Available online at www.sciencedirect.com

ScienceDirect

www.compseconline.com/publications/prodclaw.htm

Computer Law & Security Review

The role of technology in the fight against human trafficking: Reflections on privacy and data protection concerns

Felicity Gerry QC [a,*], *Julia Muraszkiewicz* [b], *Niovi Vavoula* [c]

[a] *School of Law, Charles Darwin University, Darwin, Australia*
[b] *Vrije Universiteit Brussel, Belgium*
[c] *Queen Mary, University of London, UK*

Keywords:
Human trafficking
Technology
Data protection
Privacy
Data
Drones
Tracking

A B S T R A C T

Over the past decade, policy makers, academics and activists have looked into solutions within the realm of technology as a means of stepping up the fight against human trafficking while ensuring a high level of protection of the victims. Even though different types of technology might be effective in the context of crime prevention, investigation or prosecution (whether national or transnational) and victim protection, such processes inevitably raise significant concerns particularly in relation to privacy and data protection. This article aims to offer an introduction to these challenges in order to trigger a much-needed dialogue in this regard. After outlining key terms and main provisions concerning privacy and data protection, the present article then explores three ways in which technological developments can contribute to combatting human trafficking – location tracking, data collection and drones –, through these it highlights the respective privacy and data protection concerns and attempts to offer ways forward.

> "We are still in the earliest days of understanding the power of technology for the human rights movement"[1]

1. Introduction

By its intrinsic nature, trafficking in human beings (THB) is a hidden crime, where criminal individuals or organisations quickly adapt and advance their *modus operandi* in order to respond to law enforcement strategies often acting under the guise of legitimate operations. In addition, trying to estimate the number of people it affects or the profit criminals make is a troublesome task given that exploitation can occur in multiple ways. While it is true that stakeholders, including State authorities, do not need 100% accurate statistics to take immediate action against human trafficking, it is widely recognised that improving our knowledge will enhance the prospects of tackling this crime effectively while ensuring full protection of the victims.

Over the past few years, policy makers, academics and activists have increasingly turned their attention into the multiple role of technology in the human trafficking framework. On the one hand, scholars have improved the understanding

* *Corresponding author.* QC 36 Bedford Row, London WC1R 4JH, UK.
E-mail address: Felicity.Gerry@cdu.edu.au (F. Gerry).
http://dx.doi.org/10.1016/j.clsr.2015.12.015

[1] Ian Levine, 'Will technology transform the human rights movement?' (Human Rights Watch Blog, March 26, 2014) <http://www.hrw.org/news/2014/03/26/will-technology-transform-human-rights-movement> accessed 15 October 2015.

regarding the way perpetrators utilise technological forms as means of recruiting and controlling their victims. It has been correctly pointed out that many aspects of human trafficking have been transformed by the evolution of technology because the latter has changed not only the ways in which links are made between exploiters, purchasers and victims, but also the circulation of information regarding how to engage in criminal activity.[2] On the other hand, there is growing interest in finding ways to 'exploit technology' with a view to disrupt human trafficking networks. For example, law enforcement authorities are using technological traces to identify traffickers and companies perform data mining to identify suspicious transactions.[3] Furthermore, technology has facilitated the recording, storage and exchange of victims' information after being identified as such. Reporting mechanisms for witnesses and victims via telephone or the internet have been established. In cases involving images, metadata may assist in proving the dates when the crimes were committed. The location of an offence may be proved by the content of images and geo tagging. Xif data from devices used to take images may match those devices in the possession of a particular suspect. Besides, in cases when only circumstantial evidence exists, inferences may be drawn from evidence that the suspect used fake caller ID or spyware to rebut suggestions of innocent association and to prove criminal intent. Flight bookings and bank records of cash withdrawals abroad might assist in proving transnational trafficking. The transnational, multi-dimensional and highly adaptive character of human trafficking renders the possibilities for using technology endless.

The application of technology in the human trafficking framework inevitably raises significant concerns as to how this can be effectively done without undermining the fundamental rights of both the victims and other individuals who may collaterally be affected. In particular, privacy and data protection considerations lie at the heart of the analysis. To date, an in depth discussion on privacy and data protection concerns raised by the impact of technology in the sphere of combatting human trafficking is missing. The current provisions in human trafficking legislation addressing privacy and data protection considerations relate mostly to the way criminal proceedings must take place and do not include specific guidelines regarding the application of specific technological advances in the fight against human trafficking that would take into account the special nature of the criminal activity. Furthermore, the impact of the use of different technological tools on individual privacy has been scrutinised, but an analysis emphasised particularly on human trafficking is also necessary. With regard to data collection, the 'datACT' project is committed to ensuring that victims of trafficking are 'perceived in their autonomy and not as powerless victims whose personal data must be collected and stored.'[4] The project recognises that trafficked persons enjoy an equal level of protection of their right to privacy as any other citizen.

The present article aims at sparking a much-needed dialogue in this regard by examining specific technological forms that can be used in the fight against human trafficking in the light of privacy and data protection considerations. To this end, the next section provides key terminological clarifications in relation to human trafficking, technology, privacy and data protection and outlines the relevant provisions concerning the relationship between human trafficking and privacy as it currently stands. Then the following section explores three ways in which technological development may be used for combating trafficking in human beings; location tracking, data collection and unmanned aircraft vehicles (UAVs), commonly referred to as drones. In relation to each case study, the relevant privacy and data protection concerns are analysed. Finally, a conclusion summarises the main findings of the research.

2. Human trafficking, privacy, data protection and their links – key terms and legislation

2.1. *The (changing) landscape in human trafficking, privacy and data protection*

Article 3 of The Protocol to Prevent, Suppress and Punish Trafficking in Persons Especially Women and Children, Supplementing the United Nations Convention against Transnational Organised Crime (the UN Trafficking Protocol) defines human trafficking as:

> (a) The recruitment, transportation, transfer, harbouring or receipt of persons, by means of the threat or use of force or other forms of coercion, of abduction, of fraud, of deception, of the abuse of power, or a position of vulnerability, or the giving or receiving of payments or benefits to achieve the consent of a person having control over another person, for the purpose of exploitation. Exploitation shall include, at a minimum, the exploitation of the prostitution of others or other forms of sexual exploitation, forced labour or services, slavery or practices similar to slavery, servitude or the removal or organs.
> (b) The consent of a victim of trafficking in persons to the intended exploitation set forth in subparagraph (a) of this article shall be irrelevant where any of the means set forth in subparagraph (a) have been used;

[2] M. Latonero, G. Berhane, A. Hernandez, T. Mohebi, L. Movius, 'Human Trafficking Online: The Role of Social Networking Sites and Online Classifieds' (*Technology and human trafficking*, 2011) <https://technologyandtrafficking.usc.edu/report/> accessed 15 October 2015; M. Latonero, J. Musto, Z. Boyd, E. Boyle, A. Bissel, K.Gibson, and J. Kim, 'The rise of mobile and the diffusion of technology-facilitated trafficking' (*USC Annenberg Center on Communication Leadership and Policy*, 2012) <http://technologyandtrafficking.usc.edu/2012-report/#.VbtgbHt5efQ> accessed 15 October 2015; J. Musto, 'The posthuman anti-trafficking turn: Technology, domestic minor sex trafficking, and augmented human–machine alliances' in K. K. Hoang and R. Salazar Parreñas (eds), *Human trafficking reconsidered: Rethinking the problem, envisioning new solutions* (International Debate Education Association, 2014).

[3] Mitali Thakor and D. Boyd, 'Networked trafficking: Reflections on technology and the anti-trafficking movement' *Dialectical Anthropology* (2013) Vol. 37, 277–90.

[4] The aim of datACT is to promote the rights of trafficked persons to privacy and autonomy and to protect their personal data: 'DATACT – Data Protection In Anti-Trafficking Action', DatAct, <http://www.datact-project.org/startseite.html> accessed 15 October 25 2015.

(c) The recruitment, transportation, transfer, harbouring or receipt a child for the purpose of exploitation shall be considered "trafficking in persons" even if this does not involve any of the means set forth in subparagraph (a) of this article[5];

Traffickers erode a series of human rights; right to freedom, prohibition of torture or inhumane treatment and right to dignity to name a few. Another characteristic of the crime is its diversity; it can be committed by organised transnational criminal gangs or by a single person and it can target women, men and children of all ages. Although communities traditionally think of human trafficking in the form of female sexual exploitation, according to the United Nations Office on Drugs and Crime (UNODC) the sectors most frequently associated with human trafficking are agriculture or horticulture, construction, garments and textiles under sweatshop conditions, catering and restaurants, domestic work, entertainment and the sex industry.[6] In other words, human trafficking targets sectors that exploit individuals for forced labour surrounded by secrecy that is difficult to tackle.

For a definition on technology Latonero et al. have eloquently stated that:

> 'By "technology," we refer to information and communication technologies, particularly those constituting digital and networked environments. Technologies that allow users to exchange digital information over networks include the Internet, online social networks, and mobile phones. Digital and networked technologies alter the flow of information between people and thus impact social interactions, practices, and behavior.'[7]

Furthermore, describing privacy is not as straightforward a process as in relation to the previous notions and surely cannot be effectively done within a few paragraphs. Wacks argued that privacy is 'large and unwieldy'[8] and Bennett described privacy as 'a notoriously vague, ambiguous, and controversial term that embraces a confusing knot of problems, tensions, rights and duties'.[9] Whitman regarded privacy as 'an unusually slippery concept',[10] while Solove, more recently, has stated that privacy 'is a concept in disarray. Nobody can articulate what it means.'[11] In relation to the right to private life prescribed in Article 8 of the European Convention on Human Rights (ECHR), the European Court of Human Rights (ECtHR) has stated that it extends beyond the 'right to privacy, the right to live, as far as one wishes, protected from publicity'[12] and that private life is 'a broad term not susceptible to exhaustive definition.'[13] While an in-depth examination of the respective case-law is beyond the scope of the present article, it suffice here to mention that the ECtHR has ruled that the right includes the protection against broadcasting of personal information (including images) and the right to establish relationships with other persons[14] as well as physical and psychological integrity of a person.[15] Apart from the ECHR, at international level privacy is recognised as a human right in Article 17 of the International Covenant of Civil and Political Rights (ICCPR), which mirrors the wording of Article 12 of the non-binding United Nations Declaration of Human Rights. Despite this lack of conceptual clarity, it is widely agreed that privacy comprises multiple dimensions. Solove has stated that privacy includes several aspects, which are not possible to reduce to one single notion.[16] Clarke has elaborated that privacy is divided into privacy of the person, privacy of personal data, privacy of personal behaviour and privacy of personal communication.[17] Recently, Finn, Wright and Friedewald have argued for an expansion to seven types of privacy so as to include privacy of thoughts and feelings, of location and of association.[18]

By contrast, the role entrusted to data protection is somewhat clearer; data protection rules follow and regulate in detail different instances of personal data processing through the development of key legal principles (the fair information principles), such as the principle of purpose limitation. On top of the adoption of substantive rules governing data processing, data protection also focuses on issues of procedural justice by establishing rules on remedies for the data subject. However, a definite set of data protection principles does not exist and different lists have emerged both in literature and in various data protection instruments.[19] As regards these instruments, the most important ones are the OECD Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data (1980), the Council of Europe's Convention for the Protection of Individuals with regard to Automatic Processing of

[5] Protocol to Prevent, Suppress and Punish Trafficking in Persons Especially Women and Children, supplementing the United Nations Convention against Transnational Organized Crime Adopted and opened for signature, ratification and accession by General Assembly resolution 55/25 of 15 November 2000 (Palermo Protocol).

[6] United Nations Office on Drugs and Crime, 'Human Trafficking frequently asked questions' <http://www.unodc.org/unodc/en/human-trafficking/faqs.html> accessed 15 October 2015.

[7] Latonero, Mark, Jennifer Musto, Zhaleh Boyd, and Ev Boyle, *op. cit.*, pp. 9–10.

[8] Raymond Wacks, *Law, Morality, and the Private Domain* (Hong Kong University Press, 2000) p. 222.

[9] C.J. Bennett, *Regulating Privacy Data Protection and Public Policy in Europe and the United States* (Cornell University Press, 1992) p.13.

[10] James Q. Whitman, 'The Two Western Cultures of Privacy: Dignity versus Liberty', *The Yale Law Journal* (2004) Vol. 113, pp.1153–4.

[11] Daniel Solove, *Understanding privacy* (Harvard University Press, 2008) p.12.

[12] X v Iceland (1976) 5 D. & R. 86 at 87.

[13] Peck v United Kingdom (2003) 36 E.H.R.R. 41 at 57.

[14] Ibid.

[15] Pretty v United Kingdom (2002) 35 E.H.R.R. 1 at 61.

[16] Solove, *op. cit.*

[17] C. Roger, 'What's "privacy"'? (*Australian Law Reform Commission workshop*, 28 July 2006) <http://www.rogerclarke.com/DV/Privacy.html> accessed 15 October 2015.

[18] Rachel L. Finn, David Wright and Michael Friedewald, 'Seven Types of Privacy', in Serge Gutwirth et al. (eds.), *European Data Protection: Coming of Age* (Springer, 2013) pp. 4–5.

[19] The OECD Guidelines of 1979 are often used as a starting point. See also the six "core fair information principles" of Bennett: principles of openness, individual access and correction, collection limitation, use limitation, disclosure limitation and security, Bennett, *op. cit.*, p.101.

Personal Data 108 (1981) and the United Nations (UN) Guidelines Concerning Computerized Personal Data Files (1990). At EU level, Directive 95/46/EC[20] is the leading instrument regarding the protection of personal data in the former first pillar providing a set of principles applicable to the processing of personal data and a series of rights afforded to individuals.[21]

Given that the directive expressly excludes criminal matters from its scope,[22] a framework decision regulating the exchange of personal information in the context of police and judicial cooperation has been adopted.[23] Some might argue that the protection of privacy and data in the context of criminal investigation is a boat which has already sailed. However, we suggest that, in the context of THB the issue is much more complex since there is a balance to be struck between identifying perpetrators and protecting victims.

Arguably, the said framework decision contains a number of shortcomings resulting in a significantly lower level of personal data protection than the one set out in the directive.[24] At the moment, both EU instruments are under reform.[25] The directive will be replaced by a regulation with a view to accommodating the new Internet reality as well as addressing the implementation discrepancies at the national level. Among its main changes, the draft Regulation adds new fair information principles, namely the principles of transparency and accountability, clarifies the concept of consent as a ground legitimising data processing and reforms the provisions on individuals' rights including the introduction of the formulation of a "right to be forgotten" and a "right to data portability".[26]

As for the framework decision, it will be replaced by a directive, which will apply not only to cases involving exchange of information between national authorities but also to domestic processing. The proposal prescribes specialised rules for data processing in order to accommodate the special needs of law enforcement (for example, by allowing and regulating the process of profiling), but it must be noted that to the extent possible it follows the general rules and principles of the draft Regulation.[27]

Much ink has been spilt as regards the relationship between the two concepts. Several theories have been elaborated,[28] with the most comprehensive one been developed by Gutwirth and de Hert. In a nutshell, they note that '(w)hilst privacy builds a shield around the individual, creating a zone of autonomy and liberty, data protection puts the activity of the processor in the spotlight, gives the individual subjective rights to control the processing of his/her personal data and enforces the processor's accountability.'[29] While this theory has been criticised in that it does not take into consideration the fact that to a certain extent data protection serves to safeguard the privacy of the data subject, it also shows the difference in the focus; while data protection is centred on the personal data, the interest of privacy is the individual per se. However, it must be stressed that developments such as the emergence of personal data protection as a fully fledged fundamental right enshrined in Article 8 of the EU Charter for Fundamental Rights or the convergence of privacy and data protection into a single term 'data privacy' add to the perplex landscape.[30] At the same time, the Court of Justice of the European Union (CJEU) following the ECtHR seems to suggest an approach encompassing both concepts in order to provide a holistic protection of the fundamental rights of individuals. This is achieved through the creation of a hybrid 'right to private life with regard to the processing of personal data' that endorses both concepts of privacy and data protection.[31] Against this background, it seems sensible to conclude that privacy and data protection are closely related but

[20] 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, OJ L 281/30, 23.11.1995.

[21] For an analysis on the Directive see among others Y. Poullet, 'The Directive 95/46/EC: Ten years after; *Computer Law & Security Review* (2006) Vol. 22, 206–217.

[22] Article 3(2) of the Data Protection Directive.

[23] Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial co-operation in criminal matters, OJ L 350/60, 30.12.2008.

[24] For an overview see P. de Hert and V. Papakonstantinou, 'The data protection framework decision of 27 November 2008 regarding police and judicial cooperation in criminal matters – A modest achievement however not the improvement some have hoped for', *Computer Law & Security Review* (2009) Vol. 25, 403–414.

[25] European Commission, Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), COM(2012) 11final 25.1.2012; Proposal for a Directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data, COM(2012) 10final, 25.1.2012.

[26] For an analysis on the proposed Regulation see P. de Hert and V. Papakontantinou, 'The proposed data protection Regulation replacing Directive 95/46/EC: A sound system for the protection of individuals', *Computer Law & Security Review* (2012) Vol. 28, 130–142; A. Mantelero, 'The EU Proposal for a General Data Protection Regulation and the roots of the "right to be forgotten"', *Computer Law & Security Review* (2013) Vol. 29, 229–235; B. Koops, 'The Trouble with European Data Protection Law', *International Data Privacy Law* (2014) Vol. 4, 250–261.

[27] For an analysis on the proposed Directive see P. Hert and V. Papakonstantinou, 'The Police and Criminal Justice Directive: Comment and Analysis' *Computer & Law Magazine of SCL Forum* (2012) Vol. 22(6) <http://www.vub.ac.be/LSTS/pub/Dehert/411.pdf> accessed 15 October 2015.

[28] P. De Hert and S. Gutwirth, 'Privacy, Data Protection and Law Enforcement. Opacity of the Individual and Transparency of Power' in E. Claes, A. Duff and S. Gutwirth (eds.) *Privacy and the Criminal Law* (Intersentia, 2006) 61–104; A. Rouvroy and Y. Poullet, 'The Right to Informational Self-Determination and the Value of Self-Development: Reassessing the Importance of Privacy for Democracy', in S. Gutwirth et al. (eds.) *Reinventing Data Protection* (Springer, 2009) 45–76; M. Tzanou, 'The Added Value of Data Protection as a Fundamental Right in the EU Legal Order in the Context of Law Enforcement' (Ph.D. Thesis, EUI, 2012).

[29] S. Gutwirth et al., Preface in *Reinventing Data Protection?* (Springer, 2009).

[30] What Europeans term data protection, in other jurisdictions such as in Australia or the US it is termed privacy, for example, see the Australian Privacy Act 1988.

[31] Joined Cases C-92/09 and C-93/09, Volker und Markus Schecke GbR (C-92/09), Hartmut Eifert (C-93/09) v Land Hessen, Judgment of the Court (Grand Chamber) of 9 November 2010; Joined Cases C-293/12 and C-495/12, Digital Rights Ireland Ltd (C-293/12) v Minister for Communications, Marine and Natural Resources and others, and Kärntner Landesregierung, and others (C-594/12), Judgment of the Court (Grand Chamber) of 8 April 2014.

not identical notions, because privacy protects other dimensions of a person apart from their personal data, while data protection is restricted to the protection of data albeit personal but not necessarily part of a person's private life. In cases of processing of personal data, if viewed together as the CJEU does, individuals can be shielded more effectively at all stages of information processing; from the collection to their further use and exchange.

2.2. *Privacy and data protection concerns in addressing human trafficking – the current state of play*

Having set a basic terminological and legislative background, the next step is to examine the extent to which privacy and data protection considerations are taken into account in the human trafficking environment. At the outset, it needs to be stressed that the primary focus is placed on the trafficked victims and that data protection and privacy are considered in relation to criminal proceedings rather than the whole criminal procedure. A first indication is Article 6 of the UN Trafficking Protocol, which states that:

> 'In appropriate cases and to the extent possible under its domestic law, each State Party shall protect the privacy and identity of victims of trafficking in persons, including, inter alia, by making legal proceedings relating to such trafficking confidential.'[32]

Although it goes without saying that the protection of trafficked persons' privacy should be a priority, it must be remembered that in any trafficking scenario other actors are also involved. This can include those under investigation but also others such as support services, employers, bankers receiving proceeds of crime and subject to reporting requirements. Furthermore, personal data could be useful as an evidential tool, but concerns may also be raised as to the extent to which the processing of such data may have harmful repercussions.

In any case, Article 6 is of qualified nature; neither has the binding force of a hard law nor does it provide for a clear obligation on States. In the UN framework privacy and data protection play second fiddle to other duties and therefore there is a wide margin of manoeuvre in relation to the protection of privacy of trafficked individuals. For example, an important concern involves the extent to which the exercise of such discretion is monitored per se in a similar manner as other rights systems are monitored through reporting committees like the Convention on the Elimination of All Forms of Discrimination Against Women ("CEDAW").

To a certain extent, the qualified nature of Article 6 has been rectified by the Council of Europe. Article 11 of the Convention on Action against Trafficking in Human Beings reads:

> 1 Each Party shall protect the private life and identity of victims. Personal data regarding them shall be stored and used in conformity with the conditions provided for by the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108).
>
> 2 Each Party shall adopt measures to ensure, in particular, that the identity, or details allowing the identification, of a child victim of trafficking are not made publicly known, through the media or by any other means, except, in exceptional circumstances, in order to facilitate the tracing of family members or otherwise secure the well-being and protection of the child.
>
> 3 Each Party shall consider adopting, in accordance with Article 10 of the Convention for the Protection of Human Rights and Fundamental Freedoms as interpreted by the European Court of Human Rights, measures aimed at encouraging the media to protect the private life and identity of victims through self-regulation or through regulatory or co-regulatory measures.

The reference to Convention No. 108 signifies that the purpose limitation principle, which is central in the data protection discourse, must be respected, meaning that personal data must be stored only for specified lawful purposes and are not to be used in any way incompatible with those purposes. Furthermore, such data are not to be stored in any form allowing identification of the data subject or for any longer than is necessary for the purposes for which data are recorded and stored. Finally, Convention No. 108 makes it compulsory to take 'open appropriate security measures preventing unauthorised access to an alteration or disclosure of data.'[33]

In turn, Directive 2011/36/EU on trafficking in human beings[34] includes limited references to privacy and data protection. In particular, Recital 33 states that the Directive respects fundamental rights and observes the principles recognised by the EU Charter, including the protection of personal data, but the right to private life is not mentioned. At the same time, Article 19 of the Directive requires all Member States to establish national rapporteurs or equivalent mechanisms whose tasks include carrying out assessments of trends, measuring the impact of anti-trafficking efforts and gathering data. An indirect reference to the private life of trafficked individuals is included in Article 12(4)(d) which enumerates their rights in criminal investigation and proceedings and requires that national authorities should avoid unnecessary questioning regarding the victims' private lives. However, it is noteworthy that these safeguards are complementary to the general protection provided to all victims of crime from the moment a crime takes place until the end of criminal proceedings and thereafter, as encompassed in Directive 2012/29/EU.[35]

In the light of the above, it seems the interaction between human trafficking, privacy and data protection is still limited to criminal proceedings and does not address specific

[32] Palermo Protocol, Art. 6.

[33] Council of Europe, Explanatory Report on the Convention on Action against Trafficking in Human Beings, ETS 197, 16.V.2005, para. 141.

[34] Directive 2011/36/EU of the European Parliament and of the Council of 5 April 2011 on preventing and combating trafficking in human beings and protecting its victims, and replacing Council Framework Decision 2002/629/JHA, 15 April 2011, OJ L 101/1, 15.4.2011.

[35] Directive 2012/29/EU of the European Parliament and of the Council of 25 October 2012 establishing minimum standards on the rights, support and protection of victims of crime, and replacing Council Framework Decision 2001/220/JHA, OJ L 315/57, 14.11.2012.

fundamental rights challenges related to the use of technology in combatting the crime. At the same time, privacy and data protection considerations are included in guides and toolkits that promote ethical research and data collection. Such examples include the UNODC toolkit on 'Use of standardized data collection instruments'[36] or the 'United Nations Inter-Agency Project on Human Trafficking, Guide to ethics and human rights in counter trafficking.'[37] Therefore, the increasing reliance on surveillance tools not only during criminal investigations and proceedings, but also in the context of trafficking prevention can only be examined against the general legislation on privacy and data protection by taking into consideration all competing interests and finding a balance human protection from exploitation and human protection from invasion of privacy. In raising the need to consider these concerns, we have taken a focus on EU legislation and commitments. The global nature of THB of course means that attention needs to be paid to similar concerns in other locations, particularly where concepts of privacy and data protection are less well developed.

3. Technology advancements in the fight against human trafficking – privacy and data protection concerns

The ways in which technology can facilitate and assist in the fight against human trafficking while protecting the fundamental rights and the safety of the victims cannot be exhaustively analysed in the limited space of an article. In order to highlight the debate on the privacy and data protection in human trafficking issues three key examples will be examined; location tracking, in particular relating to the possibility of gathering evidence and protecting trafficked victims through the monitoring of their location, data collection, which over the past years has been significantly stepped up in the light of technological developments and the deployment of drones in both border areas as well as in crime scenes.

3.1. *The case of location tracking*

Location tracking has become part of our everyday life. As Raab and Wright have illustrated:

> 'Location tracking is being built into many products and services, including social networking, mobile telephony, control of convicted criminals or wayward school pupils, and vehicle safety systems, often anonymously but sometimes with discriminatory effects. . .Social networking through mobile phones or other devices can enable movable locations to be mutually known – a form of "participatory surveillance". Apple has built into its terms and conditions, and its privacy policy, a provision allowing the tracking of the user's precise location.'[38]

This quote shows that location tracking is not something new and in fact in relation to various products it is common knowledge that generally individuals are not necessarily too concerned with providing their location. On the contrary, it is not uncommon that individuals voluntarily disclose information on their location, even though they may not be fully aware that their data are being accessed and processed by unknown third parties.[39]

As with almost all forms of digital technologies, location tracking fits in the human trafficking framework in a twofold manner; on the one hand, perpetrators may exploit it to facilitate the exploitation of their victims. Indeed, one of the primary functions of a trafficker is to impose and retain control over their victims. To this end, victims' phones may be manually examined, phone records may be accessed online and increasingly sophisticated spyware has become routinely available. Even after a victim has freed themselves from the traffickers 'grasp' they can still be tracked as abusers discover their whereabouts by using location trackers on their mobile phones[40]. Furthermore, apart from facilitating human trafficking, law enforcement authorities already use location tracking in order to detect the position of suspected traffickers or other individuals participating in the trafficking network. At EU level, both Directives 95/46/EC and Directive 2002/58/EC, which specifically refer to the privacy of electronic communications,[41] allow for exceptions from personal data protection in cases of investigating and prosecuting crimes.[42] In this framework, involving victims or potential victims with location tracking is the other side of the same coin and could be further scrutinised.

The traffickers' practices to track and monitor the activities of their victims prove that victims can be fairly easily

[36] United Nations Office on Drugs and Crime, 'Toolkit to Combat Trafficking in Persons' (United Nations Office on Drugs and Crime, date unknown), <http://www.unodc.org/documents/human-trafficking/Toolkit-files/08-58296_tool_9-15.pdf> accessed 15 October 2015.

[37] United Nations, 'Guide to ethics and human rights in counter trafficking,' (*United Nations Inter-Agency Project on Human Trafficking*, 2008) <http://www.endvawnow.org/uploads/browser/files/Ethics_Guidelines_Trafficking_UNIAP_2008.pdf> accessed 15 October 2015.

[38] C. Raab and D. Wright, 'Surveillance: Extending the Limits of Privacy Impact Assessment' in D. Wright and P. de Hert (eds.) *Privacy Impact Assessment* (Springer, 2012) pp. 370–371.

[39] A. S.U. Cheung, 'Location privacy: The challenges of mobile service devices', *Computer Law & Security Review* (2014) Vol. 30, 46.

[40] WESNET in Australia has identified these issues and provides training on the misuse of technology to target, track, stalk, harass and commit other acts of violence against women < http://wesnet.org.au/2015/10/safetynet-training-canberra-3/>.

[41] Directive 2002/58/EC of the European Parliament and of the Council 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), OJ L 201/37, 31.7.2002 as amended by Directive 2009/136/EC of the European Parliament and of the Council 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, OJ L 337/11, 18.11.2009.

[42] Article 13(4) of Directive 95/46/EC and Article 15(1) of Directive 2002/58/EC.

located by direct or remote interrogation of their phone. In essence, the victim becomes a walking database of evidence. At the same time, the safety of a trafficked person even after being liberated from the trafficking circle should be prioritised, along with the tackling of the phenomenon. In this context, it becomes necessary for advocates in the civil society sector to raise their awareness and become proficient at understanding technology and how it can be used. It has been submitted that in the light of the uncertainty surrounding the power and role of technology in the human trafficking context, many advocates 'simply want the technology to go away', as this would 'restore a comprehension of trafficking within their frame of reference'.[43] It goes without saying that the solution is not to remove technology from a victim as this can be incredibly disempowering. It would severely increase their isolation, while giving the abuser more power. Instead it seems a far more logical step for victims to have safe access to technology, both phones and Internet. In this context, apart from human rights advocates, it is imperative that trafficked persons learn the extent to which these technologies can be used to their benefit or against them.[44] If victims are further facilitated to use technological advances so that they obtain concrete evidence of their victimhood and assisted to safely identify of the perpetrators, their position would be empowered.

Location tracking has already been put into place in similar contexts; for example, mobile phones have already been used to track poachers of animals.[45] Furthermore, in Bahrain every migrant worker receives a SIM card and flyers by the government body of Labour Market Regulatory Authority (LMRA), when entering the country:

> 'In December 2013, the LMRA also began distributing SIM cards to workers on arrival in the country, to enable the workers to use text messaging to contact the LMRA immediately if there were problems with their employers. The Ministry of Interior continued to operate a 24 hour, toll-free hotline for trafficking victims. . .'[46]

This policy enables the respective Ministry of labour to indirectly track migrants (by having their phone numbers on a centralised database), and officially send them information related to the risk of human trafficking including hotline numbers. With the necessary amendments and caveats, a similar policy could be adopted to monitor the state of affairs as millions are confined to camps on the borders of Syria, travelling across Europe seeking asylum and prey to traffickers, or individuals are trafficked and abused within countries and from one country to another.

While tracking technology can certainly offer new opportunities to intervene in human trafficking, it must be pointed out that being a form of surveillance it can be highly invasive on a persons' privacy. In relation to the effects of location tracking, Michael and Michael have pointed out that such practices have pushed us to live in a state of 'überveillance', in which surveillance has become constant and embedded, and individuals and objects can be located and identified.[47] Indeed, location data – combined with the time and possibly the content of a specific activity – can reveal plethora of information regarding their personal life, including their affiliation with a particular religion, the development of personal relationships and associations with other individuals as well as their everyday habits. What is more, location tracking enables telecommunication or internet providers to record these activities and possibly transfer the relevant data to other companies without eliminating the risk of subsequent profiling.[48]

Despite the serious risks attached to tracking technology, it cannot be fully dismissed as a tool against human trafficking. As noted in the context of using tracking devices for patients with dementia, 'for the sake of safety a slight loss of liberty is a price worth paying and, that concern about privacy has force only if we imagine that the person involved is trying to hide.'[49] In addition, if in the question of 'why is tracking being used' the answer is 'for the benefit of the individual' then perhaps the concerns over power balance can be reduced. However, a number of safeguards should be put into place in compliance with the principle of proportionality and reliance to data protection principles is a helpful tool in this regard. First of all, it could be limited to exceptional circumstances only, for example, when there is substantiated suspicion that the safety of an ex victim is jeopardised. Blanket monitoring of all migrants – like the example in Bahrain – could have serious repercussions as regards the privacy of the individuals, especially since they are not suspected of committing any crime. In any case, strong emphasis must be placed on obtaining fully informed consent from persons who will be subjected to tracking technology. Potential or former victims should be informed about the consequences of location tracking in their private lives, the temporal character of the monitoring and the way the information from their electronic devices will be used, what type of information would that be, by which authorities it will be processed and in which context.

Furthermore, if location tracking involves a former victim and is used for collecting evidence against their perpetrators, consent could be withdrawn at any moment irrespective of whether the criminal investigation is finalised without any repercussions for the individual who collaborated with the authorities. The participation in such operations should not be in any way forced upon them as this would undermine their

[43] Thakor and Boyd, *op. cit.* p. 287.

[44] See for example WESNET, 'Internet Safety', <http://wesnet.org.au/safetynet/internet-safety/> accessed 24 February 2015.

[45] R. A. Butler, 'Discarded cell phones help fight rainforest poachers' (*Mongbay*, 24 June 2014), <http://news.mongabay.com/2014/0624-rainforest-connection-interview.html> accessed 15 October 2015.

[46] United States Department of State, '*2014 Trafficking in Persons Report – Bahrain*' (20 June 2014), <http://www.state.gov/j/tip/rls/tiprpt/countries/2014/226676.htm> accessed 15 October 2015.

[47] M.G. M. and K. Michael, 'Toward a State of Überveillance' *IEEE Technology and Society Magazine* (2010) Vol. 29(2), 9.

[48] For an overview of the effects of location tracking see among others: K. Michael and M. G. M., 'The Social and Behavioural Implications of Location-Based Services' Journal of Location Based Services (2011) Vol. 5, 121; A. S.Y. Cheung, 'Location privacy: The challenges of mobile service devices' *Computer Law & Security Review* (2014) Vol. 30, 41–54.

[49] J. Hughes and S. Louw, 'Electronic tagging of people with dementia who wander', *British Medical Journal* (2002) Vol. 325, 847–848.

consent and the individuals concerned should be able to freely choose whether they wish to obtain tracking devices. Moreover, as argued by Raab and Wright attention needs to be paid to the power implications of surveillance.[50] In a context where the State or a civil society body gives an ex victim or a potential victim a device with tracking technologies, the former is at a power advantage. Given that potential or ex trafficking victims are to a large extent third country nationals, it is vital to secure that their location data will not grow the appetite of domestic authorities to (ab)use the information for purposes unrelated to human trafficking. It would be unacceptable to use their location data for criminal law purposes in cases when national bodies suspect this group of individuals for having committed a crime or for migration control objectives even after a criminal investigation or criminal proceedings have terminated. In the light of the continuing efforts at global level to tackle irregular migration through the constant monitoring of aliens' movement, this is a serious obstacle that needs to be thought through carefully. Otherwise, tracking devices would act as a 'Trojan horse' and persons subjected to tracking technology would be trapped and further victimised at the national level. One way to bypass this issue could be to develop a monitoring and evaluation system that would ascertain that tracking technology is not used excessively or abused. In addition, opting for a system that would not involve the centralised storage of personal data of victims or potential victims would be an important safeguard.

Exploring the nexus of technology and human trafficking in this way demonstrates that the real concern should not be about whether technology can be used to combat human trafficking, but how it can be done in a manner complying with human rights. A number of questions remain open for further research in this regard; Could the extreme nature of the crime of trafficking in human beings allow the use of surveillance technology in exceptional circumstances? Is it enough to ensure that such data are not retained at all or at least only retained pending proper completion of a legitimate enquiry? There is also a need to consider to what extent technology can be employed where the tracking relates to exploitation in workplaces where criminal offending may only be suspected or where businesses are thought to be non-compliant with work place protections. At the moment, it seems that location technology could be useful in proving the forced movement of exploited people, however, further proof would be necessary as well as clear and strict limitations of the powers of national authorities.

3.2. *The case of data collection*

As mentioned in the introduction, despite the growing efforts to eliminate human trafficking, in reality reliable and holistic information on the magnitude of the problem is limited. 'The need for better data' on both the perpetrators and the trafficked persons has been repeatedly highlighted[51] under a preventive logic that 'it takes a network to defeat a network'.[52] In this direction, Rankin and Kinsella point out that:

> 'To successfully combat THB it is necessary to enhance data collection to promote trans-border cooperation, develop a capacity to collect, analyse and ultimately share relevant THB information and data. Knowledge can take the form of either intelligence or data and understanding THB is central to tackling the problem more effectively. Knowledge, from whatever source, is a key requirement in the architecture of that response.'[53]

Their statement is undoubtedly correct and the collection of data is indispensable in relation not only to the detection, investigation and prosecution of specific cases, but also it may shed more light into the future dimensions of the crime and assist in discussions regarding any anticipatory activity that may be necessary, in other words to help in answering to questions such as 'how will human trafficking look tomorrow or in three years' time'.

The value of gathering information on human trafficking and the role of technology as a facilitator in this regard are also widely recognised in the EU and since the past years data collection has become a key priority.[54] Apart from Article 19 of the Human Trafficking Directive, which, as mentioned above, is dedicated to the need for collection of data by an EU Network of National Rapporteurs or Equivalent Mechanisms, the current EU Strategy towards the eradication of human trafficking refers to the importance attached to the collection of data on numerous occasions. First, it recognises the significant steps taken towards this direction by explaining that since 2011 the Commission has collected extensive amounts of data on victims of human trafficking, police investigations, prosecutions and convictions, which are further analysed in terms of gender, age, form of exploitation and citizenship.[55] Furthermore, as a tool for more effective prosecution, the Strategy mandates the enhancement of cooperation beyond the EU borders by improving the channels of data collection both at national and transnational levels and by promoting data sharing and collaboration among relevant stakeholders such as law enforcement bodies, prosecutorial authorities, NGOs and consular staff.[56] Moreover, the need to strengthen partnerships with international organisations such as the UN, or the Council of Europe with

[50] Raab and Wright, *op. cit.*

[51] F. Laczko, 'Data and Research on Human Trafficking', *International Migration* (2005) Vol. 43 5–16.

[52] United Nations Office on Drugs and Crime, 'Transnational Organised Crime in East Asia and the Pacific: A threat Assessment' (*UNODC*, 2013), <http://www.unodc.org/documents/data-and-analysis/Studies/TOCTA_EAP_web.pdf> accessed 15 October 2015.

[53] N. Kinsella and G. Rankin, 'Human Trafficking – The Importance of Knowledge Information Exchange', in B. Akhgar and S. Yates (eds) *Intelligence Management*, (Springer, 2011), 172.

[54] C. Aradau, 'Human trafficking between data and knowledge' (paper presented at the datACT – Conference on data protection and trafficking, Berlin, 25–27 September 2013).

[55] European Commission, Communication from the European Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions 'EU Strategy towards the Eradication of Trafficking in Human Beings 2012–2016' COM(2012) 286final, 19.6.2012, 2.

[56] *Ibid.*, pp.10–11.

a view to improving data processing is also highlighted.[57] Finally, the establishment of an EU-wide system of data collection similar to the one that was developed in 2011 was announced.[58]

Although data collection involves information on all actors tangled in a human trafficking framework, Wijers points out that recent efforts have largely concentrated on the collection of personal data specifically from trafficked victims. Interestingly, she submits that the underlying rationale behind the collection is not related specifically to a criminal investigation and prosecution or the organisation of national and transnational assistance, but collection takes place for 'all other kinds of reasons' and is conducted by national governments, intergovernmental organisations, NGOs and private parties.'[59] For example, in the UK, the National Referral Mechanism (NRM) is a framework for identifying trafficked persons, but equally functions as a tool through which the State collects data about victims. According to the National Crime Agency 'this information contributes to building a clearer picture about the scope of human trafficking in the UK.'[60]

The acquisition of victims' data may indeed contribute to breaking the cloak of secrecy that surrounds human trafficking. However, safeguarding the privacy and personal data of these individuals should not be underestimated. The prosecution of traffickers and the prevention of the crime are important goals, but so is the protection of the victims. In his opinion on the aforementioned EU Strategy and referring broadly to the processing of personal data, the European Data Protection Supervisor (EDPS)[61] stressed that

> 'addressing THB is an area that requires significant processing of data, in many cases involving personal data, and consequently also creates risks of intrusions into privacy. Therefore, an effective action to address human trafficking cannot be put in place without the support of a solid data protection scheme complementing it'.[62]

The need for protecting the privacy of trafficked persons, including their personal data is vital since victims of trafficking form a particularly vulnerable group of individuals who are in need of enhanced protection. Furthermore, having suffered at the hands of their traffickers, they face great risks related to their physical safety. First, the risk of being recaptured and abused is evident. Second, they risk carrying the stigma of being implicated in trafficking proceedings that may prevent them from integrating into a societal environment, access the labour market and eventually regain their autonomy. The aim of protection includes the ability to recover, irrespective of whether this takes place in the sending country or in the receiving one.[63] This is important considering that if they return to their country of origin, in certain populations public exposure of certain events that trafficked persons may have experienced may be deemed shameful and may result in being ostracised. As correctly summarised by Gallagher, '(p)rotection from further harm is inextricably linked to protection of the trafficked person's privacy. Failure to protect privacy can increase the danger of intimidation and retaliation. It can cause humiliation and hurt to victims and compromise their recovery.'[64] Whilst combatting human trafficking is a global imperative, it would be pointless if, in doing so, greater harm were caused. At the same time, as the EDPS has pointed out, data protection should not be viewed as an impediment in the effective fight against human trafficking, but rather as a means of building of a relationship based on trust with the victims.[65] This hits on the correct issues and highlights the global nature of the problem which logically must require some degree of uniformity of approach by States in order to protect those who are trafficked, particularly from less developed nations.

In addition, it must be stressed that much depends on the different contexts in which the collection of data takes place, different safeguards as regards the protection of their personal data exist; in comparison to the gathering of data for statistical purposes, criminal investigations or cases of transnational cooperation are subject to exceptions from data protection rules to allow for flexibility and more effective results. As pointed out above, during criminal proceedings the private lives of the individuals should be touched upon as least as possible. On the contrary, if personal data of trafficked victims are recorded purely for improving knowledge on human trafficking, then their depersonalisation and anonymisation to the extent possible is a way forward. When this is not possible (and possibly it could never be possible, given technological advances in algorithmic analysis) then collecting bodies (governmental or non-governmental) should avoid not only the registration of excessive information, but also their centralised storage in large-scale databanks, where the risk of unauthorised access and abuse is significantly higher.

Furthermore, given that the information collected will be further processed, analysed and even transferred to other parties in order to obtain statistics or develop risk profiles, it is necessary to ensure that this processing is limited to purposes compatible with the one for which the data were

[57] *Ibid*., p.12.
[58] *Ibid*., p.14.
[59] Marjan Wijers, 'Where do all the data go? European data protection law and the protection of personal data of trafficked persons' (paper presented at the datACT – Conference on data protection and trafficking, Berlin, 25–27 September 2013).
[60] National Crime Agency, 'National Referral Mechanism', <http://www.nationalcrimeagency.gov.uk/about-us/what-we-do/specialist-capabilities/uk-human-trafficking-centre/national-referral-mechanism> accessed 15 October 2015.
[61] The European Data Protection Supervisor (EDPS) was established in 2001 by Regulation 45/2001 OJ 2001, L 8/01. The EDPS is the independent supervisory authority responsible for monitoring all data processing operations carried out by Community institutions or bodies (Art. 1).
[62] European Data Protection Supervisor, 'EDPS comments on the Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions - "The EU Strategy towards the Eradication of Trafficking in Human Beings 2012–2016," <https://ec.europa.eu/anti-trafficking/sites/antitrafficking/files/edps_on_the_new_eu_anti-human_trafficking_strategy_1.pdf> accessed 15 October 2015.
[63] Council of Europe, Explanatory Report on the Convention on Action against Trafficking in Human Beings, ETS 197,16.V.2005, para.138.
[64] Ann Gallagher, *The International Law of Human Trafficking* (New York: Cambridge University Press, 2010), p.303.
[65] EDPS, *op. cit.*, pp. 2–3.

originally collected. Both the purposes and the modalities of uses should be made known to the data subjects (the victims).

Besides, the danger of profiling that may lead to discriminatory treatment of trafficked persons must be taken into serious consideration. For example, Aradau has wondered about the implications of such processing to the capacity of movement of citizens originating from one of the countries of origin when encountering consular or border guards.[66] Equally one may wonder what the implications would be in cases of sex workers when a country report emphasises on the number of women in sexual exploitation.

Finally, those involved in data collection should receive appropriate training beforehand and on a regular basis. This seems to be appropriate in the light of voiced criticism that data collection bodies lack awareness and sufficient knowledge of what data protection laws signify and require.[67] Careful supervision both within the organisation or public body and at national level by an independent authority is also necessary.

3.3. *The case of drones*

The third example of a technological advancement that can assist in the fight against human trafficking relates to the employability of drones. Drones can generally be defined as aircraft devices – although land and sea-based vehicles are under development – that are used, or intended to be used, without a human pilot on board.[68] Technically they are also known as unmanned aerial vehicles (UAVs), remotely piloted vehicles (RPVs), or, in conjunction with their ground-based control stations, unmanned aerial systems (UAS) or remotely piloted aerial systems (RPAS).[69] In their latest forms, they can be 'as small as an insect or as large as charter flight'.[70] Since drones are merely aircraft devices, they do not process personal data as such, however in most cases they carry video camera devices with specialised software that process the video feed. They can be equipped with Wi-Fi sensors, microphones, biometric sensors processing biometric data, GPS systems processing the location of the person filmed, or systems reading IP addresses of all devices located in a building over which the RPAS will fly.[71] Apart from the ability to be attached to numerous payloads that can modify their functionalities, drones carry a number of operational benefits; they can be almost undetectable from the persons under surveillance, they are able to lower personnel costs and are more expandable as they can stay airborne much longer than a human crew, they are flexible in tasking and they can cover remote areas.[72]

Although drones have been primarily deployed in war zones for around a century,[73] in the light of their attributes their application has been recently expanded from the military framework to other fields such as environmental monitoring, observation of large-scale human constructions, energy infrastructure, border management and law enforcement.[74] In relation to human trafficking in particular, drones are relevant in two forums; first, they are used in domestic police operations for the surveillance of criminal activities, including human trafficking. For example, they can be used to track illegal cannabis farms, which are often staffed by victims of human trafficking. This involves the prescription of strict conditions such as the acquisition of a warrant. The second and far more common application of drones involves the patrol of external frontiers and combines border control with law enforcement purposes. Under this logic, which has been criticised as being part of the growing trend towards the militarisation of border surveillance,[75] drones are used to monitor the external borders of a specific State as a tool to prevent irregular migration and cross-border crime while rescuing – when needed – the lives of third-country nationals when in danger in their attempt to cross the border. As a matter of fact, the humanitarian element of these operations has been presented as their flagship in an attempt to justify the necessity of such border management mechanisms.[76]

---

[66] Aradau, *op. cit.*

[67] Wijers *op. cit.*

[68] This definition combines those submitted by B. Hayes, C. Jones and E. Töpfer, 'Eurodrones Inc.' (*Statewatch*, 2014) 7, <http://www.statewatch.org/news/2014/feb/sw-tni-eurodrones-inc-feb-2014.pdf> accessed 25 July 2015 and P. McBride, 'Beyond Orwell: the application of unmanned aircraft systems in domestic surveillance operations' *Journal of Air Law and Commerce* (2009) Vol. 74(3), 628. Roger Clarke has identified four characteristics of drones; the device must be heavier-than-air (i.e. balloons are excluded); the device must have the capability of sustained and reliable flight; there must be no human on board the device (i.e. it is 'unmanned') and there must be a sufficient degree of control to enable performance of useful functions. See R. Clarke, 'Understanding the Drone Epidemic' *Computer Law & Security Review* (2014) Vol. 30(3), 230–246.

[69] B. Hayes, C. Jones and E. Töpfer, *op. cit.*, p. 7.

[70] E. Bone and C. Bolkcom, '*Unmanned Aerial Vehicles: Background and Issues for Congress*' (Washington D.C., 2003) 1, <http://fas.org/irp/crs/RL31872.pdf> accessed 15 October 2015.

[71] EPDS, Opinion of the European Data Protection Supervisor on the Communication from the Commission to the European Parliament and the Council on "A new era for aviation – Opening the aviation market to the civil use of remotely piloted aircraft systems in a safe and sustainable manner", <https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2014/14-11-26_Opinion_RPAS_EN.pdf> accessed 15 October 2015.

[72] A. Brecher et al., 'Roadmap to near-term deployment of unmanned aerial vehicles (UAV) for transportation applications charge to participants (UAV 2003: A roadmap for deploying UAVs in transportation specialist workshop, Santa Barbara, 2003); P. C. Nolin, '*Unmanned Aerial Vehicles: Opportunities and Challenges for the Alliance Special Report*' (NATO Parliamentary Assembly, Canada, 2012).

[73] For an overview of the history behind the deployment of drones in the military framework see R. L. Finn and D. Wright, 'Unmanned aircraft systems: Surveillance, ethics and privacy in civil applications, *Computer Law & Security Review* (2012) Vol. 28, 185.

[74] For an overview of the different uses of drones see European Parliament, Directorate General for Internal Policies, 'Privacy and Data Protection Implications of the Civil Use of Drones' (PE 519.221, June 2015), 11.

[75] D. Bigo, 'Migration and Security' in Virginie Guiraudon and Christian Joppke (eds.) *Controlling a New Migration World* (Routledge, 2001) 121–149.

[76] Jørgen Carling and María Hernández-Carretero, 'Protecting Europe and Protecting Migrants? Strategies for Managing Unauthorised Migration from Africa', *The British Journal of Politics and International Relations (2011)* Vol. 13, 42–58; Ben Hays and Mathias Vermeulen, 'Borderline. EU Border Surveillance Initiatives. An Assessment of the Costs and Its Impact on Fundamental Rights' (Heinrich-Böll-Stiftung, 2012).

As for the function of drones in this context, considering that in numerous cases, migrants are also victims of smuggling or trafficking, drones can gather evidence of their victimhood and information on the trafficking networks, such as images of the perpetrators or those connected to them, the chosen routes and the timings of the border crossing. At the same time, information collected by drones can be processed for the purposes of risk analysis and thus improve the understanding on human trafficking. Both operations will depend on whether drones carry devices that can record images and are subject to the mind-set that is based on migration prevention rather than victim protection. The latter may well necessitate increased immigration to combat THB whereas the former is dedicated to keeping borders closed. Again we can see why the use of technology in the context of THB has to be discussed and considered particularly in transnational organised crime.

In practice, the deployment of drones by individual EU Member States is still limited.[77] The Italian authorities have used some of their disposable drones in an operation called Mare Nostrum.[78] The latter was launched in October 2013 as a response to the humanitarian crisis in the Sicily channel and had a dual aim; on the one hand, to identify the boats at risk of capsising, rescue migrants and bring them to Italy and on the other hand, to bring human traffickers to justice. It involved the participation of forces from all branches of the Italian Military Forces, Police Officers, the Coast Guard and Customs Service as well as the military personnel of the Italian Red Cross. In relation to the fight against human trafficking, the mission was stemmed with success by enabling the arrest of approximately 500 human traffickers.[79]

Overall, the momentum for transferring the technology of drones from the military domain to the non-military one is currently high. Spain has also considered using drones for sea border surveillance, mainly in the Strait of Gibraltar and over the Canary Islands.[80] Nevertheless, under the Spanish legislation the deployment of drones for civilian purposes is not allowed. Thus, military drones can only be used under strict conditions.[81] Greece and Cyprus have very recently purchased drones suitable for border surveillance.[82] FRONTEX has submitted that border management faces significant challenges in relation to weather conditions or the limited capacities of satellites and tests whether drones could be beneficial assets and remedy these deficiencies.[83] To this end, in the last few years a number of EU-funded research programmes explore this possibility.[84] At present there are limited projects of this type outside the EU where there is significant concern about the sourcing of victims for THB and also in relation to cyber surveillance.

Another example of the growing use of new technologies, including drones in the fight against human trafficking is the EUROSUR Regulation.[85] In a nutshell, the Regulation has established an EU framework for information exchange between Member States with a view to improving their situational awareness and reaction capability in combatting not only irregular migration, but also cross-border crime, particularly human trafficking. In essence, information collected by FRONTEX and Schengen States is exchanged via Eurosur. The backbone of Eurosur is a network of National Coordination Centres (NCC) established in each Member State that collect local and national information on irregular migration and criminal activity from border control authorities and serves as a forum for information exchange. This information may be collected through different surveillance tools, such as satellites and drones and is the basis for creating a 'near-real time' situational picture of the EU external land and sea borders and of 'pre-frontier' areas.

The nexus between military equipment and human trafficking is even more evident in EU naval operations such as the EUNAVFOR Med.[86] On 22–23 June 2015, the EU Ministers of Foreign Affairs decided to launch the mission with a view to disrupting the business model of traffickers and smugglers in the Mediterranean. Drones are also part of this process. While the aforementioned operation *Mare Nostrum* pursued both immigration and crime prevention purposes, the EUNAVFOR Med is oriented towards the perpetrators rather than the victims. As the EU High Representative for Foreign Affairs and Security Policy claims: 'The target, let me be very clear, are not the

[77] Luisa Marin and Kamila Krajčíková, 'Deploying drones in policing European borders: constraints and challenges for data protection and human rights', in Aleš Završnik, (ed.) *Drones and Unmanned Aerial Systems: Legal and Social Implications for Security and Surveillance* (Springer, 2016 forthcoming).

[78] Amnesty International, 'Lives Adrift: Refugees and Migrants in Peril in the Central Mediterranean' (30 September 2014) <https://www.amnesty.org/fr/documents/document/?indexNumber=eur05%2F006%2F2014&language=en> accessed 15 October 2015.

[79] ANSA, 'Alfano hails human trafficker arrests' (*ANSA*, 29 August 2014) <http://www.ansa.it/english/news/politics/2014/08/29/alfano-hails-human-trafficker-arrests_df573a4b-b1e7-41f3-abac-8c3a4c72b5a3.html> accessed 15 October 2015.

[80] Carlton Purvis, 'Spain Considering UAVs to Supplement its Maritime Border Security Lineup' (*Security Management*, 19 August 2011) <https://sm.asisonline.org/migration/Pages/spain-considering-uavs-supplement-its-maritime-border-security-lineup-008909.aspx> accessed 15 October 2015.

[81] José Luis Lorente Howell, 'Spain: Authorities working on future unmanned aerial vehicle (UAV) regulation' (*Bird&Bird*, 25 April 2014) <http://www.twobirds.com/en/news/articles/2014/spain/spain-authorities-working-on-future-unmanned-aerial-vehicle-regulation> accessed 15 October 2015.

[82] Y. Souliotis, 'Αγορά μη επανδρωμένων αεροσκαφών από ΕΛ.ΑΣ' (20 June 2014) <http://www.kathimerini.gr/772876/article/epikairothta/ellada/agora-mh-epandrwmenwn-aeroskafwn-apo-elas> accessed 25 July 2015; D. Kyprianou, 'Με μη Επανδρωμένα Αεροσκάφη και Πλοία Εξοπλίζεται η Λευκωσία' (*Protothema*, 11 January 2015) http://www.protothema.gr/politics/article/441410/me-mi-epandromena-aeroskafi-kai-ploia-exoplizetai-i-leukosia/ accessed 15 October 2015.

[83] FRONTEX, 'Border Surveillance' (*FRONTEX*) <http://frontex.europa.eu/research/border-surveillance> accessed 15 October 2015.However, up to now FRONTEX itself is not using drones. See Statewatch, 'EU: FRONTEX: "optionally-piloted" aircraft tests, but no drones. . .yet' (*Statewatch*, 29 May 2013) <http://www.statewatch.org/news/2013/may/09eu-frontex-opa.html> accessed 25 July 2015.

[84] Hayes et al. *op. cit.* p. 26.

[85] Regulation (EU) 1052/13 of the European Parliament and of the Council of 22 October 2013 establishing the European Border Surveillance System (EUROSUR), OJ L 295/11 6.11.2013.

[86] J. G. Neuger, 'EU to Deploy Drones, Warships against Human Traffickers' (*Bloomberd Business* 22 June 2015) <http://www.bloomberg.com/news/articles/2015-06-22/eu-to-deploy-drones-warships-against-mediterranean-traffickers> accessed 15 October 2015.

migrants, the targets are those who are making money on their lives and too often on their deaths. It is part of our efforts to save lives.'[87] Nevertheless, despite the growing interest in deploying drones for civilian purposes, it must be stressed that there is no proper regulatory framework either in the EU or at a global level. The current European aviation law does not allow for drones to fly in non-segregated areas.[88]

At the other side of the Atlantic, where the deployment of drones for enhancing border control is far more established, it is confirmed that 'drones have been used by the U.S. Customs and Border Protection Agency (part of the Department of Homeland Security) on the U.S.–Mexican border to monitor illegal immigration, human trafficking and drug smuggling.'[89] Furthermore, through the use of drones the US intelligence was able to establish that the Mexican army are involved in human trafficking and other crimes.[90] Ironically, as reported by the *Independent*, criminals may be one step ahead of the law enforcement bodies as they have 'reportedly started using unmanned drones fitted with heat-seeking cameras to steal from and extort illegal cannabis farms.'[91]

The deployment of drones as an instrument for combating human trafficking must be viewed as another manifestation of States adhering to the growing tendency of maximised surveillance, thus raising serious privacy concerns regarding the individuals monitored. As the EDPS has pointed out, drones 'offer a superior level of surveillance'.[92] In addition, given that their use is in most cases is combined with other technologies such as video cameras, to the extent that it involves the processing of personal data that can lead to the identification of a person, data protection requirements must also be respected.[93] However, this is not a universal approach; it needs to be stressed that the applicability of privacy and data protection provisions depends on the forum where the deployment of drones takes place.[94] For example, according to the US case law on aerial surveillance, the police can validly fly over a garden and spot elements constituting part of a criminal offence. The US Supreme Court has held that such activities would not signify an intrusion into the person's privacy as 'any member of the public flying in this airspace who glanced down could have seen everything that these officers observed.'[95] In jurisdictions where privacy is recognised in public spaces, the employability of drones should be cautiously considered due to the highly pervasive character of surveillance that it entails. Drones may not have a specific target but they are surveying an area more generally looking for the 'unnamed', thus potentially encroaching on innocent individuals pursuing legitimate activities. For instance, when used at borders they may capture images of fishermen and tourists or when used to dismantle trafficking networks in urban areas they may also survey individuals living in neighbouring regions or in cases of sex trafficking people who have chosen the company of a victim (especially in cases when they do not know about their trafficked status). The privacy of trafficked individuals should also be a matter of concern. As a result, drones may have significant repercussions in the behaviour of these individuals that may be adjusted under the idea that they are constantly watched. In other words, the creation of the 'chilling effect' is relevant also in this scenario.[96] Furthermore, they may infringe the privacy of their location and space. Informing about the existence of drones in a specific area does not seem a viable solution; while it would add transparency to the operations, at the same time it could enhance this chilling syndrome. Besides, information about the deployment of drones can hardly be provided when criminal investigations take place in relation to specific crime as this could jeopardise the purposes of the investigation.

Additionally, with specific regard to the protection of personal data, the Article 29 Working Party has pointed out that what matters is not the use of drones as such, but the rest of technologies that they can be equipped with and the subsequent use and processing of personal data that takes place.[97] As mentioned above, the use of video cameras will allow for the identification of persons whose images have been captured, thus the relevance of data protection law cannot be underestimated. In this context, the risk of function creep and the use of recorded material for purposes incompatible with the ones for which drones are originally employed must be carefully scrutinised. The danger of using recorded material to further victimise and criminalise trafficked persons is particularly evident. However, the safety and fundamental rights of the victims should remain central. To what extent could images captured by drones be used as an evidence against trafficked persons in deportation procedures or in criminal proceedings concerning their irregular status in a particular State?

[87] Council of the European Union, 'Press Release', <http://www.consilium.europa.eu/en/press/press-releases/2015/06/22-fac-naval-operation/> accessed 15 October 2015.

[88] Non-segregated airspace is airspace open to all civil air transport.

[89] J. I. Ross, 'Drones Are Different' (*Baltimore Sun*, 19 June 2012) <http://articles.baltimoresun.com/2012-06-19/news/bs-ed-drones-20120619_1_drone-strike-uavs-surveillance-tool> accessed 15 October 2015.

[90] M. Webster, 'U.S. ABP & U.S. Drones Flying Over Mexico Detecting Military Drug/Human Trafficking Camps' (*Renew America*, 1 April 2011), <http://www.renewamerica.com/columns/webster/110401> accessed 15 October 2015.

[91] A. Withnall, 'Criminals "Using Unmanned Drones And Infrared Cameras To Find Illegal Cannabis Farms" – And Then Steal From The Growers' (*The Independent, 17 April 2014*) <http://www.independent.co.uk/life-style/gadgets-and-tech/shropshire-criminals-using-unmanned-drones-and-infrared-cameras-to-find-illegal-cannabis-farms–and-then-steal-from-the-growers-9267587.html> accessed 15 October 2015.

[92] EDPS. *Op. cit.* p. 5.

[93] If drones process images of persons that are of sufficient quality so that they can lead to their identification, then they process personal data and data protection principles apply.

[94] Applications nos. 40660/08 and 60641/08, Case of *Von Hannover v. Germany (n. 2)*, Judgment of the European Court of Human Rights of 7 February 2012.

[95] US Supreme Court, California v. Ciraolo (1986).

[96] R. L. Finn, D. Wright and A. Donovan (Trilateral Research & Consulting, LLP), L. Jacques and P. De Hert (Vrije Universiteit Brussel), 'Privacy, data protection and ethical risks in civil RPAS operations' (7 November 2014), 28, <http://ec.europa.eu/DocsRoom/documents/7662> accessed 25 July 2015; Roger Clarke, 'The Regulation of Civilian Drones' Impacts on Behavioural Privacy', *Computer Law & Security Review* (2014) Vol. 30(3) 286–305.

[97] Article 29 Working Party, Opinion 01/2015 on Privacy and Data protection Issues Relating to the Utilisation of Drones, 16 June 2015.

Besides, it must not be forgotten that trafficked individuals may also be in need of international protection.[98] The rhetoric converging border control, irregular migration and fighting human trafficking demonstrate that the position of trafficked persons in particular may be precarious if the use of drones is regularised. Otherwise, the effect would be as Finn and Wright argue to target 'the usual suspects' and 'undesirables'.[99] In line with privacy and data protection requirements, one solution would be to employ drones only in specific investigations as a targeted response or for a longer period of evidential collection under strict criteria and only when there are no other less intrusive means to achieve the same purpose. Prior authorisation for an independent judicial authority could also be necessary in order to secure that police authorities do not over-rely on drones. The underlying aim should not be to allow for State authorities to invest in new toys of surveillance, but rather to 'exploit' already existing means in cases where other mechanisms have failed to provide for a solution. As regards specific guidelines, sensors could be turned on and off in flight in order to avoid continuous recording and private areas could be automatically masked. Other individuals who are accidentally captured in images and videos should be automatically detected and pixelated.[100] Similarly, the depersonalisation of trafficked victims' images should also be foreseen in order to guarantee both their safety and privacy. In this regard, a proper regulatory framework concerning the utilisation of drones for civilian purposes, including law enforcement would be a significant addition.

4. Conclusion

Combating human trafficking has become an important political priority for many governments around the world. In this context, reliance on technological developments has been equally growing. In fact, the interest in technology as a tool against the crime is expanding; for example, Microsoft has a research program specifically devoted to the role of technology in human trafficking, offering research grants.[101] Ignoring the role of technology would be a mistake and would give perpetrators, who already take advantage of it in numerous ways, an unnecessary edge. At the same time, the privacy of individuals in general and the protection of their personal data in particular must be respected to the extent possible, while balancing against the fact that many trafficking victims are at risk of torture, serious sexual abuse and even death. In the context of criminal investigations, the difference between a regular procedure in a typical case and an emergency response is crucial, because it can affect the tools that can be used and eventually the impact on the right to the private life of the individuals affected as well as to their newly-born EU fundamental right of data protection. At the same time, evidence collected through 'ambiguous' technological forms and without compliance with the conditions provided by law can be excluded before national Courts, thus adding further protection. In the context of forced labour, technology may be better harnessed by mandatory reporting and requirements to scrutiny by regulators. Ultimately there is a balance that needs to be achieved. The solution requires trust that policies and procedures will be ethically applied when such trust in many developed countries is at an all-time low and in many under developed countries is non-existent. The scale of human trafficking however requires that balance to be achieved to ensure that we have survivors not victims and no impunity for perpetrators.

Felicity Gerry QC (Felicity.Gerry@cdu.edu.au) is called to the Bar in England and Wales and admitted to the Supreme Court of the Northern Territory of Australia She has a long history in dealing with cases involving sexual offending and human trafficking and/or cybercrime and using technology in criminal cases. Since 2013, Felicity has also held a research active post in the School of Law at Charles Darwin University. Her research into the global law on human trafficking recently enabled her to assist transnationally in the reprieve from execution of Philippine national Mary Jane Veloso. In the context of computer law and security, Felicity has published papers on the Google and Microsoft cases in the context of human rights and transnational evidence collection and she recently provided a report for the ILRC of the American Bar Association Justice Defenders Programme on the draft cyber law for Cambodia.

Julia Muraszkiewicz (j.muraszkiewicz@gmail.com) is a Ph.D. Candidate at Vrije Universiteit Brussel. She explores human trafficking, EU criminal law and human rights. Her focus is on the non-prosecution or non-application of penalties to the victims of human trafficking. She is also a researcher on the EU funded TRACE (Trafficking As a Criminal Enterprise) project.

Niovi Vavoula (n.vavoula@qmul.ac.uk) is a Ph.D. Candidate and Research Assistant at Queen Mary, University of London. She explores the privacy concerns raised by the set-up and operation of EU immigration databases. Her research interests include the criminalisation of irregular migration, surveillance technologies, privacy and data protection and EU Criminal law.

[98] For instance, Article 20(5) of the EUROSUR Regulation prohibits the transmission of personal data of persons needing international protection and of asylum applicants.

[99] Finn and Wright, *op. cit.*, p.188.

[100] EDPS, *op. cit.*, p.15.

[101] Microsoft, 'The Role of Technology in Human Trafficking – RFP' (*Microsoft Research*) <http://research.microsoft.com/en-us/collaboration/focus/education/human-trafficking-rfp.aspx> accessed 25 July 2015.