, Google Inc v Agencia Espanola de Proteccion de Datos' (2014) 14 Human Rights Law Review

Goldsmith J and Wu T, *Who Controls the Internet? Illusions of a Borderless World* (Oxford University Press, 2006)

Hijmans H, 'Right to Have Links Re-moved. Evidence of Effective Data Protection' (2014) 21 MJ

Keller D, 'The Right Tools: Europe's Intermediary Liability Laws and the 2016 General Data Protection Regulation' forthcoming in Berkeley Technology Law Journal, available at <https://law.stanford.edu/publications/the-right-tools-europes-intermediary-liability-laws-and-the-2016-general-data-protection-regulation/>

Koops B-J, 'The Trouble with European Data Protection Law' (2014) 4 IDPL

Kropf J W, 'Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD). Case C-131/1' (2014) 108 AJIL

Kuner C, 'Google Spain in the EU and International Context' (2015) MJ

Kuner C, 'The Court of Justice of the EU Judgment on Data Protection and Internet Search Engines: Current Issues and Future Challenges' In Hess B and

Mariottini C (eds), *Protecting Privacy in Private International and Procedural Law and by Data Protection* (Nomos, 2015)

Laprès D A, 'L'exorbitante affaire Yahoo' (2002) Journal de droit international

Laurie B, 'An Expert's Apology' (21 November 2000) <http://apache ssl.securehost.com/apology.html>

Lessig L and Resnick A, 'Zoning Speech on the Internet: A Legal and Technical Model' (1999) 98 Michigan Law Review

Lynskey O, 'Control over Personal Data in a Digital Age: Google Spain v AEPD and Mario Costeja Gonzalez' (2015) 78, 3 Modern Law Review

Manopoulos A, 'Raising 'Cyber-Borders': The Interaction Between Law and Technology' (2003) IJLIT

Maier B, 'How Has the Law At-tempted to Tackle the Borderless Nature of the Internet?' (2010) 18 IJLIT

Muir Watt H, 'Yahoo! Cybercollision of Cultures: Who Regulates?' (2002-2003) 24 Michigan Journal of International Law

Reidenberg J, 'Yahoo and Democracy on the Internet' (2002) 42 Jurimetrics

Reimann M, 'Introduction: The Yahoo! Case and Conflict of Laws in the Cyberage' (2002-2003) 24 Michigan Journal of International Law

Rees C and Heywood D, 'The 'right to be forgotten' or the 'principle that has been remembered'' (2014) 30 Computer Law and Security Review

Reidenberg J, 'Technology and Internet Jurisdiction' (2005) 153 University of Pennsylvania Law Review

Sartor G, 'Search Engines as Controllers. Inconvenient Implications of a Questionable Classification' (2014) 21 MJ

Schultz T, ''Carving up' the Internet: Jurisdiction, Legal Orders, and the Private/Public International Law Interface' (2008) 19 EJIL

Spiecker I, 'A New Framework for Information Markets: Google Spain' (2015) 52 CML Rev

Stute D, 'Privacy Almighty? Tge CJEU's Judgment in Google Spain SL v AEPD' (2015) 36 Michigan Journal of International Law.

Svantesson D, 'Limitless Border-less Forgetfulness? Limiting the Geographical Reach of the Right to be Forgotten' (2015) Oslo Law Review

Svantesson D, 'The Extraterritoriality of EU Data Privacy Law – Its Theoretical Justification and Its Practical Effect on U.S. Business' (2014) 53 Stan J intl Law

Svantesson D, 'A 'Layered Approach' to the Extraterritoriality of Data Privacy Laws" (2013) 3 IDPL

Tambou O, 'Le droit à l'oubli numérique' (2017) 606 Revue de l'Union européenne

Tribunal de Grande Instance de Paris, order of 22 May 2000, UEJF and Licra v Yahoo! Inc. and Yahoo! France

Van Alsenoy B and Koekkoek M 'Internet and Jurisdiction after Google Spain: The Extraterritorial Reach of the 'Right to be Delisted'' (2015) 5 IDPL

Zekos G I, 'State Cyberspace Jurisdiction and Personal Cyberspace Jurisdiction' (2007) 15 IJLIT

Looking for safe harbours outside the European Union

The issue of onward transfers in EU data protection law and its external dimension

STEFANO SALUZZO[1]

1. INTRODUCTION

The rise of digitalisation of trade in the last decades has created a completely new landscape in the field of economic and commercial relations among countries and therefore calls for an update of the existing rules. In particular, the last phase of the development of international trade has been fostered by digitalisation processes and has produced an increase in supply of goods and services across the borders.[2] The movement of data around the globe is at the core of such developments, as it provides new means of sharing information, reducing costs and fostering competitiveness of companies (including small and medium enterprises). Some have claimed that through data flows, globalisation has entered a new era in which digital platforms may create more efficient and transparent global markets.[3] In this context, data flows are also the major enabler of the creation of big data sets,[4] raising numerous questions as far as privacy and consumer protection are concerned.[5]

---

[1] Postdoc fellow, Università della Valle d'Aoste. Email: stefano.saluzzo@gmail.com.

[2] Javier López Gonzàles and Marie-Agnes Jouanjean, 'Digital Trade: Developing a Framework for Analysis' in *OECD Trade Policy Papers no. 205* (OECD Publishing, Paris, 2017) 7-8.

[3] Data flows are said to even generate more economic value than traditional trade in goods. See McKinsey Global Institute, *Digital Globalization: The New Era of Global Flows* (Report) (2016) <https://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/digital-globalization-the-new-era-of-global-flows>.

[4] See Thomas H Davenport, Paul Barth and Randy Bean, 'How 'Big Data' is Different' (2012) 54 MIT Sloane Management Rev, 22, 22-23. For instance, cross-border data flows are one of the main features of cloud computing services. See in this regard, Dan Svantesson and Roger Clarke, 'Privacy and Consumer Risks in Cloud Computing' (2010) 26 Computer L and Security Rev 391.

[5] See Sheri B Pan, 'Get to Know Me: Protecting Privacy and Autonomy under Big Data's Penetrating Gaze' (2017) 30 Harvard J of L and Technology 239. For an EU perspective, see Maria Eduarda Gonçalves, 'The EU Data Protection Reform and the Challenges

The International Telecommunication Union (ITU) has highlighted the connection between data collection through transmissions and the capacity to build and analyse huge amount of data, while warning against a number of challenges arising from these processes, especially in terms of heterogeneity and incompleteness in the construction of big data sets and of privacy protection in the processing of data.[6]

Notwithstanding general optimistic views on the potential of data flows for international trade, many countries have started to introduce measures to restrict such flows in order to protect their citizens' privacy or for cybersecurity reasons.[7] This is also true in relation to the phenomenon of onward transfers, that is to operations involving the re-export of data received from one country to another third country. Domestic regulators have attempted to restrict and limit the indiscriminate recourse to such a practice, while taking into account the economic potential of data re-transfer mechanism for international commerce transactions.

The present contribution aims at identifying the legal framework applicable to onward transfers operations and framing the role of private autonomy and contractual regulation in this field. The EU regulator has left considerable room to private law instruments in disciplining onward transfers. This calls for an analysis of the issues and the problems that may arise from the concrete application of this hybrid system of regulation.

The first part of this contribution constitutes an introduction to the rules in EU law on the transfer of data outside the EU's territory, especially taking into consideration recent developments in the case-law of the European Court of

---

of Big Data: remaining Uncertainties and Ways Forward' (2017) 26 Information & Communications Technology L 90. See also the recent document by the Council of Europe 'Guidelines on the protection of Individuals with regard to the Processing of Personal Data in a World of Big Data (23 January 2017) T-PD(2017)01.

[6] See International Telecommunication Union (ITU) Recommendation ITU-T Y.3600, 'Big data - Cloud Computing Based Requirements and Capabilities' (2015) 3-4. Such issues have arisen also with regard to governments' capacities to foster security and surveillance programs through the construction of big data sets, mainly collected by relying on data transfers between private companies. See Mark Andrejvic and Kelly Gates, 'Big Data Surveillance: Introduction' (2014) 12 Surveillance and Society 185; David Lyon, 'Surveillance, Snowden and Big Data: Capacities, Consequences, Critique' (2014) 1 Big Data & Society 1.

[7] On the impact of cybersecurity measures on international trade see Nir Kshetri, *The Quest to Cyber Superiority* (Heidelberg, Springer 2016) 75-87; Shin-yi Peng, 'Cybersecurity Threats and the WTO National Security Exceptions' (2015) 18 J of Intl Economic L 449.

Justice (ECJ) and of the entry into force of the new General Data Protection Regulation (GDPR).

The second part outlines the provisions specifically dealing with onward transfers and with the different instruments of regulations the EU relies upon. This part is complemented by an analysis of the EU practice as regards international agreements with third countries for the exchange of data between public authorities for law enforcement purposes.

The last part focuses on how the EU legal framework on onward transfers has been implemented in the new Privacy Shield and addresses some of the concerns that the interactions between public and private regulation may bring to the surface.

2. TRANSFERS OF DATA OUTSIDE THE EUROPEAN UNION: AN OVERVIEW

Given the absence of a comprehensive international regime, the EU has regulated the flows of data from the territory of its Member States to third countries in a purely unilateral manner. Since the adoption of Directive 95/46 on the protection of personal data, the Union has set forth a complex mechanism subjecting the transfer of data collected within EU territories to strict requirements. These rules were originally provided by articles 25 and 26 of the Directive,[8] which will soon be replaced by the new GDPR.[9] The transfer of data from the EU to third countries falls under a different legal basis, all of them having as a common feature the evaluation of the level of protection of European data guaranteed by the legal system of the third country concerned.[10] Moreover, recent developments in the case-law of the Court of Justice of the

[8] Directive 95/46/EC of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1995] OJ L281/31.

[9] Regulation (EU) 2016/678 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and of the free movement of such data, and repealing Directive 95/46/EC (General data Protection Regulation) [2016] OJ L119/1.

[10] Note that the protection of personal data on the Internet will be addressed in a separate but complementary regulation (so called "E-Privacy Regulation"). However, the limits to data transfers outside the EU will remain entirely disciplined by the GDPR. See Commission (EC), 'Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications)' COM(2017) 10 final, 10 January 2017.

EU (CJEU) has enhanced the system protecting data transferred to third countries' jurisdiction, due to the particular nature of the data protection rights, which have acquired the status of *constitutional* rights under the Charter of Fundamental Right of the EU.[11]

According to art 25 of the Directive 95/46 (the content of which is essentially replicated in art 44 of the GDPR), the first basis on which private companies can rely for transferring data collected within the EU to third countries is the so called adequacy decision, an implementing act adopted by the Commission. The Commission takes the decision in relation to a single third State on the grounds of the level of protection afforded to personal data[12] by the receiving State's domestic legislation that according to the Directive and the Regulation must be *adequate*. According to art 25 (6) of the Directive, in assessing the adequacy of the level of protection guaranteed by the third country concerned, the Commission can take into consideration a series of factors, including domestic regulations and international agreements binding upon the receiving State.[13] The advantages deriving from an adequacy decision for companies in the receiving third State are multiple, but essentially they are linked to the fact that the decision allows an automatic transfer of data of every natural or legal person in the EU to any natural or legal person in the territory of a third State. This mechanism constitutes a valuable instrument

---

[11] See Joined Cases C-293/12 and C-594/12 *Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others* EU:C:2014:238; Joined Cases C–203/15 and C–698/15, *Tele2 Sverige AB v Post-och telestyrelsen and Secretary of State for the Home Department v Tom Watson* EU:C:2016:970; Opinion 1/15 of the Court (Grand Chamber) *Opinion on the Draft agreement between Canada and the European Union – Transfer of Passenger Name Record data from the European Union to Canada* EU:C:2017:592 (ECJ, 26 July 2017). See also in the literature, Juliane Kokott and Christoph Sobotta, 'The distinction between privacy and data protection in the jurisprudence of the CJEU and the ECtHR' (2013) 3 Intl Data Privacy L 222; Gloria González Fuster, *The Emergence of Personal Data Protection as a Fundamental Right of the EU* (Heidelberg, Springer 2014).

[12] The notion of personal data under EU law is particularly extensive and it covers the majority of data used in international online transactions. See in particular … Even if businesses activities may rely on the exchange of non personal data, the relevance of personal data transfer between companies for global trade is extensively acknowledged in the literature. See eg Asunción Esteve, 'The Business of Personal Data: Google, Facebook, and Privacy Issues in the EU and the USA' (2017) 7 Intl Data Privacy L 36.

[13] It is in this context that, by decision 2000/520, the Commission adopted the *Safe Harbour*, allowing for the automatic transfer of data from the EU to US companies.

to enhance cross-border supply of goods and services not only for big companies but also for small and medium enterprises. EU Member States, in fact, are obliged not to impede data flows from their territory once the adequacy decision is adopted in relation to a certain country.

This mechanism has undergone some exceptional developments driven by the Court of Justice of the EU. In the recent *Schrems* judgment, the Court has clarified the meaning of the term 'adequate', by considering that transfers of data to a third country can only occur when the latter offers a level of data protection 'essentially equivalent' to that provided by the EU legal order.[14] This construction not only reduces the margin of appreciation of the Commission in evaluating whether data can be transferred automatically to a certain territory, but also necessarily restricts the number of countries able to meet such a strict requirement.[15] In fact, the standard of protection applicable to data transfers is not just the one provided in EU secondary legislation, but also the higher one embodied in arts 7 and 8 of the EU Charter of Fundamental Rights.

Besides the adequacy decision, the Directive has set forth another legal basis for transferring data outside the EU territory, which was further replicated in the new GDPR in a more detailed manner. Art 46 of the GDPR provides for a number of safeguards allowing the transfer of data outside the EU when an adequacy decision is lacking. The most relevant amongst them are the model contract clauses which are protection clauses drafted and adopted by the Commission that have to be inserted in a contract providing for data transfer between controllers and between controllers and processors.[16] The role of

---

[14] See Case C-362/14 *Maximillian Schrems v Data Protection Commissioner* EU:C:2015: 650, para 73. On the Schrems judgment see… According to the Court, the Commission has to take into consideration also the developments in domestic regulations that can have an impact on the level of data protection (*Schrems* [2015] paras 75-77). This has been codified in the GDPR, which provides for an obligation upon the Commission to conduct a periodical review of the adequacy of the level of protection offered by third countries. The review should be conducted at least every four years, which could impact on the ability of companies to rely on adequacy decisions on the long term. Moreover, the Commission must also consider how the receiving jurisdiction regulates the access to data by public authorities, together with the existence of compliance mechanisms or data protection authorities.

[15] Eg in countries where data protection regulations do not enjoy a constitutional coverage or where privacy matters are balanced differently in relation to other State-policy choices.

[16] See in particular Commission Decision (EC) 2001/497/EC on standard contractual clauses for the transfer of personal data to third countries, under Directive 95/46/EC,

the Commission entails a presumption of conformity of these clauses (and thus of transfers based on them) with EU law,[17] even if the connected obligations can be particularly onerous for companies.[18] Amongst other instruments, companies may also rely on binding corporate rules, namely a set of provisions legally binding for all entities constituting the enterprises.[19] Binding corporate rules, however, may only be used for transferring data within the same company group.[20]

Finally, under art 49 single transfer operations are legitimate when one of the derogations listed by the provision applies. The first and most relevant is the express consent of the data subject to the transfer operation. A consent can be particularly difficult to obtain in relation to subsequent and unforeseeable

[2001] OJ L181/19 (amended by Commission Decision (EC) 2004/915 amending Decision 2001/497/EC as regards the introduction of an alternative set of standard contractual clauses for the transfer of personal data to third countries (notified under document number C(2004)5271) [2004] OJ L385/74; Commission Decision (EC) 2010/87/EU on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC of the European Parliament and of the Council (notified under document number C(2010)593), [2010] OJ L39/5. According to arts 44 and 45, cross-border transfers of data may also take place on the basis of model clauses adopted by single EU Data Protection Authorities in compliance with the GDPR.

[17] However, model contract clauses are currently under the scrutiny of the Court of Justice for their alleged incompliance with arts 7 and 8 of the Charter of Fundamental Right of the EU. See Irish Data Protection Commissioner, 'Update on litigation involving Facebook and Maximilian Schrems. Explanatory Memo' (16 March 2017) <https://www.dataprotection.ie/docs/16-03-2017-Update-on-Litigation-involving-Facebook-and-Maximilian-Schrems/1598.htm>.

[18] Eg in terms of applicable law and of attribution of responsibility in cases of data breach.

[19] Art 47 of the GDPR specifies the structure and the content binding corporate rules must present in order to be considered compatible with the data protection regime. Other grounds are available for justifying the transfer of data outside the EU, but they deal with rather specific situation (such as an agreement between public authorities, an approved code of conduct or an approved mechanism of certification) and they are only valuable for single transfer operations.

[20] On binding corporate rules see David Bender and Larry Ponemon, 'Binding Corporate Rules for Cross-Border Data Transfers' (2006) 3 Rutgers J of L and Urban Policy 154. See also Article 29 Working Party, 'Working Paper. Transfers of Personal Data to Third Countries: Applying Article 26(2) of the EU Data Protection Directive to Binding Corporate Rules for International Data Transfers', WP 74 (3 June 2003); Article 29 Working Party, 'Explanatory Document on the Processor Binding Corporate Rules', WP 204 (19 April 2013) (revisited on 22 May 2015).

transfers between different companies.[21] Other cases are related to transfers of data necessary for the performance of a contract between the data subject and the controller or of a contract concluded between the controller and another entity in the interest of the data subject. All other derogations refer to exceptional situations, such as reasons of public interest, the establishment and the defense of legal claims and the need to protect a vital interest of the data subject or of other persons. Evidently, these are situations in which the legal basis allows for single transfers of specific personal data and they do not entail the commercial and economic advantages already mentioned in relation to an adequacy decision.

3. THE PLACE OF ONWARD TRANSFERS IN EU DATA PROTECTION LAW

Apart from the extraterritorial claims formulated in relation to the scope of application of EU data protection law, the extensive reach of such rules is certainly confirmed by the mechanism regulating data transfers outside the Union's territory. The protection afforded to data by EU law somehow remains intact even when these data leave the territory of the EU to be transferred to third countries. This was also the reason for the Court to interpret the term *adequacy* as meaning *essentially equivalent*. The Court has in fact observed that a different construction of the adequacy system would have been incompatible with the objectives themselves of EU data protection law, namely to protect personal data collected within the EU and to guarantee this kind of protection where data are transferred to third countries. Otherwise, 'the high level of protection guaranteed by Directive 95/46 read in the light of the Charter could easily be circumvented by transfers of personal data from the European Union to third countries for the purpose of being processed in those countries'.[22] There is no doubt that at the end, the adequacy determination by the Commission will imply a strict scrutiny of third countries' national legislation and international commitments, but this is justified by the need to guarantee the effectiveness of EU law on data protection.

---

[21] Note that consent to data processing (and to data transfers as well) has been for a long time a peculiar feature of EU data protection law and only recently it has gained attention within other legal framework, such as the CoE 108 Convention. See in this regard Paul De Hert and Vagelis Papakonstantinou, 'The Council of Europe Data Protection Convention reform: Analysis of the new text and critical comment on its global ambition' (2014) 30 Computer L and Security Rev 633, 637-638.

[22] *Schrems* (n 14) para 73.

However, the entire mechanism regulating data transfers outside the Union's territory is specifically focused on the first transfer operation and, in particular, it takes into consideration the level of protection afforded to data collected in the EU by the first country of destination. The issue raised by onward transfers necessarily derives from this element and it requires to assess in which manner the extension of protection of data leaving the EU can also apply to third countries of subsequent destination. Onward transfers, in fact, might potentially involve an elevated number of different jurisdictions and they risk producing a lowering in the protection guaranteed to transferred data once they leave the first country of destination to be re-transferred. In the 108 Convention of the Council of Europe for the Protection of Individuals with regard to Automatic Processing of Personal Data, onward transfers to countries not party to the Convention (and thus not subject to the level of protection provided by it) are considered with a certain suspicion, and they can be prohibited by the contracting party if there is the risk that they might be used for circumventing the rules of the Convention itself.[23]

Directive 95/64 was silent on the matter and, as will be seen, the issue had been addressed at the time on a case-by-case basis, essentially leaving the burden of the regulation of onward transfers on the receiving State. In the GDPR, however, the european legislator has inserted a reference to onward transfers, whose concrete effects need peculiar attention. According to art 44 of the GDPR, any transfer of data outside the EU shall take place only if 'the conditions laid down in this Chapter are complied with by the controller and processor, including for onward transfers of personal data from the third country or an international organisation to another third country or to another international organisation'.[24]

[23] This is an exception to the duty of the contracting parties not to impose restrictions on the free flow of data amongst their territories. See Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data art 12, para 3, let b), according to which parties to the Convention are entitled to derogate form the obligation dealing with free data transfers 'when the transfer is made from its territory to the territory of a non-Contracting State through the intermediary of the territory of another Party, in order to avoid such transfers resulting in circumvention of the legislation of the Party referred to at the beginning of this paragraph'.

[24] Recital 101 of the GDPR highlights the rationale for including the reference to onward transfers in the opening provision of the chapter dedicated to data transfers: '[…] when personal data are transferred from the Union to controllers, processors or other recipients in third countries or to international organisations, the level of protection of natural persons ensured in the Union by this Regulation should not be un-

At a first glance, it would seem that EU law should regulate also the case of onward transfers, at least by equating the level of protection of re-transferred data to the one required for the first transfer operation. A closer look at other provisions of the GDPR, though, reveals that this is not really the case.

Indeed, art 45, dealing with transfers based on an adequacy decision, only refer to rules on onward transfers when identifying the elements that the Commission has to consider when assessing the level of protection afforded by a third country. In this context, rules on onward transfers are not provided by the EU but by the country of destination and they can only be scrutinised by the Commission in addition to other aspects of the adequacy assessment. This seems to imply that the country of destination's rules on onward transfers not necessarily have to provide the same level of protection of data of the one afforded by the EU, but they can contribute to the general assessment by the Commission as far as this level of protection is concerned. This, however, may also reduce the relevance that onward transfers regulations may have in the Commission's determinations, since they can be balanced with other aspect of the third country's national system of protection. This is particularly true as far as the nature of these rules is at stake. In fact, even if the level of protection shall be the *essentially equivalent* in the country of destination, this does not mean that the latter has to enact a legislation which is identical to that of the EU in order to meet such requirement.[25] Thus, one can assume that the norm does not prescribe the third country to regulate onward transfers of data in the same way as the EU regulates first transfer operations. The relevance of onward transfers in the adequacy assessment, however, seems confirmed by the practice of the Commission. In a number of cases, the latter has requested the third country to expressly regulate the case of onward transfers as a condition for receiving an adequacy determination. This is for instance the case for the Canada and United States adequacy decisions.[26]

---

dermined, including in cases of onward transfers of personal data from the third country or international organisation to controllers, processors in the same or another third country or international organisation'.

[25] In this sense see also *Schrems* (n 14) para 73.

[26] See Commission Decision (EC) 2002/2/EC pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data provided by the Canadian Personal Information Protection and Electronic Documents Act (notified under document number C(2001)4539) [2001] OJ L2/13; Commission Implementing Decision (EU) 2016/1250 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-US Privacy Shield (notified under document C(2016)4176) [2016] OJ L207. Some commentators have raised the issue of different treatment of countries concerned by

The regulation of onward transfers is even softer when the transfer operation is based on binding corporate rules (BCRs). In order to use BCRs as basis for data transfers, they must firstly be approved by the competent supervisory authority, according to the so called "consistency mechanism" provided by art 63 of the GDPR. In particular, BCRs must be legally binding on all members of the group, they must expressly confer enforceable rights to data subjects and they must fulfil the conditions set out in art 47, para 2, which includes the need for BCRs to specify "the requirements in respect for onward transfers to bodies not bound by the binding corporate rules".[27] Here we face a first shifting in the paradigm employed by the GDPR when dealing with onward transfers. In fact, in the case of transfers based on an adequacy decision, it seems that rules on onward transfers are those provided by the national legislation of the country of first destination. In a way, this can be conceived as an example of regulatory cooperation, in which bodies belonging to different jurisdictions exercise their regulatory power in a coordinate manner, in order to address a transnational phenomenon. Still, the regulation of onward transfers is always subject to the public intervention of the regulatory power. On the contrary, in the case of BCRs the discipline for onward transfers is left to the single company, although with a general oversight function attributed to european supervisory bodies.

This shift from a public to a private regulation approach is also visable with regard to model contract clauses as mentioned above as one of the basis for transferring data outside the Union according to art 46 of the GDPR. As already observed, these are model clauses to be inserted in a contract between two controllers (one of which is outside the EU) or between a controller and a non-EU processor and regulating the transfer of data in this context.

According to clause 5 of the Commission's model clauses on controller-to-controller transfers,[28] the importer undertakes to process the transferred

---

the adequacy assessment. While some of them have been offered an adequacy decision in exchange for certain amendments to their domestic legislation (as for rules on onward transfers) other countries have simply received a negative determination on adequacy. This approach, it has been claimed, may trigger the EU's responsibility for violation of WTO rules, in particular as far as the Most Favoured Nation clause is concerned. See in this regard Perry Keller, *European and International Media Law: Liberal Democracy, Trade and New Media* (Oxford 2011) 353; Carla L Reyes, 'WTO-Compliant Protection of Fundamental Rights: Lessons from the EU Privacy Directive' (2011) 12 Melbourne J of Intl L 1; Svetlana Yakovleva and Kristina Irion, 'The Best of Both Worlds? Free Trade in Services, and EU Law on Privacy and Data Protection' (2016) 2 Eur Data Protection L Rev 191.

[27] Art 47, para 2, let d) of the GDPR.

[28] Commission Decision (EC) 2001/497/EC, n 16, clause 5(b).

data in compliance with the mandatory requirements set forth by the Commission in Annex 2 and 3 of its Decision. Both these annexes, at principle 6, require that onward transfers from the importer to third parties (in a different country) are subject to various conditions. Data can be re-transferred only to countries which have received an adequacy assessment by the Commission. Should such a decision be lacking, re-transfers can only occur on the basis of 'unambiguous' consent of the data subject, although the exception only applies to special categories of data (such as sensitive ones).[29] The other option shows a further shift to relying increasingly on private parties' contractual regulation. The data importer can re-transfer data to a third country if the second importer agrees (with the consent of both the exporter and the original importer) to 'the adherence to the clauses of another controller which thereby becomes a party to the clauses and assumes the same obligations as the data importer'. Being the contract is a *res inter alios acta*, the second importer to which data have to be re-transferred cannot be held bound to the model clauses principles unless he becomes a party to the original contract itself or he stipulates a similar contract with the first importer. The 2004/5271 Commission decision amending the clauses for the transfer of data has specified some of the obligations of the importer in relation to onward transfers. According to clause II(i), the importer cannot proceed with an onward transfer unless "it notifies the data exporter about the transfer and:

i. the third party data controller processes the personal data in accordance with a Commission decision finding that a third country provides adequate protection, or

ii. the third party data controller becomes a signatory to these clauses or another data transfer agreement approved by a competent authority in the EU, or

iii. data subjects have been given the opportunity to object, after having been informed of the purposes of the transfer, the categories of recipients and the fact that the countries to which data is exported may have different data protection standards, or

[29] Data subjects have to receive a number of information in order to give their consent, including: 'the purposes of the onward transfer; the identification of the data exporter established in the Community; the categories of further recipients of the data and the countries of destination, and an explanation that, after the onward transfer, the data may be processed by a controller established in a country where there is not an adequate level of protection of the privacy of individuals'.

iv. with regard to onward transfers of sensitive data, data subjects have given their unambiguous consent to the onward transfer".[30]

No provision of this kind exists in relation to transfers between a controller and a processor. The latter only provides for certain obligations in the case of sub-processing contracts.[31]

It is certainly noteworthy that, intervening on the issue of model clauses between an EU controller and a non-EU controller, the Article 29 Working Party had suggested at the time not to insert any derogation for onward transfers, but simply to prohibit them. Such transfers would have been better addressed by a new contract between the EU-exporter and a different non-EU importer.[32]

4. BACK TO PUBLIC (INTERNATIONAL) LAW: THE CASE OF ONWARD TRANSFERS BETWEEN PUBLIC AUTHORITIES

While data transfers usually occur between private parties, the practice of data transfers between public authorities of different countries has sensitively expanded over the last decades. The phenomenon brings in a number of issues as far as derogation to privacy protection is concerned and the ex-

[30] See Commission Decision (EC) 2004/5271 (n 16) clause II(i).

[31] See Commission Decision (EC) 2010/87 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC of the European Parliament and of the Council (notified under document number C(2010)593), clause 11: 'The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the subprocessor which imposes the same obligations on the subprocessor as are imposed on the data importer under the Clauses. Where the subprocessor fails to fulfil its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the subprocessor's obligations under such agreement'. The reference to onward transfers has probably been excluded following the suggestion of the Article 29 Working Party in its 'Opinion 7/2001 on the Draft Commission Decision (version 31 August 2001) on standard contractual clauses for the transfer of personal data to data processors established in third countries under article 26(4) of Directive 95/46', WP 46 (13 September 2001).

[32] See Article 29 Working Party, 'Opinion 1/2001 on the Draft Commission Decision on Standard Contractual Clauses for the transfer of Personal Data to third countries under Article 26(4) of Directive 95/46', WP 38 final (26 January 2001) 4-5.

tent to which these derogations are legitimate under human rights law (including under the Charter of fundamental rights of the EU).[33] Even in this case, though, data do not simply move from one country to another to permanently be retained there, but they can be re-transferred to other public authorities in various jurisdictions for public enforcement or national security purposes.

Today, the GDPR provides for a specific legal basis in relation to cross-border data flows between public authorities. According to art 46 (2)(a), public sector data exchange may take place on the basis of an agreement between a public authority in the EU and a public authority in a third country without requiring a specific authorisation by a Data Protection Authority. Given the novelty introduced by the GDPR, no agreement of this kind is in place at the moment. Certainly, however, these agreements do not constitute international treaties and as such are subject to compliance with the GDPR and with general obligations regarding derogations from data protection rights. If one takes the standard of art 45, it seems that agreements between public authorities must provide for specific rules on onward transfers.

Besides this, EU law also provides a regulation for transfers of data within the area of freedom, security and justice (AFSJ). The framework decision 2008/977 allowed Member States to transfer data to public authorities of third countries only under certain requirements, namely that 'it is necessary for the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties' and 'when the third countries concerned provides safeguards which are deemed adequate by the Member State concerned according to its national law'.[34] The system established by

[33] See in particular art 52 of the EU Charter of Fundamental Rights, according to which '[a]ny limitation on the exercise of the rights and freedoms recognised by this Charter must be provided for by law and respect the essence of those rights and freedoms. Subject to the principle of proportionality, limitations may be made only if they are necessary and genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others'. See also Koen Lenaerts, 'Exploring the Limits of the EU Charter of Fundamental Rights' (2012) 8 Eur Constitutional L Rev 375; Steve Peers and Sacha Prechal, 'Article 52 – Scope and Interpretation of Rights and Principles', in Steve Peers and others (eds), *The EU Charter of Fundamental Rights. A Commentary* (Hart, Oxford 2014) 1455.

[34] See Council Framework Decision 2008/977/JHA on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters [2008] OJ L350/60, art 13. These rules apply both to criminal and to police cooperation with third countries' authorities (such as in the case of Europol). See Marco Borracetti, 'La collaboration entre Europol et Interpol: un parcours vers l'intégration?' in

the Directive 680/2016, which is going to repeal the Framework Decision, is far more complex. Be it sufficient to note that the mechanism is extremely similar to that enshrined in the GDPR, as it is centred both on an adequacy decision issued by the Commission and on an alternative basis such as that of a 'legally binding agreement' providing for adequate safeguards.[35] Article 35 of Directive 680/2016 further specifies that, even in the case of transfers based on an adequacy decision:

> the competent authority that carried out the original transfer or another competent authority of the same Member State authorises the onward transfer, after taking into due account all relevant factors, including the seriousness of the criminal offence, the purpose for which the personal data was originally transferred and the level of personal data protection in the third country or an international organisation to which personal data are onward transferred.

Notwithstanding such recently introduced possibilities, the EU has a wide practice in cooperation between public authorities, as it has concluded various international agreements for the purpose of data exchange between them. The first example is provided by international agreements on the exchange of Passenger Name Records (PNR), that is data information provided by passengers during the reservation and booking of tickets and when checking in on flights, as well as collected by air carriers for their own commercial purposes. Since these data can be used by enforcement agencies to prevent or combat serious crimes (including terrorism), the EU has concluded different PNR agreements for the exchange of such information. Some of them have

Catherine Flaesch-Mougin, Lucia Serena Rossi (eds), *La dimension extérierure de l'espace de liberté, de sécurité et de justice de l'Union européenne aprés le Traité de Lisbonne* (Bruylant, Bruxelles 2013) 333.

[35] See Directive (EU) 2016/680 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA [2016] OJ L119, arts 35-39. Although it is unclear whether the provision means that an international agreement between the Member State and the third country concerned must be in place. This solution seems to be excluded considering that art 39 of the Directive expressly acknowledges the case of data transfers on the basis of an international agreement between a Member State and a third country, and it implies that these agreements should comply with the Directive requirements (see in this regard also art 61).

undergone several developments, especially after the Court of Justice annulled the one concluded with the US in 2006[36] and declared the one concluded with Canada incompatible with EU fundamental rights in the recent Opinion 1/15 of July 2017.[37] In the latter, the Court made clear that agreement on exchange of data with third countries' authorities must be compatible with the standard of the EU Charter of fundamental rights, the same standard the Commission has to apply within the adequacy mechanism. Although no issue regarding onward transfers was raised in these proceedings, this does not mean that onward transfer operations are irrelevant in this context.

The recent EU-US PNR agreement, for instance, has a detailed position on onward transfers of PNR data to third countries, as it requires that such transfers 'shall occur pursuant to express understandings that incorporate data privacy protections [are] comparable to those applied' to the EU and the US by means of the agreement. The same is not true for other PNR agreements with third countries, such as those concluded with Australia and Canada.

Another example is to be found in the so called EU-US Umbrella Agreement, the aim of which is to enhance the exchange of personal data between the EU and the US in relation to the prevention, investigation, detection or prosecution of serious criminal offences, including terrorism.[38] Art 7 of the Umbrella agreement sets forth certain requirements for onward transfers, which are allowed only in so far as the original sending authority has consented to them. The first sending authority has to take into account whether the third country of destination of the onward transfer ensures 'an appropriate level of protection to personal information' and it may also request that the transfer be subjected to further conditions. These rules are to be read in conjunction with the principles enshrined in the agreement, covering any type of data transfer and especially that of the purpose limitation under art 6.[39] Interestingly, then,

---

[36] Case C-317/04 *Parliament v Council* EU:C:2006:346.

[37] Opinion 1/15 [2017] (n 11). See in particular paras 95-104, where the Court recognised that, given the close interconnection between crime prevention and data protection, the PNR agreement with Canada should be based on both art 16(1) and art 87(2) of the TFEU.

[38] See Council Decision (EU) 2016/2220 on the conclusion, on behalf of the European Union, of the Agreement between the United States of America and the European Union on the protection of personal information relating to the prevention, investigation, detection, and prosecution of criminal offences [2016] OJ L336. The purpose of the agreement is outlined in its art 1.

[39] Art 6(1) of the Agreement limits the transfer of personal information to "specific purposes authorized by the legal basis for the transfer (...)", while Article 6(5) adds that the processing must be conducted "in a manner that is directly relevant to and

art 7 also has an *external* consequence for the parties to the agreement. In fact, while the above-mentioned mechanism applies to single onward transfers in relation to a specific judicial case, in order to proceed with more general flows of data to third countries ('other than in relation to specific cases') in the form of onward transfers the parties have to conclude a separate international agreement with specific conditions and 'due justifications' for onward transfers operations.[40] This essentially entails a limitation of the parties' treaty-making power, so to ensure consistency of their international action in the field of criminal cooperation and, at the same time, not to elude the protection afforded originally by the Umbrella Agreement.

A softer regulation for onward transfer is to be found in the 2010 agreement on the processing and transfer of Financial Messaging Data from the European Union to the United States for the purposes of the Terrorist Finance Tracking Program. The possibility for the US to re-transfer data to other authorities in third countries or to international organisations is subject to the consent of the competent authority in one of the EU Member States, but only when the data belongs to an EU citizen or to an EU resident.

Other agreements on data exchange, however, do not entail any provision regulating onward transfer, as in the case of PNR agreements with third countries other than the US, such as those concluded with Australia and Canada. How is this silence to be interpreted? Does it mean that no restriction is imposed on onward PNR transfers or that, on the contrary, they are to be considered prohibited? As it is always difficult in international law to identify State's obligations in the case of silence in an international treaty,[41] the preferable solution seems to consider those agreements as allowing any kind of onward transfer with no restriction. However, this would certainly be incompatible with EU law and especially with the requirements under which derogations from fundamental rights such as privacy and data protection are considered legitimate. Recourse to international agreements in this context may

not excessive or overbroad in relation to the purposes of such processing". The protection is enhanced by the possibility under art 14(2) to discontinue the transfer when purpose limitation or onward transfer conditions are not complied with.

[40] EU-US Umbrella Agreement (n 38) art 7(3). The EDPS has warned against the risk of this situation as a potential case of bulk transfer of personal data. European Data Protection Supervisor, 'Opinion 1/2016, Preliminary Opinion on the agreement between the United States of America and the European Union on the protection of personal information relating to the prevention, investigation, detection and prosecution of criminal offences' (12 February 2016) 12.

[41] Cf. Helen Quane, 'Silence in International Law' (2014) 84 British Ybk Intl L 240; see also Anne Peters, 'Does Kosovo Lie in the Lotus-Land of Freedom' (2011) Leiden J of Intl L 95, 99.

of course be problematic, since rules enshrined therein cannot be extended to other countries and enforcement by individuals is always troublesome. These complexities could probably be overcome by means of a better and more precise drafting of rules on onward transfers in future agreements. What the practice shows, though, is that the EU has tried to influence the content of such agreements by following the patter of the adequacy mechanism, in order to extend its internal level of data protection to a potentially high number of third countries involved.

5. THEORY PUT INTO PRACTICE: A LOOK AT THE EU-US PRIVACY SHIELD

On 12 July 2016, the Commission has adopted a new adequacy decision for the transfer of data from the EU to the US, based on the legal framework provided in the US by the Privacy Shield.[42]

The Privacy Shield is not an international agreement, but – as the previous Safe Harbour – it is composed of a series of unilateral acts adopted by the Commission and by the US government aimed at regulating the transatlantic flows of data between private companies. It is composed of a number of principles to which US companies may voluntarily accede in order to obtain a certification by the US Federal Trade Commission and, consequently, to receive data collected in the territory of the EU.[43] Private companies undertaking the commitments enshrined in the Privacy Shield are also subject to various instruments of compliance and enforcement.

The Privacy Shield regulates the case of onward transfers by the "Accountability for Onward Transfers Pinciple". According to this principle, the US company wishing to re-transfer the data received from the EU to a third country has to conclude with the subsequent importer (a controller in this case) a contract by means of which the latter undertakes the obligation to use the data for a specific and defined purpose and to guarantee a level of protection equivalent to that provided by the Privacy Shield. Similar rules are provided when onward transfer occurs between a US company and an organisation acting as its agent in a third country, even if in this case a contractual *ad hoc* regime is not required.

---

[42] Commission Implementing Decision (EU) 2016/1250 (n 26).

[43] The choice of establishing a voluntary mechanism of certification is not in itself contrary to EU law, as recognised in *Schrems* (n 14) para 81. It is true that the voluntary acceptance of the principles is accompanied by the assurances offered to the EU by the US government, but this hardly could be considered as constituting an international obligation for the US themselves.

If one assumes that the level of protection afforded by the Privacy Shield is essentially equivalent to that of the EU – as acknowledged by the Commission – that same level is guaranteed to EU data transferred in third country through the Accountability for Onward Transfer Principle. However, this scenario shows a progressive shift in the nature of the sources used to afford such protection. The entire regime, in fact, is left to the contractual terms negotiated between the first receiver and the second one, with no mention as to the level of protection guaranteed by the national system of the third country involved in the onward transfer. Indeed, no adequacy assessment is deemed necessary in relation to subsequent third countries of destination,[44] being it sufficient to transit across the US via the collection by a US company. It is noteworthy that a system which originates in the regulatory power of the Commission (and the US government as well) such as the Privacy Shield turns in this case to the contractual capacity of private parties. This approach, which to a certain extent resembles the one followed for model clauses, has of course a number of consequences in terms of applicable law, responsibility and enforcement.

It is not unlikely to have a conflict between different regulations due to the fact that the processing of personal data in EU is subject entirely to EU law, while the Privacy Shield principles are considered as being part of US law. At the time of the Safe Harbour, for instance, some DPAs in Europe took the position that onward transfers from the US must still have a legal basis in EU Member States national law (and in the GDPR in the future) and have to comply with EU data protection rules, such as the proportionality requirement.[45] Today, principle 1(7) of the Privacy Shield makes clear that:

> US law will apply to questions of interpretation and compliance with the Principles and relevant privacy policies by Privacy Shield organizations, except where such organizations have committed to cooperate with European data protection authorities.

The statement, however, is not capable of solving all the issues arising from the potential clash of different applicable laws and this is especially so after the entry into force of the GDPR. The extended territorial reach of the Regulation, enshrined in its art 3, may in fact subject Privacy Shield organizations

[44] Marking a considerable difference with the discipline provided for transfers based on model contractual clauses.

[45] See in this regard Christopher Kuner, 'Onward Transfer of Personal Data under the U.S. Safe Harbour Framework' (2009) 7 Privacy and Security L Report 1, 4.

also to the regime of EU data protection law.[46] Furthermore, also third countries' organizations having received EU data by means of onward transfers may face an overlapping between the legal regime provided in the contract and the one set forth by EU law, provided that their activities fall within the territorial scope of application of the GDRP.[47]

Some of these problems have been overcome by the more detailed regulation of the Privacy Shield, whose rules on onward transfers must be read in conjunction with other Principles, such as the one on Notice and the one on Choice.[48] According to these provisions, data subjects can object the onward transfer and, in the case of sensitive data, their consent is required. Moreover, Principle 7 has also introduced a presumption of responsibility for US companies in cases of breaches of rules on onward transfers, although it is solely applicable to the case of onward transfers to third parties acting as agent of the US based organisation.[49]

The foregoing elements do not solve the issue of enforcement, which the Privacy Shield addresses by means of various instruments. All of them are based on the enforcement powers of different US agencies, but a role is reserved for EU DPAs, which can refer a complaint to the Federal Trade Commission or can investigate directly a complaint if it is related to human resources data collected in the context of an employment relationship or if the US company has voluntarily submitted to the oversight of the DPAs.

---

[46] On the territorial application of the GDPR see on this Paul De Hert and Michal Czerniawski, 'Expanding the European Data Protection Scope beyond Territory: Article 3 of the General Data Protection Regulation in its Wider Scope' (2016) 6 Intl Data Privacy L 230; Merlin Gömann, 'The New Territorial Scope of EU Data Protection Law: Deconstructing a Revolutionary Achievement' (2017) 54 CML Rev 567

[47] From the standpoint of EU enforcement procedures, the GDPR can be considered as enshrining overriding mandatory provisions in the sense of conflict of laws, which further complicates matters. See Maja Brkan, 'Data Protection and Conflict-of-Laws: A Challenging Relationship' (2016) 2 Eur Data Protection L Rev 324, 333-334.

[48] See Commission Implementing Decision (EU) 2016/1250 (n 26) recital 22.

[49] See Commission Implementing Decision (EU) 2016/1250 (n 26) Annex II, EU-U.S. Privacy Shield Framework Principles Issued by the U.S. Department of Commerce, Principle 7(d): 'In the context of an onward transfer, a Privacy Shield organization has responsibility for the processing of personal information it receives under the Privacy Shield and subsequently transfers to a third party acting as an agent on its behalf. The Privacy Shield organization shall remain liable under the Principles if its agent processes such personal information in a manner inconsistent with the Principles, unless the organization proves that it is not responsible for the event giving rise to the damage'.

A separate issue, which has gained attention after the adoption of the Privacy Shield, is that of the applicable legal framework to onward transfer of data that are subsequently accessed by third countries' public authorities. The scenarios can be different: first, a US organization may re-transfer data to private companies in third countries which do not provide strict rules on access to data by public authorities; alternatively, there can be situations in which a US agency accedes data transferred by the EU to a US company and then re-transfers those data to a third country agency, in the framework of a judicial or intelligence cooperation mechanism.

A far as the first scenario is concerned, according to the Article 29 WP, rules on onward transfers are applicable as well, and they would oblige the US organization willing to re-transfer EU data, to take into account not only the general level of protection, but also domestic rules on access to data by public agencies and to evaluate the risk to which data subjects are exposed due to the onward transfers.[50]

Far more complex is the second situation, in which a US public agency transfers data received by a US private company on the basis of the Privacy Shield to a foreign administration. In this context, the onward transfer occurs entirely between public authorities, but the original collection and transfer have been realized between private parties. One could maybe rely on the rules on onward transfers provided in the already mentioned EU-US Umbrella Agreement, although this would require an application by analogy, given that the data have not been originally transferred by a EU public authority. Moreover, it is unclear whether the Umbrella Agreement covers also exchange of data for intelligence purposes or is instead limited – as it seems – only to judicial assistance.

6. CONCLUDING REMARKS: IS THERE A CASE FOR TRANSNATIONAL PRIVATE REGULATION?

Onward transfers are at the centre of global data flows, which are amongst the major enabler of international commerce. The regulation of such a complex and wide phenomenon can be extremely challenging for single national regulators, as their activity could not be able to take into consideration all possible scenarios in which onward transfers occur and it also risks encroaching upon other countries' regulatory powers and jurisdiction. In this context, it is perfectly understandable for a regulatory power such as that of

[50] Article 29 Working Party, 'Opinion 01/2016 on the draft EU-U.S. Privacy Shield adequacy decision', WP 238 (13 April 2016) para 2.2.3.

the EU to rely on private agreements by simply fixing the minimum requirements and limits to the contractual freedom of the parties involved.

The reliance on private law instruments in order to guarantee that the level of data protection ensured by the EU does not fade or diminish in subsequent transfer of data seems to constitute a remarkable example of transnational private regulation.[51] The relationship between the two system of rules – the public and the private – is not necessarily one of competition. Quite the opposite, transnational private regulation can be complementary to public regulation and it needs a public regulation to be effective.[52]

In the context of onward transfers, the necessity for public regulation to delegate certain elements to private contractual relationships seems today inevitable.[53] The shift from a public to a private regulation allows in fact for more flexibility and for enhanced adaptability of legal sources to such a complex scenario, whereby clashes of jurisdictions (in the sense of legislative power) risk creating a legal *vacuum* or a conflict of obligations.

At the same time, public law needs to be clear and effective in identifying and regulating the spaces left to contractual autonomy. This will not always be an easy task, as shown in the case of the Privacy Shield Framework. The public regulator is in fact dealing with a subject matter having profound connections with fundamental rights protection, an element which raises the standard applicable to operations involving different jurisdictions and which does not allow for extensive derogations. The degree of flexibility guaranteed by transnational private regulation can constitute a viable solution, provided that certain guarantees are in place. Indeed, the features of this complex contractual network can have negative consequences on legal certainty and the effectiveness of redress mechanism. It is thus upon the different public regulators not only to adopt clear-cut substantive standards, but also to set up effective and transparent mechanisms of enforcement, with the aim of protecting those

---

[51] See Fabrizio Cafaggi, 'New Foundations of Transnational Private Regulations' (2010) European University Institute Working Papers 53, <http://cadmus.eui.eu/handle/1814/15284>; Fabrizio Cafaggi, 'The Regulatory Functions of Transnational Commercial Contracts New Architectures' (2013) 36 Fordham Intl L J 1557; Sandrine Clavel, 'The Challenges of Transnational Contractual Enforcement: the Relative Merits of Arbitration and State Courts Litigation' in Hans-W. Micklitz, and Andrea Weschler (eds), *The Transformation of Enforcement. European Economic Law in Global Perspective* (Hart, Oxford 2016) 303-305.

[52] Cafaggi, 'New Foundations of Transnational Private Regulations' (n 51).

[53] Such a solution was even suggested at the time the Safe Harbour was in force. See Kuner (n 45).

standards even through an institutionalised cooperation between different public authorities.

7. SELECTED LITERATURE

Andrejvic M and Gates K, 'Big Data Surveillance: Introduction' (2014) 12 Surveillance and Society 185

Bender D and Ponemon L, 'Binding Corporate Rules for Cross-Border Data Transfers' (2006) 3 Rutgers J of L and Urban Policy 154

Borracetti M, 'La collaboration entre Europol et Interpol: un parcours vers l'intégration?' in Flaesch-Mougin C and Rossi LS (eds), *La dimension extérierure de l'espace de liberté, de sécurité et de justice de l'Union européenne aprés le Traité de Lisbonne* (Bruylant, Bruxelles 2013)

Brkan M, 'Data Protection and Conflict-of-Laws: A Challenging Relationship' (2016) 2 Eur Data Protection L Rev 324

Cafaggi F, 'New Foundations of Transnational Private Regulations' (2010) European University Institute Working Papers 53, <http://cadmus.eui.eu/ handle/1814/15284>

Cafaggi F, 'The Regulatory Functions of Transnational Commercial Contracts New Architectures' (2013) 36 Fordham Intl L J 1557

Clavel S, 'The Challenges of Transnational Contractual Enforcement: the Relative Merits of Arbitration and State Courts Litigation' in Micklitz H-W and Weschler A (eds), *The Transformation of Enforcement. European Economic Law in Global Perspective* (Hart, Oxford 2016)

Davenport TH, Barth P and Bean R, 'How 'Big Data' is Different' (2012) 54 MIT Sloane Management Rev 22

De Hert P and Papakonstantinou V, 'The Council of Europe Data Protection Convention reform: Analysis of the new text and critical comment on its global ambition' (2014) 30 Computer L and Security Rev 633

De Hert P and Czerniawski M, 'Expanding the European Data Protection Scope beyond Territory: Article 3 of the General Data Protection Regulation in its Wider Scope' (2016) 6 Intl Data Privacy L 230

Esteve A, 'The Business of Personal Data: Google, Facebook, and Privacy Issues in the EU and the USA' (2017) 7 Intl Data Privacy L 36

Fuster GG, *The Emergence of Personal Data Protection as a Fundamental Right of the EU* (Heidelberg, Springer 2014)

Gömann M, 'The New Territorial Scope of EU Data Protection Law: Deconstructing a Revolutionary Achievement' (2017) 54 CML Rev 567

Gonçalves ME, 'The EU Data Protection Reform and the Challenges of Big Data: remaining Uncertainties and Ways Forward' (2017) 26 Information & Communications Technology L 90

Gonzàles JL and Jouanjean M-A, 'Digital Trade: Developing a Framework for Analysis' in *OECD Trade Policy Papers no. 205* (OECD Publishing, Paris, 2017)

Keller P, *European and International Media Law: Liberal Democracy, Trade and New Media* (Oxford 2011)

Kokott J and Sobotta C, 'The distinction between privacy and data protection in the jurisprudence of the CJEU and the ECtHR' (2013) 3 Intl Data Privacy L 222

Kshetri N, *The Quest to Cyber Superiority* (Heidelberg, Springer 2016)

Kuner C, 'Onward Transfer of Personal Data under the U.S. Safe Harbour Framework' (2009) 7 Privacy and Security L Report 1

Lenaerts K, 'Exploring the Limits of the EU Charter of Fundamental Rights' (2012) 8 Eur Constitutional L Rev 375

Lyon D, 'Surveillance, Snowden and Big Data: Capacities, Consequences, Critique' (2014) 1 Big Data & Society 1

McKinsey Global Institute, *Digital Globalization: The New Era of Global Flows* (Report) (2016), <https://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/digital-globalization-the-new-era-of-global-flows>

Pan SB, 'Get to Know Me: Protecting Privacy and Autonomy under Big Data's Penetrating Gaze' (2017) 30 Harvard J of L and Technology 239

Peers S and Prechal S, 'Article 52 – Scope and Interpretation of Rights and Principles', in Peers S and others (eds), *The EU Charter of Fundamental Rights. A Commentary* (Hart, Oxford 2014)

Peng S, 'Cybersecurity Threats and the WTO National Security Exceptions' (2015) 18 J of Intl Economic L 449

Peters A, 'Does Kosovo Lie in the Lotus-Land of Freedom' (2011) Leiden J of Intl L 95

Quane H, 'Silence in International Law' (2014) 84 British Ybk Intl L 240

Reyes CL, 'WTO-Compliant Protection of Fundamental Rights: Lessons from the EU Privacy Directive' (2011) 12 Melbourne J of Intl L 1

Svantesson D and Clarke R, 'Privacy and Consumer Risks in Cloud Computing' (2010) 26 Computer L and Security Rev 391

Yakovleva S and Irion K, 'The Best of Both Worlds? Free Trade in Services, and EU Law on Privacy and Data Protection' (2016) 2 Eur Data Protection L Rev 191

Following the digital footprints of airline passengers

An assessment of the EU-US PNR Agreement with respect to the EU right to privacy and data protection

ELIF MENDOS KUŞKONMAZ[1]

Since the attacks in the US on 11 September 2001, states have become troubled with the convergence of border controls and the fight against terrorism. At the heart of this convergence, the lust for information about people who cross borders (particularly those who travel by air transportations) has increased exponentially. The agreement signed between the EU and the US on the transfer of information about air passengers and the use of information is the result of this lust**.** This agreement has been promoted as a valuable tool for the co-operation between the EU and the US in the fight against terrorism. That said, and as demonstrated by the case-law of the Court of Justice of the European Union on privacy-intrusive measures taken in that fight, concerns over the compatibility of the relevant agreement with EU fundamental rights, particularly with the right to privacy and personal data protection, have arisen. This article aims to reflect on those concerns.

1. INTRODUCTION

The EU-US Passenger Name Records Agreement is an agreement signed between the EU and the US that obliges air carriers flying to the US to provide information about their passengers to the US border control authority, ie the US Department of Homeland Security (DHS).[2] These data, known as the Passenger Name Records (PNR), are records in air carriers' reservation systems and contain information about the passengers' travel.[3] They are gathered principally by air carriers for their own commercial and operational purposes

[1] PhD researcher and graduate teaching assistant, Queen Mary University of London. Email: e.m.kuskonmaz@qmul.ac.uk.

[2] Agreement between the United States of America and the European Union on the use and transfer of passenger name record to the United States of Department of Homeland Security [2012] OJ L 215/5 (EU-US PNR Agreement).

[3] International Civil Aviation Organization, 'Guidelines on Passenger Name Record (PNR) Data' (Doc 9944 ICAO 2010) <https://www.iata.org/iata/passenger-data-toolkit/assets/doc_library/04-pnr/New%20Doc%209944%201st%20Edition%20PNR.pdf>.

in relation to air transportation services.[4] Passengers provide some information to the air carriers when they book a flight, whilst travel agencies and tour operators can also enter information on a passenger's record without the knowledge of the passenger.[5] The PNR data can contain up to sixty data fields in which separate pieces of information are included ranging from the passengers' name and addresses to e-mail addresses, means of payment, on-flight dietary requirements, and to the need for special assistance, eg a wheelchair.[6]

This Agreement came into force on 1 July 2012 and is due to expire in seven years. However, the pathway towards its conclusion started from the terrorist attacks in the US on 11 September 2011, as a result of which the US legislature adopted legislation on the obligation of air carriers to provide the US Customs and Border Protection (CBP) – a component of the DHS, with the PNR data.[7] This legislation overlapped with the EU rules on privacy and personal data protection, which prohibited the transfer of personal data to a third country unless that country provided an adequate level of protection of personal data as guaranteed in the EU.[8] Moreover, passengers who are not US citizens and whose data had been transferred did not have privacy rights under the legislation in the US in general.[9]

---

[4] ibid.

[5] ibid.

[6] European Union Committee, *The EU/US Passenger Name Record (PNR) Agreement* (HL 2006-7) 9.

[7]Aviation and Transportation Security Act of 19 November 2001 (107-71), Interim Rules of Department of Treasury (Customs) – Passenger and Crew Manifests Required for Passenger Flights in Foreign Air Transportation to the United States (Federal Register, 31 December 2001) and Passenger Name Record Information Required for Passengers on Flights in Foreign Air Transportation to or from the United States (Federal Register, 25 June 2002).

[8] Directive 95/46/EC of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1995] OJ L 281 (The Data Protection Directive), Article 25. This Directive is in the process of being replaced by the General Data Protection Directive (GDPR), which comes in effect in all Member States by 25 May 2018. In addition to the GDPR, a new directive is introduce in relation to the processing of personal data by law enforcement authorities. Just like the GDPR, this Directive provides rules on the transfer of personal data to a third country. GDPR, art 45.

[9] Fourth Amendment protection does not cover non-US citizens who are not US resident. See Fransizka Boehm, 'A Comparison between US and EU Data Protection Legis-

As a result, an agreement on the transfer of PNR data was concluded between the EU and US on 28 May 2004[10], but it was annulled on 30 May 2006 by the then named European Court of Justice on the procedural ground that it was adopted on a wrong legal basis.[11] This Agreement was followed by an interim agreement[12], and a follow-up agreement signed on 23 July 2007, which was not ratified due to the changes made to the EU procedure for the conclusion of international agreement.[13]

The arguments in support of these agreements have hinged on their contribution in the fight against terrorism and serious transnational crime as part of border controls.[14] However, each PNR agreement with the US has been mired with criticisms over their incompliance with EU fundamental rights of privacy and protection of personal data.[15] Those criticisms reached their

lation for Law Enforcement', (Study for the LIBE Committee, 2015), <http://www.europarl.europa.eu/RegData/etudes/STUD/2015/536459/IPOL_STU%282015%29536459_EN.pdf>.

[10] Agreement between the European Community and the United States of America on the processing and transfer of PNR data by air carriers to the United States Department of Homeland Security, Bureau of Customs and Border Protection [2004] OJ L 142 M.

[11] Joined Cases Case C-317/04 and C-318/04 *European Parliament v Council of the European and European Parliament v Commission of the European Communities*) [2006] ECR I-4721, Press Release No. 46/06, 30 May 2006, <http://curia.europa.eu/jcms/upload/docs/application/pdf/2009-02/cp060046en.pdf >.

[12] Agreement between the European Union and the United States of America on the Processing and Transfer of Passenger Name Record (PNR) data by air carriers to the United States Department of Homeland Security [2006] OJ L 298/27.

[13] Agreement between the European Union and the United States of America on the processing and transfer of Passenger Name Record (PNR) data by air carriers to the United States Department of Homeland Security (DHS) [2007] OJ L 204/16.

[14] Kristin Archick, 'US-EU Cooperation against Terrorism' (Congressional Research Service for Congress, 2013).

[15] Elspeth Guild and Evelien Brouwer, 'The Political Life of Data: The ECJ Decision on the PNR Agreement between the EU and the US' (CEPS No. 109, July 2006); Paul De Hert and Rocco Bellanova, Transatlantic Cooperation on Travellers' Data Processing: From Sorting Countries to Sorting Individuals, (Washington DC, Migration Policy Institute, 2011); Gerrit Hornung and Franziska Boehm, 'Comparative Study on the 2011 draft Agreement between the United States of America and the European Union on the use and transfer of Passenger Name Records (PNR) to the United States Department of Homeland Security' (Passau/Luxembourg, 14 March 2012) <http://www.greens-efa.eu/fileadmin/dam/Documents/Studies/PNR_Study_final.pdf>; Cian Murphy, *The EU Counter-Terrorism Law: Pre-Emption and the Rule of Law* (Hart Publishing 2015).

peak following the judgment by the Court of Justice of the European Union (CJEU) on the Canadian version of the PNR data transfer agreement, of which certain provisions were found falling short of protecting the mentioned rights by the Court.[16] This article seeks to discuss whether the EU-US PNR Agreement is in line with the Court's finding in this judgment in particular, and with its case-law on privacy and data protection rights constraining measures to fight against terrorism and serious transnational crime in general.[17] The main argument advanced in this article is that the transfer of PNR data of all passengers flying to the US, regardless of their criminal background, falls short of respecting EU fundamental rights of privacy and data protection, just as the indiscriminate retention and the use of those data does. To support this argument, this article starts with delineating the key provisions of the EU-US PNR Agreement, followed by a brief illustration on how the PNR data are maintained in the US once they are transferred in accordance with this Agreement. It concludes with the assessment of the relevant articles of the Charter of the Fundamental Rights of the European Union (Charter) as interpreted by the CJEU.

2. A BRIEF SCOPE OF THE EU-US PNR AGREEMENT

The EU-US PNR Agreement consists of 27 provisions, of which only its key provisions are considered in this section. According to its preamble, the objective of the EU-US PNR Agreement is to prevent and combat terrorist offences and transnational crime while respecting the fundamental rights of privacy and of the protection of personal data.[18] The Agreement is structured

---

[16] Opinion 1/15 of the Court (Grand Chamber) *Opinion on the Draft agreement between Canada and the European Union – Transfer of Passenger Name Record data from the European Union to Canada* [2017] ECLI:EU:C:2017:592 (ECJ, 26 July 2017). It is important to note here that the agreement with Canada on the PNR data transfer has been considered as less detrimental to privacy and data protection rights. Peter Hobbing, 'Tracing Terrorists: The EU-Canada Agreement in PNR Matters', (CEPS, September 2008) <http://aei.pitt.edu/11745/1/1704.pdf>.

[17] Joined Cases C-293/12 and C-594/12 *Digital Rights Ireland v The Minister for Communications, Marine and Natural Resources and Others* EU:C:2013:845; Case C-362/*14 Maximillian Schrems v Data Protection Commissioner* EU:C:2015:650; Joined Cases C-203/15 *Tele2 Sverige AB v Post- och telestyrelsen* and C-698/15 *Secretary of State for the Home Department v Watson et al.* EU:C:2016:970.

[18] Preamble, EU-US PNR Agreement ('Determined to prevent and combat terrorist offences and transnational crime, while respecting fundamental rights and freedoms and recognising the importance of privacy and the protection of personal data and information').

around the purposes for which the PNR data can be collected, used, and processed by the DHS. These purposes are 'preventing, detecting, investigating, and prosecuting (a) terrorist offences and related crimes' and (b) 'crimes that are punishable by a sentence of imprisonment of three years or more and that are transnational in nature.'[19] It also provides for carrying out the mentioned conducts beyond the purpose of fighting against terrorist offences and serious transnational crimes as defined above such as 'on a case-by-case basis where necessary in view of a serious threat and for the protection of vital interests of any individual or if ordered by a court'[20] and in relation to 'identify persons who would be subject to closer questioning or examination upon arrival to or departure from the United States or who may require further examination.'[21]

The Agreement allows for the transfer of 19 data categories, under which up to 34 data elements can be sent.[22] It allows for up to fifteen-years retention period, which is divided into five-years retention period in an active database and a maximum period of ten-years retention period in a dormant database whose access is subject to stringent rules.[23] At the end of the latter period, the data are fully anonymised, but not deleted.[24]

3. WHAT HAPPENS TO THE PNR DATA IN THE US?

The fate of the PNR data in the US starts with their maintenance in a computerised system called Automated Targeting System, which is operated by the CBP.[25] There are public disclosures such as systems of notice records published by the CBP in accordance with the Privacy Act, and Privacy Impact Assessments published by the chief privacy officer of the DHS, which is the chief agency of the CBP. Based on what has been disclosed as of March 2017, ATS-

[19] EU-US PNR Agreement, art 4.

[20] ibid art 4(2).

[21] ibid art 4(3).

[22] ibid annex.

[23] ibid art 8.

[24] ibid art 8(4).

[25] DHS Office of the Secretary, System of Records - Notice of Privacy Act System of Records, 2 November 2006, vol 77, No. 100 <https://www.gpo.gov/fdsys/pkg/FR-2012-05-23/html/2012-12395.htm>.

UPAX is an expansive system accessible from different locations and by officers either of CBP or of DHS.[26] This system scrutinises a large volume of data for every person, cargo, vehicle that crosses the US borders.[27] This system has five sub-systems and the PNR data are processed in its component called, Automated Targeting System-Unified Passenger Module (or ATS-UPAX).[28]

ATS-UPAX processes the PNR data automatically in two ways: comparison and risk assessment.[29] The aim of the comparison functionality is to identify individuals featuring in watch lists, having criminal records or warrants.[30] The risk assessment focuses on identifying passengers who pose a greater risk for security than others but who are not known by the DHS.[31] Any flagging up of risky passenger is signalled to the CBP officers who check whether such passenger should undergo further inspections or should be allowed in the US.[32] The risk assessment is performed by way of running the PNR data against the risk-based rules, which in technical terms are algorithms, designed to target passengers that pose a risk to the US security. Information about what the instructions (ie algorithms) encompass to fulfil this task is not public due to national security concerns.[33] In light of the general information on how data analysis is carried out, educated guesses on those algorithms can be made: the algorithms run against the PNR data encompasses historical data, which in the case of the fight against terrorism and serious transnational crime might encompass the information relating to previous terrorist attacks,

---

[26] CBP, US Customs and Border Protection Passenger Name Record (PNR) Privacy Policy (21 June 2013) <https://www.dhs.gov/sites/default/files/publications/pnr_privacy_0.pdf>; DHS/CBP, Privacy Impact Assessment for the Automated Targeting System, DHS/CBP/PIA-006(a), (1 June 2012) 6.

[27] DHS/CBP, 'PIA 2012' (n 25) 2.

[28] DHS Privacy Office, 2015 Data Mining Report to Congress (February 2016) <https://www.dhs.gov/sites/default/files/publications/2015%20Data%20Mining%20Report%20FINAL.pdf.>.

[29] Commission, Report on the joint review of the implementation of the Agreement between the European Union and the United States of America on the processing and transfer of Passenger Name Record (PNR) data by air carriers to the United States Department of Homeland Security (DHS) (Brussels, 7 April 2010) <http://www.statewatch.org/news/2010/apr/eu-usa-pnr-joint-review-com.pdf> 14.

[30] ibid.

[31] ibid.

[32] The DHS Privacy Office, 'Data Mining Report of 2015' (n 27) 20.

[33] European Union Committee (n 5) 11-12 on the lack of information on the value of the PNR data.

their perpetrators, previous convictions and arrests, previous reports on possible terrorist and criminal activities, and travel and behaviour patterns attributed to terrorist and criminal activities.[34]

The crux of the use of PNR data lies in the risk assessment functionality. This is because if the emphasis was on the identification of people who are in the watch-lists, this could be done with other less controversial information sources such as Advanced Passenger Information (API) data, which refers to the data contained in the machine-readable part of passports such as the name, gender, date of birth, nationality and the passport number of passengers.[35] Therefore, the impetus behind utilising PNR data as part of security checks and borders controls is to trawl through those data to reveal the behavioural and travel patterns of passengers, and to match these patterns to those indicative of participation in terrorism or serious transnational crime.[36] This practice is at the heart of the controversies surrounding the use of PNR data in the fight against terrorism and serious transnational crime.[37]

4. ISSUES WITH RESPECT TO EU FUNDAMENTAL RIGHTS OF PRIVACY AND PERSONAL DATA PROTECTION

To say that the EU-US PNR Agreement triggers many issues with regards to EU privacy and personal data protection is not a premature judgment because it allows the systematic transfer, retention, and use of wide array of information about individuals (ie PNR data), regardless of whether suspicion has fallen upon them. In fact, the CJEU's opinion of July 2017 on the transfer of PNR data to and their use by the Canadian border control authority for the fight against terrorism is illustrative in understanding some of these issues.[38] In this opinion, the CJEU held that the agreement with Canada on the PNR data transfers could not be concluded in its current form because certain provisions were incompatible with EU fundamental rights. This opinion is of particular importance to assess the legality of the EU-US PNR Agreement because both agreements have similar functions.

---

[34] For the explanation on how data analysis is carried out by trawling through a vast amount of data (ie data mining) see: Toon Calders and Bart Custers, 'What is Data Mining and How does It Work?' in Bart Custers et al. (eds), *Discrimination and Privacy in the Information Society* (Springer 2013) 27-42, 48.

[35] De Hert and Bellanova (n 14) 6

[36] ibid; European Union Committee (n 5) 10-11.

[37] De Hert and Bellanova (n 14).

[38] Opinion 1/15 (n 15).

At the outset, one should set the scene for the EU fundamental rights of privacy and of data protection. In the EU, fundamental rights of privacy and personal data protection are guaranteed under a solid legal framework.[39] The right to privacy is guaranteed under Article 8 of the European Convention on Human Rights (ECHR) and under Article 8 of the Charter. Personal data protection originated from the jurisprudence of the European Court of Human Rights (ECtHR) when dealing with Article 8 of the European Convention on Human Rights and it is recognized as a fundamental right under Article 8 of the Charter.[40] This framework requires any privacy-intrusive practices for countering terrorism to be in line with legislative standards of the EU on the right to privacy and personal data protection.[41] For the sake of brevity, this section is limited to the relevant rights as enshrined in the Charter and interpreted by the CJEU.[42]

[39] For a comparison of different legal frameworks for right to privacy in the US and in the Europe see: Stefan Sottiaux*, Terrorism and Limitation of Right the ECHR and the US Constitution* (Hart Publishing 2008) 266-268.

[40] The relation between the right to privacy and protection of personal data at the EU level is outside the scope of this article. It is sufficient to say here that with its *Digital Rights Ireland and Schrems* decisions, the CJEU clarified that insofar as surveillance measures are concerned, data protection is not a self-standing right. Bart van der Sloot, 'Legal Fundamentalism: Is Data Protection Really a Fundamental Right' in Ronald Leenes et al. (eds), *Data Protection and Privacy: (In)visibilities and Infrastructures* (Springer 2017) 5; Antoinette Rouvroy and Yves Poullet, 'The Right to Informational Self-Determination and the Value of Self-Development: Reassessing the Importance of Privacy for Democracy' in Serge Gutwirth et al (eds), *Reinventing Data Protection* (Springer, 2009)43-76; Cf Paul De Hert and Serge Gutwirth, 'Privacy, Data Protection and Law Enforcement. Opacity of the Individual and Transparency of Power' in Erik Clased et al (eds), *Privacy and Criminal Law* (Intersentia 2006); Paul De Hert and Serge Gutwirth, 'Data Protection in the Case Law of Strasbourg and Luxembourg: Constitutionalisation in Action' in Serge Gutwirth et al (eds), *Reinventing Data Protection* (Springer 2009) 3-44; Maria Tzanou, 'Data Protection as a Fundamental Right Next to Privacy? 'Reconstructing' a not so new right' [2013] 3 International Data Privacy Law 88; Orla Lynskey, *The Foundations of EU Data Protection Role* (OUP 2015).

[41] Murphy (n 14) 149-150.

[42] It is sufficient to note here that the CJEU's case-law on privacy and data protection rights constraining measures in the context of the fight against terrorism has developed in light of the ECtHR's case-law on the matter due its constitutional constraint enshrined in Article 6 of the Treaty on European Union.

There is a line of decisions by the CJEU demonstrating the Court's rejection of systematic and indiscriminate transfer, retention, and use of personal information relating to individuals.[43] Amongst these decisions, *Digital Rights Ireland*, which dealt with the general retention of data of users of communications services, set the scenery for the relevance of the retention and access to personal data.[44] The Court noted that the retention of such data and their later access by public authorities 'directly and specifically affects' the right to privacy enshrined in Article 7 of the Charter because it

> may allow very precise conclusions to be drawn concerning private lives of the persons whose data has been retained, such as the habit of everyday life, permanent or temporary places of residence, daily or other movements, the activities carried out, the social relationships of those persons and the social environments frequented by them.[45]

In relation to the right to personal data protection guaranteed under Article 8 of the Charter, the Court observed that the retention of relevant data was a processing of personal data within the meaning of that Article, and thus, such retention fell within its protective ambit.[46] These points were reiterated in the CJEU's *Tele2*, which concerned the general retention of data reminiscent of that was brought before the Court in *Digital Rights Ireland*.[47]

Then, in Opinion 1/15, the Court had the chance to deal with the relevance of PNR data for the privacy and protection of personal data. The argument raised by the European Parliament was in line with the Court's *Digital Rights Ireland* and *Tele2* decisions, the latter being concerned with the communication's data (ie source of communication and its destination; date, time, duration, and type of communication; user's communication equipment; location of that equipment, data relating to the caller, the user).[48] That argument was that the use of PNR data 'may allow very precise conclusions to be drawn concerning the private lives of the persons whose PNR data is processed, such as their permanent or temporary places of residence, their movements and their

---

[43] *Digital Rights Ireland* (n 16); *Schrems* (n 16) , *Tele2* (n 16).

[44] *Digital Rights Ireland* (n 16).

[45] ibid, para 27.

[46] ibid, para 33.

[47] *Tele2* (n 16).

[48] *Digital Rights Ireland* (n 16) para 26.

activities.'[49] Nevertheless, the Court neither rejected nor denied this argument and held that the PNR data included information relating to identified or identifiable individuals, and thus the transfer, use, and retention of the relevant data felt within the protective ambit of art 7 of the Charter.[50] This gives the impression that the Court did not consider the effect of the PNR data on the right to privacy as strong as the retention of and access to communications data. This might be due to the difference in the nature of the relevant data, though the Court did not explicitly refer to any such difference in its opinion. The contention of this article is that the EU-US PNR Agreement affects the right to privacy guaranteed under the Charter not only because the use of the PNR data reveals information about individuals, but also such use can produce new information relating to them on the basis of the automatic analysis of those data.[51]

As for the relevance of art 8 of the Charter, from its *Digital Rights Ireland* decision forwards, the Court has been of the opinion that and the transfer, use, and retention of PNR data constituted processing of personal data, and therefore felt within the scope of the given Article.[52] The same conclusion can be drawn for the EU-US PNR Agreement as well.

4.1. Determining the necessity of using PNR data in the fight against terrorism and serious transnational crime

According to the case-law of the CJEU, a finding of interference with the right to privacy and data protection rights seems straightforward. The mere retention of personal data, access to them, and their disclosure to public authorities amount to interference with the right to privacy enshrined under art 7 of the Charter, regardless of whether the private lives of individuals concerned are affected by the mentioned conducts.[53] Furthermore, in relation to the existence of an interference with the right to personal data protection laid down

[49] Opinion 1/15 (n 15) para 36.

[50] ibid, paras 21-122

[51] When deciding on the nature of the interference caused by the Agreement to Article 7, the Court did not elaborate further on the issue of whether that interference was of a serious nature. Opinion 1/15 (n 15) para 131. ('Thus, such processing may provide additional information on the private lives of air passengers').

[52] *Digital Rights Ireland* (n 16); *Schrems* (n 16); *Tele2* (n 16).

[53] *Digital Rights Ireland* (n 16) paras 33-35.

in art 8 of the Charter, the Court considers that any measure constituting processing of personal data within the meaning of that article amounts to an interference with it.[54]

These interference findings were reiterated in the Court's Opinion 1/15 in which the Court held that the transfer of PNR data from the EU to the Canadian authorities, their subsequent retention, and transfer to other authorities, including to authorities in third countries, interfered with art 7 of the Charter.[55] Along the same line, as these operations constitute data processing within the meaning of art 8 of the Charter, the relevant article amounted to an interference with the right to personal data protection under that article.[56] The same interference findings in relation to privacy and data protection rights enshrined under the mentioned Articles can be made for the EU-US PNR Agreement.

After establishing an interference, the compatibility question boils down to whether that interference is permissible in the context of the fight against terrorism and serious transnational crime. The CJEU has been asked about this question in *Digital Rights Ireland, Tele2*, *Schrems*, and finally in Opinion 1/15. This article dwells upon this question starting from the CJEU's latest judgment.

At the outset, the CJEU held that the transfer of personal data to a third country was justified if that third country offers a level of fundamental rights protection that is essentially equivalent to that afforded in the EU.[57] In relation to this, it noted that the interferences with the right to privacy and personal data protection must be justified.[58] To this end, the interference must be in line with the principle of proportionality and must be strictly necessary to achieve the objective it pursues.[59] This strict necessity requirement encompasses the need for 'clear and precise rules governing the scope and application of the measure in question and imposing minimum safeguards'[60] and

[54] *Digital Rights Ireland* (n 16) para 35.

[55] Opinion 1/15 (n 15) para 125.

[56] ibid, para 126.

[57] Opinion 1/15 (n 15) para 134.

[58] ibid, paras 136-139.

[59] ibid, para 140.

[60] ibid, para 141.

particularly for the indications of circumstances and conditions for the adoption of data processing measure.[61] After highlighting these strict necessity requirements, the Court moved on to questioning whether the legal basis for the processing of personal data existed. At this point, the Court noted that passengers' consent could not qualify as such basis because that consent was originally provided for the reservation purposes rather than for the transfer to Canada.[62] Having found that the relevant agreement constituted such legal basis within the meaning of Charter, it considered whether there is an objective general interest justifying the interference caused by the Agreement and noted that the fight against terrorism and serious transnational crime was an objective as such.[63]

Until this point, the same conclusions can be drawn for the EU-US PNR Agreement: the passengers' consent cannot justify the processing of personal data, only the objective of the fight against terrorism and serious transnational crime can.[64] Yet, there are issues that need further attention in relation to that objective. In its Opinion 1/15, before dealing with the justification question, the Court noted the observations from the Parties on the necessity of PNR data in the fight against terrorism and serious transnational crime. Accordingly, the European Commission and the Council failed to provide precise statistics on the contribution of PNR data to that fight.[65] That said, the Court observed that the proposal for the EU PNR Directive[66], which is adopted as of April 2016 and concerned with the air carriers' obligation to transfer PNR data to EU Member States, indicated that unspecified countries had been able to make use of the PNR data in drug trafficking, human trafficking, and terrorism cases.[67] Furthermore, the Canadian authorities had provided more specific statistics before the Court: Out of 28 million air passengers that flew between the EU and Canada between April 2014 and March 2015, 178 arrests

---

[61] ibid.

[62] ibid, paras 142-143.

[63] ibid, para 148.

[64] ibid, para 149.

[65] ibid, para 55.

[66] Directive 2016/681 of 27 April 2016 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime [2016] OJ L 119/132.

[67] Opinion 1/15 (n 15) para 55. Despite not being specified in the Court's opinion, those countries are the UK, Sweden, and Belgium. See: Commission, Proposal for a Directive on the use of Passenger Name Record data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime COM(2011) 32 final.

were made, 71 drug and 2 child pornography material seizures were carried out, and 169 further investigations in relation to terrorism were made.[68] Based on these statistics, one cannot help but wonder why PNR data were only relevant in such a low number of cases against the vast number of passengers who travelled to Canada. In addition, there is no information on criminal procedures followed by those arrests or procedures. These are issues worth considering for the usefulness of the PNR data put in for the purpose of fight against terrorism and serious transnational crime. However, without touching upon these issues, in Opinion 1/15, the Court was of the opinion that the use of those data was appropriate for that fight.[69] This article argues that there must be further information on the trials made conducted as a result of the seizures made and information obtained with the PNR data in order to address the question of appropriateness. Would such use still be appropriate if those arrestees were discharged due to the lack of evidence? Alternatively, would it be appropriate considering that the low number of arrests, seizures, and investigations outweighs the privacy of millions of people?

The same questions linger for the EU-US PNR Agreement. In comparison with the Canadian authorities, the US authorities are less cautious in revealing the specific statistics in relation to the use of PNR data at the border. Some information can be found in the joint review of the Agreement by the two Parties in 2013.[70] According to this review, in 2012, out of 110 million passengers that flew to the US, 101.805 passengers were targeted with the help of their PNR data for further scrutiny at the borders.[71] Of those targeted, 53.734 passengers flew to the US from the EU.[72] The report stops there and does not provide further information on why they were targeted or whether there were any convictions in relation to their participation in terrorist offences or serious transnational crime. Exemplary cases on the use of PNR data have also been provided before the US Congress, counting only 3 cases of such use

---

[68] Opinion 1/15 (n 15) para 56.

[69] ibid.

[70] Commission, Joint Review of the implementation of the Agreement between the European Union and the United States of America on the processing and transfer of passenger name records to the Unites States Department of Homeland Security Accompanying the Report from the Commission to the European Parliament and to the Council on the joint review of the implementation of the Agreement between the European Union and the United States of America on the processing and transfer of passenger name records to the United States Department of Homeland Security COM (2013) 844 final (Brussels, 27 November 2013).

[71] ibid 6.

[72] ibid.

in relation to terrorism cases and 2 cases of human smuggling.[73] Consequently, there is not enough evidence to support that the use of PNR data is appropriate for attaining the objective of fight against terrorism and serious transnational crime. Along the same line, that use is disproportionate to attain the mentioned objective taking the big gap between the high number of passengers flying to the US and the low numbers of targeting made.

Nevertheless, the CJEU called the use of PNR data for the relevant objective appropriate, but noted that some procedural requirements must be met for an international agreement on the transfer and use of PNR data be proportionate and strictly necessary.[74] Those requirements are the following:

- There must be clear and precise rules for the transfer of PNR data from the EU;
- There must be specific, reliable and non-discriminatory models and criteria used for the automated analysis of the PNR data;
- The databases against which the PNR data are cross-checked must be limited to those used for the fight against terrorism and serious transnational crime;
- There must be substantive and procedural conditions based on objective criteria for the disclosure of the PNR data to other authorities during the passenger's stay in Canada and after they leave, except in cases where those data are necessary to revise the models and criteria used for the automated analysis of the PNR data. Such disclosure must be subject to a prior review either by a court or by an independent administrative body (except in cases of emergency), whose decision must be followed by a reasoned request by the requesting authority;
- The PNR data must not be retained after the passenger concerned leaves Canada unless there is objective evidence indicating that the passenger

[73] Statement of Thomas Bush, Executive Director of Automation and Targeting Office of Intelligence and Investigative Liaison, Customs and Border Protection before the Subcommittee on Counterterrorism and Intelligence of the Committee on Homeland Security House of Representatives (120th Congress, 1st Session, 5 October 2011) <https://homeland.house.gov/hearing/intelligence-sharing-and-terrorist-travel-how-dhs-addresses-mission-providing-security/>; Joint Prepared Statement of David Heyman, Mary Ellen Callahan, and Thomas Bush (5 October 2011) before the Subcommittee on Counterterrorism and Intelligence of the Committee on Homeland Security House of Representatives (120th Congress, 1st Session, 5 October 2011) <https://homeland.house.gov/hearing/intelligence-sharing-and-terrorist-travel-how-dhs-addresses-mission-providing-security/>.

[74] Opinion 1/15 (n 15) para 232.

presents a risk in light of the fight against terrorism and serious international crime;

- The PNR data must be disclosed to other competent authorities of third countries when there is an adequacy decision by the European Commission for the relevant country or an agreement between the EU and those authorities equivalent to that decision;
- There must be a right to individual notification for the passengers concerned for the use of their PNR data when they are in Canada or after they leave, or when those data are disclosed to other authorities;
- There must be an independent oversight mechanism.

The EU-US PNR Agreement must meet this list of procedural requirements in order to be in line with the Charter. Unfortunately, a brief review of the Agreement shows that its provisions fail to satisfy these requirements. The first issue is that the Agreement fails to provide clear and precise rules for the PNR data transfer. This is because art 4 of the Agreement defining the terrorism offences and serious transnational crimes for which the PNR data can be used provides a list of prohibited conducts for both crimes, but that list is not an exhaustive one and contains expressions such as 'including conduct that' or 'including'.[75] It is, therefore, questionable that the definitions of the terrorist offences and serious transnational crimes embrace legal certainty. Moreover, under the same article, one of the elements for a crime to be considered as serious is that the prohibited conduct should be committed in more than one country, but without specifying whether one of those countries should be the US. Also, a crime is serious if it is punishable by imprisonment for three years or more, but under which legal jurisdiction that crime should be punishable as such is not included. Based on these findings, it is questionable whether the purposes for which the PNR data can be used are defined in a clear and precise manner. Another issue concerning the quality of law in question is that the use of 'etc.' and the data elements 'all available contact information' and 'all available payment/billing information' lack precision and clarity.[76] The same conclusion can be drawn for the data elements such as Other Service Related Information (OSI), Special Services Information (SSI), and Special Service Request (SSR) because as noted by the CJEU in its Opinion 1/15, travel agencies and air carriers can include anything under these data elements.[77]

---

[75] Hornung Boehm (n 5) 59.

[76] Cf Opinion 1/15 (n 15) paras 156-159.

[77] Cf ibid, para 160.

As far as the procedural safeguards for the automated use of PNR data are concerned, the Agreement merely contains a non-discrimination clause - an issue the CJEU considered in Opinion 1/15 as insufficient to justify the interference caused by that automated use with privacy and personal data protection rights.[78] It is important to note here that based on its obligation under the Data Mining Reporting Act of 2007, the DHS Privacy Officer has to report annually to the US Congress on the use of data mining technology (ie automated use of PNR data) by federal US agencies. In its recent report of 2015, the Officer noted that models and criteria against which the PNR data are automatically used were reviewed by the Office for Civil Rights and Civil Liberties and the Office of the General Counsel to ensure that they were not discriminatory and were up-to-date.[79] Nevertheless, any such assurance is not included in the EU-US PNR Agreement. Moreover, the Agreement does not include any restriction on utilising only the law enforcement databases. Rather the only restriction that is included relates to the use of PNR data.[80]

In relation to procedural conditions for the disclosure of PNR data to other authorities, the Agreement provides that such disclosure is permitted on the basis that it is done in relation to purposes specified under Article 4 of the Agreement and that the receiving authority affords an equivalent or a comparable level of data protection that is guaranteed in the Agreement.[81] The names of the relevant authorities, on the other hand, is not mentioned in the Agreement. In Opinion 1/15, the Court found that even if the name of the authorities to whom the data can be disclosed were not mentioned in it, the fact that the contested agreement limited the authorities to those acting in the context of and the disclosures to those necessary for its purposes sufficed for legal certainty. If the related provisions of the EU-US PNR Agreement were brought before it, the Court might draw same conclusions. However, the fact that the receiving authority has a choice of affording a comparable level of data protection, and is not obligated to provide an equivalent level of data protection, as the Canada PNR Agreement prescribed, might raise privacy

[78] ibid, paras 171-172.

[79] DHS Privacy Office, A Report on the Use and Transfer of Passenger Name Records between the European Union and the United States (26 June 2015) <https://www.dhs.gov/sites/default/files/publications/privacy_pcr_pnr_review_06262015.pdf.>.

[80] It is sufficient to note here that the Privacy Impact Assessment for the ATS lists a non-exhaustive long list of utilised databases. DHS/CBP, Privacy Impact Assessment for the Automated Targeting System, DHS/CBP/PIA-006(e) (13 January 2017) <https://www.dhs.gov/publication/automated-targeting-system-ats-update>.

[81] EU-US PNR Agreement, art 16.

concerns in relation to domestic sharing of PNR data. Additionally, the disclosures in question are solely at the discretion of the DHS. This is in conflict with the CJEU's finding that they should be subject to a prior review by a court or an independent administrative body.

An in-depth analysis of the procedural requirements for the retention of PNR data when passengers arrive to, stay in, and leave Canada is given in the following sub-section.[82] It is sufficient to note here that with its excessive retention period of up to 15 years without providing any conditions for the further use and retention, those data do not meet the mentioned requirements.

Regarding the disclosure to other authorities in third countries, the EU-US PNR Agreement provides that the DHS has the discretionary power to determine to what extent the receiving authority in the third country commits itself to 'incorporate data privacy protection comparable to those applied to PNR by DHS.'[83] However, under emergency circumstances, the PNR data may be sent regardless whether that country does have the required data protection.[84] This discretionary power and deviation from the adequacy requirement is incompatible with the CJEU's finding in the Opinion 1/15.

Furthermore, the EU-US PNR Agreement requires the DHS to inform passengers of the transfer and use of their PNR data through different means such as the Federal Register, the DHS website, clauses included in the air carriers' contracts.[85] None of these means satisfied the CJEU's finding in Opinion 1/15 as the passengers concerned are not informed of that transfer and use individually.

Lastly, the EU-US PNR Agreement provides for an 'independent review and oversight by Department Privacy Officers, such as the DHS Chief Privacy Officer' as the oversight body for the privacy related issues.[86] It mentions that this review body '(a) have a proven record of autonomy; (b) exercise effective powers of oversight, investigation, intervention, and review; and (c) have the power to refer violations of law related to this Agreement for prosecution or disciplinary action, when appropriate.'[87] It further provides a list of other authorities to carry out the independent oversight of the application of the EU-

[82] Section 4(b).

[83] EU-US PNR Agreement art 17(2).

[84] ibid.

[85] ibid, art 10.

[86] ibid, art 14(1).

[87] ibid.

US PNR Agreement in the US (the DHS Office of Inspector General, the Government Accountability Office as established by Congress, the US Congress).[88] The inclusion of an independent oversight mechanism is commendable, but the question is why that mechanism is linked with the DHS, particularly with regard to privacy issues.

In light of the foregoing, it is evident that the provisions of the EU-US PNR Agreement do not correspond with the requirements set forth by the CJEU in relation to the compatibility of an international agreement on the transfer and use of personal data in the context of the fight against terrorism and serious transnational crime. It is important not to lose sight of the privacy-related concerns in relation to the mentioned provisions of the EU-US PNR Agreement that have already been raised before the CJEU's judgment in Opinion 1/15. Whilst it can be said that the Opinion 1/15 set in stone the relevant requirements, the case-law of the CJEU prior to it stated one point that this judgment was not clear about before considering the procedural requirements for which personal data can be retained, ie that general and indiscriminate retention of data is precluded from EU law.

4.2. Mass surveillance of passengers: An issue beyond procedural requirements

The procedural requirements set forth by the CJEU in its Opinion 1/15 concern the conditions once the PNR data reach the shores of a third country. It might be the case that the EU and the third country demanding the PNR data might be compelled to strike a deal that will satisfy the procedural requirements listed in Opinion 1/15. That said, this contribution argues that before reaching the stage of retention and access, the transfer of PNR data of all passengers flying to a third country without an objective evidence linking them with the participation in terrorism and serious transnational crimes is not EU fundamental rights complaint in the first place.[89]

In its *Schrems* and *Tele2* decisions, the CJEU noted the need to limit the retention of personal data and access to those retained data on the basis of a direct link between those data and the participation of persons concerned with terrorism and serious crimes.[90] The EU-US PNR Agreement makes possible not only the general retention of and access to the PNR data, but also their transfer to the US without establishing any link between passengers concerned

[88] ibid, art 14(2).

[89] *Digital Rights Ireland* (n 16); *Schrems* (n 16) , *Tele2* (n 16).

[90] *Schrems* (n 16) para 93; *Tele2* (n 16) paras 105, 111, and 118.

and threat to the US public security. The question is then whether such comprehensive transfer meets the strict necessity test. In its Opinion 1/15, the Court returned to this question. Unlike what this contribution claims, it found that the transfer satisfied that test. When reaching this decision, the Court noted that the principal aim of the automated processing of PNR data is to identify persons unknown to Canadian authorities, and who pose a potential public security risk, and thus may be subject to further examination at the border.[91] It further observed that excluding certain passengers or certain areas of origin would be detrimental in pursuance of this aim.[92] Therefore, in a way, the Court approved of the transfer of PNR data of all passengers flying to Canada even if there is not any objective evidence to indicate that they present a public security threat in Canada. It accepted that the retention of PNR data at the time of entry and exit is justified because the objectives for the automatic use of PNR data are security checks and border controls, and thus the necessary connection between those data and the mentioned objectives existed.[93] However, using its *Tele2* decision as the legal authority, the Court observed that once the passenger is admitted to Canada, the use of his or her PNR data during his or her time in Canada must be based on new circumstances.[94] The secondary use of PNR data under these new circumstances can be carried out if there are substantive and procedural conditions following from objective criteria on the basis of which the Canadian authorities can perform that use.[95] Further, those authorities should submit a reasoned request to access those retained data for prior review by a court or by an independent administrative authority.[96] The reason for that access must be limited to the prevention, detection, or prosecution of crime.[97]

The Court's acknowledgement of the existence of a connection between the retained PNR data and the objective pursued by the Canada PNR Agreement brought the retention of those data after the departure of passengers from Canada into question. Once passengers who have not been identified as a public security risk upon their arrival to, during their stay in, and on their departure from Canada, the Court found that the continued retention of PNR data

---

[91] Opinion 1/15 (n 16) para 187.

[92] ibid.

[93] ibid, para 197

[94] ibid, paras 199-200.

[95] ibid.

[96] ibid, para 202

[97] ibid.

of those passengers after they leave the country was not justified because there was no connection between those data and the Agreement's objective.[98] Such retention should only be permissible if there is objective evidence indicative of the passenger's risk to the fight against terrorism and serious transnational crime.[99] In such a case, there must be substantive and procedural conditions based on objective criteria under which the Canadian authorities can have access to those data stored beyond passengers' stay in Canada.[100] Just like the secondary use of PNR data, that access must be subject to a prior review by either a court or an independent administrative body.[101] As far as the period for which the PNR data can be retained after passengers' departure from Canada, the Court held that the five-year retention period was not excessive on the condition that those data are held in Canada and must be irreversibly destroyed at the end of that period.[102]

The Court's findings in relation to the retention and use of PNR data upon passengers' arrival to and during the stay in Canada on the one hand, and after their departure from Canada on the other hand is commendable. The provisions of the EU-US PNR Agreement are in conflict with these findings. The EU-US PNR Agreement does not make the distinction between the retention period for the time the relevant passenger is in the US and for the time he or she departs from there. Nor does it provide any procedural conditions for the further use and the continued retention of data. Once they are transferred, the PNR data can be kept up to 15 years, regardless the individual concerned still being in the country. So the retention period can go beyond the time the individual is in the US. More importantly, after 15 years, the PNR data are anonymised instead of being deleted. There does not exist any solid evidence to justify that the anonymisation is necessary for the purposes of the fight against terrorism and serious transnational crime.

One issue in relation to the compatibility of the EU-US PNR Agreement with EU fundamental rights persists, i.e. the general transfer of PNR data without any objective evidence between passengers and the fight against terrorism and serious transnational crime. The Court in its Opinion 1/15 accepted that the transfer in relation to security checks and border controls and thus demonstrating a connection between them and passengers concerned. This

[98] ibid, paras 204-206.

[99] ibid, para 207.

[100] ibid, para 208

[101] ibid.

[102] ibid, paras 209-210.

finding is a step backwards in the EU's fundamental rights protection because it allows for the monitoring of passengers upon whom no suspicion has fallen. The matter becomes all the more worrisome if one considers that this monitoring does not have evidential value within the meaning of criminal law, although it may result in arrests being made against people who have not committed a crime.[103] Moreover, as mentioned above, the mismatch between the vast number of PNR data transferred and the low number of results achieved by the use of those transfers suggests that the transfer of PNR data is not proportionate. Another point of concern relates to the added value of PNR data, whose accuracy is questionable due to the fact those data are initially collected by air carriers for their own commercial purposes, and thus their quality is lower than data collected by public authorities for law enforcement purposes.[104] What this means for the proportionality test of the EU-US PNR Agreement is that provided that the margin of error occurred on the basis of these unverified data is significant (as accepted by the CJEU in Opinion 1/15), the use of transferred PNR data is useless to attain the objective that such a transfer pursues.[105]

5. CONCLUSION

The EU-US PNR Agreement is an exemplary measure reflecting states increasing concern on the alleged connection between border controls and terrorism and their tendency to rely on monitoring of all individuals crossing borders. In this regard, the relevant agreement has been promoted as an effective measure in the fight against terrorism. However, this agreement is the channel through which a wide array of information on the US-bound air passengers regardless of their criminal background is transferred to the US border control authority. In light of the case-law of the CJEU, particularly its judgment on the Canadian version of the relevant agreement, this contribution argues that the EU-US PNR Agreement falls short of protecting the EU fundamental rights of privacy and personal data protection. Further, having accepted the importance of this judgment, this contribution notes that not only

---

[103] In fact, the CJEU recognised the use of PNR data as an intelligence tool. Opinion 1/15 (n 16) para 130. On the convergence of intelligence and evidence see; Ken Roach, 'The Eroding Distinction Between Intelligence and Evidence in Terrorism Investigations' in Andrew Lynch, Nicola McGarrity, and George Williams (eds) Counter-Terrorism and Beyond (Routledge 2010) 48-68.

[104] European Union Committee (n 5) 9-10.

[105] Bruce Schneier, 'Automated Targeting System' (Schneier on Security, 2006) <https://www.schneier.com/blog/archives/2006/12/automated_targe.html>.

the undifferentiated retention of and access to passengers' information as denounced by the CJEU does not respect the protection of the mentioned rights, but also the undifferentiated transfer of that information in the first place. The latter conduct was accepted by the CJEU's opinion on the Canadian PNR Agreement, which, in the view of this contribution, offered less fundamental rights protection. On the basis of this finding, this contribution argues that other than checking whether the provisions of the EU-US PNR Agreement satisfy the procedural requirements set forth by the Court in that opinion, an emphasis must be made on devising a system that targets air passengers with criminal backgrounds and that will respect the EU fundamental rights fully.

6. SELECTED LITERATURE

Archick K, 'US-EU Cooperation against Terrorism' (Congressional Research Service for Congress, 2013)

Boehm F, 'A Comparison between US and EU Data Protection Legislation for Law Enforcement', (Study for the LIBE Committee, 2015), <http://www.europarl.europa.eu/RegData/etudes/STUD/2015/536459/IPOL_STU%28 2015%29536459_EN.pdf>

Calders T and Custers B, 'What is Data Mining and How does It Work?' in Bart Custers et al. (eds*), Discrimination and Privacy in the Information Society* (Springer 2013)

De Hert P and Gutwirth S, 'Privacy, Data Protection and Law Enforcement. Opacity of the Individual and Transparency of Power' in Erik Clased et al (eds) *Privacy and Criminal Law* (Intersentia 2006)

De Hert P and Gutwirth S, 'Data Protection in the Case Law of Strasbourg and Luxembourg: Constitutionalisation in Action' in Serge Hutwirth et al (eds), Reinventing Data Protection (Springer 2009)

De Hert P and Bellanova R, Transatlantic Cooperation on Travellers' Data Processing: From Sorting Countries to Sorting Individuals (Washington DC, Migration Policy Institute, 2011)

Guild E and Brouwer E, 'The Political Life of Data: The ECJ Decision on the PNR Agreement between the EU and the US' (CEPS No. 109, July 2006)

Hobbing P, 'Tracing Terrorists: The EU-Canada Agreement in PNR Matters' (CEPS, September 2008) <http://aei.pitt.edu/11745/1/1704.pdf>

Hornung G and Boehm F, 'Comparative Study on the 2011 draft Agreement between the United States of America and the European Union on the use and transfer of Passenger Name Records (PNR) to the United States Department

of Homeland Security' (Passau/Luxembourg, 14 March 2012) <http://www.greens-efa.eu/fileadmin/dam/Documents/Studies/PNR_Study_final.pdf>

Lynskey O, *The Foundations of EU Data Protection Role* (OUP 2015)

Murphy C, *The EU Counter-Terrorism Law: Pre-Emption and the Rule of Law* (Hart Publishing 2015)

Roach K, 'The Eroding Distinction Between Intelligence and Evidence in Terrorism Investigations' in Andrew Lynch, Nicola McGarrity, and George Williams (eds), *Counter-Terrorism and Beyond* (Routledge 2010)

Rouvroy A and Poullet Y, 'The Right to Informational Self-Determination and the Value of Self-Development: Reassessing the Importance of Privacy for Democracy' in Serge Hutwirth et al (eds), *Reinventing Data Protection* (Springer 2009)

Sottiaux S*, Terrorism and Limitation of Right the ECHR and the US Constitution* (Hart Publishing 2008)

Schneier B, 'Automated Targeting System' (Schneier on Security, 2006) <https://www.schneier.com/blog/archives/2006/12/automated_targe.html>

Tzanou M, 'Data Protection as a Fundamental Right Next to Privacy? 'Reconstructing' a not so new right' [2013] 3 International Data Privacy Law 88

van der Sloot B, 'Legal Fundamentalism: Is Data Protection Really a Fundamental Right' in Ronald Leenes et al (eds*), Data Protection and Privacy: (In)visibilities and Infrastructures* (Springer 2017)

Surveillance for public security purposes

Four pillars of acceptable interference with the fundamental right to privacy

WOJCIECH R. WIEWIÓROWSKI[1]

1. INTRODUCTION

The problem of global surveillance systems introduced by the governments of world superpowers became one of the main leitmotifs of privacy disputes, if not the leading one, after Edward Snowden's revelations in 2013. The idea of a universal panopticon[2] was confronted with the lawful interception[3] into the private life of individuals which is introduced in order to protect society. Such intrusion had been justified already for a decade when Snowden became a prophet of the new era of state surveillance[4] with a vision of the American National Security Agency (NSA) being a modern incarnation of Foucault's panopticon[5] – a concept that was one of the main architectural structures of

[1] European Data Protection Assistant Supervisor (since December 2014); Adjunct professor, University of Gdansk, Division of Legal Informatics; Inspector General for the Protection of Personal Data (GIODO) (2010-2014); Vice Chairman, Working Party Art. 29 (February-November 2014). Email: wojciech.wiewiorowski@edps.europa.eu.

[2] David Friedman, *Future Imperfect: Technology and Freedom in an Uncertain World* (Cambridge University Press 2008) 66-79.

[3] Doctrine often exchange notions of "lawful interception" and "surveillance" stating that the lawful interception of meta-data is a targeted surveillance required by law enforcement authorities and should not be considered as mass surveillance. See: Stefan Schuster (ed.), *Mass Surveillance: Part 1 - Risks and opportunities raised by the current generation of network services and applications* (STOA Report European Parliamentary Research Service, Brussels, 2015) 8.

[4] Daniel Knapp, 'The Social Construction of Computational Surveillance: Reclaiming Agency in a Computed World' (PhD thesis, London School of Economics and Political Science 2016) 26.

[5] Sarah Horowitz, 'Foucault's Panopticon: A Model of NSA Surveillance?' in Russel A. Miller, *Privacy and Power: A Transatlantic Dialogue in the Shadow of the NSA-Affair*, (CUP 2017) 39-62. See also: Sergei Boeke and Quirine Eijkman, 'State Surveillance in Cyber Space: A new perspective on digital data practices by intelligence dervices' in Lee Jarvis, Stuart MacDonald, Thomas M. Chen (ed.), *Terrorism Online: Politics, Law and Technology* (Routledge 2016) 128-131 and Richard Stiennon, *There Will Be*

the surveillance discussion, both in Europe and at a global level.[6] Although surveillance should not always be treated as an obstruction to privacy and vice versa[7], most commentaries link the current discussion to Orwell's or Kafka's dystopias[8].

2. EUROPEAN ESSENTIAL GUARANTEES

In the heart of the discussion on the new solution, which was expected to replace the *Safe Harbour Agreement*, the Article 29 Working Party[9] – representing all European data protection authorities (DPAs) – formulated a list of requirements for surveillance mechanisms that interfere with the right to privacy and data protection. Later judgments of the Court of Justice of the European Union have confirmed the line of reasoning used by the DPAs, and four relevant pillars of accepted activity at the time of rising insecurity – known as '*European Essential Guarantees*' – have been described. They consist of:

a. the requirement that the processing should be based on clear, precise and accessible rules;

b. demonstration of the necessity and proportionality with regard to the legitimate objectives pursued;

c. existence of an independent oversight mechanism as well as

Cyberwar: How The Move To Network-Centric War Fighting Has Set The Stage For Cyberwar (IT-Harvest Press 2015) 67-77 on NSA offensive cyber capabilities.

[6] Knapp (n 4) 32-36.

[7] On unusual alliances between privacy and surveillance see Gary T. Marx, 'Coming to Terms: The Kaleidoscope of Privacy and Surveillance' in Beate Roessler and Dorota Mokrosinska (ed.) *Social Dimensions of Privacy: Interdisciplinary Perspectives* (CUP 2015) 33-34.

[8] Recapitulation of both aspects of surveillance almost ten years before Snowden's revelations: Daniel Solove, *The Digital Person: Technology and privacy in the information age* (NYU Press 2004) 168-180.

[9] Working Party on the Protection of Individuals with regard to the Processing of Personal Data established on a basis of Article 29 of the Directive 95/46/EC. It is an independent European advisory body on data and privacy protection, composed of data protection commissioners of all European Union Member States. The tasks of the group are specified in Article 30 of the Directive 95/46/EC and Article 15 of the Directive 2002/58/EC.

d. availability of effective remedies to the individual.[10]

The right to the protection of personal data as well as the right to respect for private life are included in the Charter of Fundamental Rights, and were later also enshrined in the Treaty on the Functioning of the European Union. Neither of them is an absolute right and there is no doubt they may be limited, provided that the limitations comply with the requirements laid down in Article 52(1) of the Charter itself. The limitation has to be lawful, meaning it should be provided for by law and should respect the essence of the rights. It must also genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others. Moreover, the principles of necessity and proportionality of such limitations have to be observed.

3. PROVIDED BY LAW

The Article 29 Working Party started its deliberation by explaining the first fundamental principle - i.e. the processing should be based on clear, precise and accessible rules - with reference to the foreseeability of the interference even when the action is justified. Using jurisprudence of the European Court of Human Rights (ECtHR), the Working Party states that it should be possible to assess the effect of the interference on the individual, in order to give the person an adequate protection against arbitrary actions of the state. In its judgment on the *Malone* case, the Strasbourg Court stressed that the processing must be based on a precise, clear and accessible legal basis[11]. Such a legal basis should be set out in statute law which is easily accessible for the public and which should explain the nature of the offences that may give rise to an interception or surveillance order. The law should also define the categories of people that might be subject to surveillance. The measures taken should be limited as far as the duration is concerned. Last but not least, recalling the judgment in *Weber and Saravia*, DPAs reaffirm that the procedure to be followed for examining, using and storing the data obtained, the precautions to be taken when communicating the data to other parties and the circumstances in which the materials that result from such an interference may

[10] Article 29 Working Party, Working Document 1/2016 on the justification of interferences with the fundamental rights to privacy and data protection through surveillance measures when transferring personal data (European Essential Guarantees) (WP 237) 7 <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2016/wp237_en.pdf>.

[11] *Malone v the United Kingdom* App no 8691/79 (ECtHR, 2 August 1984) para 67.

or must be destroyed, have to be foreseeable as well[12]. It is clear that the risks of arbitrariness are especially evident where a power vested in the executive is exercised in secret[13]. The law must include sufficiently clear terms in order to give citizens an adequate indication as to the circumstances in which and the conditions according to which public authorities are empowered to resort to such measures.

The same principle was recalled by the Strasbourg Court in its most important recent case *Zakharov v Russia*[14], which supplemented its line of interpretation and explained that the reference to "foreseeability" in the context of interception of communications cannot be the same as in many other fields. Foreseeability in the special context of secret measures of surveillance, such as the interception of communications, cannot mean that an individual should be able to foresee when the authorities are likely to intercept his communications so that he can adapt his conduct accordingly. The law in Member States that are parties to the Convention must be sufficiently clear in order to give citizens an adequate indication as to when and how public authorities may resort to surveillance measures.

---

[12] *Weber and Saravia* v *Germany* App no 54934/00 (ECtHR, 29 June 2006) para 95. See also: *Huvig* v *France* App no 11105/84 (ECtHR, 24 April 1990) para 34; *Kopp v Switzerland* App no 23224/94 (ECtHR, 25 March 1998) para 55; *Amann v Switzerland* App no 27798/95 (ECtHR, 16 February 2000) para 76; *Valenzuela Contreras v Spain* App no 27671/95 (ECHR, 30 July 1998) para 46; *Prado Bugallo v Spain* App no 58496/00 (ECtHR, 18 February 2003) para 30. More on that in Lee Andrew Bygrave, *Data Privacy Law. An International Perspective* (OUP 2014) 93-94.

[13] *Rotaru v Romania* App no 28341/95 (ECtHR, 4 May 2000) para 55; *Huvig v France* App no 11105/84 (ECtHR, 24 April 1990) para 29; *Zakharov v Russia* App no 47143/06 (ECHR, 4 December 2015) para 229. See also: Susana Sanchez Ferro, 'The Need for an Institutionalized and Transparent Set of Domestic Legal Rules Governing Transnational Intelligence Sharing in Democratic Societies' in Miller (n 5) 513.

[14] *Zakharov* (n 13). One of the leading ECHR judgements concerned the system of secret interception of mobile telephone communications in the Russian Federation. The applicant – an editor-in-chief of a publishing company – complained that Russian law permitted blanket interception of communications by law enforcement agencies. The Court held that there had been a violation of Article 8 of the Convention, finding that the Russian legal provisions governing interception of communications did not provide for adequate and effective guarantees against arbitrariness and the risk of abuse which was inherent in any system of secret surveillance, and which was particularly high in a system such as in Russia where the secret services and the police had direct access, by technical means, to all mobile telephone communications. Moreover, the effectiveness of the remedies available to challenge interception of communications was undermined by the fact that they were available only to persons who were able to submit proof of interception.

The Strasbourg Court ruled similarly four years ago in another Russian case initiated by *Sergiey M. Shimovolos*[15]. This case concerned the registration of a human rights activist in the so-called "surveillance database", which collected information about his movements, by train or air, within Russia, and about his arrest. The Court held that there had been a violation of Article 8 of the Convention. The judges observed that the creation and maintenance of the database and the procedure for its operation were governed by a ministerial order which had never been published or otherwise made accessible to the public. Consequently, the Court found that the domestic law did not indicate with sufficient clarity the scope and manner of exercising the discretion conferred on the domestic authorities to collect and store information on individuals' private lives in the database. In particular, it did not set out any indication of the minimum safeguards against abuse in a form accessible to the public.

4. NECESSITY AND PROPORTIONALITY

Hustinx is surely right when he writes that the European Human Rights Convention's approach is not that processing of personal data should always be considered as an interference with the right to privacy, but rather that for the protection of privacy and other fundamental rights and freedoms, any processing of personal data must always observe certain legal conditions. Such a legal condition could be the principle that personal data may only be processed for specified legitimate purposes, where necessary for these purposes, and not used in a way incompatible with those purposes. Under this approach, the core elements of Article 8 ECHR, such as that the right to privacy may only be interfered with when there is an adequate legal basis and a legitimate purpose, have been transferred into a broader context. This only works well in practice if the system of checks and balances, as set out in the Convention - consisting of substantive conditions, individual rights, procedural provisions and independent supervision - is sufficiently flexible to take account of variable contexts, and is applied with pragmatism and an 'open eye' for the interests of data subjects and other relevant stakeholders[16].

Nevertheless, all kinds of processing of personal data by government authorities are often regarded as an interference with the right to privacy and data

---

[15] In *Shimovolos v Russia* App no 30194/09 (ECtHR, 21 June 2011) the Court also held that there had been a violation of Article 5 (right to liberty and security) of the Convention.

[16] Peter Hustinx, 'European Leadership in Privacy and Data Protection' in Artemi Rallo Lombarte and Rosario García Mahamut (eds) *Hacia un nuevo régimen europeo de protección de datos* (Tirant Lo Blanch 2015) 18.

protection as they are described in the Charter and the Treaty. As it was stated before, such an action by the government – including data processing for intelligence purposes – can be justifiable only when it is necessary and proportionate in relation to a legitimate objective[17]. The Court of Justice of the EU has made it clear in its judgement in *Schrems*, that the "legislation is not limited to what is strictly necessary where it authorises, on a generalised basis, storage of all the personal data (…) without any differentiation, limitation or exception being made in the light of the objective pursued and without an objective criterion being laid down by which to determine the limits of the access of the public authorities to the data, and of its subsequent use, for purposes which are specific, strictly restricted and capable of justifying the interference which both access to that data and its use entail"[18].

The same line of interpretation was also taken by the European Court of Human Rights in its leading judgement on state surveillance last year – *Szabó and Vissy v Hungary*[19] – when the ECHR stated that "in the face of this progress the Court must scrutinise the question as to whether the development of surveillance methods resulting in masses of data collected has been accompanied by a simultaneous development of legal safeguards securing respect for citizens' Convention rights. (…) Indeed, it would defy the purpose of government efforts to keep terrorism at bay, thus restoring citizens' trust in their abilities to maintain public security, if the terrorist threat were paradoxically substituted for by a perceived threat of unfettered executive power intruding into citizens' private spheres by virtue of uncontrolled yet far-reaching surveillance techniques and prerogatives. (…) This threat to privacy must be subjected to very close scrutiny both on the domestic level and under the Convention. (…) However, it is not warranted to embark on this matter in the present case". The Court accepted that it was a natural consequence of the forms taken by present-day terrorism that governments resort to cutting-edge technologies, including massive monitoring of communications, in pre-empting impending incidents. However, the Court was not convinced that the legislation in question provided sufficient safeguards to avoid abuse. The scope of the measures could virtually include anyone in Hungary, and with

[17] Bygrave (n 12) 94-96 and 147-150.

[18] Case C-362/14 *Maximillian Schrems v Data Protection Commissioner* EU:C:2015: 650, para 95.

[19] *Szabó and Vissy v Hungary* App no. 37138/14 (ECtHR, 12 January 2016) paras 68-70. The Court further held that there had been no violation of Article 13 (right to an effective remedy) of the Convention taken together with Article 8, reiterating that Article 13 could not be interpreted as requiring a remedy against the state of domestic law.

new technologies the Government could easily intercept masses of data concerning even persons outside the original range of operation. Furthermore, according to the Court, the ordering of such measures was taking place entirely within the realm of the executive, without an assessment of whether interception of communications was strictly necessary and without any effective remedial measures, let alone judicial ones, being in place.

The Luxembourg Court has joined this line of interpretation in the *Digital Rights Ireland* case[20], invalidating the so-called Data Retention Directive[21]. The Court assessed the European Union legislation and found that it covers "all persons and all means of electronic communication" without "any differentiation, limitation or exception being made". Thus, the Court considered that the legislator failed to provide for an "objective criterion by which to determine the limits of the access (…) and their subsequent use".[22]

It was already after the Article 29 Working Party passed its working document on the essential guarantees that the Court of Justice confirmed these lines of reasoning in two judgments connected with the legality of the massive and indiscriminate collection of personal data and their re-use.

In the judgment on the joined cases *Tele2 Sverige AB v Post-och telestyrelsen* and *Secretary of State for the Home Department v Tom Watson and Others* [23] – revealed just before Christmas 2016 and thus summarising the year spent on discussing on the guarantees – the Court of Justice reaffirmed the *Digital Rights Ireland* decision on the retention of telecommunication data and assessed the Swedish and UK domestic regime. It made clear that the data retention laws of Member States must comply with EU data protection rules even in absence of the special legal act of the secondary law devoted to that

[20] Joined Cases C-293/12 and C-594/12 *Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others* EU:C:2014:238.

[21] Parliament and Council Directive 2006/24/EC of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC [2006] OJ L105/54.

[22] For an in-depth analysis of the access to private resources by state authorities (incluing data on France, Germany, Israel, Italy, Brasil, Canada, US, Australia, China, India, Japan and Korea), see Fred H Cate, James X Dempsey (eds), *Bulk Collection: Systematic Government Access to Private-Sector Data* (Oxford University Press 2017).

[23] Joined Cases C-203/15 and C-698/15 *Tele2 Sverige AB v Post- och telestyrelsen and Secretary of State for the Home Department v Davis and Others* EU:C:2016:970.

matter, and that generalised and indiscriminate surveillance is not permissible under EU law. The Court admitted that "a public whose data is likely to reveal a link, at least an indirect one, with serious criminal offenses, and to contribute in one way or another to fighting serious crime or to preventing a serious risk to public security", and thus data retention itself might be lawful if limited. The criteria which a national data retention law needs to contain include clear and precise rules and impose minimum safeguards set in the law, as well as indications of circumstances and conditions under which data retention may be adopted as a preventative measure.

The Court failed to find a significant difference between the notions of "retention" and "processing of data" stating that the latter, in connection with provisions on electronic communications, also covers the intermediate retention of such data of the relevant communications. The Court's judgement in *Tele2 Sverige* is mainly based on a proportionality assessment weighing the right to data protection versus the demands of public security concerns.

Further legal analysis on the necessity, including the necessity test applied to the right to the protection of personal data, has been provided by the European Data Protection Supervisor in 2017 in the toolkit published to help EU institutions to interpret particular requirements stemming from Article 52(1) of the Charter, in which it is stated that any limitation on the exercise of the right to personal data protection (Article 8 of the Charter) must be "necessary" for an objective of general interest or to protect the rights and freedoms of others[24].

The EDPS finds that the next test should assess whether the measure meets an objective of general interest. The objective of general interest provides the background against which the necessity of the measure may be assessed. It is therefore important to identify the objective of general interest in sufficient detail in order to allow the assessment as to whether a proposed measure, which entails the processing of personal data, is really necessary. If this test is satisfied, the proportionality of the envisaged measure will be assessed. Should the draft measure not pass the necessity test, there is no need to examine its proportionality. A measure that has not proved to be necessary should not be proposed unless and until it has been modified to meet the requirement of necessity. A proper description of the measure is, in the Supervisor's view, important as it may affect several of the criteria mentioned earlier by the Courts. The Courts, therefore, may sometimes assess the criteria in

[24] European Data Protection Supervisor (EDPS), Assessing the necessity of measures that limit the fundamental right to the protection of personal data (a toolkit), <https://edps.europa.eu/sites/edp/files/publication/17-04-11_necessity_toolkit_en_0.pdf >.

tandem. For instance, a measure that is unclearly or too broadly defined may prevent an assessment of whether it is "provided by law" and "necessary".

The EDPS also studies the relationship between proportionality and necessity, reminding that proportionality is a general principle of EU law which requires that "the content and form of Union action shall not exceed what is necessary to achieve the objectives of the treaties". He quotes the *Gauweiler* judgment stressing that "the principle of proportionality requires that acts of the EU institutions be appropriate for attaining the legitimate objectives pursued by the legislation at issue and do not exceed the limits of what is appropriate and necessary in order to achieve those objectives"[25]. It therefore, recalling judge Lenaerts, "restricts the authorities in the exercise of their powers by requiring a balance to be struck between the means used and the intended aim (or result reached)"[26].

Proportionality in a broad sense encompasses both the necessity and the appropriateness of a measure; namely the extent to which there is a logical link between the measure and the (legitimate) objective pursued. Furthermore, for a measure to meet the principle of proportionality as enshrined in Article 52(1) of the Charter, the advantages resulting from the measure should not be outweighed by the disadvantages the measure causes with respect to the exercise of the fundamental rights. This latter element describes proportionality in a narrow sense and consitutes the proportionality test. It should be clearly distinguished from necessity. Necessity implies the need for a combined, fact-based assessment of the effectiveness of the measure for the objective pursued and of whether it is less intrusive compared to other options for achieving the same goal[27].

Finally, the EDPS states that "necessity" is also a data quality principle and a recurrent condition in almost all the requirements on the lawfulness of the processing of personal data stemming from EU data protection secondary law. There is also a link between Article 8(2) of the Charter and the secondary law, as Article 8(2) refers to the legitimate basis for processing "laid down by

---

[25] Case C-62/14 *Peter Gauweiler and Others v Deutscher Bundestag* ECLI:EU:C:2015: 400, [2015], para 67, on request for a preliminary ruling from the Bundesverfassungsgericht. The case concerned the legality of the decision of the Governing Board of the European Central Bank of September 2012 on so called 'Outright Monetary Transactions' (OMT).

[26] Koen Lenaerts and Piet Van Nuffel, *European Union Law* (3rd edn, Sweet & Maxwell 2011) 141.

[27] ibid 24, 5.

law" and the Explanatory Note on Article 8 refers to this secondary law stating that the Directive 95/46 and the Regulation 45/2001 "contain conditions and limitations for the exercise of the right to the protection of personal data".

The question of whether a measure should target any crime or only serious crimes may be considered a matter of necessity; however, should such a provision be assessed to be necessary, an assessment of its proportionality and its risk of eroding the values of a democratic society would still be needed. Therefore, in practice, there is some overlap between the notions of necessity and proportionality, and, depending on the measure in question, the two tests may be carried out concurrently or even in a reverse order. In *Digital Rights Ireland*, the Court first stated that proportionality consists of the steps of appropriateness and necessity[28]. It then established that the limitation of the rights protected in Articles 7 and 8 were not necessary[29] and therefore concluded, that the limitations were not proportionate[30]. Also in *Schrems*[31] the Court analysed the necessity and found the Safe Harbour Decision to be invalid without making any reference to proportionality before reaching this conclusion. The Court of Justice is clear when it comes to the content of communications data and states in *Schrems* that public authorities should not be allowed to have access to the content of electronic communications on a generalised basis.[32] It should be also noted that the Article 29 Working Party underlined that an interference takes place not only at the time of collection of the data, but also everytime the data is accessed by a government authority for further processing for intelligence purposes[33].

---

[28] Joined Cases C-293/12 and C-594/12 *Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others* EU:C:2014:238, para 46. On more general consequences of this judgement: Sergio Carrera and others, *Access to Electronic Data by Third-Country Law Enforcement Authorities: Challenges to EU Rule of Law and Fundamental Rights* (CEPS 2015) 74.

[29] ibid, para 65.

[30] ibid, para 69.

[31] *Maximillian Schrems* (n 18) paras 92-93 and 98.

[32] On the dichotomy between law enforcement and intelligence: Liane Colonna, *Legal Implications of Data Mining: Assessing the European Union's Data Protection Principles in Light of the United States Government's National Intelligence Data Mining Practices* (PhD thesis, Stockholm University 2016) s 193. See also: *Fundamental Rights Agency, Surveillance by intelligence services: fundamental rights safeguards and remedies in the EU. Volume II: field perspectives and legal update* (Fundamental Rights Agency 2017) 28.

[33] *Maximillian Schrems* (n 18) para 95; *Uzun v Germany* App no 35623/05 (ECtHR, 2 September 2010), para 63; Hielke Hijmans, *The European Union as a Constitutional*

5. AN INDEPENDENT OVERSIGHT MECHANISM

Another pillar which is absolutely necessary in order to recognise that an interference with the right to privacy and data protection is acceptable, according to the Article 29 Working Party, is the existence of an effective, independent and impartial oversight system, in the form of either a judicial review or an activity of another independent body, such as an administrative authority or a parliamentary committee[34]. Regardless of the form of the independent supervision[35], the existence of oversight authorities forms "an essential component of the protection of individuals with regard to the processing of personal data"[36].

Hijmans deliberates on the reasons for having an independent authority in place and recapitulates a number of them as essentially convincing that an independent oversight system is necessary[37]. The oversight should be carried out by a public body (1) which acts effectively (2). The body, or rather its representatives, should know the nature of data processing and be skilled to assess it (3) and their approach to the duties of controllers should be consistent to different sectors, private or public (4). The body has to be independent from political influences (5) and, in Hijman's view, an advantage is given to institutions established solely for privacy and data protection.

The independent oversight can take place at various stages during the lifecycle of a data processing operation. It can start when the surveillance is first ordered, but it can also begin while it is being carried out and even after it has been terminated. Depending of the nature of the activities and on some external circumstances, either a prior or ex-post analysis can be recognised as acceptable according to the standards[38]. In *Zakharov,* the ECtHR has accepted the fact that the special nature of data processing for intelligence purposes makes it acceptable that the processing itself takes place without the data subject being informed. The judges write that "as regards the first two stages,

Guardian of Internet Privacy and Data Protection: The Story of Article 16 TFEU (Springer 2016) 267.

[34] *Klass and Others v Germany* App no 5029/71 (ECtHR, 6 September 1978) paras 17 and 51.

[35] See analysis in Hijmans (n 33) 385-391.

[36] Case C-518/07 *European Commission v Germany* ECLI:EU:C:2010:125, [2010] ECR I-01885, para 23.

[37] Hijmans (n 33) 352-355.

[38] *Klass* (n 34) paras 55-56; *Zakharov* (n 13) para 233.

the very nature and logic of secret surveillance dictate that not only the surveillance itself but also the accompanying review should be affected without the individual's knowledge. (…) In a field where abuse is potentially so easy in individual cases and could have such harmful consequences for democratic society as a whole, it is in principle desirable to entrust supervisory control to a judge, judicial control offering the best guarantees of independence, impartiality and a proper procedure."[39]

A similar line is taken by the CJEU in *Digital Rights Ireland* where the Court states that "the access (…) to the data retained [should also be] made dependent on a prior review carried out by a court or by an independent administrative body whose decision seeks to limit access to the data and their use to what is strictly necessary for the purpose of attaining the objective pursued and which intervenes following a reasoned request of those authorities submitted within the framework of procedures of prevention, detection or criminal prosecutions."[40] The Court made these matters clear by holding that the Data Retention Directive was invalid because it did not meet these requirements[41].

Both the Strasbourg and Luxembourg Court studied the status of the oversight organ. The ECtHR prefers the independence of oversight mechanisms, including the judge, yet exceptions are acceptable "as long as [the supervisor] is sufficiently independent from the executive."[42] The CJEU accepts that the oversight is given to administrative bodies in the European Union. Their status was especially examined in three cases on the independence of the data protection authorities in Germany[43], Austria[44] and Hungary[45].

[39] *Zakharov* (n 13) para 233.

[40] *Digital Rights Ireland* (n 20) para 62.

[41] Hijmans (n 33) 268-272.

[42] *Zakharov* (n 13) para 258.

[43] Case C-518/07 *European Commission v Germany* ECLI:EU:C:2010:125, [2010] ECR I-01885.

[44] Case C-614/10 *Commission v Austria* ECLI:EU:C:2012:631, [2012].

[45] Case C-288/12 *Commission v Hungary* ECLI:EU:C:2014:237, [2014].

6. EFFECTIVE REMEDIES AVAILABLE TO THE INDIVIDUAL

The final European Essential Guarantee is related to the effective[46] redress rights of the individual. The CJEU explained in *Schrems* that the essence of the right to an effective remedy was affected. It was stated that "[l]egislation not providing for any possibility for an individual to pursue legal remedies in order to have access to personal data relating to him, or to obtain the rectification or erasure of such data, does not respect the essence of the fundamental right to effective judicial protection, as enshrined in Article 47 of the Charter"[47] . Therefore, the Court did not even start the examination of whether such a limitation was necessary and instead decided to invalidate the whole Commission Decision on the adequacy of the Safe Harbour Principles[48].

The strongest comment on this point was provided by the German Schleswig-Holstein data protection authority, who stated in the position paper on the judgment: "If citizens of the European Union have no effective right to access their personal data or to be heard on the question of surveillance and interception and to enjoy legal protection, article 47 of the CFR is infringed (...) The USA can currently show no effective means to ensure protection essentially equivalent to the level of protection guaranteed within the European Union"[49].

---

[46] On effectiveness Hijmans (n 33) 382.

[47] *Maximillian Schrems* (n 18) para 95.

[48] Martin A. Weiss and Kristin Archick, 'U.S.-EU Data Privacy: From Safe Harbor to Privacy Shield, Congressional Research Service report' <https://fas.org/sgp/crs/misc/R44257.pdf>. For the analysis of later developments and their critical review see: Peter Swire, 'US Surveillance Law in a constitutional democracy, Safe Harbor, and Reforms since 2013' (Georgia Tech Scheller College of Business Research Paper no 36); Gert Vermeulen, 'The Paper Shield. On the degree of protection of the EU-US Privacy Shield against unnecessary or disproportionate data collection by the US intelligence and law enforcement services' in Dan Svantesson and Dariusz Kloza, *Trans-Atlantic Data Privacy Relations as a Challenge for Democracy* (Intersentia 2017) 85-126 and 127-147. See also: David Vladeck, 'Separated by Common Goals: A U.S. Perspective on Narrowing the U.S.-E.U. Privacy Divide' in Rallo Lombarte and Mahamut (eds) (n 16) 207-243.

[49] *ULD position paper on the judgment of the Court of Justice of the European Union of 6 October 2015, C-362/14* <https://www.datenschutzzentrum.de/uploads/internationales/20151014_ULD-PositionPapier-on-CJEU_EN.pdf>. See also: Shara Monteleone and Laura Puccio, *From Safe Harbour to Privacy Shield: Advances and shortcomings of the new EU-US data transfer rules* (In-Depth Analysis, European Parliamentary Research Service 2017) 11 <http://www.europarl.europa.eu/RegData/etudes/IDAN/2017/595892/EPRS_IDA(2017)595892_EN.pdf >.

For the Strasbourg Court, the question of an effective remedy[50] is inextricably linked to the notification of the individual with regard to a surveillance measure once the surveillance is over. The Article 29 Working Party rightly cites the *Zakharov* case, where the ECtHR stated that "there is in principle little scope for recourse to the courts by the individual concerned unless the latter is advised of the measures taken without his or her knowledge and thus able to challenge their legality retrospectively or, in the alternative, unless any person who suspects that his or her communications are being or have been intercepted can apply to courts, so that the courts' jurisdiction does not depend on notification to the interception subject that there has been an interception of his communications".[51]

Where no notification has been given, the ECtHR established criteria that have to be met by the independent authority. It has to be an independent and impartial body, which has adopted its own rules of procedure, and which consists of members that must hold or have held high judicial office or must be experienced lawyers. The body should be able to access all relevant information when it examines complaints by individuals, including all kinds of confidential materials[52]. Examining the case of *Uzun v Germany*[53], the Court held that there had been no violation of Article 8 of the Convention. Given that the criminal investigation had concerned serious crimes, it found that the GPS surveillance of the applicant had been proportionate, while the applicant, suspected of involvement in left-wing terrorist extremism, complained that surveillance by GPS and the use of collected data in the criminal proceedings against him had violated his right to respect for private life[54].

---

[50] On the possible role of class action Marc Rotenberg and others, 'Enforcing Privacy Rights: Class Action Litigation and the Challenge of cy pres' in David Wright and Paul de Hert (eds), *Enforcing Privacy. Regulatory, Legal and Technical Approaches* (Springer 2016) 307-334.

[51] *Zakharov* (n 13) para 234.

[52] *Kennedy v The United Kingdom* App no 26839/05 (ECtHR, 18 May 2010) para 167. However, it is not easy to reach this purpose as the long list of national case law shows in Didier Bigo and others, 'National Security and Secret Evidence in Legislation and before the Courts: Exploring the Challenges' (CEPS 2014) 77-79 <http://www.europarl.europa.eu/RegData/etudes/STUD/2014/509991/IPOL_STU(2014)509991_EN.pdf>.

[53] *Uzun v Germany* App no 35623/05 (ECtHR, 2 September 2010).

[54] A similar case – *Ben Faiza v France*, App no 31446/12 (ECtHR) – is still pending in the Court, being communicated to the French Government on 3 February 2015. The complainant protests against an interference with his private life on account of the

7. THE COURT OF JUSTICE CONFIRMS THE EUROPEAN ESSENTIAL GUARANTEES

The *Digital Rights Ireland* case had an enormous impact across the EU, but particularly in the United Kingdom close attention was being paid to the judgment.[55] The immediate effect of the judgment was however far from the expectations of privacy advocates, since some of the EU Member States logically understood that the invalidation of the Data Retention Directive actually gives the states much more flexibility. So far, the sector was co-regulated, but when the EU component of the co-regulation vanished, the only remaining part falls within the discretion of the state in light of the subsidiarity principle. This, however, was challenged by privacy advocates who still saw Article 15 of the ePrivacy Directive as the basis for co-regulation.

Subsequent activities of the Swedish[56] and UK governments led to the next important case in Luxembourg, which was expected to filter the *Digital Rights Ireland* judgement test in the joined cases *Tele2 and Watson (ex-Davis)*[57]. The first concerned the Swedish Tele2 company which decided to cease retaining data. The second involved the '*Data Retention and Investigatory Powers Act' (DRIPA)*, which was adopted by the UK government in 2014, and later challenged by British parliamentarians. The cases had first been assessed by Advocate General *Saugmandsgaard Øe* on 19 June 2016 and were finally judged by CJUE half a year later[58]. The Advocate General had no doubts that Article 51 of the Charter of Fundamental Rights is fully applicable to national provisions implementing Article 15 of the ePrivacy Directive. At the same time, he admitted that a general retention of communications may be compatible with the EU law subject to satisfying strict requirements set out by the ePrivacy Directive and the Charter. The Court followed this line of interpretation and underlined that derogations are acceptable only insofar as strictly necessary.

---

installation of a GPS tracking device in his vehicle with the aim of monitoring his movements during the course of a drug trafficking inquiry.

[55] Lucia Zedner, 'Why Blanket Surveillance Is No Security Blanket: Data Retention in the United Kingdom after the European Data Protection Directive' in Miller (n 5) 564-585.

[56] See also another case against Sweden still pending before the ECtHR: *Centrum För Rättvisa v Sweden*, App no 35252/08. The application was communicated to the Swedish Government on 21 November 2011 and 14 October 2014. The applicant, a non-profit public interest law firm, complains about the Swedish state practice and legislation concerning secret surveillance measures.

[57] *Tele2 Sverige AB* (n 22).

[58] On 21 December 2016.

Applying these rules to the facts of cases, the CJUE held that the retention of metadata is as revealing as the retention of the content since it makes profiling possible[59] and, furthermore,the data in question is liable to allow very precise conclusions to be drawn on private lives. The social knowledge on the retention gives people the feeling that they are under constant surveillance. It then affects the use of communications and the right to freedom of expression. In consequence, the Court accepted such actions only in case of serious crimes, stating that such a justified interference cannot be implemented into national legislation by provisions on the general and indiscriminate retention of data.[60]

The proportionality of intrusion has been also studied extensively when the Court of Justice was asked by the European Parliament for an opinion on the EU-Canada agreement on exchange of Passenger Name Records (PNR)[61]. Once again, the European Court confirmed that the European Commission failed to understand which legal requirements are to be observed when the,

---

[59] The distinction of communication metadata and content metadata was omitted since from a legal perspective, the communication meta-data is the only existing metadata, as content meta-data is considered to be part of the content and travels end-to-end embedded in the content. The structured nature of the meta-data is ideally suited for analysis using data mining techniques such as pattern recognition, machine learning, and information or data fusion. See: Schuster (n 3) 7 and 9.

[60] Other pending Strasbourg cases to be observed in this matter are: a) *Tretter and Others v Austria* (App no 3599/10 communicated to the Austrian Government on 6 May 2013) on amendments of the Police Powers Act extending the powers of the police authorities to collect and process personal data; b) *Big Brother Watch and Others v the United Kingdom* (App no 58170/13 communicated to the UK Government on 9 January 2014) on three NGOs and one academic working internationally likely being subjects of surveillance by UK intelligence services; c) *Bureau of Investigative Journalism and Alice Ross v the United Kingdom* (App no 62322/14 communicated to the UK Government on 5 January 2015) interception of both internet and telephone communications by government agencies and blanket interception, storage and exploitation of communication amount to disproportionate interference with journalistic freedom of expression and d) *Association confraternelle de la presse judiciaire v France et 11 autres requêtes* (App nos 49526/15, 49615/15, 49616/15, 49617/15, 49618/15, 49619/15, 49620/15, 49621/15, 55058/15, 55061/15, 59602/15 and 59621/15 communicated to the French Government on 26 April 2017) lawyers and journalists and legal persons connected with these professions, concern the French Intelligence Act of 24 July 2015.

[61] Earlier history of PNR agreements negotiated by EU is summarised in Mistale Taylor, 'Flying from the EU to the US: necessary extraterritorial legal diffusion in the US-EU Passenger Name Record agreement' (2015) 19 Spanish Yearbook of International Law 223-225.

generally acceptable, idea of PNR finds its implementation into statutory law.[62] On 26 July 2017, the Court declared that the agreement may not be concluded in the form passed to the European legislator[63]. The Parliament referred the agreement to the Court in order for the regularity of the agreement to be assessed under EU law, and in particular the Charter of Fundamental Rights of the European Union. In its Opinion, the CJEU declared that this retention of bulk data is excessive and would therefore violate fundamental rights of EU citizens. The Court of Justice admitted that the transfer itself, even when made on a systematic basis, the retention and the use of all PNR are, in essence, permissible; yet the Court agreed with the Parliament that several provisions of the draft agreement did not meet the requirements stemming from the fundamental rights of the European Union[64]. The Court questioned the systematic and continuous transfer of data of all air passengers to a Canadian authority with a view to that data being used and retained and possibly subsequently transferred to other authorities and other non-member countries, for the purpose of combating terrorism and serious transnational crime. Since the period during which the PNR data may be retained may last for up to five years, this agreement makes it possible for information on the private lives of passengers to be available for a particularly long period of time.

The Court stated that the EU-Canada agreement should determine in a more clear and precise manner how PNR data may be transferred. It should also require that the models and criteria used for the automated processing of the PNR data are specific, reliable and non-discriminatory. The use of databases should be only limited to the fight against terrorism and serious transnational crime. The law should also provide for a right to individual notification for air passengers in the event of use of the PNR data concerning them during their stay in Canada and after their departure from that country, as well as in the event of disclosure of that data to other authorities or to individuals. The Court required the guarantee that the oversight of the rules relating to the protection of air passengers with regard the processing of the PNR data is

---

[62] European Digital Rights (EDRi), 'European Court Opinion: Canada PNR cannot be signed' (2016), <https://edri.org/european-court- opinion-canada-pnr-deal-cannot-be-signed/>.

[63] Hielke Hijmans, 'PNR Agreement EU-Canada Scrutinised: CJEU Gives Very Precise Guidance to Negotiators' (2017) European Data Protection Law Review 310-312.

[64] Short description of EU PNR schemes in Wim Wensink and others, *The European Union's Policies on Counter-Terrorism: Relevance, Coherence and Effectiveness* (Study for the LIBE Committee 2017) 121-123 <http://www.europarl.europa.eu/RegData/etudes/STUD/2017/ 583124/IPOL_STU(2017)583124_EN.pdf>.

carried out by an independent supervisory authority[65]. Finally, it observed that the interferences which the envisaged agreement entails were not all limited to what is strictly necessary and were therefore not entirely justified[66].

The previous opinion in this case, issued by Advocate General Mengozzi on 8 September 2016, stressed that the draft agreement was not ready to be ratified, because it was incompatible with Article 16 TFEU and Articles 7 and 8 of the Charter. Expressing the need for a fair balance between public security and privacy and data protection, Mengozzi established lists of compatibility requirements and incompatibility features in relation to the Charter. The list of requirements for compatibility included: clear categories of attributes of PNR (with no sensitive data included), an exhaustive list of offences, identification of an authority responsible for PNR oversight, limitation of targets to reasonable suspicion, limited and specified access rights and justification for a five-year-retention period. Mengozzi also required a prior review of transfers and the monitoring by an independent Canadian authority. At the same time, his list of incompatibilities with the Charter referred to: the processing of PNR data outside the public security objective of fighting terrorism and serious transnational crime, processing of sensitive data, the right to disclose information beyond the objective, authorisation to retain PNR data for five years beyond the objective as well as transfers without prior assessment by the competent Canadian authority.

In its judgment, the Court held that all international agreements form part of the EU legal order and must be compatible with the Treaties and principles and that the PNR agreement between EU and Canada is an external equivalent of a legislative act. In the view of the Court, processing of PNR, as it is with all personal data, affects the right to privacy and data protection. It can be justified that the legitimate objectives of protecting public security, fighting terrorism and serious transnational crime are good excuses if the agreement does not adversely affect the essence of either right.

Nevertheless, the necessity of such intrusion was not clear and the agreement neither sufficiently specified the personal data to be transferred nor did it justify the processing of sensitive data for the purposes revealed. Machine models and criteria used to analyse PNR must be specific, reliable and non-

---

[65] See also Opinion C-1/15 *European Commission v Republic of Austria*, ECLI:EU:C:2016:656, Opinion of AG Mengozzi <http://curia.europa.eu/juris/documents.jsf?num=C-1/15>.

[66] *EU and Canada PNR Agreement Invalid* (SCL The IT Law Society 2016), <https://www.scl.org/news/3734-eu-and-canada-pnr-agreement-invalid>.

discriminatory, while cross-checking databases must be accurate and appropriate. The primary purpose of such processing should be, in the opinion of the Court, limited to what is strictly necessary. The retention of the data of all passengers after their departure from Canada is not strictly necessary, while it may be justifiable to retain data on specific individuals if based on objective criteria and following a prior review of the court or an independent body. The Court of Justice stated that the agreement did not guarantee in a sufficiently clear and precise manner the oversight of data protection safeguards by an independent authority not subject to external influence. In conclusion, the current draft of the agreement was incompatible with Articles 7, 8, 21 (non-discrimination) and 52(1) of the Charter.

8. EPILOGUE

The current discussion on the European expectations towards guarantees given for transfer of data outside the zone recognised as secure and on the future of domestic data protection regimes in what was a third pillar of the European Union in the past, takes place at the same time as two other challenges. American lawmakers are working on the reform of FISA Section 702, remembering it will expire on 31 December 2017. The so-called "Section 702" is still the main legal basis for mass surveillance activities in the United States, including the programs and tools used in case of data stored by non-US persons and entities on American servers[67].

At the same time, the actions by Maximilian Schrems continue and are expected to reach the Court of Justice in Luxembourg again. In the next months, another look will be taken at how US law protects the privacy rights of European customers, possibly together with the Court's assessment of the new Privacy Shield agreement. Both factors may significantly affect the practice of international transfers of data. Nevertheless, the principles described by the Article 29 Working Party and confirmed by the Courts in Luxembourg and Strasbourg will definitely stay the same.

9. SELECTED LITERATURE

Bignami F, *The US Legal System on Data Protection in the Field of Law Enforcement. Safeguards, Rights and Remedies for EU Citizens* (Study for the LIBE

[67] Fransesca Bignami, *The US Legal System on Data Protection in the Field of Law Enforcement. Safe-guards, Rights and Remedies for EU Citizens* (Study for the LIBE Committee 2015) 22-29 <http:// www.europarl.europa.eu/RegData/etudes/STUD/2015 /519215/IPOL_STU(2015) 519215_EN.pdf>.

Committee 2015) <http://www.europarl.europa.eu/RegData/etudes/STUD /2015/519215/ IPOL_STU(2015)519215_EN.pdf>

Bigo D and others, 'National Security and Secret Evidence in Legislation and before the Courts: Exploring the Challenges' (2015) 78 Liberty and Security in Europe 77-79 <http://www. europarl.europa.eu/RegData/etudes/STUD/ 2014/509991/IPOL_STU (2014)509991_EN.pd.>

Boeke S and Eijkman Q, 'State Surveillance in Cyber Space: A new perspective on digital data practices by intelligence dervices', in Jarvis L, MacDonald S and Chen T M (ed.) *Terrorism Online: Politics, Law and Technology* (Routledge 2016) 128-131

Bygrave L A, *Data Privacy Law. An International Perspective* (Oxford University Press 2014)

Carrera S and others, *Access to Electronic Data by Third-Country Law Enforcement Authorities: Challenges to EU Rule of Law and Fundamental Rights* (Centre for European Policy Studies Study 2015) 74

Cate F H, Dempsey J X (eds) *Bulk Collection: Systematic Government Access to Private-Sector Data* (Oxford University Press 2017)

Colonna L, *Legal Implications of Data Mining: Assessing the European Union's Data Protection Principles in Light of the United States Government's National Intelligence Data Mining Practices* (PhD thesis, Stockholm University 2016) 193

EU and Canada PNR Agreement Invalid (SCL The IT Law Society 2016), <https:// www.scl.org/news/3734-eu-and-canada-pnr-agreement-invalid>

European Digital Rights (EDRi), 'European Court Opinion: Canada PNR cannot be signed', <https://edri.org/european-court- opinion-canada-pnr-deal-cannot-be-signed/>

Friedman D, *Future Imperfect: Technology and Freedom in an Uncertain World* (Cambridge University Press 2008) 66-79

Hijmans H, 'PNR Agreement EU-Canada Scrutinised: CJEU Gives Very Precise Guidance to Negotiators' (2017) European Data Protection Law Review 310

Hijmans H, *The European Union as a Constitutional Guardian of Internet Privacy and Data Protection: The Story of Article 16 TFEU* (Springer International Publishing 2016) 267

Horowitz S, *'Foucalt's* Panopticon: A Model of NSA Surveillance?' in Russel A. Miller, *Privacy and Power: A Transatlantic Dialogue in the Shadow of the NSA-Affair* (Cambridge University Press2017) 39-62

Hustinx P, 'European Leadership in Privacy and Data Protection' in Artemi Rallo Lombarte and Rosario García Mahamut (eds), *Hacia un nuevo régimen europeo de protección de datos* (Tirant Lo Blanch 2015) 18

Knapp K, 'The Social Construction of Computational Surveillance: Reclaiming Agency in a Computed World' (PhD thesis, London School of Economics and Political Science 2016) 26

Lenaerts K and Van Nuffel P, *European Union Law*, (3rd edn, Sweet & Maxwell 2011) 141

Marx G T, 'Coming to Terms: The Kaleidoscope of Privacy and Surveillance', in Beate Roessler and Dorota Mokrosinska (eds) *Social Dimensions of Privacy: Interdisciplinary Perspectives* (Cambridge University Press 2015) 33-34

Miller R A, *Privacy and Power: A Transatlantic Dialogue in the Shadow of the NSA-Affair* (Cambridge University Press 2017)

Monteleone S and Puccio L, *From Safe Harbour to Privacy Shield: Advances and shortcomings of the new EU-US data transfer rules* (European Parliamentary Research Service In-Depth Analysis 2017) 11

Rotenberg M and others, 'Enforcing Privacy Rights: Class Action Litigation and the Challenge of cy pres' in David Wright and Paul de Hert, *Enforcing Privacy. Regulatory, Legal and Technical Approaches* (Springer 2016) 307-334

Sanchez Ferro S, 'The Need for an Institutionalized and Transparent Set of Domestic Legal Rules Governing Transnational Intelligence Sharing in Democratic Societies' in Miller R A, *Privacy and Power: A Transatlantic Dialogue in the Shadow of the NSA-Affair* (Cambridge University Press 2017)

Schuster S (ed.) *Mass Surveillance: Part 1 - Risks and opportunities raised by the current generation of network services and applications* (STOA Report European Parliamentary Research Service, Brussels, 2015) 8

Solove D, *The Digital Person: Technology and privacy in the information age* (NYU Press 2004) 168-180

Stiennon R, *There Will Be Cyberwar: How the Move To Network-Centric War Fighting Has Set The Stage For Cyberwar* (IT-Harvest Press 2015) 67-77

Swire P, 'US Surveillance Law in a constitutional democracy, Safe Harbor, and Reforms since 2013' in Dan Svantesson and Dariusz Kloza (eds), *Trans-Atlantic Data Privacy Relations as a Challenge for Democracy* (Intersentia 2017) 85-126

Taylor M, 'Flying from the EU to the US: necessary extraterritorial legal diffusion in the US-EU Passenger Name Record agreement' (2015) 19 Spanish Yearbook of International Law 223-225

Vermeulen G, 'The Paper Shield. On the degree of protection of the EU-US Privacy Shield against unnecessary or disproportionate data collection by the US intelligence and law enforcement services' in Dan Svantesson and Dariusz Kloza, *Trans-Atlantic Data Privacy Relations as a Challenge for Democracy* (Intersentia 2017) 127-147

Vladeck D, 'Separated by Common Goals: A U.S. Perspective on Narrowing the U.S.-E.U. Privacy Divide' in Lombarte AR and Mahamut RC (eds) *Hacia un nuevo régimen europeo de protección de datos* (Tirant Lo Blanch 2015)

Weiss M A and Archick K, 'U.S.-EU Data Privacy: From Safe Harbor to Privacy Shield, Congressional Research Service report', <https://fas.org/sgp/crs/misc/R44257.pdf>

Wensink W, Warmenhoven B, Haasnoot R et al., 'The European Union's Policies on Counter-Terrorism: Relevance, Coherence and Effectiveness', (Brussels 2017) 121-123 <http://www.europarl.europa.eu/RegData/etudes/STUD/2017/ 583124/IPOL_STU(2017)583124_EN.pdf>

Zedner L, 'Why Blanket Surveillance Is No Security Blanket: Data Retention in the United Kingdom after the European Data Protection Directive' in Miller R A, *Privacy and Power: A Transatlantic Dialogue in the Shadow of the NSA-Affair* (Cambridge University Press 2017) 564-585

Who's watching the watchers?

Between transparency and secrecy in intelligence oversight and the question of trust[1]

MARIO OETHEIMER & IOANNIS KOUVAKAS[2]

1. INTRODUCTION

In his best-known Socratic dialogue on justice, government and morality, *The Republic*, Plato describes the perfect society, which, among others, consists of a guardian class, entrusted with the task to protect the polity. Consequently, the key question put to Socrates is who will guard the guardians. The solution that Plato proposed to this essential problem of the state was that they will guard themselves against themselves. They will be told a *"noble lie"*, which will assure them that they are better than the ones they need to serve and it is thus their duty to protect the lesser.[3] The noble lie will instil in them a distaste for power and privilege, and inculcate values so that the guardians would uphold the integrity of rules.

Subsequent historical developments have apparently suggested that this strategy can be far from successful. Totalitarian regimes and their large-scale atrocities have led to the adoption of several legislative instruments and declarations,[4] which, in an effort to ensure respect for fundamental rights and freedoms, seek to identify rules and establish effective mechanisms to control the actions of those in power.[5] Most of these mechanisms enable individuals to effectively lodge complaints, either individually or collectively, and to seek redress before both national and international redress mechanisms, which are, as a result, fully empowered to thoroughly investigate claims against

---

[1] The views expressed are solely those of the authors and do not necessarily represent the views or position of the European Union Agency for Fundamental Rights (FRA).

[2] Head respectively trainee, Sector Information Society, Privacy and Data Protection, FRA. Email: Mario.Oetheimer@fra.europa.eu; Ioannis.Kouvakas@fra.europa.eu.

[3] Allan Bloom, *The Republic of Plato* (2nd edn, Basic Books 1991) 93 ff.

[4] See, for example, United Nations General Assembly (UNGA), Resolution 217 (10 December 1948), Universal Declaration of Human Rights (UDHR); Council of Europe (CoE), Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR) (1950).

[5] See, among others, UDHR Preamble; ECHR Preamble.

state authorities, conduct open hearings, compel crucial evidence and publicly hand down binding decisions.[6]

States remain confronted with the safeguarding of their citizens' rights. In the field of national security, security and intelligence services surface as modern guardians, tasked to collect, analyse and disseminate information relating to domestic and external threats respectively.[7] One of the methods deployed by these services is secret surveillance, which in the digital era attracts enhanced significance and persists as a rare field where the access of individuals to information is limited.[8] The effectiveness of these measures is inextricably connected to their covert nature[9] and leads to the "political paradox" of modern democracies relying for their protection on secret methods.[10] As a result, the latter have to rely often on third parties, which may exercise control of the aforementioned activities and ensure fundamental rights, ie privacy, are protected.

The European Court of Human Rights (ECtHR) has recognised that *"the existence of some legislation granting powers of secret surveillance over the mail, post and telecommunications is, under exceptional conditions, necessary in a*

---

[6] ECHR art 34.

[7] Hans Born and Gabriel Geisler Mesevage, 'Introducing intelligence oversight', in Hans Born and Aidan Wills (eds), *Overseeing Intelligence Services: A Toolkit* (Geneva Centre for the Democratic Control of Armed Forces (DCAF) 2012); Jean-Claude Cousseran and Philippe Hayez, *Renseigner les démocraties, renseigner en démocratie*, (Odile Jacob, 2015) 41. The lines between domestic and external threats could be sometimes blurred, however. See United Nations Human Rights Council (UNHRC), 'Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, Martin Scheinin: Compilation of good practices on legal and institutional frameworks and measures that ensure respect for human rights by intelligence agencies while countering terrorism, including on their oversight' (A/HRC/14/46, 17 May 2010) 4.

[8] UNGA, 'Resolution adopted by the General Assembly on 18 December 2013: The right to privacy in the digital age' (A/RES/68/167, 21 January 2014).

[9] See, for example, *Liberty (The National Council of Civil Liberties) and Others v The Secretary of State for Foreign and Commonwealth Affairs and Others* [2015] UKIPTrib 13_77-H (2015), para 13.

[10] Laurie Nathan, 'Intelligence Transparency, Secrecy, and Oversight in a Democracy' in Hans Born and Aidan Wills (n 7) 49.

democratic society in the interests of national security and/or for the prevention of disorder or crime".[11] In order to balance secrecy with the need of effective protection against abuse, the ECtHR has adopted a protective approach[12] as regards claimants' standing in cases of covert surveillance, assuming the individual's status as a victim and rendering applications admissible without specific details on rights' interference.[13]

Following the Snowden revelations in 2013, which exposed the invasive nature of governmental surveillance programmes and triggered several national and international parliament inquiries into the impact of covert communications' interception on fundamental rights, light was shed into an area of activities of the executive, which up to then was embedded in secrecy. The public perception was fed by totalitarian memories of the past and, in the events that followed, government officials were compared to Stasi officers or even to Orwell's 1984 Big Brother.[14]

Moreover, a European Parliament inquiry into the electronic mass surveillance of EU citizens[15] led, among others, to a request to the EU Agency for Fundamental Rights (FRA) to thoroughly research human rights protection

[11] *Klass and Others v Germany* App no 5029/71 (ECtHR, 6 September 1978) para 48.

[12] *Weber and Saravia v Germany* App no 54934/00 (ECtHR, 29 June 2006) paras 78-79; *Liberty and Others v UK* App no 58243/00 (ECtHR, 1 July 2008) para 57. See also the similar stance followed by the Court of Justice of the European Union (CJEU) and the emphasis placed on notification requirements, Joined Cases C-293/12 and C-594/12, *Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others and Seitlinger and Others* EU:C:2014:238, para 37; Joined Cases C–203/15 and C–698/15, *Tele2 Sverige AB v Post- och telestyrelsen and Secretary of State for the Home Department v Tom Watson* EU:C:2016:970, para 121.

[13] *Zakharov v Russia* App no 47143/06 (ECtHR, 4 December 2015) para 171. See also European Union Agency for Fundamental Rights, *Surveillance by intelligence services: fundamental rights safeguards and remedies in the EU, Volume II: field perspectives and legal update* (European Union Agency for Fundamental Rights 2017) 33-34.

[14] Laura Heins, 'The Intimacy of Stasi Surveillance, the NSA-Affair, and Contemporary German Cinema', in Russell A. Miller (ed.), *Privacy and Power: A Transatlantic Dialogue in the Shadow of the NSA-Affair* (CUP 2017) 643 ff.

[15] See '*Inquiry on Electronic Mass Surveillance of EU Citizens. Protecting Fundamental Rights in a Digital Age*' (European Parliament, LIBE Committee, Proceedings, Outcome and Background Documents 2013-2014).

in the context of surveillance.[16] FRA published a mapping report in 2015 analysing the legal frameworks on surveillance in place in the 28 EU Member States.[17] Additionally and to better assess the implementation of surveillance legislation in practice, it initiated fieldwork research in 2016, interviewing actors from intelligence oversight, expert bodies and national human rights institutions, as well as academia, lawyers and civil society organisations from 7 EU Member States. In October 2017, the FRA published a second report. This report contains comparative research findings, Member State promising practices and FRA opinions, namely suggestions to policy makers and legislators, on three main issues relating to surveillance: legal frameworks, oversight and remedies.[18]

The Snowden revelations had also an impact on national and European or international human rights adjudication,[19] with the ECtHR and the CJEU declaring surveillance or telecommunications retention regimes incompatible with the ECHR or EU law, respectively. Both courts sought to articulate strict standards that (targeted) surveillance must meet and placed particular emphasis on the need of effective control of surveillance activities through oversight.[20]

Drawing upon the relevant case law, international standards and literature, as well as findings from the 2015 and 2017 reports of the EU Agency for Fundamental Rights from fieldwork research, this paper will discuss three challenging aspects of intelligence oversight, namely independence, powers and competence, and public scrutiny. It will be argued that, despite major developments and improvements, full transparency is unrealistic in a field that by its very nature requires secrecy to be efficient. It is, thus, crucial to equip oversight bodies with all the necessary guarantees relating to the three aforementioned aspects, as well as with a mandate allowing also for an assessment of

---

[16] '*Resolution on the US NSA surveillance programme, surveillance bodies in various Member States and their impact on EU citizens' fundamental rights and on transatlantic cooperation in Justice and Home Affairs*' (European Parliament, 2013/2188(INI)), P7_TA (2014)0230, 2014), para 132.

[17] European Union Agency for Fundamental Rights, *Surveillance by intelligence services: fundamental rights safeguards and remedies in the EU – Mapping Members States' legal framework* (European Union Agency for Fundamental Rights 2015).

[18] European Union Agency for Fundamental Rights 2017 (n 13) 18.

[19] *Liberty* (n 9), paras 4 and 158; *Zakharov* (n 13), concurring opinion of Judge Dedov, pages 83-89.

[20] ibid *Zakharov*; *Szabo and Vissy v Hungary* App no 37138/14 (ECtHR, 12 January 2016); *Digital Rights Ireland* (n 12); *Watson* (n 12).

the proportionality of covert surveillance, which will assure individuals that their fundamental rights are respected in practice.

2. THE EU DIVERSE LANDSCAPE OF INTELLIGENCE OVERSIGHT

It would be necessary to draw some distinctions between, first, the various actors involved in intelligence oversight and, second, the stages of oversight in which these actors are involved (see Figure 1 below). FRA research suggests that oversight frameworks are organised in extremely diverse ways among EU Member States.[21] The lack of a uniform oversight model could be mainly attributed to the political, administrative and judicial organisation of each Member State. National oversight frameworks provide for several institutions, such as parliamentary committees, independent judicial or expert bodies, data protection authorities as well as other actors that perform watchdog functions. In particular, 21 Member States have one or more specialised parliamentary committees, while 16 Member States have set up one or more expert bodies, including data protection authorities, having competences in intelligence oversight.[22] The role of these institutions varies from the mere fiscal control of intelligence agencies to the legal authorisation of surveillance measures or the power to cease such measures upon the finding of an unlawful conduct.[23]

[21] European Union Agency for Fundamental Rights 2017 (n 13) 56.

[22] ibid 66-67.

[23] ibid 64 ff.

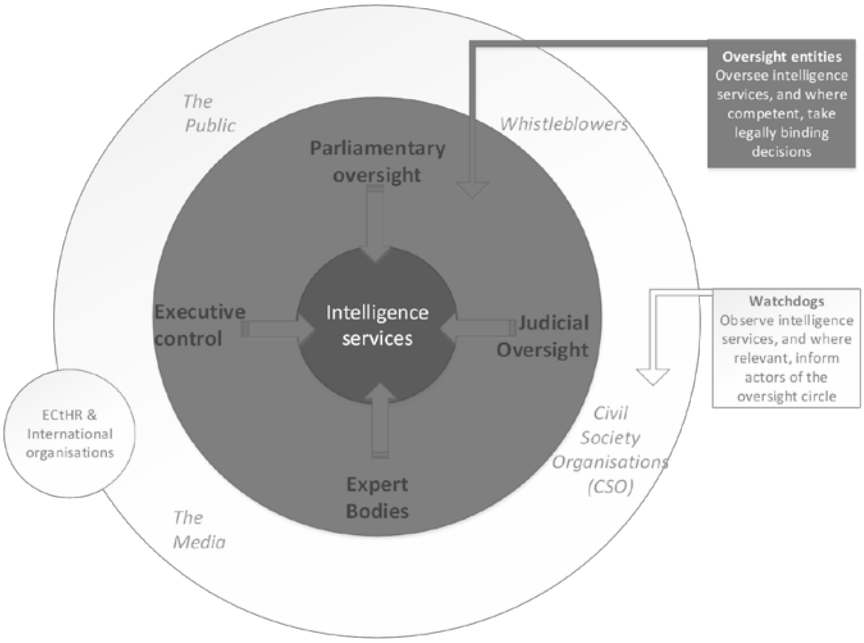


Figure 1. Intelligence services' accountability scheme (European Union Agency for Fundamental Rights, 2017)

Oversight involvement may take place either at an *ex ante*, namely before the implementation of a surveillance measure, or at an ongoing and *ex post* stage, namely during and until the end of the implementation.[24] Despite the great diversity of oversight actors and their roles, independence, powers and competence, and public scrutiny, have been recognised, by the ECtHR as three key features that contribute to the strengthening of the intelligence services' accountability.[25] These elements were also identified by the FRA fieldwork participants.[26]

[24] ibid 93 ff.

[25] ibid 73.

[26] ibid 74; see also Annex I 153 ff.

2.1. Independence (and "non-judicial" independence)

In its early case law concerning challenges against surveillance measures, the ECtHR acknowledged the importance of the judiciary for effectively preventing rights' violations and favoured oversight settings involving judges.[27] In *Klass and Others v Germany*, the Court underlined:

> [I]n a field where abuse is potentially so easy in individual cases and could have such harmful consequences for democratic society as a whole, it is in principle desirable to entrust supervisory control to a judge.[28]

Nevertheless, since several national courts were willing to defer matters regarding secret surveillance to the executive, as being the one better placed to decide what kind of action is most appropriate to prevent and detect serious threats to national security, and simultaneously lacked the appropriate technical expertise to thoroughly examine the compatibility of constantly evolving technological developments with human rights,[29] the case law has accepted that oversight could be also carried out by non-judicial bodies, provided these institutions are equipped with impartiality guarantees.

The Grand Chamber of the ECtHR in its landmark judgment in the case of *Roman Zakharov v Russia* recognised that non-judicial supervision of surveillance activities may be also compatible with the ECHR, *"provided that the oversight body is independent of the authorities carrying out the surveillance"*.[30]

Independence does not only mean the lack of any external influences or a mere legal obligation on the oversight body to act impartially. It may, additionally, entail the proportionate representation of all parties, for instance, in

---

[27] In the majority of EU Member States oversight of intelligence services is carried out by judicial bodies, see European Union Agency for Fundamental Rights 2015 (n 13) 51 ff.

[28] *Klass* (n 11) para 56.

[29] Cf, for example, the relevant UK House of Lords judgments which have repeatedly underscored this point, *Secretary of State for the Home Department v Rehman* [2001] UKHL 47, para 62; *A v Secretary of State for the Home Department* [2004] UKHL 56, para 78; *R (Lord Carlile) v* Secretary of State for the Home Department [2014] UKSC 60, para 159.

[30] *Zakharov* (n 13) para 275. See also *Digital Rights Ireland* (n 12) para 62.

oversight parliamentary committees or require the physical separation of the body's central office from the ministry or generally governmental building.[31]

The FRA research findings indicate that, although the majority of interviewees considered their oversight bodies to be independent, some concerns were raised regarding the appointment of the bodies' members by the executive and instructions frequently issued by the latter on how to perform their duties.[32] To tackle this issue, the French National Commission of Control of the Intelligence Techniques (CNCTR), for example, besides its statutory footing, also relies for the exercise of its functions on ethical rules, introduced by the French law on intelligence, which, among others, specify that the Commission members should not receive any instructions from any authority, and that they should not have incompatible mandates, links to the intelligence services, or perform any other profession or elective duty.[33]

2.2. Powers and competence

An oversight body that is secure from external influences also requires a strong mandate that puts all the necessary means to its disposal, in order to perform its functions efficiently, as underlined by the relevant European jurisprudence. [34] The term "powers and competence" mainly refers to the oversight body's expertise, the ability to intervene at various surveillance stages and issue binding decisions, and its access to (classified) information concerning the activities of the intelligence services.[35]

In *Weber and Saravia v Germany*, the ECtHR considered the compatibility of the German surveillance law (the "amended G 10 Act"), as further restricted by the German Constitutional Court, with the ECHR and summarised the aforementioned requirements as follows:

---

[31] European Union Agency for Fundamental Rights 2015 (n 13) 39. See also Hans Born and Ian Leigh, *Making intelligence accountable: Legal standards and best practice for oversight of intelligence agencies* (Publishing House of the Parliament of Norway, 2005) 85. See also Case C-518/07 *European Commission v Federal Republic of Germany* ECLI:EU:C:2010:125, [2010] ECR I-1885, paras 23 and 30; Case C-614/10 *Commission v Austria* ECLI:EU:C:2012:631 [2012], paras 36–37; Case C-288/12 *Commission v Hungary* ECLI:EU:C:2014:237 [2014], paras 47–48.

[32] European Union Agency for Fundamental Rights 2017 (n 13) 74-75.

[33] Interior Security Code (Code de la sécurité intérieure) 2012, art L832–1 and art L832–2.

[34] *Zakharov* (n 13) para 275.

[35] European Union Agency for Fundamental Rights 2017 (n 13) 75.

> As regards supervision and review of monitoring measures, the Court notes that the G 10 Act provided for independent supervision by two bodies which had a comparatively significant role to play. Firstly, there was a Parliamentary Supervisory Board, which consisted of nine members of parliament, including members of the opposition. The Federal Minister authorising monitoring measures had to report to this board at least every six months. Secondly, the Act established the G 10 Commission, which had to authorise surveillance measures and had substantial power in relation to all stages of interception. The Court observes that in its judgment in Klass and Others it found this system of supervision, which remained essentially the same under the amended G 10 Act in issue here, to be such as to keep the interference resulting from the contested legislation to what was "necessary in a democratic society.[36]

2.2.1. Necessary expertise

The constant technological developments have enabled security and intelligence services to develop new surveillance measures.[37] Paired with the need to ensure that the required checks and balances are carried out effectively, oversight bodies are nowadays confronted with a large pile of technical information.

As FRA research suggests, these actors usually lack not only adequate resources (such as time and money) to allow them for an in-depth examination of all the necessary material regarding the activities and tasks of the intelligence services, but also the necessary expertise in terms of human resources.[38] This desperate need of "more computer people", as one fieldwork interviewee has characterised it,[39] signals the necessity for oversight bodies to adapt to contemporary circumstances, a necessity which could be adequately satisfied through the participation of oversight bodies' personnel in IT seminars and training, as well as through the cooperation of the staff with information technology and national security/intelligence specialists, provided, of course, that these bodies are granted adequate funding. For example, the Dutch oversight body, the Review Committee on the Intelligence and

---

[36] *Weber and Saravia* (n 12) paras 117-118.

[37] David Anderson, *Report of the Bulk Powers Review* (Independent Review of UK Terrorism Legislation, Cm 9326, 2016) 102; *Szabo and Vissy* (n 20) para 68.

[38] European Union Agency for Fundamental Rights 2017 (n 13) 85.

[39] ibid.

Security Services (*CTIVD*), has invested additional financial resources in technical expertise, by establishing in 2014 a "knowledge network" of scientific experts in the fields of security and information technology who regularly advise the Review Committee on reports relating to legislative, technological and legal developments.[40]

In addition, the diversity of oversight actors' mandates contributes to the fragmentation of their tasks. For instance, a few Member States' data protection authorities are sometimes entrusted with oversight tasks but their powers and role are limited to a mere examination of human rights compatibility issues, in the context of surveillance,[41] while audit institutions may be, accordingly, tasked with the sole duty of financially inspecting the services.[42] Albeit necessary in order to ensure that various safeguards are in place and that surveillance activities are constantly controlled and challenged through various avenues and prisms – from parliamentary committees to civil society organisations and whistle-blowers-, this diversity of mandates should be coupled with cooperation. As shown by FRA's findings, the danger of fragmentation leading to bureaucratic inefficiency could be thus avoided through the implementation of a "constant dialogue" framework, where oversight actors could exchange the (non-classified) information at their disposal as well as their observations and concerns, providing context and substance to each other's duties.[43]

2.2.2. Binding powers

A strong cooperation framework between the various oversight actors could also compensate for the inability of some to make binding interventions. The ECtHR places emphasis on the active participation of the oversight body in the surveillance process, namely its ability to initiate investigations, to quash interception warrants, to order the halt of surveillance measures at any stage of their implementation upon the finding of an irregularity, or to impose (administrative) sanctions on employees of the intelligence services. The importance of this oversight aspect for ensuring accountability of intelligence services was also confirmed by the FRA surveillance fieldwork participants.[44]

---

[40] Review Committee on the Intelligence and Security Services (Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten, CTIVD), *Annual Report 2014-2015* (CTIVD, 2015) 10.

[41] European Union Agency for Fundamental Rights 2017 (n 13) 80.

[42] ibid 61.

[43] ibid 86.

[44] ibid 73 ff.

The requirement of binding powers is easily satisfied when oversight is conducted by a judicial body, whose constitutional standing allows for the binding (and sometimes immediate) effect of its decisions. However, non-judicial oversight bodies have been confronted with laws limiting their binding powers, in an effort to emphasise their existence more as an audience rather than a participant in the surveillance play.[45]

Against this "tied hands" practice, France has identified a balancing solution between passive and active participation. In particular, if the CNCTR considers that a surveillance measure is carried out unlawfully, then it can recommend its ceasing and the destruction of any data obtained to the prime minister, the relevant minister and the intelligence service. The prime minister must then immediately inform the CNCTR whether and how the recommendation was followed.[46] In case the CNCTR considers that its recommendation was not appropriately followed, then it can bring the case before the French Council of State (*Conseil d' Etat*).[47]

The UK and Sweden have, among other Member States, also provided more or less for binding powers of oversight bodies, with the Judicial Commissioners (JCs) being able to reject applications for interception warrants or quash those in operation,[48] and the State Inspection for Defence Intelligence Operations (SIUN) stopping on going signals surveillance and ordering the subsequent destruction of collected data when detecting incompliance, respectively. The German G 10 Commission is similarly tasked with ensuring that strategic surveillance, ie the interception of communications between Germany and foreign countries- is "permissible and necessary".[49]

---

[45] For an analytical examination of non-judicial oversight bodies' powers across the EU, see ibid 75 ff.

[46] Interior Security Code (n 33) art L833-6.

[47] ibid art L833-8.

[48] Investigatory Powers Act 2016 (IPA) part 2.

[49] Act on Restricting the Privacy of Correspondence, Posts and Telecommunications (art 10, G10 Act) (*Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses, Artikel 10, Gesetz G10)*, 2001, as amended, Section 15 (5).

2.2.3. Full access

The exercise of the powers and competence of oversight bodies to their fullest possible extent is inextricably linked with their access to intelligence related information. On the other hand, both national and international courts have acknowledged that a full disclosure of the services' techniques and operational strategies might be devastating for national security.[50]

In 2014, several NGOs led by Liberty challenged the framework for the reception, use, storage and transmission by UK authorities of material initially intercepted by foreign authorities and later shared to the former. In the course of the hearings, GCHQ agreed to disclose two paragraphs from an internal policy document, which provided "an adequate indication"[51] of the nature and content of the already existing arrangements within the services. The IPT held that *"prior to the disclosures made […], the regime governing the soliciting, receiving, storing and transmitting by UK authorities of private communications of individuals located in the UK, which have been obtained by US authorities pursuant to Prism and/or […] Upstream, contravened Articles 8 or 10 ECHR"*,[52] since there was insufficient information in the public domain. It then went on to state that after the aforementioned disclosures the regime now complied with human rights.[53] The IPT Liberty case is a good example, indicating the hesitation of the intelligence services to go public about their activities, even when those activities are deemed to be human rights compatible, and the need for a balance to be struck between full disclosure and secrecy in the national security context.[54]

---

[50] *Liberty* (n 9) para 38.

[51] ibid para 159. See also, *Malone v UK* App no 8691/79 (ECtHR, 2 August 1984) para 67.

[52] *Liberty (The National Council of Civil Liberties) and Others v The Secretary of State for Foreign and Commonwealth Affairs and Others* [2015] UKIPTrib 13_77-H (2015), para 23.

[53] On the question of whether "soft-law" practices and internal policies could pass the legality and foreseeability threshold, see Natasha Simonsen, 'The Investigatory Powers Tribunal and the rule of law' (UK Human Rights Blog, 16 February 2015) <https://ukhumanrightsblog.com/2015/02/16/the-investigatory-powers-tribunal-and-the-rule-of-law-natasha-simonsen>.

[54] For a discussion on the use of secret (intelligence) evidence before courts in the context of national security, see European Parliament, Directorate General for Internal Policies, Policy Department C: Citizens' Rights and Constitutional Affairs, Justice Freedom and Security, 'National Security and Secret Evidence in Legislation and before the

In a non-judicial context, oversight bodies are often confronted with limited access to intelligence relevant documents, policies and practices, which accordingly circumvents their ability to effectively examine the lawfulness of surveillance operations. The ECtHR has highlighted the importance of autonomous oversight, which could be defined as not relying on the intelligence services' willingness to provide information, and the need for *"the supervisory body [to have] access to all relevant documents, including closed materials and that all those involved in interception activities have a duty to disclose to it any material it require[s]"*.[55]

EU Member States seem to gradually absorb this access requirement into the statutory mandates of non-judicial expert bodies that are tasked with oversight functions.[56] For example, the Dutch CTIVD, which investigates whether surveillance activities are carried out in accordance with the existing legislative framework, is granted unlimited and direct access to the information held by the General Intelligence and Security Services (AIVD).[57] Also, the French CNCTR enjoys permanent, complete and direct access to the services' reports concerning the implementation techniques, as well as to any data intercepted and retained.[58]

The issue of access to information is more evidently witnessed in the context of international intelligence cooperation. The internationalisation of national security threats has intensified the need for joint operations as well as for intelligence sharing between various national agencies.[59] On the other hand, in *Al Nashiri v Poland*, the ECtHR characterised the oversight issues stemming from international intelligence cooperation as *"a more general problem of*

Courts: Exploring the Challenges' (European Parliament, 2014); *Secret Evidence* (Publication, Justice 2009) <http://www.statewatch.org/news/2009/jun/ uk-justice-secret-evidence-report.pdf>.

[55] *Zakharov* (n 13) para 281; *Kennedy v UK* App no 26839/05 (ECtHR, 18 May 2010) para 166.

[56] For a comparative overview of the current state of play as regards access to information of non-judicial supervisory bodies, European Union Agency for Fundamental Rights 2017 (n 13) 79 ff.

[57] Review Committee on the Intelligence and Security Services (Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten, CTIVD), *Annual Report* 2013-2014 (CTIVD, 2015) 10.

[58] Interior Security Code (n 33) art L833-2.

[59] *Szabo and Vissy* (n 20) para 78; David Anderson, *A Question of Trust. Report of the Investigatory Powers Review* (Independent Review of UK Terrorism Legislation, 2015) 198.

democratic oversight of intelligence services" and highlighted the need for adequate safeguards and guarantees also in that regard.[60] It is hence, essential, that oversight also extends to data exchanges between states' intelligence services and that supervisory actors are not excluded from accessing the relevant policies and information.[61] According to FRA recent research findings, certain Member States, namely Belgium, Sweden and the Netherlands, have provided for the full access of their respective oversight bodies also in the field of international intelligence cooperation.[62]

2.3. **Public scrutiny**

The cases and issues discussed in the previous sections refer to the overseeing of the intelligence services' activities by oversight bodies set up by law, such as parliamentary committees, data protection authorities and independent expert bodies. Our analysis has left out two other important actors in the surveillance play: civil society organisations and the public. Since, by definition, members of the public should be kept unaware of the actual implementation and extent of surveillance techniques, otherwise a general disclosure of intelligence strategies would ultimately imply the compromise of national security interests, these two actors are largely dependent upon the information provided to them by "official" supervisory bodies. In other words, transparency contributes to informing the public in a credible and reliable way about the operations undertaken by the intelligence services, as well as to assuring the public that these operations are carried out in a lawful manner.

When examining transparency (or, public scrutiny, according to the Court's terminology), the ECtHR seems to lay particular emphasis on whether the reports issued by oversight bodies are made available to the public.[63] In the case of *Szabo and Vissy v Hungary*, criticising the Hungarian oversight mechanism, which imposed an obligation on the Minister of Interior to present, at least twice a year, a report to the relevant parliamentary committee, regarding the activities of the national security services, the ECtHR noted that the

---

[60] *Al Nashiri v Poland* App no 28761/11 (ECtHR, 24 July 2014) para 498.

[61] Sarah Eskens, Ot van Daalen, Nico van Eijk, *Ten standards for oversight and transparency of national intelligence services* (Institute for Information Law (IViR) Report, University of Amsterdam, 2015) 30 ff.

[62] European Union Agency for Fundamental Rights 2017 (n 13) 107.

[63] See, *inter alia*, *Kennedy* (n 55) para 166; *Association for European Integration and Human Rights and Ekimdzhiev v Bulgaria* App no. 62540/00 (ECtHR, 28 June 2007) para 88.

Minister's report *"does not seem to be available to the public and by this appears to fall short of securing adequate safeguards in terms of public scrutiny"*,[64] while in *Roman Zakharov* it *pointed out:*

> In Russia, prosecutors must submit semi-annual reports detailing the results of the inspections to the Prosecutor General's Office. However, these reports concern all types of operational-search measures, amalgamated together, without interceptions being treated separately from other measures. Moreover, the reports contain only statistical information about the number of inspections of operational-search measures carried out and the number of breaches detected, without specifying the nature of the breaches or the measures taken to remedy them. It is also significant that the reports are confidential documents. They are not published or otherwise accessible to the public. It follows that in Russia supervision by prosecutors is conducted in a manner which is not open to public scrutiny and knowledge.[65]

However, considering that the efficiency of the surveillance techniques depends to a large extent upon their secrecy, full transparency in surveillance is neither feasible nor desirable. Given this inevitable secrecy, a public that is unable to understand why secret surveillance powers exist, what they actually entail, how they are regulated in law, exercised in practice and overseen by various supervisory institutions lacks the conceptual tools to engage in fruitful debates and is more likely to believe in allegations, myths and misconceptions that want the executive to constantly spy on citizens and curtail their right to privacy.[66] As the UK Shadow Home Secretary, Yvette Cooper, stated before the Intelligence and Security Committee (ISC) of the UK Parliament:

> [The work of the Agencies] depends on the framework of consent, and that depends on there being a level of knowledge and understanding as well. I think if we try to keep everything behind closed doors, the danger is that we will undermine the trust that we need for the Agencies to be able to do their work. So I think, in the end, it is damaging to

[64] *Szabo and Vissy* (n 20) para 82.

[65] *Zakharov* (n 13) para 281.

[66] See *Digital Rights Ireland* (n 12) para 37; *Malone* (n 51), Concurring Opinion of Judge Pettiti.

> confidence in the Agencies to try to keep everything too quiet and too silent. You need to build that confidence.[67]

Overall, FRA comparative research data shows that transparency requirements have been considerably taken into account by parliamentary committees and expert bodies and in some Member States examples of good practice can be found.[68] The reports of these supervisory bodies are not limited to a brief outline of the legislation and the services' powers but may, furthermore, contain statistical information on the number of individuals' under surveillance,[69] detailed numerical information on issued authorisations and outcomes of complaint processes,[70] recommendations to governments concerning good practices and legislative improvements,[71] as well as, in the case of parliamentary committees, extensive reporting on the budget of the intelligence services and the threats to national security during the reporting period,[72] and (full) transcripts of hearings.[73]

---

[67] *Privacy and Security Inquiry, Public Evidence Session 5, Uncorrected Transcript of Evidence given by: The Rt. Hon. Yvette Cooper, MP Shadow Home Secretary* (Intelligence and Security Committee of the UK Parliament, 2014) 10.

[68] European Union Agency for Fundamental Rights 2017 (n 13) 89, as well as Annexes 3 and 4 162-164.

[69] See, for example, *1er rapport d'activité 2015/2016* (National Commission on Control of Intelligence Techniques (*Commission nationale de contrôle des techniques de renseignement, CNCTR*, 2016) 73; *Bericht gemäß § 14 Absatz 1 Satz 2 des Gesetzes zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses (Artikel 10-Gesetz-G 10) über die Durchführung sowie Art und Umfang der Maßnahmen nach den §§ 3, 5, 7a und 8G 10* (German Federal Parliament (*Deutscher Bundestag*), Drucksache 18/11227, 2017) 5 <https://dip21.bundestag.de/dip21/btd/18/112/1811227.pdf>.

[70] European Union Agency for Fundamental Rights (n 13), *Annual Report 2015* (Review Committee on the Intelligence and Security Services 2016) 23 ff <https://english.ctivd.nl/binaries/ctivd-eng/documents/annual-reports/2017/07/24/index/CTIVD+annual+report+2016.pdf>.

[71] *Activity report 2014-2015* (Belgian Standing Intelligence Agencies Review Committee (Standing Committee I) (*Comité permanent de Contrôle des services de renseignement et de sécurité, Comité permanent R*)2016) 87 ff and 169 ff <http://www.comiteri.be/images/pdf/Jaarverslagen/Activity_Report_2014_15.pdf.

[72] *Annual Reports* (United Kingdom Intelligence and Security Committee,): <http://isc.independent.gov.uk/committee-reports/annual-reports>.

[73] *2016 Annual Report* (Italy, Parliamentary Committee for the Intelligence and Security Services and for State Secret Control (*Comitato Parlamentare di Controllo per i Servizi di Informazione e Sicurezza e per il Segreto di Stato*, *COPASIR*) [in Italian]

3. PROPORTIONALITY AND PUBLIC TRUST

Unlike targeted surveillance, general (or untargeted) interception of communications, does not initially rely upon the existence of a prior suspicion against specified individuals or premises. The peculiarity of this surveillance technique lies in the fact that it, at a first stage, must intercept large quantities of data concerning individuals who pose no security threat or are of no interest to the security and intelligence services.[74] This data may be subsequently accessed by the services to identify potential threats to national security. The importance of such pre-emptive techniques in developing fragmentary intelligence or even enriching *"seed"* information, in the light of modern day evolvement of threats, is beyond doubt[75] and has been characterised as the *"need for the haystack to find the needle"*.[76]

Such broad powers raise, however, serious concerns in terms of proportionality. In his February 2017 Report, the UN Special Rapporteur on the Right to Privacy highlighted the need for a rigorous analysis of proportionality issues relating to general surveillance measures.[77] In the case of *Szabo and Vissy v Hungary*, the ECtHR noted:

> For the Court, it is a natural consequence of the forms taken by present-day terrorism that governments resort to cutting-edge technologies in pre-empting such attacks, including the massive monitoring of communications susceptible to containing indications of impending incidents. The techniques applied in such monitoring operations have demonstrated a remarkable progress in recent years and reached a level of sophistication which is hardly conceivable for the average citizen, especially when automated and systemic data collection is technically possible and becomes widespread. In the face of this progress the Court must scrutinise the question as to whether the development of surveillance methods resulting in masses of data collected has been

<http://www.parlamento.it/application/xmanager/projects/parlamento/file/Commissione_sicurezza_repubblica_XVII_Leg/RELAZIONE_ANNUALE_2016.pdf>.

[74] European Union Agency for Fundamental Rights 2015 (n 13) 18; David Anderson 2016 (n 37) 23 ff.

[75] ibid 122-124.

[76] *Privacy International v Secretary of State for Foreign and Commonwealth Affairs et al* [2016] UKIPTrib 15_110-CH (2017), para 14.

[77] Joseph A. Cannataci, *Report of the Special Rapporteur on the right to privacy* (United Nations Human Rights Council (UNHRC), A/HRC/34/60, 24 February 2017), paras 16-18.

> accompanied by a simultaneous development of legal safeguards securing respect for citizens' Convention rights.[78]

Although the Strasbourg Court acknowledged that *"it would defy the purpose of government efforts to keep terrorism at bay, thus restoring citizens' trust in their abilities to maintain public security, if the terrorist threat were paradoxically substituted for by a perceived threat of unfettered executive power intruding into citizens' private spheres by virtue of uncontrolled yet far-reaching surveillance techniques and prerogatives"*, [79] it did not address the issue of whether such general surveillance, pre-empting techniques could be held to be proportionate but limited itself to a thorough examination of the Hungarian legal framework and found a violation of article 8 at the legality stage.[80] In the joined cases of *Tele2 Sverige and Home Secretary v Watson*, which arose from a request for a preliminary ruling from Swedish and English national courts, respectively, and concerned the implications of the Luxembourg Court's judgment in *Digital Rights Ireland* for Member States' national data retention legislation, the CJEU Grand Chamber had also the opportunity to assess the proportionality of general measures interfering with the right to privacy, in the context of EU law.[81]

The CJEU, conceding that a blanket data retention obligation imposed on Internet Service Providers (ISPs) regarding the content of individuals' communications would be disproportionate (sic), because it would interfere with the essence of the rights enshrined in articles 7 and 8 of the Charter of Fundamental Rights of the European Union, chose to indirectly address the issue of proportionality of general communications data retention measures, ruling that such obligations are *per se* incompatible with the Charter as failing to

[78] *Szabo and Vissy* (n 20) para 68.

[79] ibid.

[80] ibid Concurring Opinion of Judge Pinto de Albuquerque, para 21; see also *Zakharov* (n 11) para 232. For a critique of the Court's hesitation to engage with proportionality assessments, see Maria Helen Murphy, 'A Shift in the Approach of the European Court of Human Rights in Surveillance Cases: A Rejuvenation of Necessity?' (2014) 5 EHRLR 515.

[81] Unlike the ECtHR, the CJEU treats this test as a structured one. See Paul Craig and Gráinne de Búrca, *EU Law: Text, Cases and Materials* (6th edn, OUP 2015) 551 ff; Case C-331/88 *The Queen v Ministry of Agriculture, Fisheries and Food, ex parte FEDESA and Others* ECLI:EU:C:1990:391, [1990] ECR I-04023; Case C-343/09 *Afton Chemical Limited* ECLI:EU:C:2010:419, [2010] ECR I-07027.

meet strict necessity requirements (necessity).[82] In other words, by concluding its assessment at the necessity stage, the CJEU avoided to engage with an actual *stricto sensu* balancing of the interests at stake, namely the consequences of a blanket communications data retention measure and its security benefits (*stricto sensu* proportionality).[83]

4. CONCLUDING REMARKS

Our analysis focused on the necessary safeguards, as stipulated by the jurisprudence of both the ECtHR and the CJEU, for ensuring robust oversight of the activities of the intelligence services and secure public confidence in the latter. FRA comparative research findings from the EU Member States have indicated that most states have undertaken extensive legislative amendments and implemented practices, in order to advance independence, powers and competence and transparency of their oversight mechanisms, mainly in the field of targeted surveillance. [84] The FRA 2017 surveillance report identifies such good practices and, moreover, suggests improvements for ensuring fundamental rights' compliance of surveillance, through the FRA opinions.[85]

In a field that is shredded in secrecy, these three elements remain vital for ensuring effective oversight and, ultimately, the accountability of intelligence services. Furthermore, legislation needs to allow for both judicial and non-judicial oversight bodies to –at a final stage- examine the proportionality of general surveillance measures, balancing competing interests between privacy and security. As David Anderson put it in his 2015 Report of the Investigatory Powers Review "the silent majority sits between those poles [more privacy or more security], in a state of some confusion [and] [i]nformed discussion is hampered by the fact that both the benefits of the controversial techniques and the damage attributed to their disclosure are deemed too secret to be specified".[86]

If individuals were to accept that there are "no-go areas" regarding national security, which they will never be able to access, and to defer to someone else

---

[82] *Watson* (n 12) para 109.

[83] Cf Joined Cases C–203/15 and C–698/15, *Tele2 Sverige AB v Post-och telestyrelsen and Secretary of State for the Home Department v Tom Watson* EU:C:2016:970, paras 261-262, Opinion of Advocate General Saugmandsgaard Øe in proposing a *stricto sensu* proportionality balancing in the case of general surveillance measures.

[84] European Union Agency for Fundamental Rights 2017 (n 13) 135.

[85] ibid 11-13.

[86] Anderson (n 37) 245.

the power to "watch the watchers" on their behalf, they need to be assured that these (non) judicial oversight bodies are independent, powerful, subject to public scrutiny, and able to provide for a full merits adjudication. The ECtHR will have the opportunity to discuss the question of proportionality again in the future cases before it.[87] Noble lies might have worked to convince the citizens of a platonic polity, where everyone means good, but they do not work in democratic societies where public consent on intrusive laws depends on people trusting the authorities that they will not throw into jeopardy what they hold to be most important.

5. SELECTED LITERATURE

Anderson D, *A Question of Trust. Report of the Investigatory Powers Review* (Independent Review of UK Terrorism Legislation, 2015) 198.

Anderson D, *Report of the Bulk Powers Review* (Independent Review of UK Terrorism Legislation, Cm 9326, 2016) 102

Bloom A, *The Republic of Plato* (2nd edn, Basic Books 1991) 93

Born H and Leigh I, *Making intelligence accountable: Legal standards and best practice for oversight of intelligence agencies* (Publishing House of the Parliament of Norway 2005) 85

Born H, Leigh I and Mesevage G G, 'Introducing intelligence oversight' in Born H and Wills A (eds.), *Overseeing Intelligence Services: A Toolkit* (Geneva Centre for the Democratic Control of Armed Forces (DCAF) 2012)

Cannataci J A, *Report of the Special Rapporteur on the right to privacy* (United Nations Human Rights Council (UNHRC), A/HRC/34/60, 2017), paras 16-18

Cousseran J-C and Hayez P, *Renseigner les démocraties, renseigner en démocratie*, (Odile Jacob 2015) 41

Craig P and de Búrca G, *EU Law: Text, Cases and Materials* (6th edn, OUP 2015)

Eskens S, van Daalen O, van Eijk N, *Ten standards for oversight and transparency of national intelligence services* (Institute for Information Law (IViR) Report, University of Amsterdam, 2015)

[87] *Centrum För Rättvisa v Sweden* App no 35252/08; *Big Brother Watch and Others v the United Kingdom* App no 58170/13; *Bureau of Investigative Journalism and Alice Ross v the United Kingdom,* App no 62322/14; *10 Human Rights Organisations and Others v the United Kingdom* App no 24960/15; *Breyer v Germany* App no 50001/12. All these cases are at the stage of having been communicated to the respective governments.

Heins L, 'The Intimacy of Stasi Surveillance, the NSA-Affair, and Contemporary German Cinema' in Russell A. Miller (ed.), *Privacy and Power: A Transatlantic Dialogue in the Shadow of the NSA-Affair* (CUP, 2017) 643

Murphy M H, 'A Shift in the Approach of the European Court of Human Rights in Surveillance Cases: A Rejuvenation of Necessity?' (2014) 5 EHRLR 515

Nathan L, 'Intelligence Transparency, Secrecy, and Oversight in a Democracy' in Hans Born and Aidan Wills 49

Simonsen N, 'The Investigatory Powers Tribunal and the rule of law' (UK Human Rights Blog, 16 February 2015) <https://ukhumanrightsblog.com/2015/02/16/the-investigatory-powers-tribunal-and-the-rule-of-law-natasha-simonsen>

EU immigration databases under scrutiny

Towards the normalisation of surveillance of movement in an era of 'Privacy Spring'?

NIOVI VAVOULA[1]

The past three decades have been marked by the proliferation of highly sophisticated pan-European databases processing a wide range of personal data collected by different categories of third-country nationals. At present, three databases are fully operational; the second generation Schengen Information System (SIS II), the Visa Information System (VIS) and Eurodac. The momentum for immigration databases is currently high, as in addition to significant reforms to the legal regime of the existing schemes, the EU legislator envisages the setting up of an Entry/Exit System (EES), a European Travel and Information Authorisation System (ETIAS), as well as databases for residence permits or long-stay visas holders. In addition, interconnection between these different systems is in the pipeline, in the form of the commonly known as 'interoperability' of databases. This article aims at mapping the historical evolution of pan-European immigration databases, both existing and on paper and examines key privacy concerns raised by their establishment and operation. This is performed by dividing the historical evolution of immigration databases in three distinct waves to demonstrate the progressive generalisation of surveillance of movement via the mass collection and further processing of personal data for a multiplicity of often diverging purposes.

1. INTRODUCTION

The past three decades have witnessed a profound transformation in the way immigration control is performed. Action has externalised by moving outside and beyond the physical border[2] and emphasis has been placed on preventing the flow of migrants before they manage to reach the EU external border.[3]

---

[1] Post-doctoral Researcher, School of Law, Queen Mary University of London. Email: n.vavoula@qmul.ac.uk.

[2] For an analysis see Bernard Ryan and Valsamis Mitsilegas (eds), *Extraterritorial Immigration Control* (Martinus Nijhoff 2010).

[3] Didier Bigo and Elspeth Guild (eds), *Controlling Frontiers: Free Movement Into and Within Europe* (Routledge 2005); Dennis Broeders and James Hampshire, 'Dreaming

A key trend in this context has been the growing intertwining of immigration with criminality, as expressed in the aftermath of each terrorist event[4] from 9/11 to the most recent attacks in Brussels and London. In the EU in particular, the process of securitising migration has been twofold; on the one hand, asylum and visa applications as well as entry and exit procedures have been put under the microscope, as they are considered central also for the prevention and investigation of crimes, particular of terrorism.[5] On the other hand, security considerations have had a major impact in determining the objectives and rules of the envisaged instruments.[6] The evolution of digital technologies has been an indispensable component of these efforts to acquire –or regain- control over the movement of third-country nationals. As Bonditti has pointed out, technology has been the 'servant mistress of politics'[7] resulting to 'the digitalization of the European migration policy'.[8] In this framework, modern technological advents, particularly the most controversial ones, such as fingerprinting, 'terrorist profiling' and travel surveillance 'have been (and

of Seamless Borders: ICTs and the Pre-Emptive Governance of Mobility in Europe' (2013) 39(8) Journal of Ethnic and Migration Studies 1201; Valsamis Mitsilegas, 'Human Rights, Terrorism and the Quest for "Border Security"' in Marco Pedrazzi et al. (eds), *Individual Guarantees in the European Judicial Area in Criminal Matters* (Bruylant 2011) 85–112; 'Immigration Control in an Era of Globalisation: Deflecting Foreigners, Weakening Citizens, Strengthening the State' (2012) 19(1) Indiana Journal of Global Legal Studies 3; 'The Law of the Border and the Borders of Law – Rethinking Border Control from the Perspective of the Individual' in Leanne Weber (ed.), *Rethinking Border Control for a Globalizing World* (Routledge 2015) 15–32.

[4] Mitsilegas (n 2).

[5] For instance, The Hague Programme mentions that 'the management of migration flows, including the fight against illegal immigration, should be strengthened by establishing a continuum of security measures that effectively links visa application procedures and entry and exit procedures at external border crossings. Such measures are also of importance for the prevention and control of crime, in particular terrorism'. See The Hague Programme: Strengthening Freedom, Security and Justice in the European Union [2004] OJ C53/1, 7.

[6] For instance, see Commission, 'The European Agenda on Security' (Communication) COM (2015) 185 final.

[7] Philippe Bonditti, 'From Territorial Spaces to Networks: A Foucaultian Approach to the Implementation of Biometry' (2004) 29 Alternatives: Global, Local, Political 465.

[8] Michiel Besters and Frans Brom, '"Greedy" Information Technology: The Digitalization of the European Migration Policy' (2010) 12(4) European Journal of Migration and Law 455. See also The New Digital Borders of Europe. EU Databases and the Surveillance of Irregular Migrants' (2007) 22(1) International Sociology 71.

are still being) "tested" on migrants and refugees or otherwise legitimized at the border'.[9]

The establishment and operation of pan-European[10] immigration databases is a prime example in this context. Enabled by the technological evolution and driven by security considerations in the post-9/11 world, the EU legislator has set up a 'mille-feuille' of information processing schemes, currently comprising of three large-scale information systems, the Schengen Information System (SIS II, formerly named SIS), the Eurodac and the Visa Information System (VIS). The momentum for EU immigration databases is currently higher than ever. Therefore, in addition to consecutive enhancements of the aforementioned systems spanning from modest 'corrective' additions to radical reforms, EU centralised systems are bound to proliferate via the establishment of the Entry/Exit System (EES) and the European Travel Information and Authorisation System (ETIAS). Personal data of long-stay visa holders and holders of residence permits may also be collected and centrally stored in the future. Finally, the interconnection of the different data pots with a view to becoming interoperable in the coming years is also in the pipeline. In parallel to the establishment of the aforementioned information exchange mechanisms, the Court of Justice of the EU (CJEU) and the European Court of Human Rights (ECtHR) have released a series of judgments placing limits to practices of mass surveillance -albeit in different contexts- by highlighting the importance of the right to private life. In this context, the aim of the present contribution is to map the landscape as regards the setting up and operation of immigration databases by dividing their historical evolution in three distinct phases and by examining the key fundamental rights challenges, particularly in relation to the right to private life.

[9] Ben Hayes, *NeoConOpticon: The EU Security-Industrial Complex* (Transnational Institute/Statewatch 2009) 35. See Katja Lindskov Jacobsen, 'Making Design Safe for Citizens: A Hidden History of Humanitarian Experimentation' (2010) 14 Citizenship Studies 89.

[10] This term has been preferred as not all EU Member States participate in the systems under consideration, whereas some non-EU Member States do take part. For each case, the participating States are indicated.

2. THREE WAVES IN THE EVOLUTION OF PAN-EUROPEAN IMMIGRATION DATABASES

2.1. First wave: Setting up centralised databases for the purpose of enhancing immigration control

In the early 90's, whereby technology had not evolved as much as nowadays, the establishment of EU centralised immigration databases necessarily followed a compartmentalised approach, by first targeting individuals whose digital tracking and monitoring was eminent either because their personal conduct assimilated characteristics of criminal behaviour or because it was required for better administration of EU policies. In addition, this compartmentalisation was marketed as a means of safeguarding the limited purposes and personal scope of each database, thus complying with key principles of EU data protection law, such as the purpose limitation principle. In this context, the first wave of EU immigration databases involves the setting up of the most emblematic Schengen-wide database, the Schengen Information System (SIS), and a system functioning as the 'truth serum' of the EU asylum policy, namely Eurodac.

2.1.1. Keeping away the 'unwanted': SIS

Perhaps the best-known centralised database in the Area of Freedom, Security and Justice is the SIS, currently substituted by the SIS II (see below). At the heart of the compensatory measures for the abolition of internal border controls,[11] the SIS was conceived in 1987, established under the 1990 Convention Implementing the Schengen Agreement (CISA)[12] and incorporated as fully applicable EU law with the Amsterdam Treaty.[13] It became operational in 1995 as a support tool for national competent authorities. Its overarching

[11] Bernd Schattenberg, 'SIS: Privacy and Legal Protection' in Henry Schermers et al. (eds), *Free Movement of Persons in Europe: Legal Problems and Experience* (Martinus Nijhoff 1993) 43.

[12] Convention implementing the Schengen Agreement between the Governments of the States of the Benelux Economic Union, the Federal Republic of Germany and the French Republic on the gradual abolition of checks at their common borders [2000] OJ L239/19 (CISA). For a detailed overview of the setting of the SIS see Evelien Brouwer, *Digital Borders and Real Rights – Effective Remedies for Third-Country Nationals in the Schengen Information System* (Martinus Nijhoff 2008) 47-57.

[13] On the difficulties to assign a fitting legal basis to the SIS see Pieter Jan Kuijper, 'Some Legal Problems Associated with the Communitarization of Policy on Visas, Asylum and Immigration under the Amsterdam Treaty and Incorporation of the Schengen acquis' (2000) 37 Common Market Law Review 345.

purpose twofold: a) to maintain public order and security, including State security; and b) to enable the Contracting parties to automatically search the information on persons and objects registered therein for the purposes of border control and police investigations, control and other searches.[14] Therefore, on the one hand, it could be used by national police, customs and border control authorities when performing checks on persons at external borders or within Schengen states, and, on the other hand, it could assist immigration officers when administering third-country nationals, particularly in relation to issuing visas and residence permits.[15] By its very nature, the SIS thus served as both an immigration and a criminal law instrument. To that end, it held data categorised in the form of 'alerts' on various categories of persons and objects, in particular on people wanted for arrest for extradition,[16] missing persons,[17] witnesses or persons summoned to appear before the judicial authorities or to serve a penalty,[18] persons or objects subject to discreet surveillance or specific checks[19] and objects sought for the purpose of seizure or their use as evidence in criminal proceedings.[20] In addition, it held information on third-country nationals to be refused entry into the Schengen area.[21]

As regards the latter category of alerts, which in practice dominated the system,[22] it involved third-country nationals whose data were inserted on two main grounds. First, alerts could be registered on the basis of public policy, public security or national security grounds, either when third-country na-

[14] Art 93 CISA.

[15] Art 92 CISA.

[16] Art 95 CISA.

[17] Art 97 CISA.

[18] Art 98 CISA.

[19] Art 99 CISA.

[20] Art 100 CISA.

[21] Art 96 CISA.

[22] Elspeth Guild, 'Moving the Borders of Europe' (Inaugural lecture, University of Nijmegen, 2000, 24) <http://cmr.jur.ru.nl/cmr/docs/oratie.eg.pdf>; Brouwer (n 12) 66-68; Schengen Joint Supervisory Authority, *Final Report of the Schengen Joint Supervisory Authority on the follow-up of the recommendations concerning the use of Article 96 alerts in the Schengen Information System* (Council Document, 6434/1/11, 2011, 2010).

tionals had been convicted of an offence carrying a penalty involving deprivation of liberty for at least one year,[23] or because there were serious grounds for believing that they had committed serious criminal offences, or when there was clear evidence that they planned to commit such offences in the territory of a signatory state (Article 96(2)(b)). Second, alerts could be inserted in relation to third-country nationals who had not complied with national immigration law, on the basis of a deportation order or refusal of entry, including or accompanied by a prohibition on entry or a prohibition on residence. (Article 96(3)).

By containing both immigration and criminal law data, the SIS was inherently a system of mixed nature. It stored basic alphanumeric information (such as the name, nationality, the type of alert and any specific objective physical characteristics) and operated on a hit/no hit basis. In cases of a hit, national authorities would perform searches for supplementary information in SIRENE. As for the authorities granted access, the database was accessed by police, immigration and customs authorities responsible for checks at the borders and within the national territories.

The setting up and operation of the SIS constituted a significant step towards the securitisation of migration through digitalisation, whereby data on irregular migrants were stored within a single system alongside information on objects and individuals directly linked to law enforcement. In this context, the interrelation between immigration control and law enforcement also entailed that the system had no unitary and limited purpose and given that its main preoccupation was immigration control a de facto function creep was evident. In terms of fundamental rights challenges, particularly in relation to the right to private life and personal data protection, according to settled case law of the European Court of Human Rights, the systematic registration of personal data in centralised registers amounts to an interference with the right to private life as enshrined in Article 8 ECHR irrespective of whether the data are further used or the collection took place in an intrusive manner.[24] The existence of such interference is also recognised by the Court of Justice in a series of subsequent cases.[25] In that respect, the extent to which the inclusion of alerts on third-country nationals was necessary and proportionate

[23] Art 96(2)(a) CISA.

[24] *Amann v Switzerland* App no 27798/95 (ECtHR, 16 February 2000); *Rotaru v Romania* App no 28341/95 (ECtHR, 4 May 2000); *Kopp v Switzerland* App no 23224/94 (ECtHR, 25 March 1998).

[25] Joined Cases C-293/12 and C-594/12 *Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others* EU:C:2014:238, Opinion of the Court (Grand Chamber) of 26 July 2017.

has been doubtful. On the one hand, it has been reported that 77% of alerts were entered for the wrong reasons, raising question on the procedural fairness in decision-making.[26] In a similar vein, the decision for an irregular migrant to be registered in the SIS lied entirely in the discretion of national authorities resulting in significant discrepancies in the implementation[27] with specific Member States -Germany and Italy in particular- being more active in this regard[28] and, therefore, third-country nationals facing differentiated treatment depending on the state in which they were found irregularly entering or staying.

2.1.2. Monitoring the territorial belonging of asylum seekers and irregular migrants: Eurodac

Parallel to the establishment of the SIS in the 1990s, EU national governments called for the setting up of a central registration system that would process the fingerprints of asylum seekers as a tool to facilitate the operation of the Dublin system for the allocation of responsibility among Member States for dealing with an asylum application[29] To this end, Eurodac (standing for European Dactyloscopy), the first pan-European biometric database, was created by Regulations (EC) 2725/2000[30] and 407/2002[31] and became operational in 2003. The basic rules of its operation are as follows: every asylum seeker over the age of 14 must enter their fingerprints when they apply for international protection. The collected fingerprints are stored in the Central

---

[26] Stephen Kabera Karanja, *Transparency and Proportionality in the Schengen Information System and Border Control Cooperation* (Martinus Nijhoff 2008) 216.

[27] Brouwer (n 12) 61-62.

[28] Schengen Joint Supervisory Authority, *Article 96 Inspection – Report of the Schengen Supervisory Authority on the inspection of the use of Article 96 alerts in the Schengen Information System* (2005).

[29] For a detailed overview of the story behind Eurodac see Jonathan Aus, 'Eurodac: A Solution Looking for a Problem?' (2006) 10 European Integration online Papers; Steve Peers and Nicole Rogers (eds), *EU Immigration and Asylum Law* (Martinus Nijhoff 2006) 263-8; Niovi Vavoula, *Immigration and Privacy in the Law of the European Union: The Case of Databases* (Brill forthcoming 2018) ch 4.

[30] Council Regulation (EC) 2725/2000 of 11 December 2000 concerning the establishment of 'Eurodac' for the comparison of fingerprints for the effective application of the Dublin Convention [2000] OJ L316/1 (Eurodac Regulation).

[31] Council Regulation (EC) 407/2002 of 28 February 2002 laying down certain rules to implement Regulation (EC) No 2725/2000 concerning the establishment of 'Eurodac' for the comparison of fingerprints for the effective application of the Dublin Convention [2002] OJ L62/1.

System and are compared with fingerprints that have already been transmitted by other participating countries.[32] As with the SIS, the Eurodac functions on a hit/no hit basis and if a Eurodac check reveals that the fingerprints have already been recorded in another Member State, the asylum seeker may be returned to that Member State. In addition, the system processes the data of all migrants who are either apprehended 'in connection with the irregular crossing by land, sea or air of the Member State'[33] or they are irregularly staying within the national territory of a Member State.[34] Apart from biometric data, the database also stores limited biographical information but the person's name and nationality are not included and, thus, the individual is defined by no more than their fingerprints.[35] The fingerprints of asylum seekers are retained for a period of ten years, while those of individuals found irregularly entering for two years only. The datasets on migrants found irregularly staying are not centrally stored, but merely consulted.

The Eurodac database is a key example of the trend to deploy biometric identifiers as a means of reliable and speedy identification of individuals, which however raises grave privacy concerns. In *Schwarz*, the CJEU found that the storage of two fingerprints in biometric passports of EU citizens is proportionate since that storage takes place only 'within the passport itself, which belongs to the holder alone'.[36] In the case of biometric databases, such as Eurodac, biometrics are stored within a centralised scheme, signifying that the individual concerned loses control of their personal data. Furthermore, it has been correctly pointed out that when biometrics are centrally stored, the error rates are impacted by the number of persons subjected to the system.[37] Therefore, the larger the system, the more possible a 'hit' is based on an error. In the case of Eurodac, a possible error may have detrimental impact on the status of asylum seekers who may be wrongfully returned to another Member

[32] Eurodac Regulation, arts 4-7.

[33] According to the Council, this concept is controversially extended to cases involving third-country nationals 'apprehended beyond the external border' where they are still en route and there is no doubt that they crossed the external border irregularly. Council, Document 12314/00 ADD 1 (2000).

[34] Eurodac Regulation, arts 8-10.

[35] Elspeth Guild, 'Unreadable Papers? The EU's First Experiences with Biometrics: Examining Eurodac and the EU's Borders' in Juliet Lodge (ed.), *Are You Who You Say You Are? The EU and Biometric Borders* (Wolf Legal Publishers 2007) 32.

[36] Case C-291/12 *Schwarz v Stadt Bochum ECLI:EU:C:2013:670,* [2013], para 60.

[37] Els Kindt, *Privacy and Data Protection Issues of Biometric Applications* (Springer 2013) 59.

State. In addition, it is arguable that for the identification of asylum seekers two or four fingerprints would suffice and a ten-year retention period appears disproportionately extensive.[38]

Importantly, the mere existence of Eurodac as a support mechanism of the ill-functioning Dublin system is called into question in light of the well-known and broadly accepted failure of Dublin.[39] The system is not 'working' either for asylum seekers or for Member States; on the one hand, asylum seekers are not deterred from defying the Dublin rules and move on to the EU core to lodge their asylum application elsewhere in search of human reception conditions;[40] On the other hand, both the CJEU[41] and the ECtHR[42] have released landmark rulings condemning appalling reception conditions leading to the halt of transfers to Greece since 2011 in view of its systemic deficiencies. The case of Greece is not the sole example. Available statistics demonstrate that during the period 2008-2012, only around 25% of outgoing requests resulted in transfers, meaning that Dublin transfers take place in only around 3% of asylum cases in the EU.[43] The most recent Commission evaluation of the Dublin III Regulation confirms the very low number of transfers in comparison to the number of Dublin requests.[44] In light of the above, the failings of Dublin have a domino effect to the operation of Eurodac, stripping away its necessity.

---

[38] The storage of asylum seekers' fingerprints for ten years has never been properly justified even though the Parliament suggested reducing it to five years, an amendment that was ignored by the Council. See Aus (n 29).

[39] Elspeth Guild and others, *New Approaches, Alternative Avenues and Means of Access to Asylum Procedures for Persons Seeking International Protection* (Study for the LIBE Committee, PE509.989, 2014).

[40] On this issue see among others Jesuit Refugee Service, 'Protection Interrupted: The Dublin Regulation's impact on asylum seekers' protection (The DIASP project)' (2013) <http://www.refworld.org/docid/51d152174.html>; Susan Fratzke, *Not Adding Up: The Fading Promise of Europe's Dublin System* (Migration Policy Institute Report, 2015).

[41] Joined Cases C-411/10 and C-493/10 *NS v Secretary of State for the Home Department and ME and Others v Refugee Applications Commissioner and Minister for Justice, Equality and Law Reform* ECLI:EU:C:2011:865, [2011] ECR I-13905.

[42] *MSS v Belgium and Greece* App no 30696/09 (ECtHR, 21 January 2011); *Tarakhel v Switzerland* App no 29217/12 (ECtHR, 4 November 2014).

[43] Guild and others (n 39) 9.

[44] Commission, *Evaluation of the implementation of Dublin III Regulation – Final Report* (2016) 56-57.

Since the allocation mechanism is problematic and, therefore, must be fundamentally reformed, the need for maintaining the instrument assisting in this allocation, namely Eurodac, must also be questioned.

2.2. Second wave: Immigration databases and the 'War on Terror'

The terrorism events of 9/11 signaled a new era for pan-European immigration databases, whereby immigration control, security and criminality intertwined to a significant extent. This wave foresaw the establishment or the conceptualisation of establishment of an additional system, such as the VIS, which was designed a multipurpose tool embracing a securitised approach. This possibility of creating system with primary and ancillary purposes on the basis of the VIS model has signaled that a reform and rebranding of Eurodac from a system with a restricted administrative law objective of assisting Dublin to a database serving the ancillary purpose of a weapon in the fight against terrorism and serious crime was not only possible, but also necessary. Finally, the evolution of technology has enabled the insertion of additional features in information systems, with the collection and storage of biometrics becoming a banality.

2.2.1. Targeting visa applicants: VIS

In the post-9/11 era, the landscape as regards the mobility of third-country nationals in the Schengen area was forever changed. The securitisation of immigration control and the focus on preventing and deterring movement or risky individuals became all the more evident not only by expanding the functions of already existing schemes, but also through the conceptualisation of new centralised systems targeting different groups of potentially risky individuals.[45]

In particular, immediately after the attacks Member States decided to reform the EU visa policy and invited the Commission to submit proposals for the establishment of a network for information exchange concerning visas issued by them.[46] The underlying rationale was to reinforce extraterritorial immigration control by collecting and storing a series of personal data from visa

[45] Louise Amoore and Marieke de Goede (eds), *Risk and the War on Terror* (Routledge 2008).

[46] For an overview of the discussions see Council, Document 12019/01 (2001); Council, Document 14523/01 (2001); Council, Document 15577/01 (2001); Council, Document SN 300/1/01 (2001). On the emphasis on 'border security' see Valsamis Mitsilegas, 'Borders, Security and the Transatlantic Cooperation in the Twenty-First Century: Identity and Privacy in an Era of Globalized Surveillance' in Terri Givens and others (eds), *Immigration Policy and Security* (Routledge 2009).

holders while further exploiting this new pool of information also for law enforcement purposes. As was explicitly stated '(t)he events of 11 September 2001 have radically altered the situation, showing that visas are not just about controlling immigration but are above all an issue of EU Member States' internal security'.[47] In this context, the establishment of the VIS should be viewed as a direct consequence of the 9/11 events.[48] In February 2004, the Justice and Home Affairs Council adopted detailed conclusions on the development of the VIS stating clearly that one of the purposes of the system would be 'to contribute towards improving the administration of the common visa policy and towards security and combating terrorism'.[49] It also called for access to the system to be granted to border guards and other national authorities designated at the national level including police and internal security agencies. The first concrete steps towards the establishment of the database were taken after the Madrid bombings with the adoption of Decision 2004/512/EC,[50] which formed the legal basis for the establishment of the VIS. Soon afterwards, the Commission tabled a proposal for Regulation[51] aimed at setting out detailed rules on the use of the system for immigration purposes. As for law enforcement access, the Justice and Home Affairs Council of February 2005 called for the consultation of visa data by national authorities responsible for internal security as a tool in the prevention, detection and investigation of terrorism offences and other serious crimes.[52] To this end, a

[47] Council, Document 14523/01 (2002).

[48] Annaliese Baldaccini, 'Counter-terrorism and the EU Strategy for Border Security: Framing Suspects with Biometric Documents and Databases' (2008) 10 European Journal of Migration and Law 31, 32.

[49] Council, Document 5831/04 (2004).

[50] Council Decision 2004/512/EC establishing the Visa Information System (VIS) [2004] OJ L213/5.

[51] Commission, 'Proposal for a Regulation of the European Parliament and of the Council concerning the Visa Information System on short-stay visas' COM (2004) 835 final.

[52] Council, Document 6811/05 (2005).

separate proposal for a third pillar Decision was released in November 2005[53] and negotiation moved in parallel.[54]

The current legislative framework on the VIS comprises of Regulation 767/2008[55] governing the use of the system for border control purposes and Council Decision 2008/6333/JHA[56] prescribing the modalities of consulting visa data by law enforcement authorities and Europol. After numerous years of complications, the gradual rollout of the VIS commenced in late 2011 and concluded in February 2016.[57] The database currently constitutes the largest information exchange scheme in the EU with the capacity of storing and further processing up to 70 million applications.[58] Reflecting the security logic as outlined above, Article 2 of the VIS Regulation stipulates that the overarching purpose of the database is to improve the implementation of the common visa policy by facilitating the exchange of visa data, however it further sets

---

[53] Commission, 'Proposal for a Council Decision concerning access for consultation of the Visa Information System (VIS) by the authorities of Member States responsible for internal security and by Europol for the purposes of the prevention, detection and investigation of terrorist offences and of other serious criminal offences' COM (2005) 600 final.

[54] For an overview of the negotiations and a comparison between the Commission proposals and the final text see Council, Document 11632/06 (2006); Steve Peers, 'Legislative Update: EC Immigration and Asylum Law 2008: Visa Information System' (2009) 11 European Journal of Migration and Law 69.

[55] Council Regulation (EC) 767/2008 of 9 July 2008 concerning the Visa Information System (VIS) and the exchange of data between Member States on short-stay visas [2008] OJ L218/60 as amended by Regulation (EC) 810/2009 of the European Parliament and of the Council of 13 July 2009 establishing a Community Code on Visas (Visa Code) [2009] OJ L243/1 (VIS Regulation).

[56] Council Decision 2008/633/JHA of 23 June 2008 concerning access for consultation of the Visa Information System (VIS) by designated authorities of Member States and by Europol for the purposes of the prevention, detection and investigation of terrorist offences and of other serious criminal offences [2008] OJ L218/129 (VIS Decision).

[57] Commission Implementing Decision (EU) 2016/281 of 26 February 2016 determining the date from which the Visa Information System (VIS) is to start its operations at external border crossing points [2016] OJ L52/64.

[58] Commission, 'Proposal for a Council Decision establishing the Visa Information System (VIS)' COM (2004) 99 final, 4. In 2015, whilst the roll-out was still ongoing, the 26 Schengen States issued around 14.3 million Schengen visas. By the end of September 2015, the VIS was storing over 17 million registered visa applications, including 15.5 million data sets on Schengen visas issued. See eu-LISA, *VIS Report pursuant to Article 50(3) of Regulation (EC) No 767/2008 - VIS Report pursuant to Article 17(3) of Council Decision 2008/633/JHA* (2016) 16.

out no less than seven ancillary purposes, among which is the prevention of threats to the internal security of the EU Member States.[59] This provision, which is a strong indication of the pre-emptive nature of surveillance in the post-9/11 era, is particularly problematic since the EU legislator has included within these additional benefits not only purposes related to the EU visa policy, such as the facilitation of the visa procedure or the fight against visa fraud, but also law enforcement which is prima facie not connected.[60] Furthermore, the system stores an array of personal data of all persons subject to visa requirements irrespective of the status of their visa application (refused, granted, revoked). This data include bibliographic information, biometrics – a full set of fingerprints and a photograph-, information on persons who have issued an invitation and/or are liable to pay for the applicant's subsistence costs, purpose of the travel, residence and occupation.[61] In this context, the operation of the VIS implies an element of suspicion against visa applicants whose a priori legitimate intention to pursue a travel to the EU needs to be monitored. Crucially, this shadow of suspicion accompanies not only the travellers as such, but also family members, organisations or companies who have issued invitations or sponsored a stay within the Schengen area. An everyday activity transforms into a risk, for the management of which a series of contemporary information of private nature, such as personal associations, ends up at the hands of a wide range of domestic authorities.

While law enforcement access to the visa data is regulated in detail in the Decision, Article 3 of the VIS Regulation serves as a 'bridging clause' linking the two legal instruments and providing the main rules on the consultation of the data by law enforcement bodies and Europol. Although the then pillar structure signified that the European Parliament merely had a consultative role as regards the adoption of the Decision, these limited powers did not prevent it from vigorously negotiating this provision in an attempt to include as many

---

[59] Under the auspices of this 'umbrella' purpose, no less than seven wide-ranging objectives are encompassed: a) Facilitating the visa application procedure; b) Preventing 'visa shopping'; c) Facilitating the fight against fraud; d) Facilitating checks at external border crossing points and within national territory; e) Assisting in the identification of persons that do not meet the requirements for entering, staying or residing in a Member State; f) Facilitating the implementation of the Dublin mechanism for determining the Member State responsible for the examination of an asylum application and for examining such applications; and g) Contributing to the prevention of threats to Member States' internal security.

[60] For a critical examination of the VIS purposes see Vavoula (n 29) ch 3. The ranking of the purposes has been subject to litigation before the EU Court of Justice. See Case C-482/08 *UK v Council* ECLI:EU:C:2010:631, [2010] ECR I-10413.

[61] VIS Regulation, art 9.

safeguards as possible. In this context, law enforcement access to VIS data is allowed only when there are reasonable grounds to believe that consultation of the system will substantially contribute to the prevention, detection or investigation of terrorist offences and other serious crimes. This clause has been subject to extensive debate with the view being put forward that a higher threshold is necessary for allowing access, requiring also the existence of factual indications as the basis for the reasonable grounds mentioned above.[62] In addition, Article 3 stipulates that access to visa data by Europol is allowed 'within the limits of its mandate and when necessary for the performance of its tasks'.

The aforementioned rules are further elaborated in the VIS Decision. Overall, access is not granted on a routine basis and must be necessary in a specific case.[63] The national authorities allowed consulting the data stored are those 'responsible for the prevention, detection and investigation of terrorist offences or of other serious criminal offences' as designated at the national level.[64] This provision has attracted significant criticism as it gives huge leeway to national governments to designate a wide array of agencies that can have access to the VIS.[65] It is up to the Member States to determine which authorities are covered by this definition and the Decision does not prescribe for any other guidance, requirement or limit other than that the authorities' mandate must include the prevention, detection or investigation of terrorism or other serious criminal offences at national level. However, a number of authorities may within the remits of this definition, not excluding national intelligence agencies. Interestingly, the EDPS did not criticize this element, but he mentioned that it is welcomed that intelligence services are bound by the same rules as the rest of national authorities.[66] Besides, there is no control at EU level; the list of designated authorities is merely communicated to the Commission and published in the Official Journal. As regards the procedure

---

[62] Council, Document 5456/1/07 (2007).

[63] VIS Decision, art 5(1).

[64] ibid art 2(1)(e). The list of competent authorities is published in the Official Journal. See Notices from Member States, 'Declarations concerning Member States' designated authorities and central access point(s) for access to Visa Information System data for consultation in accordance with Article 3(2) and 3(3) respectively of Council Decision 2008/633/JHA' [2013] OJ C236/1.

[65] Mitsilegas, 'Human Rights' (n 2) 109; Brouwer (n 12) 49.

[66] European Data Protection Supervisor (EDPS), 'Opinion of the European Data Protection Supervisor on the Proposal for a Regulation of the European Parliament and of the Council concerning the Visa Information System (VIS) and the exchange of data between Member States on short-stay visas' COM (2004) 835 final [2005] OJ C181/13.

of consultation, the designated authorities have to submit a reasoned electronic request to the Central Access Point, an authority also designated at the domestic level, which will verify the extent to which the conditions of access have been met and provide access to the data. Nevertheless, this procedure falls short of the criteria as set out in *Digital Rights Ireland*, where the CJEU explicitly required that access to the data must be 'made dependent on a prior review carried out by a court or by an independent administrative body'.[67]

Another point of concern relates to the possibility of transferring data to third countries and organisations as prescribed in Article 8(4) of the Decision. While transfers of data to third parties are prohibited, in an exceptional case of urgency such data may be transferred exclusively for the purposes of the prevention and detection of terrorist offences and other serious crimes. The transfer of data raises considerable privacy concerns stemming from the adequate level of privacy standards in third countries – an issue that is left outside the scope of the provision- and the possibility of expanding access to personal data included in the VIS to a wide pool of agencies worldwide.[68]

2.2.2. SIS II: Turning SIS from a reporting into an investigation tool

A second strand of action as regards the operation of immigration databases in the wake of the 9/11 events has been the reinforcement of the functions of the SIS. For years EU Member States demonstrated their creativity by putting forward a number of initiatives in this regard.[69] At a Spanish initiative, Regulation 871/2004[70] and Council Decision 2005/211/JHA[71] were adopted stipulating wider access to certain types of data to visa, judicial and law enforcement authorities, among which Europol and Eurojust. However, in the case of Europol, access was not granted to immigration data.

Furthermore, in light of the enlargement in 2004 the need to develop a second generation SIS -the SIS II-, which would accommodate the expanded EU fam-

---

[67] *Digital Rights Ireland Ltd* (n 25) para 62.

[68] Mitsilegas (n 2) 110.

[69] For instance see Council, Document SN 4038/01 (2001); Council, Document 13530/01, (2001); Council, Document 10127/02 (2002).

[70] Council Regulation (EC) 871/2004 of 29 April 2004 concerning the introduction of some new functions for the Schengen Information System, including in the fight against terrorism [2002] OJ L162/29.

[71] Council Decision 2005/211/JHA of 24 February 2005 concerning the introduction of some new functions for the Schengen Information System, including in the fight against terrorism [2005] OJ L68/44.

ily, became pressing. The migration from the SIS to the SIS II has been regarded as a first-class opportunity to insert new functionalities to the system by taking advantage of the latest developments in the field of information technology.[72] In May 2005, the Commission tabled three proposals -two first pillar Regulations and a third pillar Decision- reflecting the fact that SIS covers both immigration and criminal law data, which would constitute the legal basis for the establishment of SIS II.[73] The Regulations were formally adopted in 2006 and the third pillar Decision some months later.[74] However, due to numerous technical complications the SIS II commenced its operation only in April 2014.

A major change involves the possibility of including biometric identifiers (photographs and fingerprints) within the system.[75] This rule should be seen in a broader context to gradually generalise their use at EU level; both VIS and Eurodac were based on the collection and storage of biometrics, whereas residence permits and EU passports were also required to include biometrics.[76] According to Article 22 of the SIS II Regulation, the introduction of biometrics

---

[72] For an overview see Joanna Parkin, 'The Difficult Road to the Schengen Information System II - The Legacy of Laboratories and the Cost for Fundamental Rights and the Rule of Law' (Paper, CEPS 2011).

[73] Commission, 'Proposal for a Regulation of the European Parliament and of the Council on the establishment, operation and use of the second generation Schengen Information System (SIS II)' COM (2005) 236 final (Proposal for SIS II Regulation); 'Proposal for a Regulation of the European Parliament and of the Council regarding access to the second generation Schengen Information System (SIS II) by the services in the Member States responsible for issuing vehicle registration certificates' COM (2005) 237 final; 'Proposal for a Council Decision on the establishment, operation and use of the second generation Schengen Information System (SIS II)' COM (2005) 238 final.

[74] Council Regulation (EC) 1986/2006 of 20 December 2006 regarding access to the Second Generation Schengen Information System (SIS II) by the services in the Member States responsible for issuing vehicle registration certificates [2006] OJ L381/1; Council Decision 2007/533/JHA of 12 June 2007 on the establishment, operation and use of the second generation Schengen Information System (SIS II) [2007] OJ L205/63 (SIS II Decision); Council Regulation (EC) No 1986/2006 of 20 December 2006 regarding access to the Second Generation Schengen Information System (SIS II) by the services in the Member States responsible for issuing vehicle registration certificates [2006] OJ L 381/1.

[75] SIS II Regulation, art 22.

[76] Evelien Brouwer, 'The Use of Biometrics in EU Databases and Identity Documents – Keeping Track of Foreigners' Movements and Rights' in Juliet Lodge (ed.), *Are You Who You Say You Are? – The EU and Biometric Borders* (Wolf Legal Publishers 2007) 45–66; Baldaccini (n 47).

would take place in two phases; in the first stage, biometrics will be used only for confirming someone's identity by comparing the biometric identifiers of the person only with those existing in the system under this person's name; however, in the future biometrics would also be used for searches where biometric data of one person will be compared against the whole system. Currently this new function is in the process of being officially deployed, with the Commission having certified in a 2016 Report the readiness and availability of the system.[77] The decision has deemed as a technical issue and will be taken at a comitology level thus raising serious concerns of transparency and democratic scrutiny.[78] This development has significant implications as it transforms the nature of the database to a general intelligence weapon, as biometrics could be used in the course of investigations and enable speculative searches (the so-called 'fishing' expeditions), whereby the persons stored in the system constitute a suspected population.[79] Central in this respect is the possibility to use biometrics as a search key in order to reveal links to other alerts, another of the system. The Commission report on the readiness and availability of fingerprints for identification purposes confirms these fears, as it is stated that a comparison of fingerprints to those already stored 'might identify links with other alerts'.[80] Therefore, biometrics are not merely collected and stored to 'sort out' the 'welcomed' from the 'unwanted', but also to enhance the investigative powers of national law enforcement authorities.

As noted above, the second indication that the SIS is gradually transformed to general investigation tool is the possibility of interlinking alerts, not only those inserted within the criminal law branch of the, but also interconnecting alerts inserted under a different legal basis. Such interlinking is allowed only if there is a clear operational need, but is subject to the national law of the Member State that decides to use this option – thus rendering possible the creation of significantly different systems across the EU. The potential for profiling through the interlinking of alerts is significant with the European Data Protection Supervisor noting in this regard that 'the person is no longer "assessed" on the basis of data relating only to him/her, but on the basis of

[77] Commission, 'The availability and readiness of technology to identify a person on the basis of fingerprints held in the second generation Schengen Information System (SIS II)' (Report) COM (2016) 93 final.

[78] Mitsilegas, Valsamis, *EU Criminal Law* (Hart 2009) 240.

[79] Ben Hayes, *From the Schengen Information System to the SIS II and the Visa Information System (VIS): The Proposals Explained* (Statewatch Report 2004) 4; Baldaccini (n 47) 38.

[80] Commission (n 77) 7.

his/her possible association with other persons',[81] which may lead to their treatment with greater suspicion if they are deemed to be associated with criminals or wanted persons. Besides, although authorities with no right of access to certain categories of alert will not be able to see the link to an alert to which they do not have access, this may not necessarily mean that these authorities will be unaware of the existence of a link.[82]

2.2.3. The use of Eurodac data for law enforcement purposes

Another clear indication of how the boundaries between immigration and police databases are blurred is the re-configuration of Eurodac from a tool serving the Dublin system to a weapon in the fight against serious crime. A year after the database had begun its operation, the Hague Programme called for the maximization of effectiveness and interoperability of EU information systems and 'an innovative approach to the cross-border exchange of law enforcement information'.[83] Furthermore, in November 2005, the Commission published a Communication on improved effectiveness, enhanced interoperability and synergies of EU information systems stating that 'authorities responsible for internal security could … have access to Eurodac in well-defined cases, when there is a substantiated suspicion that the perpetrator of a serious crime had applied for asylum'.[84] Law enforcement access to Eurodac data has been a particularly contentious issue, resulting in that the Commission had to draft no less than four proposals –a record-breaking number in the field of the AFSJ-, two of which contained no reference to this issue and one

[81] European Data Protection Supervisor (EDPS), 'Opinion of the European Data Protection Supervisor on the Proposal for a Council Decision on the establishment, operation and use of the Second Generation Schengen Information System (SIS II) COM (2005) 230 final, the Proposal for a Regulation of the European Parliament and of the Council on the establishment, operation and use of the Second Generation Schengen Information System (SIS II) COM (2005) 236 final, and the Proposal for a Regulation of the European Parliament and of the Council regarding access to the Second Generation Schengen Information System (SIS II) by the services in the Member States responsible for issuing vehicle registration certificates COM (2005) 237 final' [2006] OJ C91/38, 46.

[82] Mitsilegas (n 77) 241.

[83] See the Hague Programme (n 5) 7.

[84] Commission, 'Improved effectiveness, enhanced interoperability and synergies among European databases in the area of Justice and Home Affairs' (Communication) COM (2005) 597 final.

being blocked by the European Parliament in 2009.[85] In the fourth attempt[86] and largely under the pressure of finalising the second phase of the Common European Asylum System,[87] the recast Eurodac Regulation was adopted in June 2013,[88] allowing law enforcement access to asylum seekers data.

---

[85] Commission, 'Proposal for a Regulation of the European Parliament and the Council concerning the establishment of 'Eurodac' for the comparison of fingerprints for the effective application of Regulation (EC) No [.../...] [establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person] (Recast version)' COM (2008) 825 final; 'Amended proposal for a Regulation of the European Parliament and of the Council concerning the establishment of 'EURODAC' for the comparison of fingerprints for the effective application of Regulation No [.../...] [establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person] (Recast version)' COM (2009) 342 final; 'Proposal for a Council Decision on requesting comparisons with EURODAC data by Member States' law enforcement authorities and Europol for law enforcement purposes' COM (2009) 344 final; 'Amended proposal for a Regulation of the European Parliament and the Council concerning the establishment of 'EURODAC' for the comparison of fingerprints for the effective application of Regulation (EC) No [.../...] [establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person] (Recast version)' COM (2010) 555 final.

[86] Commission, 'Amended proposal for a Regulation of the European Parliament and of the Council on the establishment of 'EURODAC' for the comparison of fingerprints for the effective application of Regulation (EU) No [.../...] (establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person) and to request comparisons with EURODAC data by Member States' law enforcement authorities and Europol for law enforcement purposes and amending Regulation (EU) No 1077/2011 establishing a European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice (Recast version)' COM (2012) 254 final.

[87] See Brigitta Juster and Vassilis Tsianos, 'Erase Them! Eurodac and Digital Deportability' (2013) Transversal/EIPCP multilingual webjournal <http://eipcp.net/transversal/0313/kuster-tsianos/en>.

[88] Council Regulation (EU) 603/2013 of 26 June 2013 on the establishment of 'Eurodac' for the comparison of fingerprints for the effective application of Regulation (EU) No. 604/2013 establishing the criteria and mechanisms for determining the Member States responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person and on re-

This further use of data for law enforcement purposes constitutes a prime example of the inherent danger creeping in centrally storing personal data, as once information is stored for a specific purpose, the possibility of the system being re-purposed for objectives that were not initially conceived is more than rhetoric. In that sense, the purpose of a database becomes fragile and almost dead letter. Furthermore, the transformation of Eurodac raises serious privacy concerns and signifies that asylum seekers, which are a particularly vulnerable group, are also considered a priori as suspects of terrorism and criminality.[89] The principal purpose of supporting the implementation of the Dublin rules remains, however as with the VIS, law enforcement is listed as an ancillary purpose. Following the VIS model, consultation of Eurodac data does not take place on a routine basis and involves only the prevention, detection and investigation of terrorist offences and other serious crimes.[90] The requesting authority, designated at the national level, would need to fulfill a series of conditions that the Regulation sets out, which are stricter than the ones prescribed in the VIS Decision. In particular, an additional step is included; the prior consultation of national fingerprint databases, as well as the automated fingerprinting identification systems (AFIS) of other Member States[91] and the VIS and such consultation must have been futile.[92] Furthermore, the necessity to consult the database is further defined; according to

quests for the comparison with Eurodac data by Member States' law enforcement authorities and Europol for law enforcement purposes, and amending Regulation (EU) No. 1077/2011 establishing a European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice (Recast version) [2013] OJ L180/1 (recast Eurodac Regulation).

[89] Niovi Vavoula, 'The Recast Eurodac Regulation: Are Asylum Seekers Treated as Suspected Criminals?' in Céline Bauloz and others (eds), *Seeking Asylum in the European Union: Selected Protection Issues Raised by the Second Phase of the Common European Asylum System* (Brill 2015) 260.

[90] Recast Eurodac Regulation, recital 31. European Data Protection Supervisor (EDPS), 'Opinion of the European Data Protection Supervisor on the amended proposal for a Regulation of the European Parliament and of the Council on the establishment of "EURODAC" for the comparison of fingerprints for the effective application of Regulation (EU) No […/…] (Recast version)' [2013] OJ C28/3 (executive summary) para 54; Standing Committee of Experts on International Immigration, Refugee and Criminal Law (Meijers Committee), 'Note on the proposal for a Regulation on the establishment of Eurodac' COM (2012) 254 (CM1216, 2012).

[91] On the basis of Council Decision 2008/615/JHA on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime [2008] OJ L210/1 (Prüm Decision).

[92] Recast Eurodac Regulation, art 20(1).

Article 20(1)(b), 'there must be an overriding public security concern which makes the searching of the database proportionate'. These provisions as well as the explicit exclusion of national intelligence authorities[93] are welcomed steps. On the downside, as in the case of the VIS, the role of checking whether the requirements of the criteria is entrusted to a verifying authority which does not comply with the CJEU's standards as set out in *Digital Rights Ireland.*[94]

2.3. Third wave: Generalisation of surveillance of movement of third-country nationals

Since the reform of Eurodac, the evolution of pan-European immigration databases has escalated in a number of ways; the establishment of new systems is in the pipeline in an attempt to fill in the 'informational gaps' created by the compartmentalised approach followed already since the 90's; the corrective reforms in the existing systems with a view to enhancing their usefulness and effectiveness; and the possibility to connect the 'data pots' with a view to making the systems interoperable. Whereas certain developments were in the pipeline prior to their pursuit in the past years, their rigorous prioritisation and speedy adoption has been prompted particularly in the aftermath of the terrorism events in France and Belgium in 2015, leading to the need to establish a 'Security Union'.[95]

2.3.1. Non-visa holders as risky travelers: EES and ETIAS

Although the aforementioned databases create a rather comprehensive network of information exchange schemes concerning third-country nationals, they do not cover those originating from countries not subject to visa regime. Under the direct influence of similar initiatives in the US, particularly the US-VISIT programme (now IDENT), this alleged 'informational gap' was hinted

[93] ibid, art 5(1).

[94] See above in relation to the VIS access by law enforcement authorities. For a detailed overview of the privacy concerns see Vavoula, 'The Recast Eurodac Regulation' (n 88) 265. It is argued that law enforcement access to Eurodac was advocated by certain Member States which already stored asylum seekers' data in their national AFIS. As a result, under Prüm they already share asylum seekers' information with other Member States. This design of the national AFIS, which is rather disturbing in itself, because it equates criminals' and asylum seekers' data, was part of the justification proposed by the Commission when explaining the necessity of the measure granting access to law enforcement agencies.

[95] See Commission (n 6).

in the Hague Programme[96] and in the Commission Communication on improved effectiveness, enhanced interoperability and synergies among information systems.[97] For years the discussions revolved around the scope and feasibility of the new system, with the Commission delaying to adopt its proposals.[98]

Against this background, on 28 February 2013 the Commission presented three legislative proposals forming the commonly referred to 'Smart Borders Package', which comprised of a proposal to establish the EES at the EU external borders[99] accompanied by a proposal for a 'Registered Travellers Programme' (RTP) to facilitate the border crossing of pre-screened *bona fide* travellers[100] and one on amendments to the Schengen Borders Code.[101] Due to serious privacy concerns,[102] the Commission withdrew the package and committed to submitting revised proposals in early 2016. However, in the a the aftermath of the terrorist events in 2015 with France, the momentum for the establishment of yet another database is currently high, with that Member States even proposing of further extending the reach of the system to EU

[96] The Hague Programme (n 5) 7.

[97] Commission (n 84) 9.

[98] For the debate see Commission, 'Preparing the next steps in border management in the European Union' (Communication) COM (2008) 69 final; Commission, 'Smart Borders – options and the way ahead' (Communication) COM (2011) 680 final.

[99] Commission, 'Proposal for a Regulation of the European Parliament and of the Council establishing an Entry/Exit System (EES) to register entry and exit data of third country nationals crossing the external borders of the member states of the European Union' COM (2013) 95 final.

[100] Commission, 'Proposal for a Regulation of the European Parliament and of the Council establishing a Registered Traveller Programme' COM (2013) 97 final.

[101] Commission, 'Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EC) No 562/2006 as regards the use of the Entry/Exit System (EES) and the Registered Traveller Programme (RTP)' COM (2013) 96 final.

[102] For criticism see among others EDPS, 'Opinion of the European Data Protection Supervisor on the proposals for a Regulation establishing an Entry/Exit System (EES) and a Regulation establishing a Registered Traveller Programme (RTP)' [2014] OJ C32/25 (executive summary); Article 29 DPWP, 'Opinion 05/2013 on Smart Borders' (WP206, 2013); Standing Committee of Experts on International Immigration, Refugee and Criminal Law (Meijers Committee), 'Note on the Smart Borders proposals' COM (2013) 95 final, COM (2013) 96 final and COM (2013) 97 final (CM1307, 2013).

nationals, a possibility that has not been completely overruled for the future.[103] On 6 April 2016, the Commission released its revised proposals, abandoning the idea of the RTP and modifying the rules on the functioning of the EES without, however, abandoning the overarching policy choices.[104] On 25 October 2017, the European Parliament and Council agreed on the final text after speedy negotiations in view of the urgency to promote internal security.

The EES will register border crossing both at entry and exit for all third-country nationals admitted for a short stay, irrespective of whether they are required to obtain a Schengen visa or not. It will also apply to third-country nationals whose entry for a short stay has been refused. As with the VIS, the EES is envisaged as a multi-purpose tool aimed at reducing border check delays, improving the quality of border checks by automatically calculating the authorised stay of each traveller, ensuring systematic and reliable identification of overstayers and strengthening internal security and the fight against terrorism by allowing law enforcement authorities access to travel history records. To these ends, the system will register the identities of third-country nationals, by storing alphanumeric data, four fingerprints and facial image, along with details of their travel documents and will link these to electronic entry and exit records. The current practice of stamping travel documents will be abolished. Instead, the system will automatically calculate the maximum term of authorised stay in accordance with the Schengen Borders Code.[105] An information mechanism will be included to identify cases where there are no records of exit. Reflecting the Commission's proportionality concerns, the 2013 proposal left law enforcement access and the inclusion of biometrics for future determination.[106] However, the vast majority of Member States desired the opening up of the database for criminal law purposes based

[103] Council, Document 12272/15 (2015).

[104] Commission, 'Proposal for a Regulation of the European Parliament and of the Council establishing an Entry/Exit System (EES) to register entry and exit data and refusal of entry data of third country nationals crossing the external borders of the member states of the European Union and determining the conditions for access to the EES for law enforcement purposes and amending Regulation (EC) No 767/2008 and Regulation (EU) No 1077/2011' COM (2016) 194 final; Commission, 'Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EU) 2016/399 as regards the use of the Entry/Exit System' COM (2016) 196 final.

[105] Council Regulation (EU) 2016/399 of 9 March 2016 on a Union Code on the rules governing the movement of persons across borders (Schengen Borders Code) [2016] OJ L77/1.

[106] Commission, 'EES Proposal of 2013' (n 98) recital 23.

on the VIS and Eurodac examples.[107] In the light of this, the revised proposal envisages law enforcement access to EES data from the beginning of its operation largely on the basis of both the Eurodac and the VIS models, thus raising similar concerns as regards the necessity of such access, the strictness of the criteria and the procedure for consulting the data in the course of criminal investigations. However, in this case these concerns are exacerbated considering the huge amount of persons that monitoring will entail and the wide range of data that will be processed. Furthermore, contrary to the other schemes, the 2016 proposal requires the registration of four fingerprints, however, it remains to be seen whether this issue will remain intact during negotiations, particularly in the light of law enforcement access to the EES data.

In any case, the added value of a new database monitoring the movement of essentially all foreign travellers is not yet evident, particularly in the light of the recent operation of the VIS, which has only recently been fully rolled out worldwide.[108] Furthermore, the extent to which the system will tackle the issue of overstayers is highly uncertain; the information mechanism envisaged does not signify that the person is necessarily an overstayer as there may be other reasons why a person has not exited properly (illness, application for asylum, death).[109] Importantly, national authorities will not have further information as regards the whereabouts of the person in question.[110]

More worryingly, the establishment of the EES signifies the introduction of yet another mechanism of surveillance of mobility for all travellers grounded on automaticity, the collection and further processing of biometrics and the well-established link between immigration control and law enforcement. With the future setting up of the EES all third-country nationals irrespective of the country they come from will be considered as suspect population.[111] This merging of the risk prevention logic with border security entails signifi-

[107] Council, Document 9863/13 (2013) 5.

[108] Valsamis Mitsilegas, *The Criminalisation of Irregular Migration in Europe – Challenges for Human Rights and the Rule of Law* (Springer 2015) 34.

[109] Ben Hayes and Mathias Vermeulen, 'Borderline – The EU's New Border Surveillance Initiatives' (Heinrich Böll Stiftung 2012) 41.

[110] Meijers Committee (n 102) 2.

[111] EDPS (n 102) 7.

cant consequences for the protection of fundamental rights and the relationship between the individual and the state,[112] as well as EU nationals and the 'others'. Furthermore, it is noteworthy that the initial discussions on the setting up of the new database took place without impetus from terrorist events, thus pointing to the direction that surveillance of mobility has ceased to be considered as an exceptional response, but has rather become the norm.

The European Travel Information and Authorisation System (ETIAS) was originally conceptualised in a Communication of 2008 next to the EES, whereby the Commission briefly mentioned that it would examine the possibility of introducing an Electronic System of Travel Authorisation (ESTA) to pre-screen third-country nationals, irrespective of whether they were subject to a visa regime, in order to verify that they fulfill the entry conditions before travelling to the EU.[113] In 2011, the Commission decided not to proceed 'as the potential contribution to enhancing the security of the Member States would neither justify the collection of personal data at such a scale nor the financial cost and the impact on international relations'.[114] Nevertheless, the liberalisation of visa policy coupled by highly securitised political framework in the aftermath of the terrorist attacks in Paris and Brussels have resulted in the reemergence of this idea in the past years.[115] The proposal on establishing the ETIAS,[116] which largely resembles the US ESTA system, foresees that all travellers to the Schengen area not subject to visa requirements shall be obliged to obtain authorisation prior to their departure through an online application whereby they would disclose a series of personal data regarding their identity and their travel arrangements. The pre-screening and provision of authorisation shall take place on the basis of the automated processing (comparison) of applicant personal data held in existing immigration and police databases, an special ETIAS watchlist and specific risk indicators.

---

[112] Valsamis Mitsilegas, 'The Borders Paradox – The Surveillance of Movement in a Union without Internal Frontiers' in Hans Lindahl (ed.), *A Right to Inclusion and Exclusion? Normative Faultlines of the EU's Area of Freedom, Security and Justice* (Hart 2009).

[113] Commission, 'Preparing the next steps in border management' (n 97). A study was released in this respect. See Commission, 'Policy Study on an EU Electronic System for Travel Authorisation' (PwC, 2011).

[114] Commission (n 84) 7.

[115] Commission, 'Stronger and smarter information systems for borders and security' (Communication) COM (2016) 205 final, 13.

[116] Commission, 'Proposal for a Regulation of the European Parliament and of the Council establishing a European Travel Information and Authorisation System (ETIAS) and amending Regulations (EU) No 515/2014, (EU) 2016/399, (EU) 2016/794 and (EU) 2016/1624' COM (2016) 731 final.

The creation of an ETIAS is a bold move towards preemptive surveillance of movement through extensive risk assessments on the basis of providing a wide range of personal information. As noted by the Dutch Presidency:

'The possible added value […] lies in the information which is given by the traveller when registering before travelling, in the possibility to assess this information and use it for pre-screening, in a possible deterrent effect on *mala fide* travellers and in the facilitation of the border procedures after a traveller has obtained the travel authorisation.'[117]

However, the necessity of the ETIAS is doubtful as the Commission did not produce an impact assessment prior to the adoption of the proposal.[118] Furthermore, the proportionality concerns of such a system are evident. Its establishment will impose an additional layer of control under the assumption that, in principle, all travellers are suspected lawbreakers. The ETIAS will constitute as large a database as the EES and containing as much wealth of personal information as the VIS, thus combining the worst of both worlds, and will be used for a variety of purposes. It will allow authorities to construct complete profiles of visa-exempt travellers who are previously unsuspected of any offence. Coupled with the EES, the ETIAS will constitute both a massive catalogue of third-country nationals and a powerful surveillance tool geared by the logic of risk prevention transplanted once again into immigration control.[119] Importantly, the ETIAS should be conceived of as a platform for mining and profiling personal data rather than just a platform for issuing automated or manual travel authorisation decisions. The ETIAS screening rules are meant to identify persons who are otherwise unknown to national competent authorities but are *assumed* to be of interest for immigration control or security purposes and therefore are *likely* to commit criminal offences in the future. These persons would be flagged not because of specific actions they have engaged in but because they display particular category traits in a probabilistic logic without concrete evidence.[120]

---

[117] Council, Document 8590/16 (2016) 3. Emphasis original.

[118] See Susie Alegre, Julien Jeandesboz and Niovi Vavoula, 'European Travel Information and Authorisation System (ETIAS): Border management, fundamental rights and data protection' (Study for the European Parliament, PE 583.148, 2017) 27.

[119] Vavoula (n 29) Ch 6.

[120] Alegre, Jeansdesboz and Vavoula (n 118) 23-26.

2.3.2. Repackaging the existing information systems: SIS II, Eurodac and VIS under refurbishment

On 4 May 2016, the Commission tabled an amended proposal on Eurodac,[121] as part of a first package of a broad reform of the CEAS. The proposal signals a landmark change in Eurodac's purpose from being a system ensuring the effective implementation of the Dublin mechanism into an instrument serving *wider immigration purposes*, including the return of irregular migrants. This change has affected a series of provisions. In particular, on top of a full set of fingerprints, Member States shall be obliged to take and transmit a facial image in relation to all three categories falling within the personal scope of Eurodac.[122] Therefore, for the first time since the establishment of the database, information on persons who were found irregularly present will be centrally stored. The age threshold for children is significantly reduced to the age of six.[123] The categories of data held in the database are also considerably thus getting closer to the VIS paradigm, in order to 'allow immigration and asylum authorities to easily identify an individual'.[124] In other words, the Eurodac reform has taken place both quantitatively, through the expansion of the scope *ratione personae* and the obligation to register additional categories of data, including sensitive ones, and qualitatively, by detaching Eurodac from its original Dublin context and re-conceptualising it as a multi-purpose tool.

The Eurodac case is a prime example of the serious risks attached to centralised storage, whereby once information is collected it can then be used in a multiplicity of contexts, even without prior scrutiny or much justification, even if the individuals concerned have not been informed about it beforehand. It is regrettable that in addition to the registration of fingerprints, applicants for international protection and irregular migrants will also be photographed and their facial image will be recorded in the system. This process

---

[121] Commission, 'Proposal for a Regulation of the European Parliament and of the Council on the establishment of 'Eurodac' for the comparison of fingerprints for the effective application of [Regulation (EU) No 604/2013 establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless persons], for identifying an illegally staying third-country national or stateless person and on requests for the comparison with Eurodac data by Member States' law enforcement authorities and Europol for law enforcement purposes (Recast version)' COM (2016) 272 final.

[122] ibid art 2(1).

[123] ibid art 2(2).

[124] ibid 13.

enhances the negative connotations with criminality generated by fingerprinting and deepens the feeling that the movement of these individuals is monitored. Furthermore, the revised framework transforms Eurodac from a relatively restricted database, compared to VIS and the SIS II, into a powerful tool of mass surveillance of movement, with the aid of which national authorities shall be able to track third-country nationals whose data are recorded within the EU for as long as they remain on EU territory. Moreover, this expansion seems to disregard the fact that the SIS II already stores alerts on persons who must be refused entry or stay, therefore a mechanism enhancing the implementation of the return policy is already in place.

The SIS II is also under refurbishment since December 2016.[125] The Commission proposal followed its three-year evaluation,[126] according to which the lack of harmonised national criteria for entering alerts constituted a major flaw of the system. The Commission proposal constitutes a significant step in rectifying this characteristic through the mandatory registration of entry bans.[127] However, this development is not without problems. The obligation of national authorities to accompany entry bans with a SIS II alert inevitably raises the question of the relationship between the Return Directive[128] that regulates the imposition of entry bans and the SIS II Regulation as regards the conditions for issuing entry ban decisions against irregular migrants and how

---

[125] Commission, 'Proposal for a Regulation of the European Parliament and of the Council on the establishment, operation and use of the Schengen Information System (SIS) in the field of border checks, amending Regulation (EU) No 515/2014 and repealing Regulation (EC) No 1987/2006' COM (2016) 882 final; 'Proposal for a Regulation of the European Parliament and of the Council on the establishment, operation and use of the Schengen Information System (SIS) in the field of police cooperation and judicial cooperation in criminal matters, amending Regulation (EU) No 515/2014 and repealing Regulation (EC) No 1986/2006, Council Decision 2007/533/JHA and Commission Decision 2010/261/EU' COM (2016) 883 final; 'Proposal for a Regulation of the European Parliament and of the Council on the use of the Schengen Information System for the return of illegally staying third- country nationals' COM (2016) 881 final.

[126] Commission, 'Report to the European Parliament and Council on the evaluation of the second generation Schengen Information System (SIS II) in accordance with arts 24 (5), 43 (3) and 50 (5) of Regulation (EC) No 1987/2006 and arts 59 (3) and 66(5) of Decision 2007/533/JHA and an accompanying Staff Working Document' COM (2016) 880 final.

[127] Commission, 'SIS II Proposal of 2016' (n 125) art 24(3).

[128] Directive 2008/115/EU of 16 December 2008 on common standards and procedures in Member States for returning illegally staying third-country nationals [2008] OJ L 348/98.

these have been transposed at the national level. According to Article 11(1) of the Return Directive, an entry ban *must* be issued where a return decision was ordered without a period for voluntary departure being granted, or where the obligation to return has not been complied with. In other cases, an entry ban *may* be issued. Therefore, entry bans may be implicitly issued even if a period for voluntary departure has been granted and even if the return decision has been complied with.[129] Hence, there is no objective and standardised mechanism, as Member States have been granted wide discretion on this issue. This discretion is reflected in the more recent evaluation of the Return Directive, whereby in no less than 11 Schengen States an entry ban is automatically issued alongside a return decision, whereas in 14 countries irregular migrants are issued with an entry ban on the basis of the criteria set out in Article 11(1).[130] In three states only the entry ban decision is taken on a case-by-case basis.[131] This means that in a significant number of Member States, SIS II alerts are registered in bulk and on the basis of automaticity solely because third-country nationals have been issued return decisions, and with minimum guarantees that the seriousness of each case has been individually evaluated.[132] This implies that, at least in certain Member States, the entry of SIS II alerts involving irregular migrants carries the characteristics of massive registration without any limitations, exceptions or distinctions, thus raising serious proportionality concerns.

As for the VIS, whereas currently there is no proposal under negotiation, in 2018, it is expected that the Commission will present a revised proposal so as to change the (already relaxed) conditions of law enforcement access to the system and lower the age threshold for fingerprinting on the basis of the Eurodac model.

---

[129] Steve Peers, *EU Justice and Home Affairs Law* (3rd edn, Cambridge University Press 2011) 570.

[130] Commission, 'Evaluation on the application of the Return Directive (2008/115/EC)' (2013) 165-6.

[131] ibid.

[132] For further information on national practices see European Migration Network (EMN), 'Ad Hoc Query on registering entry bans in the SIS' (2015) <http://ec.europa.eu/dgs/home-affairs/what-we-do/networks/european_migration_network/reports/docs/ad-hoc-queries/border/2014.628_emn_ahq_registering_entry_bans_in_the_sis_(wider_diss)_update.pdf >.

2.3.3. Establishment of new systems in the pipeline?

The EU initiatives do not end with the establishment of the new systems or the corrective reforms to magnify the performance of existing mechanisms. Certain categories of third-country nationals, namely holders of residence permits, residence cards and long-stay visa holders, still elude centralised storage.[133] In a Communication on stronger and smarter information systems, the Commission identified the lack of information on long-stay visa holders as a information gap.[134] Even though most Member States do not centrally record such data,[135] the Roadmap for information exchange and information management flags up the establishment of a Residents Permits Repository as a way forward, and would store information on residence cards, residence permits and long-stay visas.[136] Such a system would fill the last gap in information exchange in terms of scope *ratione personae* as *all* third-country nationals will be monitored without exceptions. The underlying logic is the decentralised management of the documents issued, though this has a collateral effect on immigration control. Of particular risk is the fact that the identities of residence card and long-stay visa holders cannot be biometrically verified, an issue that is considered 'a security risk that should be addressed'.[137] Additionally, such a system would be useful in facilitating their border crossing.[138]

2.3.4. From compartmentalisation to interoperability

The final step to achieve 'Security Union' has been the growing interest in interconnecting the different 'data pots' in the form of interoperability. Debates in that respect first started in the aftermath of 9/11,[139] but after the Madrid bombings, the European Council, in its Declaration on combating terrorism, invited the Commission to submit proposals for enhanced interoperability between SIS II, VIS and Eurodac. In its Communication on improved effectiveness, enhanced interoperability and synergies among EU databases, the Com-

---

[133] For the discussion on the merits of registering residence permit holders see Council, Document 12527/15 (2015).

[134] Commission (n 115) 3.

[135] Council, Document 12527/15 (2015).

[136] Council, Document 9368/1/16 (2015) 55.

[137] ibid.

[138] ibid.

[139] Council, Document 13176/01 (2001).

mission defined interoperability as the 'ability of IT systems and of the business processes they support to exchange data and to enable the sharing of information and knowledge'.[140] However, details on the legal aspect for the interoperability of databases were spared, as the concept was reduced to a technical rather than a legal or political matter.[141] Since the Paris attacks of 13 November 2015, the connection of the 'data jars' has gained fresh impetus. The European Council Conclusions of 18 December 2015 clearly referred to the need to ensure interoperability of all relevant systems to ensure security checks.[142] After the Brussels events of 24 March 2016, JHA Ministers adopted a Joint Statement at their extraordinary meeting in which interoperability was treated as a matter of urgency.[143] In the Communication on stronger and smarter borders, the Commission identified four different models of interoperability, which correspond to a gradation of convergence among the systems:

a. A single search interface to query several information systems simultaneously and to produce combined results on one single screen;

b. Interconnectivity of information systems where data registered in one system will automatically be consulted by another system;

c. Establishment of a shared biometric matching service in support of various information systems; and

d. Common repository of data for different information systems (core module).

With a view to addressing the legal, technical and operational aspects of the different options, including the necessity, technical feasibility and proportionality of available options and their data protection implications, an Expert Group on Information Systems and Interoperability has been set up.[144] In the meantime, Member States have already agreed in the Roadmap to enhance

---

[140] Commission (n 83).

[141] For a critique see Paul De Hert and Serge Gutwirth, 'Interoperability of Police Databases within the EU: An Accountable Political Choice?' (2006) 20 International Review of Law Computers & Technology 21, 22; EDPS, 'Comments on the Communication of the Commission on interoperability of European databases' (2006) <https://secure.edps.europa.eu/EDPSWEB/webdav/shared/Documents/Consultation/Comments/2006/06-03-10_Interoperability_EN.pdf>.

[142] Council, Document EUCO 28/15 (2015) 3.

[143] Council, Document 7371/16 (2016) pt 5.

[144] Commission Decision of 17 June 2016 setting up the High Level Expert Group on Information Systems and Interoperability [2016] OJ C257/3.

information exchange and information management, to implement the first option as a matter of priority, and the remaining options to be discussed in the medium and longer term.[145] The undertone for future development is evident and a convergence between criminal law and immigration control systems seems to be in the making. Although the Roadmap refers to all information systems in the AFSJ, related to both immigration and law enforcement, it is explicitly stated that the interlinkages between all different information exchange schemes are highlighted, which 'will contribute to ensuring the cooperation between the authorities and agencies […] and the interoperability between information systems'.[146]

In addition to the aforementioned efforts, interoperability is already embedded in the recent EES, ETIAS and Eurodac proposals, thus preempting this development with proper impact assessment as regards the protection of fundamental rights.[147] Furthermore, the Expert Group has released its final report on interoperability giving the 'green light' for implementing options (a), (b) and (d)[148] and the Commission adopted a proposal essentially aiming at extending the mandate of eu-LISA, the EU Agency entrusted with the task of managing large-scale information systems, so as to supervise and execute the technical arrangements for ensuring interoperability.[149]

Interoperability is a rather complex legal issue with far reaching implications for individuals, and should not be viewed as a merely technical matter. It significantly enhances the surveillance powers of the EU by enlarging the number of national authorities which could have access to the data, and nullifies the limited purposes for which databases have been set up. In that sense, interoperability 'disrespects the importance of separated domains and cuts through their protective walls'.[150] Through the aggregation of information

---

[145] Council, Document 9368/1/16 (n 136) 5. Also see Council, Document 7711/16 (2016).

[146] ibid 4.

[147] Commission (n 103) recital 13 and art 7; Commission (n 120) 5.

[148] High Level Expert Group on Information Systems and Interoperability, 'Final Report' (2017) <http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetailDoc&id=32600&no=1>.

[149] Commission, 'Proposal for a Regulation of the European Parliament and of the Council on the European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice, and amending Regulation (EC) 1987/2006 and Council Decision 2007/533/JHA and repealing Regulation (EU) 1077/2011' COM (2017) 352 final.

[150] De Hert and Gutwirth (n 141) 7.

from different systems, a brand powerful system might emerge.[151] Surveillance will be intensified and authorities will be able to draw more precise conclusions on the private lives of individuals who would not be able to foresee how the collected information will be used. Individual rights, particularly the right to information, will be more difficult to exercise. Due to divergent rules regarding several aspects, such as the retention periods, the inclusion of biometric data or the possibility of transfers, interoperability may lead to significant revisions in information systems with a view to aligning the modalities for the sake of efficiency. Interoperability could thus be seen as the first step to a gradual transition from a compartmentalised system of independent immigration databases to a single EU information system.

3. CONCLUSION

The aim of this contribution was to map the evolution of pan-European immigration databases and highlight a series of privacy concerns arisen by their establishment, operation and reconfiguration over time. Through the systematic categorisation of these centralised systems in three distinct eras, it has been demonstrated that their establishment entails the collection and storage of a wide range of personal data, including biometrics, which are sensitive personal data, and their further processing for multiple and often diverging purposes. The consistent merging of purposes has utterly blurred the boundaries between immigration and criminal law with significant repercussions as regards the protection of privacy and the perception of third-country nationals. Furthermore, depending on the use of the data it has pointed out that certain categories of information should not be available to specific authorities. With the routine registration of biometrics, the provision of extensive retention period and the use of data for law enforcement purposes, immigration control progressively acquires characteristics of mass surveillance. Particularly in the cases of the VIS and the EES, the deployment of surveillance techniques stems from the need to monitor everyday, legitimate activities.[152] It has been demonstrated that surveillance of mobility has been gradually deployed to the extent that the existing cases have a direct effect in subsequent proposals and provisions, thus deepening surveillance and rendering a permanent and normal means of addressing not only immigration issues but also terrorism concerns. The gradual normalisation of surveillance may even expand to EU nationals challenging not only privacy but also EU citizenship

[151] EDPS (n 141) 4.

[152] See David Lyon, *Surveillance Society: Monitoring Everyday Life* (Open University Press 2001).

rights. EU immigration databases currently score high in the EU agenda, either in the form of setting up new systems, or modernising the existing ones or interconnecting them in order to magnify their effectiveness. Nevertheless, in an era of security and consecutive terrorism event, it appears that fundamental rights have not been taken into account properly particularly due to the fast-track procedures followed at EU level. With a series of proposal currently on the negotiating table, it remains to be seen what the future will bring to the ongoing battle between maintaining security and safeguarding fundamental rights.

4. SELECTED LITERATURE

Alegre S, Jeandesboz J and Vavoula N, 'European Travel Information and Authorisation System (ETIAS): Border management, fundamental rights and data protection' (Study for the European Parliament, PE 583.148, 2017)

Amoore L and de Goede M (eds), Risk and the War on Terror (Routledge 2008)

Aus J, 'Eurodac: A Solution Looking for a Problem?' (2006) 10 European Integration online Papers

Baldaccini A, 'Counter-terrorism and the EU Strategy for Border Security: Framing Suspects with Biometric Documents and Databases' (2008) 10(1) European Journal of Migration and Law 31

Besters M and Brom F, '"Greedy" Information Technology: The Digitalization of the European Migration Policy' (2010) 12(4) European Journal of Migration and Law 455

Bigo D and Guild E (eds), Controlling Frontiers: Free Movement Into and Within Europe (Routledge 2005)

Bonditti P, 'From Territorial Spaces to Networks: A Foucaultian Approach to the Implementation of Biometry' (2004) 29 Alternatives: Global, Local, Political 465

Broeders D, 'The New Digital Borders of Europe. EU Databases and the Surveillance of Irregular Migrants' (2007) 22(1) International Sociology 71

Broeders D and Hampshire J, 'Dreaming of Seamless Borders: ICTs and the Pre-Emptive Governance of Mobility in Europe' (2013) 39(8) Journal of Ethnic and Migration Studies 1201

Brouwer E, 'The Use of Biometrics in EU Databases and Identity Documents – Keeping Track of Foreigners' Movements and Rights' in Lodge J (ed.), Are You Who You Say You Are? – The EU and Biometric Borders (Wolf Legal Publishers 2007) 45–66

Brouwer E, *Digital Borders and Real Rights – Effective Remedies for Third-Country Nationals in the Schengen Information System* (Martinus Nijhoff 2008) 47-57

De Hert P and Gutwirth S, 'Interoperability of Police Databases within the EU: An Accountable Political Choice?' (2006) 20 International Review of Law Computers & Technology 21

Fratzke S, Not Adding Up: The Fading Promise of Europe's Dublin System (Migration Policy Institute Report, 2015)

Guild E, 'Unreadable Papers? The EU's First Experiences with Biometrics: Examining Eurodac and the EU's Borders' in Lodge J (ed.), Are You Who You Say You Are? The EU and Biometric Borders (Wolf Legal Publishers 2007) 32

Guild E and others, New Approaches, Alternative Avenues and Means of Access to Asylum Procedures for Persons Seeking International Protection (Study for the LIBE Committee, PE509.989, 2014)

Guild E, 'Moving the Borders of Europe' (Inaugural lecture, University of Nijmegen, 2000, 24) <http://cmr.jur.ru.nl/cmr/docs/oratie.eg.pdf>

Hayes B, From the Schengen Information System to the SIS II and the Visa Information System (VIS): The Proposals Explained (Statewatch Report 2004)

Hayes B, NeoConOpticon: The EU Security-Industrial Complex (Transnational Institute/Statewatch 2009)

Hayes B and Vermeulen M, 'Borderline – The EU's New Border Surveillance Initiatives' (Heinrich Böll Stiftung 2012)

Juster B and Tsianos V, 'Erase Them! Eurodac and Digital Deportability' (2013) Transversal/EIPCP multilingual webjournal <http://eipcp.net/transversal/0313/kuster-tsianos/en>

Kabera Karanja S, Transparency and Proportionality in the Schengen Information System and Border Control Cooperation (Martinus Nijhoff 2008) 216

Kindt E, Privacy and Data Protection Issues of Biometric Applications (Springer 2013)

Kuijper PJ, 'Some Legal Problems Associated with the Communitarization of Policy on Visas, Asylum and Immigration under the Amsterdam Treaty and Incorporation of the Schengen acquis' (2000) 37(2) Common Market Law Review 345

Lindskov Jacobsen K, 'Making Design Safe for Citizens: A Hidden History of Humanitarian Experimentation' (2010) 14(1) Citizenship Studies 89

Lyon D, Surveillance Society: Monitoring Everyday Life (Open University Press 2001)

Mitsilegas V, 'The Borders Paradox – The Surveillance of Movement in a Union without Internal Frontiers' in Lindahl H (ed.), A Right to Inclusion and Exclusion? Normative Faultlines of the EU's Area of Freedom, Security and Justice (Hart 2009)

—— 'Borders, Security and the Transatlantic Cooperation in the Twenty-First Century: Identity and Privacy in an Era of Globalized Surveillance' in Givens T and others (eds), Immigration Policy and Security (Routledge 2009)

—— 'Human Rights, Terrorism and the Quest for "Border Security"' in Pedrazzi M et al. (eds), Individual Guarantees in the European Judicial Area in Criminal Matters (Bruylant 2011) 85–112

—— 'Immigration Control in an Era of Globalisation: Deflecting Foreigners, Weakening Citizens, Strengthening the State' (2012) 19(1) Indiana Journal of Global Legal Studies 3

—— The Criminalisation of Irregular Migration in Europe – Challenges for Human Rights and the Rule of Law (Springer 2015)

—— 'The Law of the Border and the Borders of Law – Rethinking Border Control from the Perspective of the Individual' in Weber L (ed.), Rethinking Border Control for a Globalizing World (Routledge 2015) 15–32

Parkin J, 'The Difficult Road to the Schengen Information System II - The Legacy of Laboratories and the Cost for Fundamental Rights and the Rule of Law' (Paper, CEPS 2011)

Peers S and Rogers N (eds), EU Immigration and Asylum Law (Martinus Nijhoff 2006) 263-8

Peers S, 'Legislative Update: EC Immigration and Asylum Law 2008: Visa Information System' (2009) 11 European Journal of Migration and Law 69

—— EU Justice and Home Affairs Law (3rd edn, Cambridge University Press 2011) 570

Ryan B and Mitsilegas V (eds), Extraterritorial Immigration Control (Martinus Nijhoff 2010)

Schattenberg B, 'SIS: Privacy and Legal Protection' in Schermers H et al. (eds), Free Movement of Persons in Europe: Legal Problems and Experience (Martinus Nijhoff 1993) 43

Valsamis M, *EU Criminal Law* (Hart 2009)

Vavoula N, 'The Recast Eurodac Regulation: Are Asylum Seekers Treated as Suspected Criminals?' in Bauloz C and others (eds), Seeking Asylum in the European Union: Selected Protection Issues Raised by the Second Phase of the Common European Asylum System (Brill 2015)

—— Immigration and Privacy in the Law of the European Union: The Case of Databases (Brill forthcoming 2018)

A scoping review of predictive analysis techniques for predicting criminal events

ANNELEEN RUMMENS,[1] WIM HARDYNS[2] & LIEVEN PAUWELS[3]

Decision-making processes are increasingly based on intelligence gained from 'big data', ie large and extensive datasets. In the context of crime data analysis, the large amount of crime data available in police databases can be considered an example of big data, that could inform us about current and upcoming patterns of crime. In recent times, scholars working in the field of criminology are discovering the topic, and increasingly explore the practical implications for crime prevention and control. Predictive analysis techniques can be used in crime data analysis to objectively inform policy decisions, strategies and tactical operations, by identifying and predicting previously unknown patterns and trends in crime data. One of the most challenging applications is the prediction of criminal events (places, times, victims or perpetrators at high-risk of being subjected to criminal events). The need for methods which can handle and extract insights from big datasets, the shift to more proactive methods and the strive to continuously improve predictions of criminal events, have led to the development of predictive policing methods. These methods claim to improve criminal event predictions compared to previous traditional methods such as hotspot analysis and time series modelling. In this article, we present a scoping review of predictive policing methods. The main objective of this review is to identify and provide an overview of the current predictive policing methods reported in the scientific literature for predicting criminal events, and to describe and compare their main characteristics, strengths and weakness, focusing on their methodological parameters (context, method, crime types, input variables, unit of analysis), predictive ability and what is known about their effectiveness for crime control and prevention. The results indicate that predictive policing is a topic which has

[1] PhD researcher, Institute for International Research on Criminal Policy (IRCP), Department Criminology, Criminal Law and Social Law, Faculty of Law, Ghent University. Email: anneleen.rummens@ugent.be.

[2] Assistant Professor of Criminology, Institute for International Research on Criminal Policy (IRCP), Department Criminology, Criminal Law and Social Law, Faculty of Law, Ghent University. Email: wim.hardyns@ugent.be.

[3] Associate Professor of Criminology, Director Institute for International Research on Criminal Policy (IRCP), Department Criminology, Criminal Law and Social Law, Faculty of Law, Ghent University. Email: lieven.pauwels@ugent.be.

recently gained in prominence. Although multiple empirical studies show that these methods can effectively be used to predict crime, it is surprising to see that only marginally attention has been given to the effect of methodological choices such as input variables, method, grid and temporal resolution and the effect of common data quality problems (eg missing data) on predictive ability. Additionally, only a few experimental studies have been conducted, making it not possible yet to conclusively determine the value of these methods for crime control and prevention. We subscribe that this gap in the literature may explain the scepticism that prevails under some scholars. The implications of our findings are discussed.

1. INTRODUCTION

1.1. Big data and predictive analysis

Decision-making processes are increasingly based on intelligence gained from 'big data'. Big data refers to datasets that are generally extremely large in volume, are collected near or in real time, link different sources or levels of information together, and which contain diverse variables that are detailed and tend to be exhaustive in scope.[4] In the context of crime data analysis, the large amount of crime data available in police databases can be considered an example of big data, that may inform us about current and upcoming spatio-temporal trends in criminal events. Advances in information technology and artificial intelligence have further increased our ability to extract useful insights from these big datasets. To extract these insights, a set of quantitative methods aimed at prediction, collectively called predictive analysis (or predictive analytics), is used.

Currently, predictive analysis based on big data is applied in various fields. In healthcare, it is used to analyse and support administration and delivery, clinical decisions, consumer behaviour, and support services.[5] One of the most popular applications of predictive analysis is churn prediction, which consists of predicting which customers are about to leave the company, based on the available customer data (eg in telecom[6]). These customers can then be en-

[4] Rob Kitchin, 'Big Data, new epistemologies and paradigm shifts' (2014) Big Data & Society 1-12.

[5] Rebecca Hermon and Patricia AH Williams, 'Big data in healthcare: What is it used for?' (Australian eHealth Informatics and Security Conference 2014).

[6] See Mohammed Hassouna and others, 'Customer Churn in Mobile Markets: A Comparison of Techniques' (2015) 8 International Business Research 224.

ticed to stay by offering them a special promotion or discount. Another prominent application can be found in marketing,[7] for example the advertisements and recommended products on websites such as Amazon, Netflix and Facebook. These are determined by predicting the interests of the website visitor, based on the data they collect from their clients. There are many other examples of successful applications of predictive analysis such as credit risk prediction at banks, detecting fraud, etc.[8]

In the last years, the topic has been emerging in the field of criminology as well.[9] Scholars are increasingly interested in the practical implications for situational crime prevention and control. Specifically, predictive analysis techniques can be used in crime data analysis to objectively inform policy decisions, strategies and tactical operations, by identifying and predicting previously unknown patterns and trends in crime data.[10] For example, using social network analysis to examine gang membership or using text mining to extract structured meaningful information from police reports. The objective of using these techniques, is to provide a more proactive, efficient and information-based use of police resources, in contrast to reactive crime response strategies.[11]

1.2. **Theoretical frameworks of predicting crime**

In the field of criminology, one of the most challenging applications of big data and predictive analysis is the prediction (or forecasting) of criminal events. The potential to predict crime follows from the empirical observation that crime does not happen randomly, but tends to be concentrated in time and space in so-called crime hotspots[12] or micro-places[13] (see infra). Characteristics of micro-places (the so-called opportunity structure) affects formal and informal control mechanisms in micro-places. The criminal opportunity

---

[7] Eric Siegel, *Predictive Analytics: The power to predict who will click, buy, lie, or die* (John Wiley & Sons 2013).

[8] For an overview, see Siegel (n 7).

[9] Janet Chan and Lyria Benett Moses, 'Is Big Data challenging criminology?' (2015) 20 Theoretical Criminology 21.

[10] Colleen McCue, *Data Mining and Predictive Analysis: Intelligence Gathering and Crime Analysis* (2nd edn, Elsevier Science Publishing 2015).

[11] McCue (n 10); Jerry Ratcliffe, *Intelligence-led policing* (2nd edn, Routlegde 2016).

[12] Lawrence Sherman, Patric R Gartin and Michael E Buerger, 'Hot spots of predatory crime: routine activities and the criminology of place' (1989) 27 Criminology 27.

[13] David L Weisburd, Gerben JN Bruinsma and Wim Bernasco, *Putting crime in its place: Units of analysis in spatial crime research* (Springer 2009).

structure can be identified and used to determine where ('hot-spot') and when ('burning times') there is an increased risk of crime events occurring.[14] Concentrations of crime at micro-places are considered a consequence of (1) daily routines of inhabitants and users (ie commuters, students, tourists), (2) perceived costs (perceived sanction risks, perceived risk of being caught) and benefits of committing a crime at a certain place, (3) the perceived incentives and disincentives in interaction with (4) the presence or absence of temptations and provocations, and (5) the presence or absence of capable guardians/deterrent agents, like place managers.[15]

This is documented by situational theories in criminology, specifically rational choice theory, routine activity theory and crime pattern theory. Rational choice theory[16] emphasizes the bounded rationality of the offender, who makes a cost-benefit assessment of offending, which needs to be in his favour for crime to occur. According to routine activity theory[17] a criminal event is the consequence of the physical convergence in time and space of (minimally) the following three factors: (1) a motivated offender, (2) a suitable target and (3) the absence of a capable guardian. Structural changes in routine activity patterns (daily routines) can affect this and therefore affect crime rates. Crime pattern theory[18] sees crime as a complex event that requires many different elements for it to occur. It emphasizes the dynamic nature of the decision-making processes of offenders to commit a crime at a particular time and place. To understand how the physical and social environment is related to crime opportunities, crime pattern theory has developed the concept of 'awareness space', which is formed by past and present (routine) activities (eg work, home, recreation, …) and shapes place and time of

---

[14] Paul J Brantingham, 'The theory of target search' in Francis T Cullen and Pamela Wilcox (eds), *The Oxford handbook of criminological theory* (Oxford University Press 2013); John E Eck and David L Weisburd, 'Crime places in crime theory' (2015) 4 Crime and Place: Crime Prevention Studies 1; Bryan J Kinney and others, 'Crime attractors, generators and detractors: Land use and urban crime opportunities' (2008) 34 Built Environment 62.

[15] John E Eck, 'Drug Markets and Drug Places: A Case-Control Study of the Spatial Structure of Illicit Drug Dealing' (University of Maryland 1994).

[16] Derek Cornish and Ronald Clarke, 'Understanding crime displacement: An application of rational choice theory' (1987) 25 Criminology 933.

[17] Lawrence E Cohen and Marcus Felson, 'Social change and crime rate trends: A routine activity approach' (1979) 44 American Sociological Review 588.

[18] Paul J Brantingham and Patricia L Brantingham, *Patterns in Crime* (Macmillan 1984); Patricia L Brantingham, 'Crime pattern theory' in BS Fisher and SP Lab (eds), *Encyclopedia of victimology and crime prevention* (SAGE Publications 2010).

future activities. Crime takes place where the awareness space of a motivated offender overlaps with that of an attractive target.[19]

The clustering of crime in space and time is also documented by the recurrent empirical finding of repeat and near-repeat victimization.[20] Repeat victimization is repeatedly being a target of criminal victimization, either repeatedly being a victim of the same crime type or repeatedly being a victim of multiple crime types. Near-repeat victimization is a spatial extension of repeat victimization: it suggests that the higher risk of being victimized after an initial crime extends to the people or properties in spatial proximity to the initial crime event. If for example a certain property is burglarized, then for a short time both this property and the properties in its immediate neighbourhood have a higher risk of being burglarized again. Although the phenomenon of near-repeat victimization is commonly associated with burglary, it has also been observed for other crime types. Both repeat and near-repeat victimization have been empirically validated in different contexts.[21]

Repeat and near-repeat victimization are explained by the flag and boost account theories and their interaction.[22] The flag account theory states that properties have certain characteristics which flag them as being vulnerable. For example, poor door or window security, low visibility and the absence of guardians or social control. These characteristics serve as cues to potential

---

[19] Brantingham (n 14).

[20] Graham Farrell and Ken Pease, *Once bitten, twice bitten: Repeat victimisation and its implications for crime prevention* (Police Research Group Crime Prevention Unit Series 1993); Lucia Summers, 'Virtual repeats and near repeats' in Bonnie S Fisher and Steven P Lab (eds), *Encyclopaedia of Victimology and Crime Prevention* (Sage 2010); Ken Pease and Andromachi Tseloni, *Using Modeling to Predict and Prevent Victimization* (Springer 2014).

[21] Shane D Johnson and others, 'Near Repeats: A Cross National Assessment of Residential Burglary' (2007) 23 Journal of Quantitative Criminology 201; Andromachi Tseloni and Ken Pease, 'Repeat victimization: 'Boosts' or 'flags'?' (2003) 43 British Journal of Criminology 196; Andromachi Tseloni and Ken Pease, 'Repeat personal victimisation: Random effects, event dependence and unexplained heterogeneity' (2004) 44 British Journal of Criminology 931; Michael T Townsley, Ross Homel and Janet Chaseling, 'Infectious Burglaries: A Test of the Near Repeat Hypothesis' (2003) 43 British Journal of Criminology 615.

[22] Wim Bernasco, 'Them again? Same offender involvement in repeat and near repeat burglaries' (2008) 5 European Journal of Criminology 411; Shane D Johnson, 'Repeat burglary victimisation: A tale of two theories' (2008) 4 Journal of Experimental Criminology 215.

offenders that a property seems to be an easy target. According to boost account theory, future victimization is boosted by an initial incident. After this first crime, the offender has knowledge of the property lay-out, accessibility, presence of goods which can be stolen, etc. which facilitate a new crime. The boost account theory also applies to properties situated in the neighbourhood, because the offender is familiar with the area after the first crime and neighbouring properties are more likely to be similar in lay-out, accessibility and presence of goods worth stealing compared to properties in a further away area. Offender interviews and empirical findings suggest that most burglaries are actually committed by repeat burglars committing multiple burglaries, instead of multiple burglars committing one or two burglaries.[23]

A final theoretical framework which serves as a useful tool to understand repeat and near-repeat victimization is optimal foraging theory.[24] Optimal foraging was originally developed in (evolutionary) biology to model the trade-off an animal makes between the energy value of its food and the required time and energy expenditure to obtain it. However, this key idea can be applied to crime as well. Offenders likewise return to a property or its neighbourhood in short space of time to maximise their gains from this area before moving on. This foraging behaviour is consistent with the findings of offender interviews.[25]

1.3. **Towards prospective methods for predictive policing**

The clustering of crime in time and space has since long been recognized in criminology.[26] Examining and describing these concentrations is at the core of many traditional and standard techniques used by criminologists working in the field of situational crime prevention and environmental criminology, urban geographers and crime analysts. Crime does not only vary in space, it also varies in time. The study of the spatio-temporal distribution of crime has developed later than the geographical distribution of crime. In early criminological inquiries, temporal analyses were restricted to the study of crime

---

[23] Lucia Summers, Shane D Johnson and George Rengert, 'The Use of Maps in Offender Interviewing' in Wim Bernasco (ed), *Offenders on Offending* (Willan 2010).

[24] Shane D Johnson and Kate J Bowers, 'The Stability of Space-Time Clusters of Burglary' (2004) 44 British Journal of Criminology 55; Wim Bernasco, 'Foraging strategies of homo criminalis: Lessons from behavioural ecology' (2009) 2 Crime Patterns and Analysis 5.

[25] Spencer Chainey, *JDI Briefs: Predictive mapping (predictive policing)* (UCL Jill Dando Institute of Security and Crime Science, 2012).

[26] Martin A Andresen, *Environmental Criminology: Evolution, theory and practice* (Routledge 2004).

trends over years, decades, and even historical[27] and evolutionary[28] time scales. Some scholars even argued that neighbourhoods developed criminal careers (in the metaphorical sense).[29] The temporal and spatial dimensions of crime are nowadays typically studied by time series and hotspot analysis respectively. Time series analysis involves the analysis of time series, which is a sequence of data points taken at successive equally spaced points in time, for example crime rates over a certain period of time. The objective of this method is to extract characteristics and trends of the data related to the time dimension. These data can also be modelled to predict future values based on the previously observed values (called forecasting). Time series analysis of crime data can also be used for intervention analysis, which studies how the time series changes as a consequence of an impactful event such as a change in policy. The general principle of hotspot analysis is that crime events are mapped to find high concentrations of crime during a certain time period.

Crime patterns and trends can thus be identified and described using a range of (advanced) statistical models, ranging from change score analysis to seasonal decomposition and others. However, these techniques have some downsides. For the purposes of predicting crime these conventional (regression) models are considered retrospective, in the sense that these methods are highly focused on describing patterns and trends and that predictions or forecasts based on these methods are merely past patterns extrapolated as-is to the present. Here, the inductive fallacy looms. This means that these predictions work under the premise that past patterns repeat identically in the future. In reality however, crime patterns are more dynamic, and subtle changes or shifts might go unnoticed initially.

Therefore, there has been a call for more prospective methods, shifting away from describing to modelling future patterns, ideally incorporating both the space and time dimensions, to obtain a more dynamic picture of crime trends and detect future patterns earlier.[30] Hence the emergence of prospective

---

[27] Manuel Eisner, 'Long-Term Historical Trends in Violent Crime' (2003) 30 Crime and Justice 83.

[28] Steven Pinker, *The Blank Slate: The Modern Denial of Human Nature* (Penguin Books 2002).

[29] Robert J Bursik and Harold G Grasmick, *Neighborhoods and Crime: The Dimensions of Effective Community Control* (Lexington Books 1993).

[30] Elizabeth R Groff and Nancy G La Vigne, 'Forecasting the future of predictive crime mapping' (2002) 13 Crime Prevention Studies 29; Wilpen L Gorr and Andreas M Olligschlaeger, *Crime hot spot forecasting: Modeling and comparative evaluation* (Final Project Report 2002) <https://www.ncjrs.gov/pdffiles1/nij/grants/195167.pdf>;

methods, which aim to support a more proactive approach. Groff and La Vigne provided an overview in 2002 of the, at that time prospective methods for predicting future crime concentrations. They remarked that their overview of methods was still premature, given that the more sophisticated methods for crime prediction, such as neural networks and raster GIS models, were at that time still in the development stage and still needed to be tested by the end users. A concrete example of such prospective methods, is prospective hotspot analysis, proposed by Bowers et al.[31] In prospective hotspot analysis, hotspots are formed not by the areas with the highest concentration of crime, but by the aggregation of risk zones surrounding each incident. These risk zones are temporary, making the hotspots more dynamic.

Efforts to obtain a more dynamic picture of crime have also led to the use of increasingly smaller units of analysis in the spatial analysis of crime. There are several reasons for the fact that the unit of analysis has increasingly became smaller than the neighbourhood level of analysis. First, even within neighbourhoods, a lot of variation exists: a neighbourhood may be identified as a high crime area because of the presence of one or more crime-sensitive micro-places. Second, a whole neighbourhood may be identified as a high-crime area because of the fact that scholars often have to rely on artificial boundaries. Therefore, micro-places have been proposed in criminological research in order to explain the unequal distribution of crime[32] and the micro-geographic unit of analysis (eg street segments) has been put forward as the new standard[33] in crime mapping and analysis. The use of the micro-geo-

Spencer Chainey, Lisa Tompson and Sebastian Uhlig, 'The utility of hotspot mapping for predicting spatial patterns of crime' (2008) 21 Security Journal 4; Jerry Ratcliffe, 'Crime Mapping: Spatial and Temporal Challenges' in Alex R Piquero and David L Weisburd (eds), *Handbook of Quantitative Criminology* (Springer Science 2010).

[31] Kate J Bowers, Shane D Johnson and K Pease, 'Prospective hot-spotting: The future of crime mapping?' (2004) 44 British Journal of Criminology 641; see also Kate J Bowers and Shane D Johnson, 'Domestic Burglary Repeats and Space-Time Clusters: The Dimensions of Risk' (2005) 2 European Journal of Criminology 67; Kate J Bowers and Shane D Johnson, 'Who commits near repeats? A test of the boost explanation' (2004) 5 Western Criminology Review 12.

[32] David L Weisburd, Gerben JN Bruinsma and Wim Bernasco, *Putting crime in its place: Units of analysis in spatial crime research* (Springer 2009); David L Weisburd, Elizabeth Groff and Sue Ming Yang, *The criminology of place: Street segments and our understanding of the crime problem* (Oxford University Press 2012).

[33] David L Weisburd, Elizabeth Groff and Sue Ming Yang, *The criminology of place: Street segments and our understanding of the crime problem* (Oxford University Press 2012).

graphic level is considered to be more suitable and accurate as it better reflects the existing variability at that level of both crime and socio-economic variables and provides more predictable crime patterns compared to previously used higher geographic units of analysis such as census tracts, neighbourhoods or districts.[34]

Using the micro-geographic unit of analysis has another consequence: it inevitably leads to larger amounts of data as crime and socio-economic variables need to be collected at smaller, more precise levels. In combination with the tendency to register and collect new and various additional variables, datasets for crime analysis and predictions increasingly become big datasets, in the sense that these are extensive and complex datasets, for which traditional data storage and analysis techniques are increasingly insufficient. Although this evolution offers new sources of data for crime analysis and prediction, such as additional meta-data when registering crime (eg emergency call information), text mining of social media (ie the automatic retrieval of key words), ANPR (automatic number plate recognition) data, crowd data based on Bluetooth use, etc., the data collection and analysing processes are also becoming more complex.

The interest of criminology in predictive analysis as applied in other fields should be situated within the need for methods which can handle and extract insights from these big datasets, the earlier discussed shift to more proactive methods and the strive to continuously improve predictions of criminal events. Being able to improve predictions of criminal events could have important strategic and tactical value for law enforcement agencies. It would allow especially police forces to proactively allocate resources with the goal to increase the efficiency of patrols and interventions. It is assumed that the insights crime predictions provide, could also better inform situational preventative measures and increase their efficiency as well, for example by anticipating the emergence of crime events, the emergence of new areal concentrations and spatio-temporal displacement. This has led to the development of predictive policing.[35]

Predictive policing can be defined as: "the use of historical data to create a spatiotemporal forecast of areas of criminality or crime hot spots that will be the basis for police resource allocation decisions with the expectation that

---

[34] David L Weisburd, Elizabeth Groff and Sue Ming Yang, *The criminology of place: Street segments and our understanding of the crime problem* (Oxford University Press 2012).

[35] "Predictive policing" as a term is first mentioned in publications in 2009, starting with Beck & McCue, 2009.

having officers at the proposed place and time will deter or detect criminal activity."[36] Predictive policing can also be defined more broadly, as in Perry et al. (2013) who distinguish three main objectives of predictive analysis in criminological applications: (1) predicting perpetrators, (2) predicting victims, and (3) predicting when and where there is a higher risk of new crime events.[37] The latter definition will be used further throughout this study.

Predictive policing is characterised by its use of relatively new and advanced methods (see infra). However, these methods are largely unproven and there is the danger that these methods are considered better than the traditional methods just because they are new and innovative. Additionally, there is the danger of relying too much on new technology, without taking into account its inherent limits and constraints.[38] Some authors maintain that more traditional or 'classic' methods are equally capable to provide reliable crime predictions within the framework of predictive policing.[39] This is important, as these classic methods are generally less complex, require less advanced knowledge of statistics or GIS and expertise related to these methods is generally already present in law enforcement. Therefore, we need to gain more insight into the potential merits or flaws of predictive policing methods.

1.4. Objective and research questions

The main objective of this review is to identify and provide an overview of the current methods in the scientific literature for making spatiotemporal predictions of crime, and to describe and compare their main characteristics, focusing on applicable crime types, input variables, unit of analysis and effectiveness assessment (both predictive ability and effectiveness for situational crime control and prevention). To address this, we will make use of the following primary and secondary research questions:

---

[36] Jerry Ratcliffe, 'What is the future of... predictive policing?' (2014) 6 Translational Criminology 4.

[37] Walter L Perry and others, *Predictive Policing: The Role of Crime Forecasting in Law Enforcement Operations* (RAND Research Reports 2013).

[38] Lyria Bennett Moses and Janet Chan, 'Algorithmic prediction in policing: Assumptions, evaluation and accountability' (2016) Policing and Society 1.

[39] Spencer Chainey, Lisa Tompson and Sebastian Uhlig, 'The utility of hotspot mapping for predicting spatial patterns of crime' (2008) 21 Security Journal 4; Miguel Camacho-Collados and Federico Liberatore, 'A Decision Support System for predictive police patrolling' (2015) 75 Decision Support Systems 25.

I. How have predictive policing methods been approached and handled in the scientific literature over the last decade?
   i. What are the main (groups of) predictive policing methods which have been introduced in the last decade to predict criminal events?
   ii. Has the frequency of scientific predictive policing studies increased over the last decade (ie has predictive policing become more prominent in scientific literature)?
   iii. Which types of studies have addressed predictive policing?

II. What are the main methodological properties and parameters used in empirical studies of predictive policing methods?
   i. In which contexts (locations) did the empirical studies take place?
   ii. To which predictive method group do the used techniques belong?
   iii. For which types of crimes are the predictions made?
   iv. Which input variables are used?
   v. Which units of analysis are used?
   vi. How is predictive ability measured?

III. What is currently known about the effectiveness of predictive policing methods for crime control and prevention?

Predictive policing is a new development in criminology, which has gained in prominence in the last years. Applications of predictive policing are currently being used by law enforcement in the US, the UK, the Netherlands, Germany, and Switzerland.[40] Other countries, especially in Europe, such as Austria, are currently exploring the possibility of implementing predictive policing. Several companies, for example IBM,[41] Hitachi and Microsoft,[42] are also providing predictive analysis software packages aimed specifically at law enforce-

[40] Wim Hardyns and Anneleen Rummens, 'Predictive policing as a new tool for law enforcement? Recent developments and challenges' (2017) European Journal of Criminal Policy and Research (forthcoming).

[41] IBM, *Predictive analysis for crime prediction and prevention: Helping police departments known better* <https://www-01.ibm.com/software/analytics/spss/11/na/cpp/>.

[42] Hitachi, *Hitachi Data Systems unveils new advancements in predictive policing to suppport safer, smarter societies* (2015) <https://www.hitachivantara.com/en-us/news-resources/press-releases/2015/gl150928.html>; Daniel Rivero, '*Microsoft is developing an app that can predict crimes of the future' Fusion* (2015).

ment. However, at this time, there are few scientific overview or review studies on the topic.[43] There is therefore a need to gain more insight in the current knowledge of predictive policing and identify possible gaps for further research. Before discussing the review methodology and results, the following section gives an overview of the main predictive policing methods which will be the focus of this review.

2. PREDICTIVE POLICING METHODS

Predictive policing is a term which can denote multiple methods. They share the common objective to "forecast where and when the next crime or series of crimes will take place".[44]

Although predictive policing builds on a long tradition of (predictive) crime mapping and prediction (see supra), its innovation lies in (i) the use of big data (ii) the use of the micro-geographic level and (iii) the use of advanced statistical modelling and GIS methods. We distinguish three main method groups which conform to these three criteria and which claim to improve crime predictions compared to previous traditional methods such as hotspot analysis and time series modelling. They can be distinguished based on their underlying working principle: (1) near-repeat methods, (2) supervised machine learning methods and (3) risk terrain modelling.

Near-repeat methods are based on the empirical phenomenon of near-repeat victimization (see supra): once a crime has taken place, there is an increased risk of a new crime occurring within a certain geographical and time window.[45] This process is then modelled to predict the risk of new crimes occurring. A leading example is self-exciting point process modelling,[46] which was originally used to predict aftershocks of earthquakes. It works as follows: based on the historical crime data, the current rate at which new crimes appear (the background rate) is estimated. This background rate acts as a basic

[43] Groff and La Vigne (n 30); Perry and others (n 37); Jennifer Bachner, *Predictive Policing: Preventing Crime with Data and Analytics* (Improving Performance Series 2013); Moses and Chan (n 38).

[44] Marco C Uchida, '*Linking theory to practice: testing geospatial predictive policing in a medium-sized police agency – A proposal submitted to the National Institute of Justice*' (Unpublished document 2013).

[45] Perry and others (n 37).

[46] George O Mohler and others, 'Self-exciting point process modeling of crime' (2012) 106 Journal of the American Statistical Association 100.

risk rate which depends on environmental characteristics acting as predictors of crime, supplemented with temporal effects (for example, a temporary increase during winter months). If a crime happens, the risk for new criminal events will temporarily increase in a pre-determined radius (eg 500m) and for a pre-determined time (eg three weeks). This higher risk decays the longer no new crime happens, until it falls back to the background rate.

Supervised machine learning methods[47] learn from patterns in historical data (training data) and are aimed at prediction of unknown or future values of the variable we are trying to predict. This is in contrast to unsupervised learning (or data mining), which is more concerned with identifying patterns in the data and describing them. Machine learning models are characterized by a higher predictive power and offer an improved prediction performance when handling complex data relative to traditional regression methods. The methods in this group often approach predicting crime as a classification problem, ie they learn from the training data how to separate high crime risk micro-places from low risk micro-places. The lead example in this group is neural network modelling.[48] A neural network learns to recognize and adapt to patterns in the data based on (a simplification of) the way neurons in the human brain work. Neural networks are mainly effective for complex classification problems, but this is in itself also a complex method. It is seen as a black box method: the network structure does not give insight into the actual relationship between the inputs and the outputs. This means, practically, that neural networks have no explaining value, only a predictive value. Another prominent example is ensemble modelling, which is the synthesizing of several models, for example the combination of logistic regression with a neural network, to obtain better results than the constituent models separately. Additionally, using different classes of models enables their different strengths to be utilized.[49]

Risk terrain modelling (RTM)[50] uses a geographic information system (GIS), to create a risk map of locations sensitive to high crime rates, based on their spatial characteristics and the interactions of those characteristics. It operates under the assumption that there are no standard crime patterns which

---

[47] For more information, see Robert Tibshirani, Daniela Witten and Trevor Hastie, *An Introductio to Statistical learning with Applications in R* (Springer 2013).

[48] Simon Haykin, *Neural networks and learning machines* (3rd edn, Pearson 2009).

[49] Zhi-Hua Zhou, *Ensemble methods: Foundations and algorithms* (CRC Press 2012).

[50] Joel M Caplan and Leslie W Kennedy, *Risk Terrain Modeling Manual: Theoretical Framework and Technical Steps of Spatioal Risk Assessment for Crime Analsyis* (Rutgers 2010).

are valid across settings, but that each context has a unique spatial dynamic of environmental features which attract crime. RTM identifies the risks that come from these features and model how they co-locate to create unique behaviour settings for crime, to compute a probability of criminal behaviour occurring (ie where it is statistically most likely to occur). This composite model of spatial vulnerabilities to crime is created at the micro-geographic level.

Each group of methods comes with its own advantages and disadvantages for predicting criminal events. Table 1 gives an overview of the main advantages and disadvantages for each of the three groups of methods.

Method group	**Advantages**	**Disadvantages**
Near-repeat methods	- Only crime data needed - Predicts place and time - Relatively simple	- Doesn't make use of a wide range of crime indicators - Only suitable for predicting
Supervised machine learning methods	- Makes use of a wide range of data - Predicts place and time - Versatile	- Complex, requires advanced statistical expertise - Only suitable for predicting
Risk terrain modeling	- Makes use of a wide range of data - Relatively simple - Can also be used as a diagnostic tool	- Only predicts place, not time

Table 1: Advantages and disadvantages of the different methods

Near-repeats methods only make use of crime data. There are some advantages to this approach. In the first place, the data collection process is simplified, as only a limited number of variables are needed, which can likely be collected from one source (police registered crime data). In comparison, using a wider range of variables requires a larger amount of data to be collected from various sources (police registered crime data, census data, …) and likely a longer data cleaning and aggregating process to acquire a uniform dataset. Another advantage, which is mentioned by some authors[51] and in the promotion of software using near-repeat methods (eg PredPol), is minimizing profiling bias, which can be associated with using perpetrator data and socio-economic data such as ethnicity. However, this is also their main disadvantage: they only focus on this near-repeat phenomenon and are not flexible

[51] Jerry Ratcliffe and George Rengert, 'Near-Repeat Patterns in Philadelphia Shootings' (2009) 21 Security Journal 58; George O Mohler and others, 'Randomized controlled field trials of predictive policing' (2016) Journal of the American Statistical Association 1399.

enough to incorporate other information as well. Not making use of additional data which are known to be predictors of crime, might hamper the predictive effectiveness. Additionally, because of the use of one specific source, bias associated with the registration process of crime data might be exacerbated.

Supervised machine learning predicts both time and place and uses a wide range of data. Compared to the other methods, its main advantage is its versatility: the methods in this group can handle a variety of methodological parameters. Most notably, only this group of methods is able to predict at the individual level (victim or perpetrator), as the other two groups are specified towards predicting location. The main disadvantage of this group of methods is that the underlying methods are very complex. They require knowledge of advanced statistical methods and might as a consequence be harder and costlier to apply in practice, as additional expertise is needed. Near-repeat methods and risk terrain modelling are comparatively simpler and more intuitive methods. Additionally, as most methods in this group are so-called 'black box' methods, they can only be used for predicting, not to explain the high risk of criminal events.

Risk terrain modelling can and does generally make use of a wide range of data: not only crime variables are included, but also socio-economic and environmental variables. It is also a relatively simple method to apply, provided the user has knowledge of GIS. In contrast to near-repeat and supervised machine learning methods, RTM can also be used as a diagnostic tool to explain why crime clusters over time at a certain place, specifically which environmental features serve as crime attractors and generators. This allows to prioritize certain risk factors and take more specific situational preventative measures, eg if convenience stores are highly related to a high risk of new criminal events, police patrols can be instructed to focus on checking convenience stores. However, in contrast to machine learning and near-repeat methods, risk terrain modelling focuses solely on a location-based prediction and is less suited to predict the risk of new criminal events for specific time windows.

3. REVIEW METHODOLOGY

A literature review allows to take stock of what has gone before, place individual studies in the context of how it contributes to an understanding of the subject under review as a whole, assess the available evidence on a subject and shed light on gaps in the current literature for further research.[52] Currently, it is good practice to use a systematic approach when conducting a literature review. This requires an explicit, methodical and transparent approach during the different phases of the review process: searching the literature, selecting relevant studies, synthesizing and reporting the results. This is meant to minimize bias and maximize clarity and reproducibility.[53]

Several types of systematic approach reviews exist, from the golden standard systematic review to a rapid review, which assess what is already known about a policy or practice issue in a limited time frame.[54] The most suited review type is dependent on the main objectives of the review, its audience, time constraints and the available resources. To address the main objective of this review and answer its related research questions, a scoping review is conducted, following the framework set out by.[55] The main aim of a scoping review is to map existing literature in a specific area, identifying the extent and nature of research evidence and assessing the quantity and quality of the available literature.[56] Compared to a systematic review, its focus lies more explicitly on the description of the main characteristics of the literature and the identification of key points and potential gaps. Unlike a systematic review, all study designs can be included and its focus lies on breadth of coverage, which makes it especially useful to map a research area.[57]

The search for studies is performed using a range of keywords related to among others predictive policing, near-repeat methods, supervised machine learning methods and risk terrain modelling in the Web of Science, Open Grey

---

[52] Andrew Booth, Diana Papaioannou and Anthea Sutton, *Systematic approaches to a succesful literature review* (SAGE Publications 2012).

[53] ibid.

[54] Maria J Grant and Andrew Booth, 'A typology of reviews: An analysis of 14 review types and associated methologies' (2009) 26 Health Information & Libraries Journal 91.

[55] Hilary Arksey and Lisa O'Malley, 'Scoping studies: Towards a methodological framework' (2005) 8 International Journal of Social Research Methodology 19.

[56] Booth and others (n 52).

[57] Arksey and O'Malley (n 55).

and Google Scholar databases (see appendix I for the review protocol). In addition to the database search, studies will also be searched and identified through hand searching of reference lists. As the focus of this review lies on predictive policing methods (see supra), the studies included in this review are selected according to the following eligibility criteria:

- published 2007 – 2017
- aimed at predicting near-future criminal events (place, time, victim or perpetrator)
- use of near-repeat, supervised machine learning methods or risk terrain modelling methods
- use of micro-geographical or individual level of analysis

To collate and summarize the available literature, a three-step approach is used. Initially, all studies conforming to these four criteria are selected and their main characteristics (publication year, main themes, study type) analyzed (cfr. research question I). In a second step, the empirical studies are selected from this group and analyzed more in-depth (cfr. research question II), focusing on applicable crime types, input variables, unit of analysis and predictive ability assessment. Finally, we discuss further the current knowledge on the effectiveness of predictive policing for crime control and prevention (cfr. research question III).

4. REVIEW RESULTS

The review research process resulted in 1244 hits (see Appendix II for the review flow diagram). To put this into perspective, searching for predictive analysis in conjunction with marketing resulted in almost ten times as many hits (10235). Based on the studies' records (title, authors and journal) 246 studies were initially selected. Additionally, 35 records were identified by hand searching reference lists. From those 281 studies, 83 relevant studies were selected based on their abstract and 65 (21 empirical and 44 non-empirical studies were selected in total for final inclusion (see Appendix III for an overview of the selected studies with their main characteristics).

4.1. Predictive policing as a topic in scientific literature

Before going into further detail regarding the empirical studies, it is interesting to take a closer look at how the topic of predictive policing has been approached in the scientific literature. Looking at the publication dates of these studies (see figure 1), it is evident that there is a recent increase in the number of studies, reflecting the current academic interest in predictive policing.

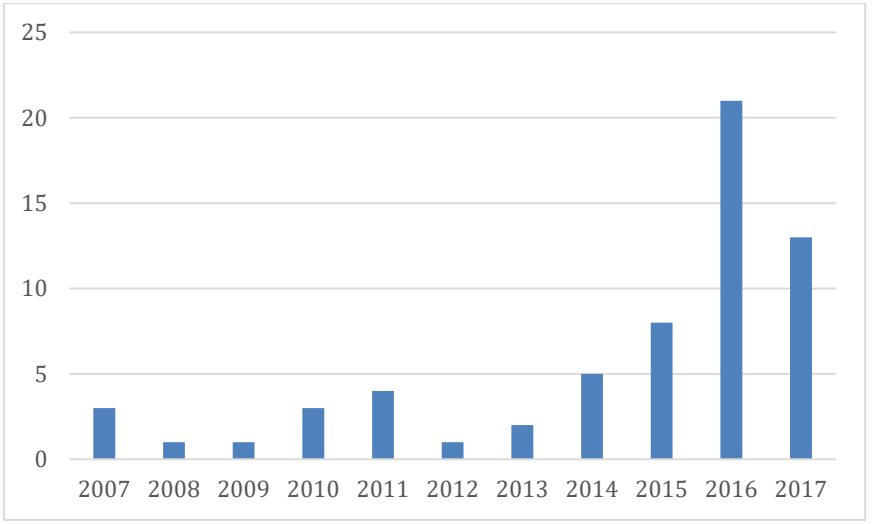


Figure 1: Number of predictive policing studies per year (N=65)

Within this body of literature, three main groups of publications (types of research) can be distinguished: empirical studies (N=21), overview and conceptual studies (N=11) and studies addressing ethical, juridical and other considerations in the application of predictive policing (N=33). However, especially in the empirical studies group many studies are isolated and lack inter-citation. This mirrors the concern of Groff and La Vigne in 2002 that "individual researchers and analysts will continue to experiment with their own methods – possibly reinventing the wheel – rather than learning from each other".[58] Additionally, a large part of the predictive policing literature, among which the two main overview works of predictive policing,[59] appeared as grey literature reports, ie outside peer-reviewed academic channels and outside the scope of primary academic databases such as Web of Science.

4.2. **Empirical studies of predictive policing methods**

In the previous section, we discussed the predictive policing literature as a whole. In this section, we focus on the available empirical studies of predictive policing methods, which are the main focus of this review. In total, 21 empirical studies were identified.

[58] Groff and La Vigne (n 30).

[59] Jennifer Bachner, *Predictive Policing: Preventing Crime with Data and Analytics* (Improving Performance Series 2013); Perry and others (n 37).

4.2.1. Study locations

From the previous section we know that scientific interest in predictive policing methods has increased steadily in the last years. In the body of empirical studies, when looking at the locations of the studies (see table 2), we see that the majority of studies (18 out of 21) are geographically clustered in the US, with only three studies taking place elsewhere.

Study location	**Number of studies**
United States	18
Canada	1
Belgium	1
South-Africa	1

Table 2: Study locations (N=21)

This can be explained by the US having a longer tradition in the use of advanced quantitative methods for analyzing and predicting crime. Consequently, not much empirical evidence exists on the application of predictive policing methods in other parts of the world (eg Europe). However, in practice several applications of predictive policing have already made their way to (Western-)Europe.[60]

4.2.2. Study method groups

As mentioned before, three main methods groups can be distinguished: near-repeat methods, machine learning and risk terrain modelling. Table 3 gives an overview of the number of studies for each method group.

Method group	**Number of studies**
Machine learning	13
Near-repeat modelling	4
Risk terrain modelling	4

Table 3: Study methods (N=21)

When looking at the empirical studies selected for this review, the total number of studies is divided among these three types as follows: four studies apply risk terrain modeling, four studies employ near-repeat methods, and 13 studies make use of machine learning. When looking at the practical applica-

[60] Wim Hardyns and Anneleen Rummens, 'Predictive policing as a new tool for law enforcement? Recent developments and challenges' (2017) European Journal of Criminal Policy and Research (forthcoming).

tions used by law enforcement, we see that near-repeat methods and machine learning are most popular.[61] Risk terrain modelling has only recently been adopted by law enforcement, for example in Atlantic City (US).[62]

4.2.3. Crime types

Table 4 gives an overview of the different crime types to which predictive policing methods are applied in the studies under review.

Crime type	**Number of studies**
Violent crimes	6
Domestic burglary	5
Property crimes	3
Gun violence	3
Bank robbery	1
Homicide	1
Child maltreatment	1
Sexual violence	1

Table 4: Crime types (N=21)

The majority of studies focus on high-volume and high-impact (street) crimes such as violent crimes and domestic burglary. The high-volume characteristic of these types of crimes ensures an adequate amount of data is available to enable useable predictions. As these types of crimes tend to have a high impact on the well-being of the victims, these crime types are often prioritized by law enforcement,[63] driving the need to employ predictive methods that are seen as innovative and (seemingly) better than traditional methods.

4.2.4. Input variables

The amount and type of variables used depends on the method used. Near-repeat methods only make use of crime data and are generally limited to collecting data on time, place and crime type of previous crime events. Machine learning and risk terrain modelling on the other hand, make use of a larger amount (from tens to even hundreds different variables) and wider range of

[61] Wim Hardyns and Anneleen Rummens, 'Predictive policing as a new tool for law enforcement? Recent developments and challenges' (2017) European Journal of Criminal Policy and Research (forthcoming).

[62] Ssmantha Melamed, 'Can Atlantic City's bold experiment take racial bias out of predictive policing?' (The Philadelphia Inquirer 2017).

[63] Moses and Chan (n 38).

data: in addition to crime data, they included socio-economic and environmental data. One study also made use of social media data.[64] Wang et al. improved a previous model[65] by including keywords of a news agency feed determined by text mining (a method for automatic retrieval of keywords in a text). The opportunities offered by the introduction of big data within criminology to use newly available data such as crowd data, ANPR data, etc. have thus currently not been used yet to their fullest extent in empirical studies of predictive policing.

4.2.5. Unit of analysis

Table 5 gives an overview of the different units of analysis found in the studies under review.

Unit of analysis	**Number of studies**
Grid	16
Individual level	5
Street segment	0

Table 5: Unit of analysis (N=21)

Five studies use the individual level to make predictions. Two of them predicted potential victims, while two predicted potential perpetrators. The remaining study[66] predicted 'persons of interest' related to gun violence, ie people at a high risk of becoming either a victim or a perpetrator of gun violence. The majority of studies (16) make use of a grid to aggregate data. Nine of these studies use a grid cell size between 100 and 200 m^2, 5 studies use a smaller size and two studies a larger size. As discussed earlier, the street segment has recently been introduced as a new type of micro-geographical unit of analysis. Some authors consider the street segment also an improvement over grid-based analysis,[67] as it better captures the variability of crime at the

[64] Xiaofeng Wang, Donald E Brown and Matthew S Gerber, 'Spatio-temporal modeling of criminal incidents using geographic, demographic and Twitter-derived information' (IEEE International Conference on Intelligence and Security Informatics 2012).

[65] Xiaofeng Wang and Donald E Brown, 'Spatio-temporal modeling for criminal incidents' (2012) 1 Security Informatics 1.

[66] Jessica Saunders, Priscilla Hunt and John S Hollywood, 'Predictions put into practice: a quasi-experimental evaluation of Chicago's predictive policing pilot' (2016) 12 Journal of Experimental Criminology 347.

[67] Gabriel Rosser and others, 'Predictive Crime Mapping: Arbitrary Grids or Street Networks?' (2017) 33 Journal of Quantitative Criminology 569; John R Hipp JR and Young

micro-level and can thus provide a better predictive accuracy. However, none of the studies under review employ the street segment as the level of analysis. Empirical studies using the street segment as the unit of analysis do exist, but generally their objective is to retest Weisburd's law of crime concentration[68] or to study the existence of meaningful micro-geographical variation in crime.

4.2.6. Predictive ability assessment

When evaluating predictive policing methods, an assessment of predictive ability is important to consider. Predictive ability can consist of only accuracy (ie the proportion correctly predicted events), but is generally supplement with other measures such as precision (ie does the model minimize incorrectly predicted events?) and interpretability (ie the understanding and insight provided by the model). These results gain in meaning if compared to other methods, such as the traditional methods (so we can tell whether the new methods are better than the old ones) or other predictive policing methods (so we know which method is most suitable for a specific context).

Predictive ability assessment	**Number of studies**
Only predictive ability	13
Comparison with traditional methods (hotspot analysis and time series modelling)	7
Comparison with predictive policing methods from the same method group	1
Comparison with predictive policing methods from another method group	0

Table 6: Predictive ability assessment (N=21)

The majority of studies (13 studies, see table 6) focus on predictive ability only when evaluating the predictive method under consideration. Seven of the empirical studies made a comparison between the newly proposed predictive policing method and traditional methods such as hotspot analysis and time series modelling. As mentioned before, predictive policing consists of

An Kim, 'Measuring Crime Concentration Across Cities of Varying Sizes: Complications Based on the Spatial and Temporal Scale Employed' (2017) 33 Journal of Quantitative Criminology 595.

[68] David L Weisburd, 'The Law of Crime Concentration and the Criminology of Place' (2015) 53 Criminology 133.

multiple methods and therefore it would be interesting to compare the different methods with each other. However, at this time only one study[69] compares different predictive policing methods within the same method group (neural network and ensemble modelling from the supervised machine learning group). Comparisons between different method groups are at this time non-existent.

Three studies also focused on the implementation of predictive policing in the police departments where it was tested, by conducting field trials.[70] These are the only scientifically published experimental studies at this time: In the following section, these studies are discussed further in-depth.

4.3. Effectiveness of predictive policing for situational crime control and prevention

Predictive analysis has proven its usefulness in other areas, but because it is a rather new development within criminology. There is limited empirical evidence regarding its effectiveness for policing. Perry et al. conducted interviews with police practitioners and found that very few evaluations of the effectiveness of the predictions or the interventions that followed the predictions have been conducted.[71] Some internal evaluations have been conducted, but these are either in the context of promoting predictive policing software or their results are inconclusive at best.[72]

Although there are multiple empirical studies showing that predictive policing can predict crime accurately, experimental studies showing that predictive policing is also effective for crime control and prevention, are rare. At this time, only three experimental studies have been published: the Shreveport Police

---

[69] Anneleen Rummens, Wim Hardyns and Lieven Pauwels, 'The use of machine learning in spatiotemporal crime forecasting: Building and testing a model in an urban context' (2017) Applied Geography.

[70] George O Mohler and others, 'Randomized controlled field trials of predictive policing' (2016) Journal of the American Statistical Association 1399; Jessica Saunders, Priscilla Hunt and John S Hollywood, 'Predictions put into practice: a quasi-experimental evaluation of Chicago's predictive policing pilot' (2016) 12 Journal of Experimental Criminology 347; Priscillia Hunt, Jessica Saunders and John S Hollywood, *Evaluation of the Shreveport Predictive Policing Experiment* (Rand, 2014).

[71] Walter Perry and others, *Predictive Policing: The Role of Crime Forecasting in Law Enforcement Operations* (RAND Research Reports 2013).

[72] Bas Mali Carla Bronkhorst-Giesen and Mariëlle den Hengst, *Predictive policing: lessen voor de toekomst. Een evaluatie van de landelijke pilot* (2016).

predictive policing experiment, the Los Angeles predictive policing experiment and the Chicago predictive policing pilot.[73] Mohler et al. (2016) and Hunt et al. (2014) apply a randomized controlled trial, while Saunders et al. (2016) is a quasi-experimental study, making use of a control group, but without random assignment. See table 7 for an overview of the main characteristics of these studies.

Experimental study	Location	Study type	Method group	Results
Hunt et al., 2014	Shreveport (US)	Randomised controlled	Supervised machine learning	Inconclusive, only increased cost-effectiveness
Mohler et al., 2016	Los Angeles (US)	Randomised controlled	Near-repeat method	Effective, 7,4% crime reduction in function of patrol time
Saunders et al., 2016	Chicago (US)	Quasi-experimental (control group, but no random assignment)	Supervised machine learning	Inconclusive, not successful to predict victimization, but could predict arrest

Table 7: Characteristics of the existing empirical studies (N=3)

The results of the Shreveport Police predictive policing experiment, one of the first field experiments of predictive policing, show that not all predictive policing applications are successful, especially when there is no attention for implementation issues. Shreveport Police (Louisiana, US) set up a randomised field experiment in 2012), evaluating the implementation of predictive policing against the current standard analysis based on intelligence-led policing.[74] Although the costs of predictive policing were 6 to 10% lower than the standard analysis, no significant decrease in crime rate was established. The results thus indicated that the use of predictive policing was no better than the current standard practice except from a cost-effectiveness point of view. The authors did report some problems which could have affected the results: (1) the low statistical power of the test (statistical power was only 20% while 80% is the general standard), meaning the test was unable to detect a difference in

[73] Priscillia Hunt, Jessica Saunders and John S Hollywood, *Evaluation of the Shreveport Predictive Policing Experiment* (Rand, 2014); George O Mohler and others, 'Randomized controlled field trials of predictive policing' (2016) Journal of the American Statistical Association 1399; Jessica Saunders, Priscilla Hunt and John S Hollywood, 'Predictions put into practice: a quasi-experimental evaluation of Chicago's predictive policing pilot' (2016) 12 Journal of Experimental Criminology 347.

[74] Priscillia Hunt, Jessica Saunders and John S Hollywood, *Evaluation of the Shreveport Predictive Policing Experiment* (Rand, 2014).

crime rates or it was caused by inadequate operational implementation by the police department; and (2) the actual amount of resources used turned out to decrease near the end of the test and varied significantly depending on the neighbourhood.[75] The problems of the Shreveport Police experiment demonstrate that there are some practical hurdles that need to be overcome for predictive policing to be implemented effectively. If police departments cannot effectively use predictive policing in practice, it ultimately does not matter how well its crime predictions are. A key lesson to be learned is to clearly communicate to and involve police officers in the data collection process and evaluation of predictive policing and to allow them to implement their intuition and knowledge in making use of the resulting crime predictions. Otherwise, police might refuse the use of predictive policing as they consider its predictions to be not grounded in reality or superfluous.[76]

Mohler et al. (2016) conducted a randomised controlled experiment in Los Angeles (US), testing the effectiveness of a self-exciting point process model, which capitalizes on the near-repeat phenomenon to make crime predictions (see supra). In Los Angeles, predictive accuracy was tested by creating crime risk maps each day from May 2012 to January 2013 using self-exciting point process models and hot-spot analysis and comparing their predictive accuracy head to head. Additionally, a single-blind field trial was conducted in three Los Angeles Police Department divisions (Foothill, Hollywood and Southwest) in six-month periods between November 2011 and January 2013. Self-exciting point process model predictions or hot-spot predictions were randomly assigned according to day, each day officers received either self-exciting point process model predictions or hot-spot predictions without them knowing which type of predictions they were using. The results showed that self-exciting point process models were able to predict 1,4 to 2,2 more crime on average in Los Angeles than the crime analysis using hot-spot maps. On average, the use of self-exciting point process model predictions by police patrols in Los Angeles led to a 7,4% reduction in crime volume as a function of patrol time, whereas the control group (hot spot predictions) showed less than half of the treatment effect at a non-significant statistical level.[77]

---

[75] Priscillia Hunt, Jessica Saunders and John S Hollywood, *Evaluation of the Shreveport Predictive Policing Experiment* (Rand, 2014) 49, 50.

[76] Alene Tchekmedyian, 'Police push back agains using crime-prediction technology to deploy officers' (*Los Angeles Times* 2016).

[77] George O Mohler and others, 'Randomized controlled field trials of predictive policing' (2016) Journal of the American Statistical Association 1399, 1400.

In Chicago, a predictive policing pilot study was conducted in 2012, designed to reduce gun violence.[78] The program estimated which people were at a high risk of becoming either a victim or a perpetrator of gun violence, which were put on a Strategic Subject List (SSL). Social network modelling using first-degree and second-degree co-arrest links was used. A first-degree link refers to a subject previously co-arrested with a later homicide victim. The second-degree link refers to a subject co-arrested with an intermediary person who was co-arrested with a later homicide victim. The number of co-arrests was counted for a period of five years and weighted for recency. A quadratic model was fitted to these data, such that the probability of being at risk for gun violence increased at an increasing rate with respect to the count of links. These people were then referred to local police commanders for tailored preventative intervention. The results showed that subjects on the SSL were not more or less likely to become a victim of gun violence compared to the control group. However, they were more likely to be arrested for a shooting. The authors suggest that increased chance of being arrested for a shooting if being on the list, was actually a consequence of some officers using the list to close shooting cases. One of their main recommendations is that law enforcement should be better informed about what to do with the predictions. In the pilot, district commanders and police officers in the field received almost no guidance and district commanders might have been too cautious about intervening, generally recommending their officers only to increase contact with individuals on the list, without evidence that increasing contact is a relevant strategy to reduce violence.[79] As was the case with the Shreveport Predictive policing experiment, this study shows that implementation issues cannot be ignored if predictive policing predictions are to be used successfully for crime control and prevention.

5. DISCUSSION & CONCLUSIONS

Predictive policing is a relatively new development. It is, especially in practical applications, seen as an innovative and promising methodology to predict crime. Despite the increasing use and its promotion, predictive policing also faces many criticisms that need to be addressed appropriately: a major problem remains the restricted validity of some official crime data (eg it is known from victim surveys that clearance rates are low). Therefore, some skepticism is understandable. Its merits have been largely untested - especially with respect to its implementation in police departments - and there are privacy (sensitive information due to geo-coding at very low levels of aggregation),

[78] Saunders, Hunt and Hollywood (n 66).

[79] Saunders, Hunt and Hollywood (n 66) 367.

security (how should access to this sensitive information be managed?) and bias issues (data quality - validity) regarding the (big) data collection process. This raises questions such as: what data can be collected? Who can collect these data for which purposes? How should the data be stored? Who should have access? The answers to these questions should ideally maximize the privacy and security of those involved. In reality, a balance needs to be found between the privacy needs of individual citizens and the obligation of the government to provide the best possible security for all citizens. Additionally, some of the applications are managed by private companies, which complicates this process by adding another actor with its own interests (ie making a profit).

Questions also arise regarding how law enforcement should make use of the predictions and how they should account for decisions based on these predictions.[80] This relates to basic principles such as probable cause and the presumption of innocence. For example, it can be argued whether the fact that someone is present in a risk area constitutes probable cause. This particular concern is even more pressing in the case of the specific application of predicting perpetrators, which is in itself considered problematic, because of the inherent danger of breaching the presumption of innocence. For example, the question arises whether a prediction is sufficient for police officers to take action and whether this might lead to a higher risk of ethnic profiling and the neglect of basic principles such as the presumption of innocence.[81] This is also connected to data quality: if the model makes use of biased data to make predictions, these predictions will also be biased. One of the most important sources of bias is in the registration of crime data: not all crimes are reported and not all crimes are reported correctly. To successfully apply predictive analysis, these challenges need to be addressed.

Although the number of practical applications of predictive policing keeps increasing, many crucial methodological questions remain unanswered by academic studies. In particular, the effect of main methodological and statistical choices such as grid resolution, temporal resolution and the length of the historical time frame on predictive accuracy need further in-depth inquiry. There is, at this time, virtually no empirical evidence available of the impact of varying the methodological parameters and the impact of common data problems (such as missing data).

---

[80] Lyria Bennett Moses and Janet Chan, 'Algorithmic prediction in policing: Assumptions, evaluation and accountability' (2016) Policing and Society.

[81] Andrew G Ferguson, 'Predictive Policing and Reasonable Suspicion' (2012) 62 Emory Law Journal 259.

Predictions of a high risk of a new criminal event occurring can be made at the level of the victim, perpetrator or time and/or location. Each approach has its own advantages and disadvantages. Predicting at the individual level might seem straightforward, but has ethical and juridical issues: predicting at the individual level also means that potentially sensitive and private data need to be collected and analyzed (and therefore accessed) falsely considering an individual a high-risk perpetrator is a costly mistake. Therefore, predicting time and/or location of new crime events is more common. However, predicting time and/or location at a low aggregated level cannot fully circumvent some of the ethical and juridical issues, it would also be false to claim that predicting time and/or location of new crime events and an aggregated level is completely without such issues. These predictions are still heavily dependent on the quality of the historical data, the precision level at which data is registered is an important factor to consider in this respect: it would not be possible to predict at a more precise level than the level at which it is registered. If a grid is used, a suitable grid resolution needs to be determined. The determination of grid resolution is usually a trade-off between the required precision of the predictions, the data limits and the needs and limits of police officers in the field. It is however an important methodological parameter with a potentially high, but as of yet unknown, impact on the prediction results. it also introduces other issues: the balance between predictive accuracy and practical use in the field, the so-called Modifiable Areal Unit Problem (MAUP). When determining grid cell size some considerations need to be balanced against each other. The cells need to be small enough to allow efficient deployment of police patrols, but large enough such that the precision of the predictions does not suffer because of it. As is the case with grid resolution, the determination of temporal resolution is also a consideration between the required precision of the predictions, the data limits and the needs of police officers in the field. It is however likewise an important methodological parameter having an impact on the prediction results. This can vary depending on crime type, for example home burglaries tend to have a less precise time range, while the registration of robberies is not always associated with a precise location.

The best suited unit of analysis might also depend on the context: whereas in a city with a regular street grid the street segment might be the better option, but for a city with an irregular street grid or in any other context with longer streets a grid might be more suitable. When looking at the existing empirical studies of predictive policing methods, it seems that the majority of empirical studies takes place in the US and in the context of a metropolis. The latter is likely a consequence of the larger amount of data available and possibly also because it is easier to acquire the necessary data. The problem of too few his-

torical data might be solved by aggregating at a larger unit of analysis, although the resulting loss of precision might mean the predictive methods lose one of their biggest advantages, namely the ability to predict crime in a small geographical area and within a short time frame. Near-repeat methods might have an advantage here as they are less dependent on a wide range and large amount of data. However, this assertion has not been formally tested yet.

Near-repeat methods, machine learning and risk terrain modelling methods for predictive policing have gained in importance, as can be evidenced by the increasing number of publications discussing these methods in the last few years. Although the existing empirical studies indicate that these methods have a good predictive ability, three crucial questions remain largely unanswered: are these methods better than the more traditional methods such as (prospective) hotspot analysis or time series analysis (eg the exponential smoothing method) methods? Secondly, how do these methods compare to each other? It would be interesting to compare the different method groups on the same dataset, to examine their respective strengths and weaknesses and whether their predictions are comparable or divergent. And thirdly, are these methods more efficient or easier to work with for police departments? At this time, not much attention has been given to factors influencing implementation and the effect of confounding factors (eg displacement effects). The effectiveness of predictive policing for crime control and prevention has not been proven conclusively. Yet ultimately these aspects (implementation and effectiveness) are at least as important for the ultimate success of these new methods as their predictive ability. Additionally, we shouldn't lose sight of the actual goal of using these predictive methods: reducing crime rates through improved detection and determent of criminal activity. This means that police deployment strategies and their effectiveness are equally crucial to the predictive policing process. In the worst-case scenario, the police run a serious risk of confirmation bias. Thus, it is time the problem of evaluating these predictive policing techniques are put on the agenda of quantitative criminology.

6. SELECTED LITERATURE

Andresen MA, *Environmental Criminology: Evolution, theory and practice* (Routledge 2004)

Arksey H and O'Malley L, 'Scoping studies: Towards a methodological framework' 8 International Journal of Social Research Methodology 19

Bachner J, *Predictive Policing: Preventing Crime with Data and Analytics* (Improving Performance Series, 2013)

Beck C and McCue C, 'Predictive Policing: What can we learn from Wal-Mart and Amazon about Fighting Crime in a Recession?' 76 The Police Chief

Berk R and others, 'Forecasting murder within a population of probationers and parolees: a high stakes application of statistical learning' 172 Journal of the Royal Statistical Society: Series A (Statistics in Society) 191

Bernasco W, 'Foraging strategies of homo criminalis: Lessons from behavioural ecology' 2 Crime Patterns and Analysis 5

Bernasco W, 'Them again? Same offender involvement in repeat and near repeat burglaries' 5 European Journal of Criminology 411

Booth A, Papaioannou D and Sutton A, *Systematic approaches to a succesful literature review* (SAGE Publications 2012)

Bowers KJ and Johnson SD, 'Domestic Burglary Repeats and Space-Time Clusters: The Dimensions of Risk' 2 European Journal of Criminology 67

Bowers KJ and Johnson SD, 'Who commits near repeats? A test of the boost explanation' 5 Western Criminology Review 12

Bowers KJ, Johnson SD and Pease K, 'Prospective hot-spotting: The future of crime mapping?' 44 British Journal of Criminology 641

Brantingham PJ and Brantingham PL, *Patterns in Crime* (Macmillan 1984)

Brantingham PJ, 'The theory of target search' in Cullen FT and Wilcox P (eds), *The Oxford handbook of criminological theory* (Oxford University Press 2013)

Brantingham PL, 'Crime pattern theory' in Fisher BS and Lab SP (eds), *Encyclopedia of victimology and crime prevention* (SAGE Publications 2010)

Bursik RJ and Grasmick HG, *Neighborhoods and Crime: The Dimensions of Effective Community Control* (Lexington Books, 1993)

Byrne J and Marx G, 'Technological Innovations in Crime Prevention and Policing. A Review of the Research on Implementation and Impact' 3 Cahiers Politiestudies 17

Camacho-Collados M and Liberatore F, 'A Decision Support System for predictive police patrolling' 75 Decision Support Systems 25

Caplan JM and Kennedy LW, *Risk Terrain Modeling Manual: Theoretical Framework and Technical Steps of Spatioal Risk Assessment for Crime Analsyis* (Rutgers 2010)

Caplan JM, Kennedy LW and Piza EL, 'Joint Utility of Event-dependent and Environmental Crime Analysis Techniques for Violent Crime Forecasting' 59 Crime & Delinquency 243

Chainey S, *JDI Briefs: Predictive mapping (predictive policing)* (UCL Jill Dando Institute of Security and Crime Science, 2012)

Chainey S, Tompson L and Uhlig S, 'The utility of hotspot mapping for predicting spatial patterns of crime' 21 Security Journal 4

Chan J and Moses LB, 'Is Big Data challenging criminology?' Theoretical Criminology 1

Chung-Hsien Y and others, *Crime Forecasting Using Data Mining Techniques* (11th IEEE International Conference on Data Mining Workshops, 2011)

Cloete CE and Spies JS, 'Combating Crime in Gauteng, South Africa: A Paradigm Shift' 108 WIT Transactions on the Built Environment 137

Cohen J, Gorr WL and Olligschlaeger AM, 'Leading indicators and spatial interactions: a crime-forecasting model for proactive police deployment' 39 Geographical Analysis 105

Cohen LE and Felson M, 'Social change and crime rate trends: A routine activity approach' 44 American Sociological Review 588

Cornish D and Clarke R, 'Understanding crime displacement: An application of rational choice theory' 25 Criminology 933

Daley D and others, 'Risk terrain modelling predicts child maltreatment' 62 Child abuse & Neglect 29

Drawve G, 'A Metric Comparision of Predictive Hot Spot Techniques and RTM' 33 Justice Quarterly 369

Eck JE and Weisburd DL, 'Crime places in crime theory' 4 Crime and Place: Crime Prevention Studies 1

Eck JE, 'Drug Markets and Drug Places: A Case-Control Study of the Spatial Structure of Illicit Drug Dealing' (University of Maryland 1994)

Eisner M, 'Long-Term Historical Trends in Violent Crime' 30 Crime and Justice 83

Farrell G and Pease K, *Once bitten, twice bitten: Repeat victimisation and its implications for crime prevention* (Police Research Group Crime Prevention Unit Series 1993)

Ferguson AG, 'Predictive Policing and Reasonable Suspicion' 62 Emory Law Journal 259

Fitterer J, Nelson TA and Nathoo F, 'Predictive crime mapping' 16 Police Practice and Research 121

Gorr WL and Lee Y, 'Early Warning System for Temporary Crime Hot Spots' 31 Journal of Quantitative Criminology 25

Gorr WL and Olligschlaeger AM, *Crime hot spot forecasting: Modeling and comparative evaluation* (Final Project Report 2002) <https://www.ncjrs.gov/pdffiles1/nij/grants/195167.pdf>

Grant MJ and Booth A, 'A typology of reviews: An analysis of 14 review types and associated methologies' 26 Health Information & Libraries Journal 91

Groff ER and La Vigne NG, 'Forecasting the future of predictive crime mapping' 13 Crime Prevention Studies 29

Habeman CP and Ratcliffe J, 'The Predictive Policing Challenges of Near-Repeat Armed Street Robberies' 6 Policing 151

Hardyns W and Rummens A, 'Predictive policing as a new tool for law enforcement? Recent developments and challenges' European Journal of Criminal Policy and Research

Hassouna M and others, 'Customer Churn in Mobile Markets: A Comparison of Techniques' 8 International Business Research 224

Haykin S, *Neural networks and learning machines* (3rd edn Pearson 2009)

Henry DB and others, 'Community Monitoring for Youth Violence Surveillance: Testing a Prediction Model' 15 Prevention Science 437

Hermon R and Williams PAH, *Big data in healthcare: What is it used for?* (Australian eHealth Informatics and Security Conference, 2014)

Hipp JR and Kim Y, 'Measuring Crime Concentration Across Cities of Varying Sizes: Complications Based on the Spatial and Temporal Scale Employed' 33 Journal of Quantitative Criminology 595

Hitachi, *Hitachi Data Systems unveils new advancements in predictive policing to suppport safer, smarter societies* (2015) <https://www.hitachivantara.com/en-us/news-resources/press-releases/2015/gl150928.html>

Hollywood JS and others, 'Predictive Policing: What It Is, What It Isn't and Where It Can Be Useful' International Association of Chiefs of Police Law Enforcement Information Management

Hunt P, Saunders J and Hollywood JS, *Evaluation of the Shreveport Predictive Policing Experiment* (Rand, 2014)

IBM, *Predictive analysis for crime prediction and prevention: Helping police departments known better* <https://www-01.ibm.com/software/analytics/spss/11/na/ cpp/>

Johnson SD and Bowers KJ, 'The Burglary as Clue to the Future: The Beginnings of Prospective Hot-Spotting' 1 European Journal of Criminology 237

Johnson SD and Bowers KJ, 'The Stability of Space-Time Clusters of Burglary' 44 British Journal of Criminology 55

Johnson SD and others, 'Near Repeats: A Cross National Assessment of Residential Burglary' 23 Journal of Quantitative Criminology 201

Johnson SD, 'Repeat burglary victimisation: A tale of two theories' 4 Journal of Experimental Criminology 215

Kennedy LW, Caplan JM and Piza EL, 'Risk Clusters, Hotspots, and Spatial Intelligence: Risk Terrain Modeling as an Algorithm for Police Resource Allocation Strategies' 27 Journal of Quantitative Criminology 339

Kianrnehr K and Alhajj R, 'Effectiveness of support vector machine for crime hot-spots prediction' 22 Applied Artifical Intelligence 433

Kinney JB and others, 'Crime attractors, generators and detractors: Land use and urban crime opportunities' 34 Built Environment 62

Kitchin R, 'Big Data, new epistemologies and paradigm shifts' Big Data & Society 1

Levine ES and others, 'The New York City Police Department's Domain Awareness System' 47 Interfaces 70

Mali B, Bronkhorst-Giesen C and den Hengst M, *Predictive policing: lessen voor de toekomst. Een evaluatie van de landelijke pilot* (2016)

McCue C, *Data Mining and Predictive Analysis: Intelligence Gathering and Crime Analysis* (2nd edn Elsevier Science Publishing 2015)

Melamed S, 'Can Atlantic City's bold experiment take racial bias out of predictive policing?' *The Philadelphia Inquirer* (2017)

Mohler GO and others, 'Randomized controlled field trials of predictive policing' Journal of the American Statistical Association

Mohler GO and others, 'Self-exciting point process modeling of crime' 106 Journal of the American Statistical Association 100

Mohler GO, 'Marked point process hotspot maps for homicide and gun crime prediction in Chicago' 30 International Journal of Forecasting 491

Moses LB and Chan J, 'Algorithmic prediction in policing: Assumptions, evaluation and accountability' Policing and Society

Peachey P, 'The Real Minority Report? Kent Constabulary tests computer program to predict crime' *The Independent* (2013)

Pease K and Tseloni A, *Using Modeling to Predict and Prevent Victimization* (Springer 2014)

Perry WL and others, *Predictive Policing: The Role of Crime Forecasting in Law Enforcement Operations* (RAND Research Reports 2013)

Pinker S, *The Blank Slate: The Modern Denial of Human Nature* (Penguin Books 2002)

Ratcliffe J and Rengert G, 'Near-Repeat Patterns in Philadelphia Shootings' 21 Security Journal 58

Ratcliffe J, 'Crime Mapping: Spatial and Temporal Challenges' in Piquero AR and Weisburd DL (eds), *Handbook of Quantitative Criminology* (Springer Science 2010)

Ratcliffe J, 'What is the future of... predictive policing?' 6 Translational Criminology 4

Ratcliffe J, *Intelligence-led policing* (2nd edn Routlegde 2016)

Rivero D, '*Microsoft is developing an app that can predict crimes of the future*' Fusion (2015)

Rossellini AJ and others, 'Using administrative data to identify US Army soldiers at high-risk of perpetrating minor violent crimes' 84 Journal of Psychiatric Research 128

Rosser G and others, 'Predictive Crime Mapping: Arbitrary Grids or Street Networks?' 33 Journal of Quantitative Criminology 569

Rummens A, Hardyns W and Pauwels L, 'The use of machine learning in spatiotemporal crime forecasting: Building and testing a model in an urban context' Applied Geography

Santos RB, 'The Effectiveness of Crime Analysis for Crime Reduction: Cure or Diagnosis?' 30 Journal of Contemporary Criminal Justice 147

Saunders J, Hunt P and Hollywood JS, 'Predictions put into practice: a quasi-experimental evaluation of Chicago's predictive policing pilot' 12 Journal of Experimental Criminology 347

Sherman L and Weisburd DL, 'General deterrent effects of police patrol in crime "hot spots": a randomized, controlled trial' 12 Justice Quarterly 625

Sherman L, Gartin PR and Buerger ME, 'Hot spots of predatory crime: routine activities and the criminology of place' 27 Criminology 27

Short MB and others, 'A Statistical Model of Criminal Behavior' 18 Mathematical Models and Methods in Applied Sciences 1249

Short MB and others, 'Measuring and Modeling Repeat and Near-Repeat Burglar Effects' 25 Journal of Quantitative Criminology 325

Siegel E, *Predictive Analytics: The power to predict who will click, buy, lie, or die* (John Wiley & Sons 2013)

Street AE and others, 'Developing a Risk Model to Target High-Risk Preventive Interventions for Sexual Assualt Victimizaton Among Female U.S. Army Soldiers' 4 Clinical Psychological Science 939

Summers L, 'Virtual repeats and near repeats' in Fisher BS and Lab SP (eds), *Encyclopaedia of Victimology and Crime Prevention* (Sage 2010)

Summers L, Johnson SD and Rengert G, 'The Use of Maps in Offender Interviewing' in Bernasco W (ed), *Offenders on Offending* (Willan 2010)

Tchekmedyian A, 'Police push back agains using crime-prediction technology to deploy officers' *Los Angeles Times* (2016)

Telep CW, 'Police Interventions to Reduce Violent Crime: A Review of Rigorous Research' (Reducing Violent Crime at Places: The Research Evidence)

Tibshirani R, Witten D and Hastie T, *An Introductio to Statistical learning with Applications in R* (Springer 2013)

Townsley MT, Homel R and Chaseling J, 'Infectious Burglaries: A Test of the Near Repeat Hypothesis' 43 British Journal of Criminology 615

Tseloni A and Pease K, 'Repeat personal victimisation: Random effects, event dependence and unexplained heterogeneity' 44 British Journal of Criminology 931

Tseloni A and Pease K, 'Repeat victimization: 'Boosts' or 'flags'?' 43 British Journal of Criminology 196

Van Brakel R and De Hert P, 'Policing, surveillance and law in a pre-crime society: Understanding the consequences of technology based strategies' 3 Cahiers Politiestudies 163

Wang X, Brown DE and Gerber MS, 'Spatio-temporal modeling of criminal incidents using geographic, demographic and Twitter-derived information' (2012 IEEE International Conference on Intelligence and Security Informatics)

Wang X and Brown DE, 'Spatio-temporal modeling for criminal incidents' 1 Security Informatics 1

Weisburd DL, 'The Law of Crime Concentration and the Criminology of Place' 53 Criminology 133

Weisburd DL, Bruinsma GJN and Bernasco W, *Putting crime in its place: Units of analysis in spatial crime research* (Springer 2009)

Weisburd DL, Groff ER and Yang S, *The criminology of place: Street segments and our understanding of the crime problem* (Oxford University Press 2012)

Zhou Z-H, *Ensemble methods: Foundations and algorithms* (CRC Press 2012)

7. APPENDIX I: REVIEW PROTOCOL

Keywords

"machine learning" AND crime/offence; crime/offence AND predict*/forecast*/map*; "predictive policing"; "risk terrain modeling/modelling"; "prospective hot spot/hot-spot analysis/mapping"; "prospective hot-spotting"; "spatiotemporal crime forecasting"; "predictive/prospective crime mapping/analysis"; near-repeat AND crime/offence AND predict*/forecast*/map*; "machine learning" AND crime/offence AND predict*/forecast*/map*;

Databases

- Web of Science
- Open Grey
- Google Scholar

Eligibility criteria

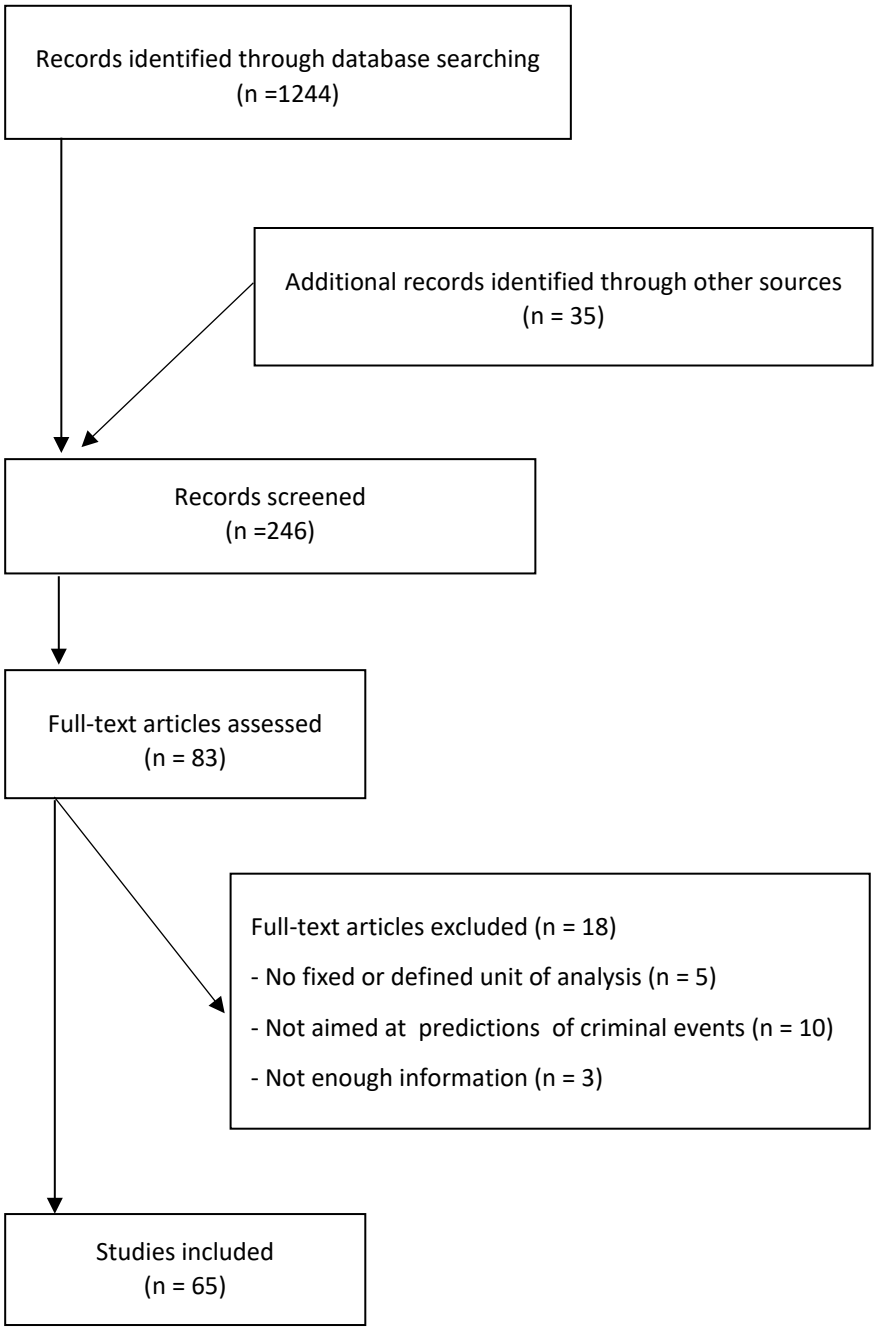
- published 2007 - current
- aimed at predicting near-future high-risk criminal events (place, time, victim or perpetrator)
- use of near-repeat methods, machine learning or risk-terrain modelling
- use of micro-geographical or individual level of analysis
- empirical study or at least an empirical chapter (eg example dataset analysis)

Search strategy

- Database search
- Hand searching of reference lists to identify missed studies

Date of last search: 27/09/2017

8. APPENDIX II: REVIEW FLOW DIAGRAM



9. APPENDIX III: OVERVIEW OF THE SELECTED STUDIES WITH THEIR MAIN CHARACTERISTICS

Authors	Year	Location	Method group	Crime types	Variables	Unit of analysis
Berk et al.	2009	US (Pennsylvania)	supervised machine learning	homicide	crime data	individual perpetrator (parolee/probationer)
Caplan et al.	2013	US (New Jersey)	risk terrain modelling	violence	crime and environmental data (N=5)	30m (100ft) grid
Chung-Hsien et al.	2011	US (unknown)	supervised machine learning	domestic burglary	crime and environmental data (N=6)	800m (0,5mi) and 400m (0,25mi) grid
Cloete & Spies	2009	South-Africa	supervised machine learning	bank robbery	crime data	individual victim (bank)
Daley	2016	US (Texas)	risk terrain modelling	child maltreatment	crime and socio-economic data	120m (400ft) grid
Drawve	2016	US (unknown)	risk terrain modelling	gun violence	crime, socio-economic and environmental data	grid (multiple cell sizes)
Fitterer et al.	2015	Canada	supervised machine learning	domestic burglary	crime, socio-economic and environmental data (N=10)	200m grid
Hunt et al.	2014	US (Louisiana)	supervised machine learning	property crime	crime data (N=7)	120m (400ft) grid
Kennedy et al.	2011	US (unknown)	risk terrain modelling	violence	crime data (N=7)	45m (145ft) grid
Kianrnehr et al.	2008	US (unknown)	supervised Machine learning	general crime	crime data	50m grid
Levine et al.	2017	US (New York)	supervised machine learning	general crime	crime data	200m grid
Mohler*	2014	US (California)	near-repeat method	homicide and gun crime	crime data (N=6)	150m grid
Mohler et al.	2011	US (California)	near-repeat method	domestic burglary	crime data (N=2)	200m grid
Mohler et al.*	2015	US (California)	near-repeat method	property crime and violence	crime data (N=2)	150m grid
Ratcliffe & Rengert	2008	US (Pennsylvania)	near-repeat method	gun violence	crime data	175m grid
Rosellini et al.	2017	US (nationwide)	supervised machine learning	Violence	crime and socio-economic data	individual perpetrator (within U.S. Army)
Rummens et al.	2017	Belgium	supervised machine learning	property crime and violence	crime, socio-economic and environmental data (N=26)	200m grid
Saunders et al.	2016	US (illinois)	supervised machine learning	gun violence	crime data	individual victim or perpetrator (person of interest)
Street et al.	2016	US (nationwide)	supervised machine learning	sexual violence	crime and socio-economic data	individual victim (within U.S. Army)

Wang & Brown*	2012	US (Virginia)	supervised machine learning	general crime	crime, socio-economic and environmental data (N=12)	32m grid
Wang et al. *	2012	US (Virginia)	supervised machine learning	general crime	crime, socio-economic, environmental and social media data (N=35)	32m grid

∗ These studies make use of the same dataset.

Big data in the pharmaceutical sector

Current developments and legal challenges

CLAUDIA SEITZ[1]

1. INTRODUCTION

Advances in sciences – both in information technology and molecular biology – have enabled new understandings of biological processes, advanced forms of therapies and new treatment options which lead to an ongoing paradigm shift. In the last several decades digitalization has become a major trend in the healthcare sector. New forms of data collection and electronic documentation have created strong health benefits and have reduced costs.[2] In the EU the e-health card has been introduced for medically necessary, state-provided healthcare, which uses technically sophisticated telematic infrastructures for interconnecting medical professionals.[3]

E-health data collections store a huge amount of health data, such as treatments and prescriptions, and have been criticized for the insufficient protection of data. The so called "see-through or transparent patient" with genetic fingerprint is increasingly enabling an individual approach of medical prediction and treatment and raises questions of legal protection. Technical progress in such big data generation and management has opened previously unprecedented possibilities for research and new products and has tremendously highlighted public fears of abuse.

---

[1] Max Geldner Assistant Professor, Faculty of Law, University of Basel. Email: claudia.seitz@unibas.ch.

[2] For an overview of the recent trends towards digitalization and large-scale data analytics in healthcare and the impacts of these trends in the way healthcare will be organized in the future, see Volker Tresp and others, 'Going Digital: A Survey on Digitalization and Large-Scale Data Analytics in Healthcare', Proceedings of the IEEE 2016, 2180 <http://ieeexplore.ieee.org/document/7600349/>.

[3] The European Health Insurance Card gives access to medically necessary, state-provided healthcare during a temporary stay in any of the 28 EU countries, Iceland, Liechtenstein, Norway and Switzerland, under the same conditions and at the same cost as people insured in that country, for further information see <http://ec.europa.eu/social/main.jsp?catId=509&langId=en>.

Indeed, big data research raises new technical and regulatory concerns due to its specific characteristics: the vast amount of data generated at an unprecedented speed, by using internet search engines and algorithms, comprises data from virtually any field and presents challenges on various levels of data flows, ranging from extraction of information to data analysis. This results in an exponential growth of generated data which may lead to innovation and new products and services. This development creates data protection, privacy and confidentiality issues, since most persons who have made data available (eg through social media) are not aware of the possible uses. Many consumers and patients do not know that data managers may reverse anonymity through the combination of various databases.

The rise of big data in the healthcare and pharmaceutical sectors raises specific challenges in terms of privacy, security, data ownership as well as data stewardship and governance.[4] Besides the legal questions concerning the data ownership the concern of data privacy and security raises unexpected issues regarding the general rights of personality and privacy as well as the right of informational self-determination as a right of individuals to determine the use of their private data as long as the data is not aggregated or has been transformed into an anonymous form. For all personal data that has not been anonymised data protection laws apply. Moreover, from a data protection law perspective, health related data is considered as especially sensitive personal data.

This paper shall discuss the question when and to what extent data protection laws apply to big data in the healthcare and pharmaceutical sector. Big data in these sectors lead to a tremendous number of data protection questions, for instance regarding information and consent regarding automated data collection and data processing. It is not possible to address all questions regarding big data in the healthcare sector in this paper. For this reason, this paper shall focus on several aspects of data protection issues in the field of new pharmaceutical technologies.

The paper shall address questions on which technologies have arisen during the last years and what kind of data is concerned. It shall assess the question to what extent the new EU data protection legislation may protect that kind of data and it shall analyze potential gaps that need to be addressed by legislation. Based on these questions the paper starts after a short introduction (1) with a short chapter on big data in the pharmaceutical sector (2). It shall then continue with an explanation of genetics and genomics and new phar-

[4] See Javier Andreu-Perez and others, 'Big Data For Health' (2015) 19 IEEE Journal of Biomedical and Health Informatics 1193.

maceutical technologies (3) and it shall explain to what extent these new developments can be used in the pharmaceutical sector for the screening, early detection and treatment of diseases by explaining the new research and development fields of predictive and personalized medicine (4). It shall further clarify some of the challenges and risks which are specific for genetic information and data (5). Based on this assessment the fundamental principles of the European Convention on Human Rights and the Oviedo Convention shall be presented (6) as well as the UNESCO Declaration on the Human Genome and Human Rights (7). It shall also be analyzed whether the new developments in EU data protection law with the entry into force of the new General Data Protection Regulation (GDPR)[5] will enable protection for data collected in the pharmaceutical sector (8). Finally, the paper shall identify regulatory gaps for the protection of data in the pharmaceutical sector and shall draw some conclusions for future regulatory requirements (9).

2. BIG DATA DEVELOPMENTS IN THE PHARMACEUTICAL SECTOR

2.1. Development of big data research

Big data research using electronic health records and social media available through the internet are a constantly improving means to generate knowledge about the function of human beings and society. Such data is extremely useful to answer important research questions related to health, functioning and behavior of various populations globally. This type of research is valuable in different disciplines, especially for the pharmaceutical industry, and could be used for the creation of new pharmaceutical products, for example in the form of personalized medicines, as well as for new compensation models, such as pay for performance models.

Through excessive data collection and combination it is possible to develop user profiles which might be used for behavioral targeting and for discriminatory strategies, such as real-time personalized pricing for online sales and price adjustments if there is information concerning the willingness to pay of individual customers.[6]

---

[5] Parliament and Council Regulation (EU) 2016/679 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L119/1.

[6] This does not only raise questions concerning the ownership of such data collections but also whether these collections may lead to product markets and raise competition law issues.

2.2. Big data and the pharmaceutical industry

The developments in digitalization and information technology have led to huge data collections already. Various private actors, such as pharmaceutical companies, healthcare providers, insurance companies and laboratories as well as public organizations have stored data, ranging from research data and data on tests and chemical substances to patient records, into databases. In addition, several information technology companies are collecting health-related data that may be used for additional services or which could be sold to companies in the healthcare sector.

The pharmaceutical industry has always generated large amounts of data, resulting from human research and clinical trials in the context of regulatory requirements as well as pharmacovigilance obligations after a drug has entered the market. Whereas in the past the data was stored in hard copy form, the data is nowadays collected, processed and stored electronically. Driven by mandatory requirements and the potential to improve the quality of pharmaceutical products and healthcare delivery meanwhile reducing the costs, these massive quantities of data hold the promise of supporting a wide range of medical and healthcare functions, including among others clinical decision support, disease surveillance, and population health management.[7]

These vast volumes of data may be accessed very rapidly and easily allow researchers in pharmaceutical companies, public institutions and academia to mine this data to identify new substances, conduct studies in a more efficient way, verify the most effective treatments for particular conditions, develop further medical use for other indications or identify side effects. The use of electronic databases of chemical substances and genetic information could increase the success rate of new active ingredients, shorten the process of screening and developing new drugs and could also consider individual diversities in drug response.

3. GENETICS AND GENOMICS AS NEW PHARMACEUTICAL TECHNOLOGIES

3.1. Analysis of genomes

Conventional drug research and discovery is undergoing a fundamental change. The completion of the entire genome sequence of many experimental organisms as well as the human organism allow to compare several genomic

[7] Wullianallur Raghupathi and Viju Raghupathi, 'Big Data Analytics in Healthcare: Promise and Potential' (2014) 2 Health Information Science and Systems 3.

sequences (comparative genomics), to get valuable information for gene discovery and functional genomics.[8]

New technologies resulting from studies of the genome, such as next-generation DNA sequencing (NGS) are already revolutionizing the understanding of genetic variation among individuals and lead to new possibilities for pharmaceutical products.[9] The study of the genome comprises the analysis of all genes expressed in a cell, organism, tissue or body fluids by using methods of DNA extraction as well as sequencing tools. This new technology enables pharmaceutical research to understand the genetic background of specific diseases.

3.2. **Pharmacogenomics**

Pharmacogenetics deals with heredity and response of drugs as a branch of science that attempts to explain the variability of one or another drug response, and to search for the genetic basis of such variations or differences.[10] Although pharmacogenetic studies are primarily concerned with the human species, the science can, in principle, be applied to all subjects, primitive or complex that are capable of responding to a drug or to an environmental chemical.[11]

Pharmacogenetic – or pharmacogenomic[12] – studies and chemical genomic investigations are quickly becoming fundamental techniques for genomic drug discovery.[13] In addition, they may also allow for gene mapping and by using biomarkers may identify genetic causes for certain diseases such as genetic mutations. Based on this technology of analyzing genes it is possible to study the results of a drug treatment for a specific patient in advance. This

---

[8] See Yoshinobu Baba, 'Development of Novel Biomedicine based on Genome Science', (2001) 13 European Journal of Pharmaceutical Sciences 3.

[9] For further information regarding the next-generation DNA sequencing (NGS) projects, such as the 1000 Genomes Project: see Aaron McKenna and others, 'The Genome Analysis Toolkit: A MapReduce Framework for Analyzing Next-Generation DNA Sequencing Data' (2010) Genome Research 1297.

[10] Werner Kalow, 'Historical Aspects of Pharmacogenetics', in Werner Kalow and others (eds), *Pharmacogenomics* (Taylor & Francis 2001) 1.

[11] Kalow (n 9) 1.

[12] Pharmacogenetics has been defined as the study of variability in drug response due to heredity. Since in the last years a trend of adding the suffix "... omics" to areas of research emerged, the term "pharmacogenomics" has been introduced, see Munir Pirmahamed, 'Pharmacogenetics and Pharmacogenomics', Br J Clin Pharmacol. 2 345.

[13] Baba (n 8) 3-4.

possibility of pharmacogenomics allows evaluating all effects of substances and active ingredients on the physiological process of a patient.

4. PREDICTIVE AND PERSONALIZED MEDICINE

4.1. Pharmacogenomics and data analysis

The combination of genomics and clinical health data together with big data analytics will leverage personalized medicine.[14] Technologies such as genome sequencing, gene expression profiling, proteomic and metabolomics analyses, electronic medical records, and patient-reported health information have produced large amounts of data on various populations, cell types, and disorders which may be integrated and analyzed in order to produce models or concepts about physiological functions or mechanisms of pathogenesis.[15]

4.2. Personalized medicine

Personalized medicine is generally defined as developing tailored therapies, including drugs, drug dosage and other remedies, based on an individual's specific biological characteristics. Personalized or precision medicine is based on the idea to offer patients a more effective, tailored, precise and targeted treatment based on the specific genetic profile of the patient. Tailoring the best medical intervention to the right individual or patient can dramatically improve health.[16] Moreover, it allows for adjusting the doses of active substances in so far as it is necessary for the treatment and at the same time avoiding treating with overdoses and thus reducing side effects of the drug.

Technological advancements have allowed molecular-based testing that was once done on a research-only basis to be adopted for routine use in clinical laboratories.[17] Whereas these types of techniques were labor intensive and highly complex, the introduction of automated processes combined with an improved understanding of human genetic variation has allowed molecular

---

[14] Kevin Wing and others, 'Development of Predictive Genetic Tests for Improving the Safety of New Medicines: the Utilization of Routinely Collected Electronic Health Records' (2014) 19 Drug Discovery Today 357.

[15] Benjamin Wooden and others, 'Using Big Data to Discover Diagnostics and Therapeutics for Gastrointestinal and Liver Diseases' (2017) 152 Gastroenterology 53.

[16] Christos Katsios and Dimitrios H Roukos, 'Individual Genomes and Personalized Medicine: Life Diversity and Complexity' (2010) 7 Personalized Medicine, Editorial.

[17] Charles J. Sailey and others (eds), *Molecular Genetics and Personalized Medicine* (Springer, 2012).

testing to expand into clinical diagnostics, where it is not yet considered an essential aspect of patient care. The use of personalized medicine to improve both the prevention and cure of disease is potentially achievable through predicting both the disease risk among healthy individuals in the general population and the therapeutic response among patients.[18] Thus, genomic information from individuals or patients can substantially contribute to biomarker-based guided personalized prevention and treatment.[19]

4.3. Use of data for pharmaceutical studies

Information-based research technologies revolutionize several stages of the process of pharmaceutical product development. Genetic screening as a new experimental tool to identify and select a phenotype of a patient can provide information on gene functions and may predict a specific biological process of a disease.[20] This new technique enables more precise and better prediction of diseases and can be used to treat certain diseases (eg cancer gene therapies).[21] It raises, however, various ethical and legal concerns, especially concerning the protection of human dignity.[22]

---

[18] Katsios and Roukos, (n 16).

[19] Katsios and Roukos, (n 16).

[20] For further information on genetic screening, see Anne E Carpenter and David M Sabatini, 'Systematic Genome-Wide Screens of Gene Function' (2004) 5 Nature Review Genetics 11.

[21] For further information on cancer gene therapy, see Ullrich Kleeberg and Alfred G Hildebrandt, 'Introduction to Principles and Examples of Somatic Gene Therapy' in Stefan Müller and others (eds.) *Interdisciplinary Approach to Gene Therapy: Legal, Ethical and Scientific Aspects* (Springer 1997).

[22] See George J. Annas and Elias Sherman, *Gene Mapping: Using Law and Ethics as Guides* (Oxford 1992), 291; Ruth Chadwick and Urban Wiesing, 'Moral and Philosophical Issues. Introduction' in Ruth F Chadwick and others (eds), *The Ethics of Genetic Screening* (Springer 1999) 167; Roger Hoedemaekers, 'Genetic Screening and Testing a Moral Map' in Ruth F Chadwick and others (eds), *The Ethics of Genetic Screening* (Springer 1999) 207; Hans-Peter Kröner, 'From Eugenics to Genetic Screening. Historical Problems of Human Genetic Applications' in Ruth F Chadwick and others (eds), *The Ethics of Genetic Screening* (Springer 1999) 131; Mairi Levitt, 'A Sociological Perspective on Genetic Screening' in Ruth F Chadwick and others (eds), *The Ethics of Genetic Screening* (Springer 1999) 157; Edward E Wallach and John A Robertson, 'Ethical and Legal Issues in Preimplantation Genetic Screening' (1992) 57 Fertility and Sterility 1.

The new technologies support screening of new substances, drug discovery as well as preclinical and clinical studies by providing an analysis of large volumes of diverse data, such as molecular structures, genetic information, biomarkers, biological activities and scientific literature.[23]

The possibility to use health-related data instead of conducting clinical trials on active ingredients or drugs with human beings does not only avoid the exposure to risks of unknown substances and side effects but also enables research for specific diseases where it would be costly to start research or where there are not enough patients to test the substances.

This is especially the case for so called rare diseases where it is often difficult to find enough patients to test the active ingredients.[24] Not all diseases occur with the same frequency and many diseases are so rare, that they affect only a small percentage of the population. In the European Union, rare diseases are defined as diseases that affect less than 5 patients per 10´000 people in the general population. According to recital 5 of the EU Regulation on orphan medicinal products a prevalence of not more than five affected persons per 10 thousand is generally regarded as the appropriate threshold.[25] In such cases it is often very difficult to find an appropriate number of patients to test new substances and drugs. For some rare diseases there may be only a handful of similar patients worldwide, and their data may be stored in diverse clinical and research databases and as a consequence computational methods could enable finding similar patients across the growing number of patient repositories and registries.[26] Thus, the use of data could not only reduce the costs for drugs for rare diseases but could lead to robust information on the

[23] See for further information, Donald B. Bailey and others, 'Ethical, Legal and Social Concerns About Expanded Newborn Screening: Fragile X Syndrome as a Prototype of Emerging Issues' (2008) 121 Pediatrics 693.

[24] For the use of genetic technologies to detect and treat rare diseases, see Kym M Boycott and others, 'Rare-Disease Genetics in the Era of Next-Generation Sequencing: Discovery to Translation' (2013) 14 Nature Reviews Genetics 681.

[25] Parliament and Council Regulation (EC) No 141/2000 of 16 December 1999 on orphan medicinal products [1999] OJ L18/1.

[26] For further information on the matchmaker exchange project see the information of Matchmaker on <http://www.matchmakerexchange.org/>, and Orion J. Buske and others, 'The Matchmaker Exchange API: Automating Patient Matching Through the Exchange of Structured Phenotypic and Genotypic Profiles' (2015) 36 Human Mutation 922.

effects of new substances without testing these substances on patients and it allows parallel sequencing of patients with rare diseases.[27]

For this reason, a specific program, the 'Matchmaker Exchange Application Programming Interface', has been created as a data format for exchanging phenotype and genotype profiles to enable matchmaking among patient databases, facilitate the identification of additional cohorts, and increase the rate with which rare diseases can be researched and diagnosed.[28]

4.4. Conducting human research trials and use of big data

Drug development has been a costly and lengthy process with an extremely low success rate and a lack of consideration of individual diversity in drug response and toxicity.[29] Over the past decade, an alternative big data approach has been expanding at an unprecedented pace based on the development of electronic databases of chemical substances, disease genes or protein targets, functional readouts, and clinical information covering inter-individual genetic variations and toxicities.[30]

The use of data instead of conducting clinical trials, for example, does not only make human research with test persons redundant but also establishes new tools which lead to time and resource-efficient processes for clinical trials and studies. This paradigm shift has enabled systematic, high-throughput, and accelerated identification of novel drugs or repurposed indications of existing drugs for pathogenic molecular aberrations specifically present in each individual patient.[31]

5. RISKS AND CHALLENGES IN RELATION TO GENETIC TESTS

5.1. Informing patients and informed consent

According to data protection legislation a person needs to be informed if personal data is collected, processed or stored. Whereas a patient can be informed concerning the results of genetic tests and the test may be conducted after the informed consent of this person the genetic test may also affect other

---

[27] See Sarah B Ng and others, 'Massively Parallel Sequencing and Rare Disease' (2010) 19 Human Molecular Genetics, 119.

[28] See Buske (n 26).

[29] Rosa S. Kim and others, 'Use of Big Data in Drug Development for Precision Medicine' (2016) 1 Expert Review of Precision Medicine and Drug Development, 245.

[30] Kim (n 29).

[31] Kim (n 29).

persons, especially the relatives of the patient. With any genetic tests, there could be results that give information about blood relatives of the person. In the case of genetic tests those relatives are neither informed nor have they consented to the genetic test that could also provide some information on their genetic profile.

5.2. Possibilities of misuse of genetic tests

The rapid progress in the development of genetic tests has led to some new forms of self-testing, such as the so-called "Direct-to-Consumer Genetic Tests" where people may get genetic information even if there is no medical purpose of such tests. In addition, the simplification of genetic tests has led to some form of abusive behavior towards genetic information. Nowadays it is possible to send human material abroad and get assessments of genetic information based on this material. There are for example several start-up companies in Asia, eg India or China, offering genetic tests that screen for health risks and predict other person-related information based on the genetic profile. It is questionable whether a person should rely on such information. Moreover, it is also possible to ask for a genetic test of material from another person without their consent or even without their knowledge.

6. EUROPEAN CONVENTION ON HUMAN RIGHTS AND THE OVIEDO CONVENTION

6.1. The right to private life and the right to information

The European Convention of Human Rights (ECHR)[32] comprises the fundamental right to privacy and encompasses the right to data protection.[33] Article 8(1) of the ECHR incorporates the right to privacy, according to which everyone shall have the right to respect for his private and family life, his home and his correspondence. In addition, Article 8(2) of the ECHR prohibits any interference by a public authority with the exercise of this right unless such interference is in accordance with the law and necessary in a democratic

[32] The Convention for the Protection of Human Rights and Fundamental Freedoms, signed on 4 November 1950 and ratified by all 47 Member States of the Council of Europe ("European Convention on Human Rights", "ECHR").

[33] See for the relationship between ethics, privacy and genetic information, Bryce Goodman, 'What´s Wrong with the Right to Genetic Privacy: Beyond Exceptionalism, Parochialism and Adventitious Ethics' in Brent Daniel Mittelstadt and Luciano Floridi (eds) *The Ethics of Biomedical Big Data* (Springer 2016) 139; Brent Daniel Mittelstadt and Luciano Floridi, 'The Ethics of Big Data: Current and Foreseeable Issues in Biomedical Contexts' in Brent Daniel Mittelstadt and Luciano Floridi (eds) *The Ethics of Biomedical Big Data* (Springer 2016) 445.

society in cases of public interest as listed in Article 8(2) of the ECHR. The right to privacy has usually been considered as the most prominent fundamental right to protect in data-intensive (big data) health research.[34]

Personal data processing could fall within the scope of Article 8 ECHR, when the personal data processing engages aspects of the private life.[35] The question whether this is the case depends on the nature of the data, the context in which the data is processed, the way the data is used and the results of the processing.[36]

6.2. General principles of human rights in the field of biomedicine

The Oviedo Convention guarantees a minimum common standard for the protection of human rights in the field of biomedicine.[37] The Convention is the first legally-binding international text designed to preserve human dignity, rights and freedoms, through a series of principles and prohibitions against the misuse of biological and medical advances.[38] The Convention comprises a set of general principles to guarantee human rights such as the primacy of the human being, equitable access to healthcare and especially the general

[34] Menno Mostert and others, 'From Privacy to Data Protection in the EU: Implications for Big Data Health Research', (2017) 24 EJHL 1.

[35] Mostert and others (n 34).

[36] Mostert and others (n 34).

[37] The Convention for the Protection of Human Rights and Dignity of the Human Being with regard to the Application of Biology and Medicine of the Council of Europe, signed on 4 April 1997 in Oviedo ("Oviedo Convention"). Regarding a comment concerning the Oviedo Convention, see for example Roberto Andorno, 'The Oviedo Convention: A European Legal Framework at the Intersection of Human Rights and Health Law' (2005) 2 Journal of International Biotechnology Law 133; F. William Dommel and Duane Alexander, 'The Convention on Human Rights and Biomedicine of the Council of Europe' (1997) Kennedy Institute of Ethics Journal 259; Sally Wheatley, 'Human Rights and Human Dignity in the Resolution of Certain Ethical Questions in Biomedicine' (2011) European Human Rights Law Review 312; Herman Nys and others, 'Patient Rights in EU Member States after the Ratification of the Convention on Human Rights and Biomedicine' (2007) Health Policy 223.

[38] See Council of Europe <https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/164>.

right of personality and autonomy as well as the principle of respect for human dignity.[39] Several provisions of the Convention have the objective to protect the human dignity, although the concept of human dignity is not defined.[40] Article 8 of the Oviedo Convention guarantees the right that all patients have the right to be informed about their health and it also comprises the right not be informed. The information about their health includes also genetic information such as results of predictive genetic tests. Article 12 of the Oviedo Convention comprises the following general rule: tests which are predictive of genetic diseases or which serve either to identify the subject as a carrier of genes responsible for a disease or to detect a genetic predisposition or susceptibility to a disease may be performed only for health purposes or for scientific research linked to health purposes, and subject to appropriate genetic counseling.

6.3. **Genetic testing and protection of the human genome**

The Oviedo Convention also contains a rule for interventions on the human genome. According to Article 13 an intervention seeking to modify the human genome may only be undertaken for preventive, diagnostic or therapeutic purposes and only if its aim is not to introduce any modification in the genome of any descendants. The general principle in Article 13 of the Oviedo Convention is amended by the Additional Protocol concerning Genetic Testing for Health Purposes.[41] This Protocol comprises several principles, especially concerning the quality of genetic services, prior information and consent as well as genetic counseling and establishes general rules for conducting genetic tests. Fundamental human rights which need to be protected by this protocol are the protection of private life as well as the right to information resulting from genetic testing.

According to Article 2(1) of the Protocol the provisions apply to tests, which are carried out for health purposes, involving analysis of biological samples

---

[39] For the judicial interpretation of the principle of human dignity, see the comment of Christopher McCrudden, 'Human Dignity and Judicial Interpretation of Human Rights' (2008) European Journal of International Law 655.

[40] For a critical view of the protection of human dignity, see Ruth Macklin, 'Dignity is a Useless Concept: It Means No More Than Respect for Persons or their Autonomy' (2003) BMJ 1419: "*Although the aetiology may remain a mystery, the diagnosis is clear. Dignity is a useless concept in medical ethics and can be eliminated without any loss of content*."

[41] Additional Protocol to the Convention on Human Rights and Biomedicine concerning Genetic Testing for Health Purposes of the Council of Europe, signed on 27 November 2008 in Strasbourg.

of human origin and aiming specifically to identify the genetic characteristics of a person which are inherited or acquired during early prenatal development. These tests are defined as "genetic tests". The provisions of the Protocol, however, do not apply to genetic tests carried out for research purposes, according to Article 2(2) of the Protocol. Thus, genetic tests for clinical trials are not covered by the Protocol whereas genetic tests in the context of predictive or personalized medicine may be covered by the Protocol.

7. UNESCO DECLARATION ON THE HUMAN GENOME AND HUMAN RIGHTS

The Universal Declaration on the Human Genome and Human Rights was adopted unanimously and by acclamation at UNESCO on 11 November 1997.[42] One of the main principles of the UNESCO Declaration is stated in Article 1, ie that the human genome underlies the fundamental unity of all members of the human family, as well as the recognition of their inherent dignity and diversity. Rights concerning privacy are comprised in Article 5 of the UNESCO Declaration. According to Article 5(a) the prior, free and informed consent of the person concerned shall be obtained in all cases. Pursuant to Article 5(b) the right of each individual to decide whether or not to be informed of the results of genetic examination and the resulting consequences should be respected.

The most relevant provision concerning human genetic data is comprised in Article 7: "*Genetic data associated with an identifiable person and stored or processed for the purpose of research or any other purpose must be held confidential in the conditions set by law*". For the Member States of the Council of Europe that have signed the Oviedo Convention this objective of the UNESCO Declaration is already covered.

[42] Universal Declaration on the Human Genome and Human Rights of 11 November 1997, <http://portal.unesco.org/en/ev.php-URL_ID=13177&URL_DO=DO_TOPIC&URL_SECTION=201.html>. The following year, the United Nations General Assembly endorsed the Declaration.

8. EU DATA PROTECTION LAW

8.1. EU Charter of Fundamental Rights

In the European Union, the Charter of Fundamental Rights[43] contains the right to respect for private life in Article 7 and in addition the right to the protection of personal data in Article 8.[44] Article 8(1) of the Charter states that "*everyone has the right to the protection of personal data concerning him or her*". Article 8(2) provides that "*such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law*". In addition, Article 8(2) guarantees that "*everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified*".

8.2. General Data Protection Regulation

In 2016, the European Union approved the General Data Protection Regulation (GDPR)[45] which replaces the Data Protection Directive. One of the reasons for the new GDPR was the objective to protect data and data ownership from cyber security threats and to harmonize data privacy laws across the Member States of the European Union. The goal is to protect EU citizens from privacy and data breaches, as well as reshape the way in which organizations across the region approach data privacy.[46] The GDPR applies if the data controller or processor is based in the EU and it also applies to persons or organizations outside the EU if they collect or process personal data from EU residents. The GPDR covers personal data and as such all non anonymised data collected and processed in the context of genomic research.[47]

---

[43] Charter of Fundamental Rights of the European Union [2000] OJ C364/1.

[44] For further information concerning the jurisprudence of the EU Courts, see Juliane Kokott and Christoph Sobotta, 'The Distinction between Privacy and Data Protection in the Jurisprudence of the CJEU and the ECtHR' (2013) 3 International Data Privacy Law 222.

[45] General Data Protection Regulation (n 5).

[46] For an overview, see Paul De Hert and Vagelis Papakonstantinou, 'The Proposed Data Protection Regulation Replacing Directive 95/46/EC: A Sound System for the Protection of Individuals' (2012) Computer Law & Security Review 130.

[47] See Dara Hallinan and Paul De Hert, 'Many Have It Wrong – Samples Do Contain Personal Data: The Data Protection Regulation as a Superior Framework to Protect Donor Interests in Biobanking and Genomic Research' in Brent Daniel Mittelstadt and Luciano Floridi (eds) *The Ethics of Biomedical Big Data* (Springer 2016) 119.

The GDPR stipulates requirements concerning consent. This means that, except if another ground for lawful processing applies, the person must give consent for the collection of his or her personal data. According to recital 34 of the GDPR "genetic data should be defined as personal data relating to the inherent or acquired genetic characteristics of a natural person which result from the analysis of a biological sample from the natural person in question, in particular chromosomal, deoxyribonucleic acid (DNA) or ribonucleic acid (RNA) analysis, or from the analysis of another element enabling equivalent information to be obtained".

According to Article 4(1) personal data also comprises the genetic identity of a natural person. Genetic data is defined in Article 4(13) as personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question. Article 9(1) stipulates that the processing of genetic data for the purpose of uniquely identifying a natural person shall be prohibited. Article 9(2) lists exceptions to this prohibition, such as when a person gives explicit consent (except where Union or Member State law provide that the prohibition may not be lifted by the data subject). This provision, however, lays down only a minimum standard: pursuant to Article 9(4) the Member States may maintain or introduce further conditions, including limitations, with regard to the processing of genetic data or data concerning health.

The GDPR strictly regulates the processing of special categories of data, the so-called "sensitive personal data", such as health data, genetic data and biometric data because of their potential risks regarding the rights and freedoms of the data subject. Health related data and especially genetic data are highly sensitive data as long as the data are not anonymized. This data could be used in an abusive manner to discriminate persons in the form of genetic discrimination. Genetic discrimination refers to discrimination directed against an individual or family based solely on an apparent or perceived genetic variation from the "normal" human genotype.[48] Insurance companies, private employers, governments and educational institutions all have an immediate or potential interest in promoting large-scale genetic screening to identify individuals carrying disease-associated genes.[49] In addition, economic pressures to apply genetic tests to broader sections of the population may increase as

[48] Paul R. Billings and others, 'Discrimination as a Consequence of Genetic Testing' (1992) 50 Am. J. Hum. Genet 476.

[49] Billings (n 52).

biotechnology companies develop and sell genetic testing products and services.[50] This creates several possibilities to discriminate a person based on his or her genetic profile and may increase the pressure to agree to a genetic test.

8.3. EU data protection law in the pharmaceutical sector

Since the new data protection legislation will now apply to all companies processing the personal data of subjects in the European Union regardless of the location of the pharmaceutical company it may also cover pharmaceutical studies and genetic tests outside the EU. In case of non-compliance with the obligations of the GDPR increased fines of up to 4% of a company's global revenues may be imposed. The GDPR has also specifically focused on patient consent.[51]

Under the new regulation, the request for consent must be formulated in an "*intelligible and easily accessible form"* with the purpose of data processing attached to that consent. Research should – if this is possible – take into account the de-identification and anonymization of clinical data. De-identification involves removing or recoding health information that could identify an individual such as patient identifiers, free text verbatim terms or references to dates. This means that data anonymization involves destroying all links between the de-identified datasets and the original datasets.

In summary, the GDPR adopts a new general risk-based approach intended to facilitate the case-by-case identification of data protection issues, because personal data processing and the use of sensitive personal data such as genome-based information are crucial for the advances of health research activities such as clinical research and translational research, for practicing whole genome sequencing, for research biobanking or the creation of research databases.[52] One very important example for the necessity of collecting and processing such genome-based information is the field of predictive or personalized medicine.

---

[50] Billings (n 52).

[51] See for further information, Martine C Ploem and Marie-Louise Essink-Bot, 'Proposed EU Data Protection Regulation is a Threat to Medical Research' (2013) British Medical Journal 1.

[52] Gauthier Chassang, 'The Impact of the EU General Data Protection Regulation on Scientific Research' (2017) Ecancermedicalscience 709.

9. CONCLUSIONS

New developments in information technologies and in biotechnology have led to a tremendous increase in health-related data, resulting from data collections and data processing of various stakeholders in the healthcare sector, such as pharmaceutical companies, health insurers, hospitals, laboratories, research institutions and universities. Big data in the pharmaceutical sector brings numerous advantages: it enables new treatment options like predictive and personalized medicine which allows a tailored treatment of the individual patient. Big data offers the basis for research and development of drugs for rare diseases, especially if there are only a few patients who could take part in clinical studies. In addition, big data in the pharmaceutical sector led to a change in paradigm since data may reduce the number of human research trials and thus is time and cost saving.

In contrast, big data leads to fundamental questions such as the protection of the human dignity, the right of personality and autonomy as well as the issue of discrimination based on genetic information. Some of these questions have already been addressed by the law, for example through the requirement of the consent of the patient before conducting a genetic test as comprised in the Additional Protocol to the Oviedo Convention. However, several questions have not been solved so far. These concern, for instance, the question of informed consent of blood relatives of a patient or the issue of a genetic test of human material of somebody else without consent or even information. These examples show that there is still a lack of regulation. The legislator needs to act to close these gaps. Regulations on an international level would be desirable.

10. SELECTED LITERATURE

Andorno R, 'The Oviedo Convention: A European Legal Framework at the Intersection of Human Rights and Health Law' (2005) 2 Journal of International Biotechnology Law 133

Annas G J and Sherman E, *Gene Mapping: Using Law and Ethics as Guides* (Oxford 1992), 291

Andreu-Perez J and others, 'Big Data For Health' (2015) 19 IEEE Journal of Biomedical and Health Informatics 1193

Baba Y, 'Development of Novel Biomedicine Based on Genome Science' (2001) 13 European Journal of Pharmaceutical Sciences 3

Bailey D B and others, 'Ethical, Legal and Social Concerns About Expanded Newborn Screening: Fragile X Syndrome as a Prototype of Emerging Issues' (2008) 121 Pediatrics 693

Billings P R and others, 'Discrimination as a Consequence of Genetic Testing' (1992) 50 Am. J. Hum. Genet 476

Boycott K M and others, 'Rare-Disease Genetics in the Era of Next-Generation Sequencing: Discovery to Translation' (2013) 14 Nature Reviews Genetics 681

Buske O and others, 'The Matchmaker Exchange API: Automating Patient Matching Through the Exchange of Structured Phenotypic and Genotypic Profiles' (2015) 36 Human Mutation 922

Carpenter A E and Sabatine D M, 'Systematic Genome-Wide Screens of Gene Function' (2004) 5 Nature Review Genetics 11

Chassang G, 'The Impact of the EU General Data Protection Regulation on Scientific Research' (2017) Ecancermedicalscience 709

Katsios C and Roukos D H, 'Individual Genomes and Personalized Medicine: Life Diversity and Complexity' (2010) 7 Personalized Medicine, Editorial

Chadwick R and Wiesing U, 'Moral and Philosophical Issues. Introduction' in Chadwick R F and others (eds), *The Ethics of Genetic Screening* (Springer 1999) 167

De Hert P and Papakonstantinou V, 'The Proposed Data Protection Regulation Replacing Directive 95/46/EC: A Sound System for the Protection of Individuals' (2012) Computer Law & Security Review 130

Dommel F and Alexander D, 'The Convention on Human Rights and Biomedicine of the Council of Europe' (1997) Kennedy Institute of Ethics Journal 259

Goodman B, 'What´s Wrong with the Right to Genetic Privacy: Beyond Exceptionalism, Parochialism and Adventitious Ethics' in Mittelstadt BD and Floridi L (eds) *The Ethics of Biomedical Big Data* (Springer 2016) 139

Hallinan D and De Hert P, 'Many Have It Wrong – Samples Do Contain Personal Data: The Data Protection Regulation as a Superior Framework to Protect Donor Interests in Biobanking and Genomic Research' in Mittelstadt B D and Floridi L (eds) *The Ethics of Biomedical Big Data* (Springer 2016) 119

Hoedemaekers R, 'Genetic Screening and Testing. A Moral Map' in Chadwick R F and others (eds), *The Ethics of Genetic Screening* (Springer 1999) 207

Kalow W, 'Historical Aspects of Pharmacogenetics', in Kalow W and others (eds), *Pharmacogenomics* (Taylor & Francis 2001) 1

Katsios C and Roukos, D H, 'Individual Genomes and Personalized Medicine: Life Diversity and Complexity' (2010) 7 Personalized Medicine, Editorial

Kleeberg U and Hildebrandt A G, 'Introduction to Principles and Examples of Somatic Gene Therapy' in Müller S and others (eds) *Interdisciplinary Approach to Gene Therapy: Legal, Ethical and Scientific Aspects* (Springer 1997)

Kim R and others, 'Use of Big Data in Drug Development for Precision Medicine', (2016) 1 Expert Review of Precision Medicine and Drug Development, 245

Kokott J and Sobotta C, 'The Distinction between Privacy and Data Protection in the Jurisprudence of the CJEU and the ECtHR' (2013) 3 International Data Privacy Law 222

Kröner H-P, 'From Eugenics to Genetic Screening. Historical Problems of Human Genetic Applications' in Chadwick R F and others (eds), *The Ethics of Genetic Screening* (Springer 1999) 131

Levitt M, 'A Sociological Perspective on Genetic Screening' in Chadwick R F and others (eds), *The Ethics of Genetic Screening* (Springer 1999) 157

Macklin R, 'Dignity is a Useless Concept: It Means No More than Respect for Rersons or their Autonomy' (2003) BMJ 1419

McCrudden C, 'Human Dignity and Judicial Interpretation of Human Rights' (2008) European Journal of International Law 655

McKenna A and others, 'The Genome Analysis Toolkit: A MapReduce Framework for Analyzing Next-Generation DNA Sequencing Data' (2010) Genome Research 1297

Mittelstadt B D and Floridi L, 'The Ethics of Big Data: Current and Foreseeable Issues in Biomedical Contexts' in Mittelstadt B D and Floridi L (eds) *The Ethics of Biomedical Big Data* (Springer 2016) 445

Mostert M and others, 'From Privacy to Data Protection in the EU: Implications for Big Data Health Research', (2017) 24 EJHL 1

Ng S B and others, 'Massively Parallel Sequencing and Rare Disease' (2010) 19 Human Molecular Genetics, 119

Nys H and others, 'Patient Rights in EU Member States after the Ratification of the Convention on Human Rights and Biomedicine' (2007) Health Policy 223

Ploem M and Essink-Bot M, 'Proposed EU Data Protection Regulation is a Threat to Medical Research' (2013) British Medical Journal 1

Raghupathi W and Raghupathi V, 'Big Data Analytics in Healthcare: Promise and Potential' (2014) 2 Health Information Science and Systems 3

Sailey R and others (eds), *Molecular Genetics and Personalized Medicine* (Springer 2012)

Tresp V and others, 'Going Digital: A Survey on Digitalization and Large-Scale Data Analytics in Healthcare', Proceedings of the IEEE 2016, 2180, <http://ieeexplore.ieee.org/document/7600349/>

Wallach E E and Robertson J A, 'Ethical and Legal Issues in Preimplantation Genetic Screening' (1992) 57 Fertility and Sterility 1

Wheatley S, 'Human Rights and Human Dignity in the Resolution of Certain Ethical Questions in Biomedicine' (2011) European Human Rights Law Review 312

Wing K and others, 'Development of Predictive Genetic Tests for Improving the Safety of New Medicines: the Utilization of Routinely Collected Electronic Health Records' (2014) 19 Drug Discovery Today 357

Wooden B and others, 'Using Big Data to Discover Diagnostics and Therapeutics for Gastrointestinal and Liver Diseases' (2017) 152 Gastroenterology 53

Targeting children with personalised advertising

How to reconcile the (best) interests of children and advertisers[1]

VALERIE VERDOODT[2] & EVA LIEVENS[3]

Children are increasingly confronted online with targeted advertising that is personalised on the basis of their personal characteristics and behaviour. The tracking, profiling and targeting practices that enable personalisation are sophisticated and opaque, and as such, significantly impact children's ability to make carefully considered and critical commercial decisions or decisions concerning their privacy and personal data. This raises important issues from a children's rights perspective, particularly for their rights to development, privacy and protection against economic exploitation. Nevertheless, the digital advertising industry plays an important role in the creation and maintenance of good-quality content and digital environments for children. Whereas the regulatory framework in place already covers existing tracking, profiling and targeting practices, this chapter questions whether the framework is appropriate for reconciling the interests of advertisers and children.

1. CHILDREN('S RIGHTS) AND PERSONALISED ADVERTISING

Children grow up in a commercial environment in which they, from an early age, come across advertising for a multitude of products and services.[4] Throughout their childhood, they learn how to cope with the overload of such

[1] This chapter builds on research carried out in the framework of two research projects: (1) AdLit: Advertising Literacy in a New Media Environment Investigating Minors' Persuasion Knowledge in Relation to New Advertising Formats, Research Fund Flanders and (2) A children's rights perspective on privacy and data protection in the digital age: a critical and forward-looking analysis of the General Data Protection Regulation and its implementation with respect to children and youth, Special Research Fund Ghent University.

[2] PhD researcher, Centre for IT and IP Law, KU Leuven. Email: valerie.verdoodt@kuleuven.be.

[3] Assistant professor of Law & Technology, Faculty of Law, Ghent University. Email: e.lievens@ugent.be.

[4] Barrie Gunter, *Kids and Branding in a Digital World* (Manchester University Press 2016) 1.

commercial information and develop critical decision-making skills.[5] Scholars refer in this regard to children's 'advertising literacy', which includes their advertising-related knowledge, attitudes, and skills, such as the ability to recognise commercial messages, to understand the persuasive intent of such messages, and to critically evaluate them. Children already display some level of brand consciousness at a very young age (even starting from the age of 2 years old).[6] This is part of the reason why advertisers and marketers target children from the earliest stages of their lives, essentially transforming them into young consumers. Moreover, the digital environment, in which children spend a lot of their time,[7] is increasingly permeated with sophisticated and personalised forms of advertising.[8] Increased computing capabilities allow commercial entities to track children's online behaviour and preferences, on the basis of which they are then profiled and targeted with tailored marketing campaigns.[9] While the advertising industry argues that personalised advertising (eg online behavioural advertising or location-based advertising) is more relevant and efficient[10], the tracking, profiling and targeting of children may raise significant questions from a children's rights perspective.

---

[5] Veroline Cauberghe and others, 'Reclamewijsheid Bij Kinderen En Jongeren: Onderzoeksrapport in Opdracht van Vlaams Ministerie van Cultuur, Jeugd, Sport En Media' (2012) <https://biblio.ugent.be/publication/4130480/file/4130494>; Esther Rozendaal and others, 'Reconsidering Advertising Literacy as a Defense Against Advertising Effects' (2011) 14 Media Psychology 333.

[6] Gunter (n 4) 2; Liselot Hudders and others, 'Shedding New Light on How Advertising Literacy Can Affect Children's Processing of Embedded Advertising Formats: A Future Research Agenda' (2017) 46 Journal of Advertising 333.

[7] Stéphane Chaudron and others, *Young Children (0-8) and Digital Technology: A Qualitative Exploratory Study across Seven Countries.* (Publications Office 2015) <http://dx.publications.europa.eu/10.2788/00749>; Sonia Livingstone, John Carr and Jasmina Byrne, 'One in Three: Internet Governance and Children's Rights' (Centre for International Governance Innovation and the Royal Institute of International Affairs 2015) 22 <https://www.cigionline.org/publications/one-three-internet-governance-and-childrens-rights>.

[8] Valerie Verdoodt, Damian Clifford and Eva Lievens, 'Toying with Children's Emotions, the New Game in Town? The Legality of Advergames in the EU' (2016) 32 Computer Law & Security Review 599.

[9] Amanda Lenhart and Mary Madden, 'Teens, Privacy and Online Social Networks' <http://www.pewinternet.org/2007/04/18/teens-privacy-and-online-social-networks/>.

[10] Howard Beales, 'The Value of Behavioral Targeting' (2010) 1 Network Advertising Initiative <https://pdfs.semanticscholar.org/e2eb/6726f5a29d9c14dafaf056be9a3ade877b0a.pdf>. Sophie C Boerman, Sanne Kruikemeier and Frederik J Zuiderveen

This chapter analyses how these personalised advertising practices are currently regulated, while looking through the lens of the children's rights framework. In the first section, targeted and personalised advertising is conceptualised, and the potential impact thereof on children's advertising literacy is discussed. Secondly, the regulatory framework that is relevant for such types of advertising is mapped. Ultimately, the chapter questions how the regulatory framework may contribute to the reconciliation of the different interests of children and advertisers in the digital environment.

1.1. Tracking, profiling and targeting: three different steps

Before personalised advertisements are targeted at children, a chain of events takes place.

First, children's personal data are collected, on the basis of which the commercial message may be tailored. For instance, for online behavioural advertising[11] – a specific form of personalised advertising – this would be the tracking or monitoring of children's online behaviour.[12] It may consist *inter alia* of tracking their search history, media consumption (eg videos, songs, news articles) and communication data.[13] The majority of existing online tracking technologies is based on cookies, or use cookies as the backbone.[14] KOSTA

Borgesius, 'Online Behavioral Advertising: A Literature Review and Research Agenda' (2017) 46 Journal of Advertising 363.

[11] Boerman and others define online behavioural advertising as: "*the practice of monitoring people's online behaviour and using the collected information to show people individually targeted advertisements*". Boerman, Kruikemeier and Zuiderveen Borgesius (n 10). According to the IAB Europe Framework, OBA is "*the collection of data from a particular computer or device regarding web viewing behaviours over time and across multiple web domains not under common control for the purpose of using such data to predict web user preferences or interests to deliver online advertising to that particular computer or device based on the preferences or interests inferred from such web viewing behaviours*." See also: Article 29 Data Protection Working Party, 'Opinion 2/2010 on Online Behavioural Advertising WP 171' (2010) <http://ec.europa.eu/justice_home/fsj/privacy/index_en.htm>.

[12] Other forms include location-based advertising or for instance social ads including friends' names, or advertising based on other elements such as a person's age, sex, etc.

[13] Frederik J Zuiderveen Borgesius, 'Mensen Aanwijzen Maar Niet Bij Naam Noemen: Behavioural Targeting, Persoonsgegevens En de Nieuwe Privacyverordening' (2016) Tijdschrift voor Consumentenrecht en handelspraktijken <https://www.ivir.nl/publicaties/download/1786>.

[14] Georgia Skouma and Laura Léonard, 'On-Line Behavioral Tracking: What May Change after the Legal Reform on Personal Data Protection', *Reforming European Data*

clarifies that cookies are files that contain certain information on specific users and their interests and preferences.[15] The information is transmitted via the cookie from a server to the web browser of the user and back each time the user accesses a server's page using the same browser. As a result, KOSTA explains, the website 'knows' what language or the type of advertising specified users prefer.[16] Other popular technologies include plugins and device fingerprinting.[17] In 2015, an international network of data protection authorities conducted a privacy sweep of 1494 children's websites and apps, which showed that 67% of the websites and apps were in fact collecting children's personal data and 50% shared this personal data with third parties.[18]

A second step that forms part of the serving of personalised advertising consists of profiling. Profiling can be understood as a data mining method, which involves data harvesting and conversion of data into profiles. More specifically, BOSCO et al. describe profiling as an (semi-)automated process to examine large data sets in order to create classes or categories of characteristics.[19] The categories can be used to generate profiles (ie sets of correlated data) of *inter alia* individuals, groups or places. Subsequently, statistical methods can be used to generate analytical information regarding future trends or to predict future behaviours or developments. In other words, profiling transforms data into a new form of knowledge, by identifying patterns that are invisible to the human eye.[20] A similar definition was adopted in the Recommendation

Protection Law (Springer 2015); Frederik J Zuiderveen Borgesius, 'Personal Data Processing for Behavioural Targeting: Which Legal Basis?' (2015) 5 International Data Privacy Law 163; E Kosta, 'Peeking into the Cookie Jar: The European Approach towards the Regulation of Cookies' (2013) 21 International Journal of Law and Information Technology 380.

[15] Kosta (n 14).

[16] ibid.

[17] Ibrahim Altaweel, Nathan Good and Chris Jay Hoofnagle, 'Web Privacy Census' [2015] Technology Science <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2703814>.

[18] Global Privacy Enforcement Network, 'Children's Privacy Sweep' (2015) <http://194.242.234.211/documents/10160/0/GPEN+Privacy+Sweep+2015.pdf>.

[19] Francesca Bosco and others, 'Profiling Technologies and Fundamental Rights and Values: Regulatory Challenges and Perspectives from European Data Protection Authorities', *Reforming European Data Protection Law* (Springer 2015) 4.

[20] Mireille Hildebrandt, 'Profiling: From Data to Knowledge' (2006) 30 Datenschutz und Datensicherheit-DuD 548; Claude Castelluccia, 'Behavioural Tracking on the Internet: A Technical Perspective' in Serge Gutwirth and others (eds), *European Data*

of the Committee of Ministers of the Council of Europe on the protection of individuals with regard to automatic processing of personal data in the context of profiling.[21] According to that Recommendation, profiling is an automatic data processing technique that consists of applying a 'profile' to an individual, particularly in order to take decisions concerning her or him or for analysing or predicting her or his personal preferences, behaviours and attitudes.[22] This Recommendation specifies that profiling entails that data on individual behaviour or characteristics is collected, which is analysed to correlate certain behaviour(al characteristics), and then the correlation is applied to an identified or identifiable person in order to deduct previous, current or future characteristics.

Third, on the basis of a specific consumer profile, advertisers tailor their commercial messages to have a more persuasive effect. Messages are targeted at persons, including children, who have been profiled as potentially interested in or receptive to the products or services that are promoted.

1.2. Persuasive tactics and the impact on children's advertising literacy skills

It has been argued that personalised advertising techniques allow a more effective transmission of the commercial message, as advertisers can respond explicitly to a specific user's developmental level and knowledge base.[23] This is a distinct advantage when it comes to building a strong and lasting personal interaction and connection with the child consumer. Indeed, studies have shown that commercial messages that correspond with the interests and behaviour of consumers will lead to a more positive brand attitude, as the message is perceived as less instrusive, more relevant and useful, ultimately increasing consumers' purchase intentions.[24] In addition, YAN et al. found that

Protection: In Good Health? (Springer Netherlands 2012) <http://www.springerlink.com/index/10.1007/978-94-007-2903-2_2>.

[21] Council of Europe, *The Protection of Individuals with Regard to Automatic Processing of Personal Data in the Context of Profiling, Recommendation CM/Rec(2010)13 and Explanatory Memorandum* (Council of Europe 2010).

[22] ibid.

[23] Sandra L Calvert, 'Children as Consumers: Advertising and Marketing' (2008) The Future of Children 205; Cauberghe and others (n 5).

[24] Laura F Bright and Terry Daugherty, 'Does Customization Impact Advertising Effectiveness? An Exploratory Study of Consumer Perceptions of Advertising in Customized Online Environments' (2012) 18 Journal of Marketing Communications 19; Anindya Ghose and Sha Yang, 'An Empirical Analysis of Search Engine Advertising:

the click-through rates of advertisements employing behavioral targeting techniques increased enormously.[25] However, regardless of the effectiveness of such techniques, other important considerations should be taken into account when deciding whether it is fair that advertisers target children with this type of advertising.

First, the tracking of consumers' online information and activities often happens covertly. BOERMAN et al. argue that this covertness may be harmful as well as unethical, since consumers are not aware of the persuasive techniques used.[26] Furthermore, although the advertising sector has rapidly adopted personalisation techniques, research on the effects thereof on children's advertising literacy remains scarce.[27] DE PAUW ET AL. recently found that while children between 9 and 11 recognised a personalised advertisement (not integrated in the media content), few of them immediately understood that the advertisement was based on previous browsing behaviour. In general, children's commercial literacy increases gradually as they get older. For instance, research has shown that children between 12 and 16 years old have less knowledge of social media advertising and are less critical than youngsters above 16 years.[28] However, studies on personalised advertising and adolescents, a group of avid social media users who are frequently exposed to such advertising, paint an interesting picture. The level of personalisation of advertising may be different depending on the types and amount of personal data used.[29] If the level of personalisation of a commercial message is too

Sponsored Search in Electronic Markets' (2009) 55 Management Science 1605; Robert S Moore, Claire Allison Stammerjohan and Robin A Coulter, 'Banner Advertiser-Web Site Context Congruity And Color Effects On Attention And Attitudes' (2005) 34 Journal of Advertising 71.

[25] Jun Yan and others, 'How Much Can Behavioral Targeting Help Online Advertising?', *Proceedings of the 18th international conference on World wide web* (ACM 2009). <http://dl.acm.org/citation.cfm?id=1526745>; Pieter De Pauw and others, 'From Persuasive Messages to Tactics: Exploring Children's Knowledge and Judgement of New Advertising Formats' (2017) New Media & Soceity 1.

[26] Boerman, Kruikemeier and Zuiderveen Borgesius (n 10).

[27] Brahim Zarouali and others, '"Do You like Cookies?" Adolescents' Skeptical Processing of Retargeted Facebook-Ads and the Moderating Role of Privacy Concern and a Textual Debriefing' (2017) 69 Computers in Human Behavior 157

[28] Cauberghe and others (n 5).

[29] Boerman, Kruikemeier and Zuiderveen Borgesius (n 10).

high, consumers may view this as a breach of their privacy.[30] ZAROUALI et al. confirmed this in a recent study on the impact of retargeting on adolescents.[31] First, the direct effect of retargeted advertising on adolescents' purchase intention was indeed higher than for non-retargeted advertising, meaning that in general adolescents responded quite favourably to this advertising technique. However, the study also found that a retargeted ad indirectly leads to a negative effect on the purchase intention when adolescents are made aware that their personal information was being used to target the commercial message at them. In other words, personalisation techniques may also trigger skepticism and privacy concerns. In addition, ongoing research by ZAROUALI et al. uncovered rather worrying findings about adolescents' understanding of personalised advertising techniques employed in social media. Preliminary results of the study show that although the level of advertising literacy of children for these techniques gradually increases when they get older, almost half of 17 year olds have a really low understanding of persuasion tactics.[32]

1.3. **Balancing children's and advertisers' interests**

In the context of personalised advertising, several children's rights are at stake. The largely opaque practices and techniques employed, paired with children's low level of advertising literacy vis-à-vis personalised advertising most importantly affects children's right to development (article 6 United Nations Convention on the Rights of the Child; UNCRC), right to privacy (article 16 UNCRC) and right to protection against economic exploitation (article 32 UNCRC). In addition, article 3 UNCRC states that in all actions concerning children their best interests should be the primary consideration (article 3 UNCRC).[33] In other words, this principle requires governments, public and private bodies to conduct child impact assessments and evaluate the impact of any proposed law, policy or decision on children's rights.[34] The first paragraph of article 3 UNCRC seems to indicate that the best interests of a child

[30] Marjolijn L. Anteunis and Guda Van Noort, 'Interactivity effects in social media marketing on brand engagement: an investigation of underlying mechanisms' (2011) The 10th ICORIA 2011 Berlin: June 23rd-25th 2011: conference programme.

[31] Zarouali and others (n 27).

[32] Brahim Zarouali and others, 'Adolescents' advertising competences and institutional privacy protection strategies on social networking sites: Implications for regulation' (Forthcoming) AdLit Project.

[33] General UN Committee on the Rights of the Child, 'General Comment No. 5 (2003) General Measures of Implementation of the Convention on the Rights of the Child (arts 4, 42 and 44, para 6)' (2003) para 45.

[34] ibid.

must be assessed inividually. However, in many decisions related to the digital environment this is not what happens in practice.[35] For instance, when setting an age threshold from which a child can consent with the processing of his or her personal data in the context of information society services (infra), rather than an individual assessment, the best interests of children as a group or in general are at the centre of the consideration. The principle also requires that States must ensure that the best interests of the child are taken as a primary consideration in decisions and actions undertaken by the private sector. In the context of personalised advertising, this could be interpreted as requiring that the parties involved in the advertising chain must consider the best interests of children when profiling children, and tailoring and targeting their advertisements to this particular group of consumers.

From the perspective of the rights to development, privacy and protection from economic exploitation, it is important to acknowledge that children often do not grasp the scope of underlying data processing activities and business models of online actors.[36] Moreover, research has shown that children generally consider themselves as having a right to privacy online from their parents or peers (ie social privacy), but do not understand that their privacy may also be infringed upon by (State or) commercial actors.[37] The right to privacy also has an important participatory dimension for children, as it is essential for their individual autonomy and self-determination, and a precondition of participation. It is important to realise that personalised advertising has the capacity not only to compartmentalise children, but also to shape their preferences and interests accordingly, ultimately affecting their autonomy and development. In this regard, SAVIRIMUTHU warns that the increased

[35] Eva Lievens and others, 'Children's Rights and Digital Technologies', in Ursula Kilkelly and Ton Liefaard (eds), *International Children's Rights Law* (Springer 2018) (forthcoming).

[36] According to the OECD for example, children lack the awareness and capacity to foresee the potential long-term privacy consequences of the disclosure of their personal data online. OECD, 'The Protection of Children Online - Recommendation of the OECD Council, Report on Risks Faced by Children Online and Policies to Protect Them' (2012).

[37] Lievens and others (n 35); Ofcom Office of Communications, 'Social Networking A Quantitative and Qualitative Research Report into Attitudes, Behaviours and Use' (Ofcom Office of Communications 2008).

role of algorithms in defining children's consumer experience should not disregard the value of a child's emotional space, which should not be subject to the inside the box-thinking that underpins profiling-based decisions. [38]

These considerations should be offset against the fact that advertising revenue allows for the development of children's media content and digital platforms. At the moment, the dominant business model for online services remains advertising-based. Users often do not have to pay for the services, but in exchange personal information is collected and advertisements are part of the environment. As such, the creation of content and online spaces enables the exercise of other children's rights, including *inter alia* their right to information, to access and to participation in digital media. Moreover, for children to grow up to be critical, informed consumers, within these spaces they should have the opportunity to develop and practice advertising literacy skills which are needed to make balanced commercial decisions. The regulatory framework in place, encompassing both self-regulation and legislation, should enable the reconciliation of the interests of children and advertisers in relation to personalised advertising.

2. PERSONALISED ADVERTISING IN THE CURRENT REGULATORY FRAMEWORK

2.1. Collecting and processing of children's personal data under the GDPR and the proposed ePrivacy Regulation

At the EU level, the collection and processing of children's data is covered by the General Data Protection Regulation ("GDPR") [39] and the ePrivacy Directive (infra). The GDPR, which was adopted by the European Union Parliament and Council on 27 April 2016, and will be applicable as of 25 May

[38] Joseph Savirimuthu, 'Unfair Commercial Practies, the Consumer Child and New Technologies: What Should We Regulate? Some Policy Provocations' (2014) <https://www.liverpool.ac.uk/media/livacuk/law/european-childrens-rights-unit/BriefingNote.pdf>.

[39] Parliament and Council Regulation (EU) 2016/679 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L119/1.

2018,[40] applies to (most often fully or partially automated)[41] processing[42] of personal data[43] (Article 2 GDPR). This revised regulatory framework is underpinned by the idea that individuals should have control of their own personal data.[44] The GDPR pays particular attention to children and acknowledges that they merit 'specific protection' regarding their personal data. This is because children are less aware of the risks and the consequences of the processing of their personal data on their rights.[45] Moreover, the GDPR recognises that the processing of children's personal data may result in risks to their rights and freedoms.[46] Specific protection should be awarded to children especially when their personal data is processed in the context of marketing and profiling, or in relation to services offered directly to a child.[47] Ad-

[40] Until then the Data Protection Directive (Parliament and Council Directive 95/46/EC of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1995] OJ L281/31) remains applicable.

[41] As well as to '*processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system*' (art 2 GDPR).

[42] Processing is '*any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction*' (art 4(2) GPDR).

[43] Personal data is '*any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person*' (art 4 (1) GDPR).

[44] Recital 7 GDPR.

[45] Recital 38 GDPR.

[46] Recital 75 GDPR.

[47] Recital 38 GDPR.

vertisers that want to process children's personal data for the delivery of personalised advertising[48] will have to comply with the principles and requirements[49] for data controllers[50] and the specific protection for children in the GDPR. One of these requirements entails that personal data may only be processed to the extent that there is a 'legitimate ground' justifying the processing.[51] In the context of personalised advertising, the consent of the data subject[52] or the legitimate interest of the controller are possible legitimation grounds. If the former is relied upon as a legitimate ground for processing children's personal data, article 8 of the GDPR requires verifiable parental consent for the processing of personal data of children under 16 (or lower[53]) in the context of 'information society services'[54] directly offered to a child.[55] Regarding the latter ground, recital 47 GDPR specifies that 'direct marketing'

---

[48] It has been argued by behavioural targeting companies that, as long as they do not tie names to data they hold about individuals, they do not process any personal data, and that, therefore, the data protection framework does not apply to them. Zuiderveen Borgesius, however, argues that when data is used to single out an individual to target him or her with tailored advertising, the data protection legislation should apply: Zuiderveen Borgesius (n 13).

[49] This includes inter alia the principles of fairness, transparency, data minimisation, accuracy, purpose limitation, storage limitation, but also obligations with regard to data subjects' rights. For a comprehensive overview see Brendan Van Alsenoy, 'Regulating Data Protection: The Allocation of Responsibility and Risk among Actors Involved in Personal Data Processing' (2016) <https://lirias.kuleuven.be/handle/123456789/545027>.

[50] A data controller is the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; Art 4 (8) GDPR.

[51] Art 6 GDPR.

[52] The consent has to be freely given, specific, informed and unambiguous. The definition of consent can be found in recital 32 GDPR and article 4 (11) GDPR.

[53] Member States may lower this threshold to a minimum of 13 years. For a mapping of the recent national guidance and proposals in this context, see Eva Lievens and Ingrida Milkaite, 'Better Internet for Kids - Age of Consent in the GDPR: Updated Mapping' <https://www.betterinternetforkids.eu/web/portal/practice/awareness/detail?articleId=2019355>.

[54] Information society services (eg social media, search engines, apps) often rely on personalised advertising as an essential element of their business model.

[55] For more information see Eva Lievens and Valerie Verdoodt, 'Looking for Needles in a Haystack: Key Children's Rights Issues in the General Data Protection Regulation' [2017] Computer Law & Security Review.

may constitute a legitimate interest for the controller and hence offer a legitimation ground other than the consent of the data subject.[56] This, however, must entail a careful balancing of the legitimate interest of the controller against the interests, fundamental rights and freedoms of children.[57] If children are involved, the GDPR clarifies that their interests may override those of the controller more easily, implying a heavier responsibility for controllers using this ground for processing (Article 6, 1) (f) GDPR). Yet, in relation to direct marketing it has been argued by the Belgian Privacy Commission that obtaining consent remains a best practice.[58] Also in relation to online behavioural advertising it has been argued by scholars that consent is the only appropriate legitimation ground.[59]

The ePrivacy Directive[60] contains rules for the processing of personal data in the electronic communication sector and the free movement of such data and of electronic communication equipment and services.[61] As such, it forms an additional layer of protection, complementing[62] the GDPR. At the moment,

---

[56] Recital 47 GDPR.

[57] In this regard, Macenaite and Kosta argue that this processing ground potentially protects children more than relying on consent, should data controllers fully consider all factors of data processing and ensure children's interests and fundamental rights are duly taken into account. Milda Macenaite and Eleni Kosta, 'Consent for Processing Children's Personal Data in the EU: Following in US Footsteps?' (2017) 26 Information & Communications Technology Law 146.

[58] Belgian Privacy Commission, 'Recommendation No. 02/2013 of 30 January 2013 Regarding Direct Marketing and the Protection of Personal Data' (2013) <https://www.privacycommission.be/sites/privacycommission/files/documents/aanbeveling_02_2013.pdf> 12.

[59] Zuiderveen Borgesius (n 14).

[60] Parliament and Council Directive 2002/58/EC of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) [2002] OJ L201/37, which was amended in 2009 by the Parliament and Council Directive 2009/136/EC of 25 November 2009 amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws [2009] OJ L337/11 (hereafter the ePrivacy Directive).

[61] Recital 24 ePrivacy Directive: 'any information' that is stored on the terminal equipment of a user, rather than personal data.

[62] It is a lex specialis to the GDPR and as such complements it.

the current ePrivacy Directive, which already covers popular tracking technologies such as cookies[63], is under review. In January 2017, the European Commission launched its proposal for an ePrivacy Regulation,[64] which is set to replace the ePrivacy Directive and align the rules for electronic communications with the new standards of the GDPR.[65] The proposed Regulation significantly expands its scope of application, *inter alia* by explicitly including Over-the-Top communications services or 'OTTs' (ie online services that could to a certain extent substitute traditional media and telecom services, such as Skype, WhatsApp, Facebook Messenger).[66] It also brings about important changes for the players involved in targeted advertising, by requiring the same type of consent as in the GDPR for the placement and accessing of cookies or the use of other tracking technologies (eg device finger printing).[67] According to the most recent draft legislative resolution of the European Parliament, users need to be provided with granular settings for consent, distinguishing between different categories: (1) tracking for commercial purposes or for direct marketing for non-commercial purposes (eg behavioural adver-

[63] Article 5(3) of the Directive provides that the installation of and access to cookies on users' terminal equipment (eg smartphones, laptops) is only allowed with their consent, except for 'functional cookies' or 'similar technologies'.

[64] Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications) 2017.

[65] The European Commission hopes to finalise the Regulation by the 25th of May 2018, when the GDPR becomes applicable. The draft proposal was discussed and voted by the LIBE committee of the European Parliament (EP) in October 2017.

[66] Regarding territorial scope, it does not only envisage entities in the EU, but any electronic communication service provided to end-users within the EU and devices located in the EU, regardless of the service provider's location.

[67] Art 7(4) of the GDPR requires consent to be 'freely given, specific, informed and unambiguous' and must be expressed by way of a 'statement or by a clear affirmative action.' Recital 20 of the Parliament's draft legislative resolution requires in relation to tracking that "*users should receive all information about the intended processing in clear and easily understandable language*." European Parliament, Draft legislative resolution on the proposal for a regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications) (2017) <http://www.europarl.europa.eu/sides/getDoc.do?type=REPORT&reference=A8-2017-0324&language=EN> (hereafter 'EP Draft Legislative Resolution').

tising); (2) tracking for personalised content; (3) tracking for analytical purposes; (4) tracking of location data; (5) providing personal data to third parties (including providing unique identifiers to match with personal data held by third parties).[68] Furthermore, one of the amendments explicitly states that the regulation should prevent the use of tracking or cookie walls (ie a barrier that users can only pass if they consent to tracking by third parties)[69]. According to the EP, "*tracking walls do not help users to maintain control over their personal information and privacy or become informed about their rights*".[70]

Yet, whereas the GDPR explicitly recognises children as a vulnerable group of individuals that deserve specific protection when it comes to the processing of their personal data (supra), especially in the context of profiling and marketing, the original proposal for an ePrivacy Regulation contained no references to children.[71] However, as children are increasingly targeted directly by services tailored to a young audience it would make sense to align the proposed Regulation with the GDPR, by recognising that children need specific protection when it comes to the processing of their communications data. As mentioned above, research has shown that children have little or no understanding of and knowledge about the tracking technologies used and the extent and sensitivity of the data collected for personalised advertising.[72] These findings resonate in the viewpoint of the Article 29 Working Party, who argued in 2013 that in the best interest of the child companies '*should not process children's personal data for behavioural advertising purposes, neither directly nor indirectly, as this will be outside the scope of a child's understanding and therefore exceed the boundaries of lawful processing'*.[73] Moreover, it has been argued in this context, for instance by BEUC, that specific limitations on

[68] Recital 23 EP Draft Legislative Resolution.

[69] Frederik J Zuiderveen Borgesius and others, 'Tracking Walls, Take-It-Or-Leave-It Choices, the GDPR, and the EPrivacy Regulation' (2017) 3 European Data Protection Law Review 353.

[70] Recital 22 EP Draft Legislative Resolution.

[71] Most notably, article 8 GDPR is not reflected in the proposal.

[72] This includes a reference to the specific standard of consent as introduced by art 8 GDPR.

[73] Article 29 Data Protection Working Party, 'Opinion 02/2013 on Apps on Smart Devices, WP202' (2013) <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp202_en.pdf>; Article 29 Data Protection Working Party, 'Opinion 2/2010 on Online Behavioural Advertising WP 171' (n 11).

the collection and use of children's communication data are needed.[74] In the Opinion of the Committee on the Internal Market and Consumer Protection,[75] these ideas were integrated in a proposal for a new recital 16a:

> Regulation (EU) 2016/679 of the European Parliament and of the Council explicitly recognises the need to provide additional protection to children, given that they may be less aware of the risks and consequences associated with the processing of their personal data. This Regulation should also grant special attention to the protection of children's privacy. They are among the most active internet users and their exposure to profiling and behaviourally targeted advertising techniques should be prohibited.

Parallel to the consideration included in recital 38 of the GDPR, a new recital 23a was proposed confirming the need for specific protection with regard to children's online privacy, as they are less aware of the risks and consequences associated to their online activities, as well as less aware of their rights. For that reason, the IMCO Opinion stresses that specific safeguards are necessary in relation to the use of children's data, notably for the purposes of marketing and the creation of personality or user profiles. As a result of these considerations, the Opinion proposed a new paragraph 1 to be added to article 6 asserting that

> Electronic communications data that is generated in the context of an electronic communications service designed particularly for children or directly targeted at children shall not be used for profiling or behaviourally targeted advertising purposes.

In addition, a new paragraph 4a to article 8 was proposed stating that '*[t]erminal equipment that is intended particularly for children's use shall implement specific measures to prevent access to the equipment's storage and processing capabilities for the purpose of profiling of its users or tracking their behaviour with commercial intent.*'

---

[74] Beuc, 'Data Collection, Targeting and Profiling of Consumers Online' (2010) <http://www.beuc.eu/publications/2010-00101-01-e.pdf>.

[75] European Parliament Committee on the Internal Market and Consumer Protection, Opinion on the proposal for a regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications) (2017) <http://www.europarl.europa.eu/sides/getDoc.do?type=REPORT&reference=A8-2017-0324&language=EN>.

However, in the end, these amendments, which would have had a significant impact on current advertising practices that target and personalise commercial messages to and for children, were not included in the EP's Draft Legislative Resolution.

In relation to the profiling of children, recital 75 GDPR states that processing personal data "in order to create or use personal profiles" may give rise to risks to the rights and freedoms of natural persons.[76] As profiling is a complex and 'invisible'[77] process, which is very difficult to understand for adults, let alone children, the GDPR did aim to introduce specific protection for children in relation to profiling.[78] First, it is recognised in recital 38 that circumstances in which personal data of children are processed in order to create personal or user profiles require extra protection. There is no further guidance, though, as to how this protection should be put into practice. In any case, data subjects must be informed about the fact that profiling is being deployed and the potential consequences thereof.[79] Especially when this occurs vis-à-vis children, the information provided will need to be clear and understandable for them.[80] In relation to profiling for direct marketing purposes, data subjects, including children, also have the right to object at any time to profiling to the extent that it is related to direct marketing.[81] The data controller needs to clearly and explicitly inform the data subject of this right.[82] Second, according to recital 71, a decision which may include a measure evaluating personal aspects relating to a data subject, which is based solely on automated processing and produces legal effect for or similarly significantly affects the data

[76] Recital 75 GDPR underlines that the processing of personal data may result in a risk to the rights and freedoms of natural persons, in particular "[…] where personal aspects are evaluated, in particular analysing or predicting aspects concerning performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements, *in order to create or use personal profiles*" (emphasis added by the authors).

[77] See the work of Esther Keymolen, who has coined the notion 'invisible visibility' in relation to online interactions: Esther Keymolen, *Trust on the Line: A Philosophical Exploration of Trust in the Networked Era* (Wolf Legal Publishers 2016); Esther Keymolen, 'Onzichtbare Zichtbaarheid. Helmuth Plessner Ontmoet Profiling' (2006).

[78] Lievens and Verdoodt (n 55).

[79] Recital 60 GDPR.

[80] Art 12 GDPR. Lievens and Verdoodt (n 55).

[81] Recital 70 and art 21, (2) GDPR.

[82] Recital 70 GDPR.

subject, should not concern children.[83] In its recent guidelines on automated individual decision-making and profiling, the Article 29 Working Party ("Working Party") confirms that there is no absolute prohibition on the profiling of children in the GDPR.[84] Indeed, the Working Party recognises that under certain circumstances it may be necessary for controllers to carry out such decision-making, for instance to protect children's welfare. Nevertheless, the Working Party stresses that targeted advertising may, depending on the particular characteristics of the case, have a 'similarly significant' effect on individuals. Factors that may influence the assessment thereof are, for instance, the intrusiveness of the profiling process, the expectation and wishes of the individuals concerned, the way the advert is delivered, or the particular vulnerabilities of the data subjects targeted. Especially in relation to children, the Working Party recognises that they "can be particularly susceptible in the online environment and more easily influenced by behavioural advertising" and, therefore, "organisations should, in general, refrain from profiling them for marketing purposes."[85] Interestingly, it should be noted that a 'child' is not defined in the GDPR. The question thus arises whether this statement by the Working Party refers to all under 18-year olds. The same observation can be made in relation to the EP draft legislative resolution on the e-Privacy Regulation.

From a children's rights perspective, a number of crucial concerns arise with regard to the rules on the profiling of children. It has been argued that profiling children may restrict their right to privacy, as well as their right to development.[86] According to ARIELY and BERNS, the creation of profiles may negatively impact children's development, as the collection and use of personal data for the purpose of profiling may undermine children's rights to experiment with and critically reflect upon their interactions.[87] In that regard, the

---

[83] Recital 71, first paragraph, final sentence GDPR.

[84] However, the Working Party recommends data controllers not to rely upon the exceptions in Article 22 (2) GDPR to justify such profiling (ie necessary for the performance of a contract, authorised by law, consent of the data subject). Article 29 Data Protection Working Party, 'Guidelines on Automated Individual Decision-Making and Profiling for the Purposes of Regulation 2016/679' (2017).

[85] ibid 26.

[86] Lievens and Verdoodt (n 55).

[87] Dan Ariely and Gregory S Berns, 'Neuromarketing: The Hope and Hype of Neuroimaging in Business' (2010) 11 Nature Reviews Neuroscience 284; also cited by Savirimuthu (n 38).

lack of control by children over their personal data may harm their capacities to develop, get to know and experiment with their own identity.[88]

2.2. Personalised advertising in the Unfair Commercial Practices Directive?

Another layer of protection for children in the context of personalised advertising may be found in EU legislation on unfair commercial practices (ie the Unfair Commercial Practices Directive, "UCP Directive").[89] Aside from protections against misleading advertising[90], the UCP Directive protects consumers against so-called 'aggressive' commercial practices. Marketing techniques are deemed aggressive if they "*by harassment, coercion or undue influence significantly impair the freedom of choice or conduct of the average consumer*".[91] While actual harassment or coercion (eg the use of physical force) can hardly be argued to occur in the context of personalised advertising, undue influence could perhaps arise. Article 2 (j) of the UCP Directive specifies that undue influence means "*exploiting a position of power in relation to the consumer so as to apply pressure, even without using or threatening to use physical force, in a way which significantly limits the consumer's ability to make an informed decision*". In this regard, the European Consumer Organisation (BEUC) has argued that advertisers hold a position of power as they collect a lot of personal information of consumers (including children) without them being aware of what is happening.[92] Moreover, the repetitive aspect of behavioural advertising (eg through retargeting on social media) may put pressure on children, while the selection of advertising based on the presumed consumer choice may prevent the display of other advertisements thereby restricting the comparison with other advertisements and, hence, making an informed commercial decision.[93] The qualification of 'undue influence' will depend on the specificities of the particular case, and when children are involved, their vulnerability should be taken into account.[94]

---

[88] ibid.

[89] Verdoodt, Clifford and Lievens (n 8) 599.

[90] For a clear overview see ibid.

[91] Art 8 UCPD.

[92] Beuc (n 74) 6.

[93] ibid.

[94] Forbrugerombudsmanden, 'Guidance on Children, Young People and Marketing' (2014) <https://www.consumerombudsman.dk/media/14560/guidance-on-children-young-people-and-marketing.pdf>.

3. SELF-REGULATION AND TARGETING CHILDREN WITH PERSONALISED ADVERTISING

In addition to existing legislation that is relevant to certain forms of advertising, there is a strong tradition of self-regulation[95] in the advertising sector. At international, European and national level, advertisers have committed to observing certain standards that are often laid down in codes of conduct, which are enforced by self-regulatory bodies.[96] Such codes of conduct also contain provisions in relation to advertising aimed at children, direct marketing and behavioural advertising.

Section D7.4 of the ICC Consolidated Code,[97] for instance, states that children of 12 years and younger should not be targeted by a behavioural advertising campaign. Along the same lines, in the Framework for OBA,[98] created by the Interactive Advertising Bureau Europe (IAB Europe), companies agree not to create segments for OBA purposes that are specifically designed to target children, meaning people age 12 and under.[99] This Framework is also guiding

---

[95] Self-regulation entails the creation, implementation and enforcement of rules by a group of actors, industry in particular, with minimal or no intervention by the state; Eva Lievens, *Protecting Children in the Digital Era: The Use of Alternative Regulatory Instruments* (Brill 2010).

[96] It has been argued before that drawbacks of self-regulation are a lack of effective enforcement and often mild sanctions; however, the advertising sector is one of the sectors where – depending on the self-regulatory body in question – decisions on violations of the codes of conduct are often complied with. See Eva Lievens, 'Is Self-Regulation Failing Children and Young People? Assessing the Use of Alternative Regulatory Instruments in the Area of Social Networks', in Seamus Simpson and others (eds), *European media policy for the twenty-first century: Assessing the past, setting agendas for the future* (Routledge 2016).

[97] International Chamber of Commerce, 'Advertising and Marketing Communication Practice Consolidated ICC Code' <https://cdn.iccwbo.org/content/uploads/sites/3/2011/08/ICC-Consolidated-Code-of-Advertising-and-Marketing-2011-English.pdf>.

[98] The IAB Europe is a European business organisation that develops industry standards, offers legal advice, education and training and conducts research for the European digital advertising industry. The Framework is self-regulatory and creates obligations for any of the members that self-certify their compliance with the principles: <https://www.iabeurope.eu/policy/iab-europe-eu-framework-for-online-behavioural-advertising/>.

[99] The framework also contains obligation related to notice and choice, including the principles that internet users must be given notice of the OBA data collection and use practices by the relevant third parties as well as the website operator (ie of its OBA arrangements with third parties), and that third parties have to provide internet users

the activities of the European Interactive Digital Advertising Alliance, which has been set up by a coalition of the European advertising industry, including advertisers, the advertising agency sector, the direct marketing sector, the advertising network sector and the media sector. Its main objective is to licence the "Online Behavioural Advertising Icon" to companies that are involved in the OBA business across Europe. This icon notifies consumers of data collection for OBA purposes and the delivery of OBA advertising to them, and refers consumers to an online portal: 'www.youronlinechoices.eu', which intends to offer information on the practice of OBA and where consumers can turn off OBA by some or all companies.[100] Research into the effectiveness of the OBA icon, however, has found that only one-quarter of the respondents remembered OBA disclosure icons, and only 12% remembered seeing a tagline (eg, "Why did I get this ad?" or "AdChoices") and correctly selected the tagline they had seen from a list. Also, none of the taglines were understood to be links to pages where you can make choices about OBA, nor did they increase knowledge about OBA.[101] However, it has been argued that the standard icon could effectively increase OBA awareness and understanding when

with a mechanism to exercise their choice regarding the use of their data for OBA purposes. It has been argued, for instance, by King and Jensen that in general the IAB principles do not offer consumers sufficient transparency nor do they ensure meaningful access to the information contained in the consumer profiles that are used for behavioral advertising purposes; Nancy King and Pernille Wegener Jessen, 'Profiling the Mobile Customer – Is Industry Self-Regulation Adequate to Protect Consumer Privacy When Behavioural Advertisers Target Mobile Phones? – Part II' (2010) 26 Computer Law & Security Review 595.

[100] When accessing the portal, the user will be asked to select his or her location. The user must then navigate to "Your Ad Choices", at which point the site collects the users' "status" from the participating companies. Once complete, the individuals can either "turn off" individual companies one by one or scroll down to the setting "turn off all companies". Brendan Van Alsenoy and others, 'From Social Media Service to Advertising Network - A Critical Analysis of Facebook's Revised Policies and Terms' <https://www.law.kuleuven.be/citip/en/news/item/facebooks-revised-policies-and-terms-v1-2.pdf>. However, according to the Article 29 Data Protection Working Party, such an opt-out approach "is not an adequate mechanism to obtain average users informed consent" for purposes of online behavioural advertising. Article 29 Data Protection Working Party (n 11) 15.

[101] Boerman, Kruikemeier and Zuiderveen Borgesius (n 10).

accompanied by an explanatory label stating, "This ad is based on your surfing behavior".[102] It remains to be seen whether this finding is also valid vis-à-vis children.

With regard to direct marketing, the Federation of European Direct Marketing (FEDMA), an organisation representing the Direct and Interactive Marketing sector at the European Level, has adopted a Code of Practice for the Use of Personal Data in Direct Marketing.[103] According to the FEDMA Code, direct marketing is to be understood as: *"the communication by whatever means (including but not limited to mail, fax, telephone, on-line services etc...) of any advertising or marketing material, which is carried out by the Direct Marketer itself or on its behalf and which is directed to particular individuals".*[104] The Code contains, general principles on data protection applied to direct marketing, but also specific provisions that apply to the processing of children's personal data. The Code defines children as "*any individual aged under 14 years old unless otherwise defined in national legislation/self-regulation*". Direct marketers that collect children's personal data are required to make 'every reasonable effort' to ensure that the concerned child and/or the parent are properly informed about the purpose(s) for processing the data. Such a notice should be prominent, readily accessible and understandable by children. Direct marketers also have to obtain parental consent prior to the processing of the data, in accordance with applicable laws and self-regulation. Furthermore, they do not only have to obtain parental consent, but they also have to use every reasonable endeavour to verify whether the consent was actually given by the parent of the concerned child (and for instance not by the child himself). According to the Code, parents should be able to exercise their children's rights as data subjects. More specifically these rights are (in line with EU data protection legislation) the right to object to the processing of their child's data or to the disclosure of that data to a third party, the right to access and rectification or deletion of the data in case the processing does not comply with applicable data protection legislation. Finally, in relation to

---

[102] Guda van Noort, Edith G Smit and Hilde AM Voorveld, 'The Online Behavioural Advertising Icon: Two User Studies', *Advances in Advertising Research (vol IV)* (Springer 2013), 365.

[103] The Code was drafted in collaboration with the Article 29 Working Party; see Article 29 Data Protection Working Party, 'Opinion 4/2010 on the European Code of Conduct of FEDMA for the Use of Personal Data in Direct Marketing, WP 174' (2010) <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2010/wp174_en.pdf>.

[104] Please note that this not necessarily means that the commercial message is also personalised.

games, direct marketers should not demand more personal data than is strictly necessary when children want to participate in a game, when they may receive a prize or in relation to any other activity involving a promotional benefit.

Complementary to the provisions of the Code of Practice, FEDMA also adopted an Electronic Communications Annex that contains provisions specifically applicable to online direct marketing (or electronic mail marketing).[105] According to this annex, direct marketers who want to process children's data will have to inform them about the processing. This information has to be expressed in easily understandable language. Moreover, direct marketers will have to obtain prior parental consent for the processing of personal data of children who have not yet reached the age required by law to give their consent. Important to note is that parents may withdraw their consent at any point in time. Direct marketers are also required to have an age verification mechanism in place. The mechanism should be able to guarantee that the age of the child as well as the authenticity of the parental consent has been effectively checked. The Annex does not provide any further guidance regarding the type of mechanism, but merely requires that direct marketers use 'reasonable efforts'. Furthermore, the Annex contains certain limitations direct marketers need to keep in mind:

- Data of family members: These data cannot be collected from the child, without the permission of the person to whom the data refer.[106]
- Sensitive data[107]: Direct marketers may not invite children to share this type of data without the prior consent of their legal representative.
- Incentivise children to share more data: Direct marketers may not incentivise children to provide their own personal data or personal data of a

[105] FEDMA, 'European Code of Practice for the Use of Personal Data in Direct Marketing - Electronic Communications Annex (the On-Line Annex)' <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2010/wp174_annex_en.pdf>.

[106] Nevertheless, data regarding the identity and address of the parent or legal representative may still be processed for authorisation and verification purposes. FEDMA (n 105).

[107] Sensitive data are data revealing the racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, or the processing of data concerning health or sex life of the child, as well as the financial situation of the child or any third party such as their friends or family. FEDMA (n 105).

third party for marketing purposes, in exchange for a material or virtual reward.[108]

4. RECONCILING CHILDREN'S AND ADVERTISERS' (BEST) INTERESTS

The digital advertising industry undoubtedly plays an important part in the creation and maintenance of content, services and digital spaces for children. The sophistication and opaqueness of today's tracking, profiling and targeting practices, however, make it difficult for children to make carefully considered and critical commercial decisions or decisions concerning their privacy and personal data, and as such, raise issues related to their rights to development, privacy and protection against economic exploitation. The current regulatory framework provides for certain specific protections for children in this context. However, this chapter questioned whether this framework is appropriate for reconciling the interests of advertisers and children. While the current data protection and privacy laws and policies cover existing tracking, profiling and targeted advertising practices, certain improvements may be proposed.

First, the GDPR foresees in specific protection for children, which is laudable, but it remains problematic that the text does not contain a definition of a 'child'. This leads to uncertainty regarding the age group(s) to which certain protection measures should apply. This could be clarified by data protection authorities and the Article 29 Working Party or the European Data Protection Board. Furthermore, aside from refraining from profiling children for marketing purposes, general default limitations on the collection of personal data of children should be considered.[109] In this regard, data controllers, also in the advertising sector, should take up their responsibility, and carry out an in-depth data protection impact assessment,[110] with attention for the best interests and rights of children, when setting up digital marketing campaigns. The age and level of maturity of the child will also play an important role in such an assessment.

---

[108] This includes invitations to provide personal data in order to be able to participate in a game of chance, tombola or lottery. FEDMA (n 105).

[109] Kathryn C Montgomery and Jeff Chester, 'Data Protection for Youth in the Digital Age: Developing a Rights-Based Global Framework' (2015) 1 European Data Protection Law Review 291.

[110] Art 35 and recital 91 GDPR.

Second, the ePrivacy Regulation should be aligned with the GDPR, as was proposed in the IMCO Opinion of October 2017, by recognising that children require specific protection when it comes to the processing of their communications data. Adding specific limitations on the collection and use of children's communications data and special protection for terminal equipment or software that is developed for children would be a step forward. Finally, a prohibition for services specifically targeted towards children to use profiling and behavioural marketing techniques would be beneficial for the protection of children's rights (eg the right to privacy and to protection against economic exploitation). However, the same concern regarding the fact of whether this applies or should apply to all under 18-year olds arises.

Third, the Unfair Commercial Practices Directive may provide additional protection for children against personalised advertising, as this advertising practice may qualify as a form of undue influence. It could even be considered to add behavioural advertising practices aimed towards children to the blacklist of practices which are under all circumstances deemed unfair.

Fourth, the industry has been very active in self-regulating personalised advertising practices (ie direct marketing and online behavioural advertising). While it could be argued that the commitment not to create segments targeting children for 12-year olds and under is laudable, it does not provide any protection for children above the age of 12, even though these targeted advertising practices may also have significant privacy implications for 12 to 18-year olds.[111] Moreover, different ages can be found in different self-regulatory instruments (eg 12 and under, under 14s), which could lead to confusion. Existing self-regulatory initiatives focus mostly on information provision and transparency (eg notice requirements, labelling), as well as on the requirement of (verifiable) parental consent for personalised advertising, rather than on actual limitations on the processing of children's personal data for marketing and advertising practices. Whereas such limitations might go against commercial interests of advertisers, the best interests of children might require this, also taking into account the fact that for advertising to be innovative and fun for children, collecting and using children's personal data is not a precondition.

Finally, research has shown that children's level of advertising literacy gradually develops over the years. Therefore, for them to grow up to be ad-literate adults, they should be able to practice their commercial decision-making skills throughout their childhood. As a part of their rights to development and

[111] King and Wegener Jessen (n 99).

education, they should be taught from an early age about how to cope with advertising, also in the digital environment, at school and by their parents.

5. SELECTED LITERATURE

Altaweel I, Good N and Hoofnagle CJ, 'Web Privacy Census' [2015] Technology Science <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2703814>

Ariely D and Berns GS, 'Neuromarketing: The Hope and Hype of Neuroimaging in Business' (2010) 11 Nature Reviews Neuroscience

Beales H, 'The Value of Behavioral Targeting' (2010) 1 Network Advertising Initiative <https://pdfs.semanticscholar.org/e2eb/6726f5a29d9c14dafaf056be9a3ade877b0a.pdf>

Belgian Privacy Commission, 'Recommendation No. 02/2013 of 30 January 2013 Regarding Direct Marketing and the Protection of Personal Data' (2013) <https://www.privacycommission.be/sites/privacycommission/files/documents/aanbeveling_02_2013.pdf>

Beuc, 'Data Collection, Targeting and Profiling of Consumers Online' (2010) <http://www.beuc.eu/publications/2010-00101-01-e.pdf>

Boerman SC, Kruikemeier S and Zuiderveen Borgesius FJ, 'Online Behavioral Advertising: A Literature Review and Research Agenda' (2017) 46 Journal of Advertising 363

Bosco F and others, 'Profiling Technologies and Fundamental Rights and Values: Regulatory Challenges and Perspectives from European Data Protection Authorities', *Reforming European Data Protection Law* (Springer 2015)

Bright LF and Daugherty T, 'Does Customization Impact Advertising Effectiveness? An Exploratory Study of Consumer Perceptions of Advertising in Customized Online Environments' (2012) 18 Journal of Marketing Communications 19

Calvert SL, 'Children as Consumers: Advertising and Marketing' (2008) The Future of Children 205

Castelluccia C, 'Behavioural Tracking on the Internet: A Technical Perspective' in Serge Gutwirth and others (eds), *European Data Protection: In Good Health?* (Springer Netherlands 2012)

Cauberghe V and others, 'Reclamewijsheid Bij Kinderen En Jongeren: Onderzoeksrapport in Opdracht van Vlaams Ministerie van Cultuur, Jeugd, Sport En Media' (2012) <https://biblio.ugent.be/publication/4130480/file/4130494>

Chaudron S and others, *Young Children (0-8) and Digital Technology: A Qualitative Exploratory Study across Seven Countries.* (Publications Office 2015) <http://dx.publications.europa.eu/10.2788/00749>

De Pauw P and others, 'From Persuasive Messages to Tactics: Exploring Children's Knowledge and Judgement of New Advertising Formats' (2017) New Media & Society

FEDMA, 'European Code of Practice for the Use of Personal Data in Direct Marketing - Electronic Communications Annex (the On-Line Annex)' <http://ec.europa.eu/justice/data-protection/article-29/documentation/ opinion-recommendation/files/2010/wp174_annex_en.pdf>

Forbrugerombudsmanden, 'Guidance on Children, Young People and Marketing' (2014) <https://www.consumerombudsman.dk/media/14560/guidance-on-children-young-people-and-marketing.pdf>

Ghose A and Yang S, 'An Empirical Analysis of Search Engine Advertising: Sponsored Search in Electronic Markets' (2009) 55 Management Science 1605

Global Privacy Enforcement Network, 'Children's Privacy Sweep' (2015) <http://194.242.234.211/documents/10160/0/GPEN+Privacy+Sweep+2015.pdf>

Van Noort G, Smit EG and Voorveld HAM, 'The Online Behavioural Advertising Icon: Two User Studies', *Advances in Advertising Research (vol IV)* (Springer 2013)

Gunter B, *Kids and Branding in a Digital World* (Manchester University Press 2016)

Hildebrandt M, 'Profiling: From Data to Knowledge' (2006) 30 Datenschutz und Datensicherheit-DuD 548

Hudders L and others, 'Shedding New Light on How Advertising Literacy Can Affect Children's Processing of Embedded Advertising Formats: A Future Research Agenda' (2017) 46 Journal of Advertising 333

International Chamber of Commerce, 'Advertising and Marketing Communication Practice Consolidated ICC Code' <https://cdn.iccwbo.org/content/uploads/sites/3/2011/08/ICC-Consolidated-Code-of-Advertising-and-Marketing-2011-English.pdf>

Keymolen E, 'Onzichtbare Zichtbaarheid. Helmuth Plessner Ontmoet Profiling' (2006)

——, *Trust on the Line: A Philosophical Exploration of Trust in the Networked Era* (Wolf Legal Publishers 2016)

King N and Wegener Jessen P, 'Profiling the Mobile Customer – Is Industry Self-Regulation Adequate to Protect Consumer Privacy When Behavioural Advertisers Target Mobile Phones? – Part II' (2010) 26 Computer Law & Security Review 595

Kosta E, 'Peeking into the Cookie Jar: The European Approach towards the Regulation of Cookies' (2013) 21 International Journal of Law and Information Technology 380

Lenhart A and Madden M, 'Teens, Privacy and Online Social Networks' <http://www.pewinternet.org/2007/04/18/teens-privacy-and-online-social-networks/>

Lievens E, *Protecting Children in the Digital Era: The Use of Alternative Regulatory Instruments* (Brill 2010)

——, 'Is Self-Regulation Failing Children and Young People? Assessing the Use of Alternative Regulatory Instruments in the Area of Social Networks', in Seamus Simpson and others (eds), *European media policy for the twenty-first century : assessing the past, setting agendas for the future* (Routledge 2016)

—— and others, 'Children's Rights and Digital Technologies', in Ursula Kilkelly and Ton Liefaard, *International Children's Rights Law* (Springer 2018) (forthcoming)

—— and Milkaite I, 'Better Internet for Kids - Age of Consent in the GDPR: Updated Mapping' <https://www.betterinternetforkids.eu/web/portal/practice/awareness/detail?articleId=2019355>

—— and Verdoodt V, 'Looking for Needles in a Haystack: Key Children's Rights Issues in the General Data Protection Regulation' [2017] Computer Law & Security Review

Livingstone S, Carr J and Byrne J, 'One in Three: Internet Governance and Children's Rights' (Centre for International Governance Innovation and the Royal Institute of International Affairs 2015) 22 <https://www.cigionline.org/publications/one-three-internet-governance-and-childrens-rights>

Macenaite M and Kosta E, 'Consent for Processing Children's Personal Data in the EU: Following in US Footsteps?' (2017) 26 Information & Communications Technology Law 146

Montgomery KC and Chester J, 'Data Protection for Youth in the Digital Age: Developing a Rights-Based Global Framework' (2015) 1 European Data Protection Law Review 277

Moore RS, Stammerjohan CA and Coulter RA, 'Banner advertiser-web site context congruity and color effects on attention and attitudes' (2005) 34 Journal of Advertising 71

Ofcom Office of Communications, 'Social Networking A Quantitative and Qualitative Research Report into Attitudes, Behaviours and Use' (Ofcom Office of Communications 2008)

Rozendaal E and others, 'Reconsidering Advertising Literacy as a Defense Against Advertising Effects' (2011) 14 Media Psychology 333

Savirimuthu J, 'Unfair Commercial Practies, the Consumer Child and New Technologies: What Should We Regulate? Some Policy Provocations' (2014) <https://www.liverpool.ac.uk/media/livacuk/law/european-childrens-rights-unit/BriefingNote.pdf>

Skouma G and Léonard L, 'On-Line Behavioral Tracking: What May Change after the Legal Reform on Personal Data Protection', *Reforming European Data Protection Law* (Springer 2015) <http://link.springer.com/chapter/10.1007/978-94-017-9385-8_2>

Van Alsenoy B, 'Regulating Data Protection: The Allocation of Responsibility and Risk among Actors Involved in Personal Data Processing' (2016) <https://lirias.kuleuven.be/handle/123456789/545027>

——, 'From Social Media Service to Advertising Network - A Critical Analysis of Facebook's Revised Policies and Terms' <https://www.law.kuleuven.be/citip/en/news/item/facebooks-revised-policies-and-terms-v1-2.pdf>

Verdoodt V, Clifford D and Lievens E, 'Toying with Children's Emotions, the New Game in Town? The Legality of Advergames in the EU' (2016) 32 Computer Law & Security Review 599

Yan J and others, 'How Much Can Behavioral Targeting Help Online Advertising?', *Proceedings of the 18th international conference on World wide web* (ACM 2009) <http://dl.acm.org/citation.cfm?id=1526745>

Zarouali B and others, '"Do You like Cookies?" Adolescents' Skeptical Processing of Retargeted Facebook-Ads and the Moderating Role of Privacy Concern and a Textual Debriefing' (2017) 69 Computers in Human Behavior 157

Zuiderveen Borgesius FJ, 'Personal Data Processing for Behavioural Targeting: Which Legal Basis?' (2015) 5 International Data Privacy Law 163

——, 'Mensen Aanwijzen Maar Niet Bij Naam Noemen: Behavioural Targeting, Persoonsgegevens En de Nieuwe Privacyverordening' [2016] Tijdschrift

voor Consumentenrecht en handelspraktijken <https://www.ivir.nl/publicaties/download/1786>

—— and others, 'Tracking Walls, Take-It-Or-Leave-It Choices, the GDPR, and the EPrivacy Regulation' (2017) 3 European Data Protection Law Review 353

Since the Snowden revelations, the adoption in May 2016 of the General Data Protection Regulation and several ground-breaking judgments of the Court of Justice of the European Union, data protection and privacy are high on the agenda of policymakers, industries and the legal research community.

Against this backdrop, *Data Protection and Privacy under Pressure* sheds light on key developments where individuals' rights to data protection and privacy are at stake. The book discusses the persistent transatlantic tensions around various EU-US data transfer mechanisms and EU jurisdiction claims over non-EU-based companies, both sparked by milestone court cases. Additionally, it scrutinises the expanding control or surveillance mechanisms and interconnection of databases in the areas of migration control, internal security and law enforcement, and oversight thereon. Finally, it explores current and future legal challenges related to big data and automated decision-making in the contexts of policing, pharmaceutics and advertising.

Gert Vermeulen is full professor of international and European criminal law and director of the Institute for International Research on Criminal Policy (IRCP) at Ghent University, and privacy commissioner at the Belgian DPA.

Eva Lievens is assistant professor of law and technology at Ghent University.

www.maklu.eu
isbn 978-90-466-0910-1