Report from Dagstuhl Perspectives Workshop 14401

# Privacy and Security in an Age of Surveillance

**Edited by**

**Bart Preneel[1], Phillip Rogaway[2], Mark D. Ryan[3], and Peter Y. A. Ryan[4]**

1 **KU Leuven and iMinds, BE,** Bart.Preneel@esat.kuleuven.be
2 **University of California, Davis, US,** rogaway@cs.ucdavis.edu
3 **University of Birmingham, GB,** m.d.ryan@cs.bham.ac.uk
4 **University of Luxembourg, LU,** peter.ryan@uni.lu

## Abstract

The Snowden revelations have demonstrated that the US and other nations are amassing data about people's lives at an unprecedented scale. Furthermore, these revelations have shown that intelligence agencies are not only pursuing passive surveillance over the world's communication systems, but are also seeking to facilitate such surveillance by undermining the security of the internet and communications technologies. Thus the activities of these agencies threatens not only the rights of individual citizens but also the fabric of democratic society.

Intelligence services do have a useful role to play in protecting society and for this need the capabilities and authority to perform targeted surveillance. But the scope of such surveillance must be strictly limited by an understanding of its costs as well as benefits, and it should not impinge on the privacy rights of citizens any more than necessary.

Here we report on a recent Dagstuhl Perspectives Workshop addressing these issues – a four-day gathering of experts from multiple disciplines connected with privacy and security. The meeting explored the scope of mass-surveillance and the deliberate undermining of the security of the internet, defined basic principles that should underlie needed reforms, and discussed the potential for technical, legal and regulatory means to help restore the security of the internet and stem infringement of human-rights by ubiquitous electronic surveillance.

**Perspectives Workshop** September 28 to October 2, 2014 – http://www.dagstuhl.de/14401
**1998 ACM Subject Classification** E.3 Data Encryption, K.4.1 Public Policy Issues, K.4.2 Social Issues, K.5.2 Governmental Issues, K.6.4 Security and Protection
**Keywords and phrases** Big data, encryption, mass surveillance, privacy
**Digital Object Identifier** 10.4230/DagRep.4.9.106

## 1 Executive Summary

*Bart Preneel*
*Phillip Rogaway*
*Mark D. Ryan*
*Peter Y. A. Ryan*



Revelations over the last few years have made clear that the world's intelligence agencies surveil essentially everyone, recording and analyzing who you call, what you do on the web, what you store in the cloud, where you travel, and more. Furthermore, we have learnt that intelligence agencies intentionally subvert security protocols. They tap undersea cables.


Privacy and Security in an Age of Surveillance, *Dagstuhl Reports*, Vol. 4, Issue 9, pp. 106–123
Editors: Bart Preneel, Phillip Rogaway, Mark D. Ryan, and Peter Y. A. Ryan

Dagstuhl Reports
Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

They install malware on an enormous number targets worldwide. They use active attacks to undermine our network infrastructure. And they use sophisticated analysis tools to profile individuals and groups.

While we still understand relatively little about who is doing what, the documents leaked by Snowden have led to the conclusion that the Five Eyes[1] organizations are going far beyond anything necessary or proportionate for carrying legitimate intelligence activities. ot an equivalent access to documents Governmental assurances of oversight have come to ring hollow, as any oversight to date seems to have been ineffectual, and is perhaps a complete sham.

Can democracy or nonconformity survive if the words and deeds of citizens are to be obsessively observed by governments and their machines? The rise of electronic surveillance thus raises questions of immense significance to modern society. There is an inherent tension. Machine-monitored surveillance of essentially everything people do is now possible. And there are potential economic, political, and safety benefits that power may reap if it can implement effective population-wide surveillance. But there is also a human, social, economic, and political harm that can spring from the very same activity.

The goal of our workshop was to gather together a mix of people with knowledge and expertise in both the legal and technological aspects of privacy and surveillance, to try to understand the landscape that we now live in, and to debate approaches to moving forward. We invited people from a wide range of domains, including members of the intelligence community. All invitees in the intelligence community declined the invitations – in most cases choosing not even to reply. Also, we found that we had more success in getting positive replies from members of the technical community than members of the legal or regulatory communities. Consequently, the makeup of the workshop was not as diverse and balanced as we had hoped. Nonetheless, we felt that we achieved a healthy mix, and there was plenty of lively debate. The issues addressed by this workshop were unusually contentious, and discussions at times were highly animated, even heated.

It is often argued that privacy is not an absolute right. This is true, but this is also true of other rights. The right to freedom must be tempered by the fact that people who are convicted of crimes may forfeit this right for a period. Equally, someone for whom there are sound grounds for suspicion might forfeit some privacy rights. But in any event, any such breaches must be targeted and proportionate and justified by well-founded grounds for suspicion.

An important observation that came up repeatedly in discussions is that privacy is not just an individual right but essential to the health of a democratic society as a whole.

How can society as whole be provided strong assurance that intelligence services are "playing by the rules" while at the same time allowing them sufficient secrecy to fulfill their role? It seems feasible that technical mechanisms can contribute to solving this problem, and indeed a number of presentations addressed aspects of it. One might imagine that something analogous to the notion of zero-knowledge proofs might help demonstrate that intelligence agencies are following appropriate rules while not revealing details of those activities. Another possibility that was proposed is to make the amount of surveillance public in a verifiable fashion but without revealing the targets. Thus one might imagine that a specified limit be placed on the proportion of traffic available to intelligence services. The effect would be to force the agencies to be correspondingly selective in their choice of targets.

The crypto and security community should invest a substantial effort to make all layers

[1] This term is used to indicate Australia, Canada, UK, USA, and New Zealand.

of the internet and our devices more secure and to strengthen the level of privacy offered. This may create a natural barrier to mass surveillance and will also bring a more robust network infrastructure to a society that is increasingly reliant on it for critical services. Such a development may eventually increase the cost for targeted surveillance, but there is no indication that this would become prohibitive.

As is traditional for Dagstuhl, we started with a round table of quick introductions from the participants, including brief statements of what they hoped to get out of the workshop. We then had an open discussion on the goals of the workshop and of how best to organise the workshop to achieve these goals. It was decided to structure discussions into three strands:

- Principles
- Research directions
- Strategy

The outcomes of these discussions are detailed in a separate "Manifesto" document. The workshop was then structured into a number of plenary sessions alternating with breakouts into the three strands. The plenary sessions were made up of presentations from participants and feedback from the breakouts followed by discussion.

The problems addressed in this workshop are immensely challenging, and carry vast implications for society as a whole. It would not be reasonable to expect a small group of people – and a group not particularly representative of society as a whole – to produce solutions in the course of four days. Our goal was to gain some understanding of guiding principles and ways forward.

## 2 Table of Contents

# 3 Talks

A total of 20 talks were given over course of the workshop, most of these taking around 30 minutes each. Abstracts for 18 of these talks are given below.

## 3.1 An introduction and brief overview of NSA and IC surveillance – from dragnets to drone strikes.

*Jacob Appelbaum (The Tor Project, Cambridge US)*



Surveillance is ultimately about power relationships. Various intelligence agencies wish to have total control through total surveillance. They attempt to sabotage cryptography in service of surveillance and censorship. Such power is used in concert with other agencies to perform actions ranging from harassment to political assassinations with drones.

## 3.2 How to Wiretap the Cloud without almost anybody noticing

*Caspar Bowden (Independent privacy advocate, EU)*



As Microsoft's Chief Privacy Adviser, I warned them about the effects of FISA 702 on the rest of the world's privacy in 2011. Shortly afterwards I was made redundant (and I did not know about PRISM, or that Microsoft was PRISM's first "corporate partner" since 2008).

My analysis was based on close scrutiny of open sources, and from Sep 2011 I tried to warn EU institutions, including the Commission (at the Cabinet level) and Data Protection Authorities. However no notice was taken. I contributed to a report to the European Parliament in Sep 2012 which laid out the precise legal mechanisms of FISA 702.

After the Snowden revelations the European Parliament phoned me up and said "Caspar ... it's all true!" and asked me to write the official briefing Note for the EP inquiry. The analysis (if not all the Conclusions) was accepted in the official inquiry resolution and the findings of the Commission EU-US "Working Group' report.

A central conclusion is still under-reported. The actual definition in FISA 1801(e) of "foreign intelligence information" is conditioned on US nationality. A legal standard of "necessity" applies to Americans, but otherwise any information which relates to US foreign policy interests is caught. This structure appears to be unique. In the surveillance law of most other nations the distinction is based on international vs. domestic communications, but only a few other countries (AU, NZ, CA, DE) afford more rights to their own citizens.

This gives rise to extreme asymmetries in Cloud computing: for example, US citizens' data has equal protection to that of US residents' under European law, but the US recognizes no privacy rights in EU data reciprocally under US "national security" laws. The structure of FISA 702 amounts to a double-discrimination by nationality, which prima facie is incompatible with ECHR and ICCPR (but the US, UK, and Israel reject this interpretation).

There are also suspicious "FISA-shaped loopholes" buried deep in EU data protection laws, and more so even in the new proposed General Data Protection Regulation. Contrary

to the mood music from the EU Commission that somehow the GDPR was the solution to post-Snowden privacy, several new bureaucratic mechanisms were invented to widen loopholes into floodgates. Similarly, the official EU DPAs were sanguine about Cloud computing before Snowden, in the face of clear warnings, but then were obliged to issue two "clarifications" on Cloud computing which have been some of the most richly amusing "Privacy theatre" on the stage. The last fifteen years of work by Data Protection institutions has crumbled into an abyss, and must now be reconstructed on foundations of computer science. In private, DPAs admit this.

## 3.3 Rigorous Survey on Privacy Attitudes Toward Privacy in Products

*Jon Callas (Silent Circle and Blackphone, CH)*



It is commonly asserted that privacy is a niche concern, that general consumers don't care enough about privacy to make it a significant factor in their decision to choose one product over another. But what is the reality, especially in the present world of surveillance? This presentation will show data collected from a statistically significant populations in the US and Germany, controlled for sex and broad population versus ICT-savvy people that suggests that whatever the anecdotes are, general consumers care about privacy.

## 3.4 On-line Privacy post-Snowden: what future? A European perspective

*Joe Cannataci (University of Malta, MT, and University of Groningen, NL)*



Like Charles Raab[2], I think that there is a good deal of work to be done on further conceptualising privacy in the context of security & open government, but I don't think that sorting out our conceptualisation of privacy will be key to doing something practical about privacy protection and surveillance in the short and mid-term.

In recent EU-supported research projects such as CONSENT[3], SMART[4], and RESPECT[5], the results of quantitative and qualitative research which involved thousands of EU citizens from across all 28 EU member states, suggest that:

- People care deeply about privacy even though their conceptualisation of it may be imprecise
- People care about privacy ... or say they do but will indulge in privacy-unfriendly behaviour especially if that behaviour is more convenient, easier, the path of least resistance etc. etc.

[2] Charles D. Raab, "Regulating surveillance: the importance of principles," in *Surveillance in Europe*, David Wright and Reinhard Kreissl, Routledge 2014; and Charles D> Raab, "Beyond the Privacy Paradigm: Implications for Regulating Surveillance," http://privacylaw.berkeleylawblogs.org/2013/05/24/charles-raab-beyond-the-privacy-paradigm-implications-for-regulating-surveillance/

[3] http://www.consent.law.muni.cz/

[4] http://smartsurveillance.eu/

[5] http://respectproject.eu/

- People care about surveillance, don't like pervasive surveillance . . . but their level of trust in the state varies depending on which state may live in;

When considering the prevailing set of realities and emerging trends it would seem that:

- on the one hand, in the world of big data, privacy invasion is often the business model;
- on the other hand, the very corporations which have grown huge on the back of advertising revenue derived from their ability to target individual customers, thanks to the profiling of their on-line activities and preferences, are ironically doing their utmost to retain or attract customers by introducing and leading the adoption of military-grade encryption in data transfer and data "at rest" whether in e-mail or other form of communication apps;

In this presentation, I use the MAPPING project[6] as a case study and an example of the latest European policy initiatives in cyberspace. MAPPING is a "Science in Society" project which is investigating practical ways forward at the points of intersection of internet governance, privacy protection and intellectual property rights. It is currently exploring the feasibility and desirability of a blended approach as the way forward by investigating:

- Technological solutions such as encryption;
- Overlay software solutions and eventually underlay architectural change as a method of improving user privacy and possibly by creating "parallel internets" or "parallel universes";
- Innovative legal instruments, especially in the sphere of international law, including a multi-lateral treaty which could serve as a new "magna charta for the internet"

When tackling the options listed above it is clear that a few home-truths need to be faced:

- Governments, organised crime and large corporations will continue to attempt surveillance against anybody/everybody;
- Governments will only "come to the table" if they have to, if they are made to do so;
- Technology, including cryptography, can be one of the ways to bring governments to the table;
- Personal data has become part of the business model for a multi-billion dollar per year industry;
- Re-thinking the business model is necessary but will encounter very stiff resistance from those with vested interests including their political allies;
- Having convenient (i.e. super-easy to use, low/non-cost) crypto is part of the answer;

A number of EU states do see eye-to-eye on the matter but they must co-exist in a space which, surveillance-wise, is currently dominated by the US, the UK and is assailed by at least ten (10) other nation states most of which are outside Europe. So what should Europe do? Build its own cyberspace under its own value-system and hope that others will eventually join it? Additionally, to complicate matters there's the spectre of cyberwar. Do you arm for it? Do you use it as an excuse? Or do you outlaw cyberwar? That is, do you declare cyberspace as a zone where no warfare shall be carried out in the spirit of, say, the START (nuclear) process or the Chemical Warfare treaty? The current stalemate in USA-EU relations over the matter of data protection and privacy law especially in the area of national security and mass surveillance, means that the European Commission's suggestion that the USA sign and ratify the Council of Europe's 1981 Data Protection Convention is unrealistic and insensitive to US domestic traditions and priorities. This suggests that new avenues need to be explored to try to resolve the stalemate and improve momentum on achieving a new consensus position. The MAPPING project is striving to explore such avenues in a number of ways. These

[6] http://www.mappingtheinternet.eu/

include the creation of a Working Group on Technical Solutions for cyberspace considering the feasibility and desirability of parallel internets where cryptography is not only welcome but indeed the norm. MAPPING has also created a Working Group on Legal Solutions which is investigating the feasibility and desirability of new legal instruments including that of a multilateral convention on surveillance in cyberspace. In doing so it raises the issue of which cyberspace? The current one or a cyberspace divided into a number of inter-connected but distinct networks subject to different jurisdictions. This extends the vision of the Internet as a "network of networks" to that of a "network of networks of networks".

The work in the MAPPING Project will be taken forward by meetings of its WP4 Technical Working Party on 12–13 November 2014 in Berlin and the WP4 Legal Working Party in Paris on 15–16 December 2015. Both Working Parties will then meet in Washington DC in the USA on 23–25 March 2015 with other meetings planned to be held in other locations including possibly Beijing. These Working Party meetings will prepare the ground for the MAPPING Annual General Assembly for stakeholders scheduled for 22–23 Sep 2015 and subsequent MAPPING General Assemblies for stakeholders scheduled for 2016, 2017 and 2018. The success of the European MAPPING project will depend on its continued ability to engage stakeholders world-wide and rise above the factors that have bogged down other internet governance and on-line privacy initiatives.

## 3.5 The technical and public policy ramifications of the Snowden revelations

*George Danezis (University College London, GB)*



The documents leaked to journalists by Edward Snowden have dominated the news for over a year, however the fragmented way in which they have been published makes it difficult to define their overarching narrative, and assess the overall impact of their substance. In this talk I will present a unified view of the pervasive monitoring operation of the NSA and GCHQ, spanning from different modes of access, to advanced analysis of the collected material. This unified approach will lead me directly to a number of technology public policy options for countries subject to such surveillance to protect their citizens and create incentives for a cyber-investigation regime that is more compatible with rule of law.

## 3.6 DP5: Privacy-preserving Presence Protocols

*Ian Goldberg (University of Waterloo, CA)*


**Joint work of** Borisov, Nikita; Danezis, George; Goldberg, Ian
**Main reference** N. Borisov, G. Danezis, I. Goldberg, "DP5: A Private Presence Service," Technical Report 2014-10, Centre for Applied Cryptographic Research, University of Waterloo, 2014.
**URL** http://cacr.uwaterloo.ca/techreports/2014/cacr2014-10.pdf

Users of social applications like to be notified when their friends are online. Typically, this is done by a central server keepingtrack of who is online and offline, as well as of the complete friendgraph of users. However, recent NSA revelations have shown that addressbook and

buddy list information is routinely targetted for massinterception. Hence, some social service providers, such as activistorganizations, do not want to even possess this information about their users, lest it be taken or compelled from them. In this talk, we present DP5, a new suite of privacy-preserving presence protocols that allow people to determine when their friends are online (and to establish secure communications with them), without acentralized provider ever learning who is friends with whom. DP5 accomplishes this using an implementation of private information retrieval (PIR), which allows clients to retrieve information fromonline databases without revealing to the database operators what information is being requested.

## 3.7 We fix the Net!

*Christian Grothoff (TU München, DE)*



GCHQ, CSET and the NSA are colonizing the Internet, and the IETF is unwilling to commit to serious changes to the architecture to stop mass surveilance. The GNUnet project develops an alternative network architecture, initially to be deployed as an overlay network, to help civilization escape from PRISM.

## 3.8 Procurement – Privacy and Security

*Marit Hansen (Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein – Kiel, DE)*



Procurement procedures can be very influential concerning the choice for or against privacy and security features and guarantees. This talk discusses legal requirements from European data protection law as well as further advanced regional data protection legislation that demands that preference is given to products or systems that can prove compliance with law (State Data Protection Act Schleswig-Holstein from 2000) with a reference to certification procedure.

The data protection framework is not addressing security-relevant information, though. This became clear when journalists, on the basis of the Snowden revelations, reported on companies being active on behalf of the German government on the federal and on the state level that have connections with the NSA or are at least legally obliged to disclose privacy- or security-related information to government bodies (e.g. secret services). The reaction of the German federal government was a No-spy decree demanding a self-declaration of tenderers, and in fact they stopped the contract with some companies. This may be an interesting and potentially effective approach. However, it may be legally challenged as to be discriminating and not being in line with the European Procurement Directive.

## 3.9 The Tragedy of Privacy: Abstract and request for feedback

*Amir Herzberg (Bar-Ilan University, IL)*



Privacy is mostly viewed as a right of every *individual* to restrict collection, distribution and use of information related to him or herself. Most regulations, technologies and debate related to privacy, focus on this aspect, i.e., allowing individuals to control access to their private information, mainly by requiring *informed consent*. However, we argue that the informed-consent requirement may not suffice to protect the interests of individuals. Furthermore, we argue that there is insufficient attention to the *important role of privacy for society* as a whole; this implies a need for establishing additional privacy-protecting mechanisms.

We focus on the privacy threats due to the growing popularity of Big-Data Web-Services, which provide (usually free) services to huge populations, in return to permission to use user's information for commercial purposes such as advertising. We analyze potential applications of the big-data services, and argue that these corporations offer an increasingly-attractive deal for consumers, making the big-data services the ultimate resellers and providers of goods, services and information.

We argue that these advantages turn Big-Data Web-Services into a significant risk to global economy and society. The risk is due to their huge competitive advantage, and further differences compared to traditional businesses, mainly: (1) huge entrance barrier making this an exclusive club of few huge companies, (2) modest employee base and (3) mobility of assets and production facilities, allowing them to optimize location for tax-minimization and other considerations.

We argue that, in spite of concerns regarding personal privacy, it is perfectly *rational* for users to give their consent, even if they conceive dire implications from the establishment of huge collections of private information; we draw parallel to the well-known *tragedy of the commons*, and hence refer to this phenomena as the *tragedy of privacy*. This situation is aggravated due to cognitive processes that result in failure of individuals to properly evaluate the long-term implications of the sharing of private information, by themselves and by society at large, and due to the huge media-influence and branding of the Big-Data Web Services. The limited, arguably insufficient 'price' demanded by users for their information, is supported by experimental evidence, as well as by observations over existing practices.

We conclude that society should protect privacy by legislative measures, however, we offer a pessimistic forecast on the feasibility of adoption of effective measures that will restrict the collection and use of private information, properly protecting individuals and society. We note that the feasibility of adoption is further reduced by the cooperation between big-data services and governmental surveillance and intelligence agencies, which will further increase as gradual adoption of encryption technologies will reduce the value of eavesdropping. Another factor which works against adoption of privacy-protecting legislation is the growing use and dependency of politicians on big-data services, both processes further eroding privacy. One hope may be that governments may act to restrict privacy exposures to *foreign* corporations.

## 3.10 Back to the typewriters? – Rethinking informational self-determination in the era of mass state surveillance

*Eleni Kosta (Tilburg University, NL)*



The right to informational self-determination encompasses the right of individuals to determine who can use their data, for what purposes, under what conditions, and for how long. In private relationships, this is expressed primarily via individuals' consent to the processing of their personal data. Recent publications on the PRISM and TEMPORA surveillance programmes demonstrate that citizen data are being secretly – without their knowledge and consent – collected by the state via private companies, at a massive scale. This blanket and mass citizen surveillance seriously undermines individuals' informational self-determination and effective legal protection. The current checks and balances in consumer-business relationships are based on the assumption that government access to industry-processed data is an exception, which does not require regulation in the consumer-business realm. Now that the exception is effectively becoming the rule, the current legal framework of citizen protection presents a major gap. Therefore, consumer-business data protection requires rethinking. Building on the theories of informational self-determination and constitutionalisation of data protection, the proposed research will identify the required systemic revisions in the European data protection framework, in particular in the system of checks and balances to compensate for the loss of citizen control over state access to citizen data via private companies. For identifying the systemic revisions needed to compensate for this loss of control, rights and principles such as due process, transparency and accountability will be studied, as fundamental elements of the European legal tradition. The proposed research will contribute to transparency in business practices, to enhance legal certainty for users and companies. It will also be of great value to regulators and policy-makers, providing guidance on how the legal and regulatory framework can be adapted to offer effective legal protection when states access citizen data via the databases of private companies.

## 3.11 Search on Encrypted Data Can Be Practical (Use It!)

*Hugo Krawczyk (IBM TJ Watson Research Center – Hawthorne, US)*


**Joint work of** Cash, David; Faber, Sky; Jaeger, Joseph; Jarecki, Stanislaw; Jutla, Charanjit; Krawczyk, Hugo; Nguyen, Quan; Rosu, Marcel; Steiner, Michael

I will discuss some advances in practical solutions to the problem of searchableencryption in which a data owner outsources a database to an external server E (e.g., the cloud) in encrypted form. Later D can authorize clients to search thedata at E while hiding information about the database and queried values from E,and preventing clients from learning information they are not authorized for. We also consider the PIR-like requirement by which the data owner D needs to authorize queries while minimizing the information it learns about queried values. In all cases, searches at E are performed without ever decrypting dataor queries (in particular, E never gets the decryption keys). A solution developed by IBM Research and UC Irvine teams presents a majoradvance relative to prior work that focused on single-keyword search, singleclient, and implementations in small-size databases. This new work supportssearch via any boolean expression applied to sets of keywords associated withdocuments in the

database as well as range queries. Our implementation of theproposed protocol has been tested on databases with billions of index entries (document-keyword pairs), e.g., a US-scale census database with 100 millionrecords each with 1,000 associated keywords and a very large collection ofcrawled web-pages that includes, among others, a full snapshot of the English Wikipedia. Recently, we expanded the system to support more costly queries including substring, wildcard and phrase searches. The availability of such technology enables privacy solutions that secure databy separating encrypted data from the keys use to decrypt it, and by applying fine-grain access control and delegation mechanisms at the data owner end. The data is secured against insider and outsider attacks on the outsourced database: the holder of such database cannot disclose the information even atgun point, it simply has no access to it. Applications range from conformance toprivacy regulations, secure and controlled sharing of information, and defenses against surveillance (even when the data is stored at foreign entities). This work is documented in the following papers:

- http://eprint.iacr.org/2013/169,
- http://eprint.iacr.org/2013/720,
- http://eprint.iacr.org/2014/853.

## 3.12 Dancing with Governments

*Susan Landau (Department of Social Science and Policy Studies, Worcester Polytechnic Institute, US)*



We have the tools and they have the problems, yet there's a mismatch. They don't take our solutions and we don't solve their problems. If the research community really wants to provide scientific advice to government, there are a number of steps to take, the first of which is to understand their problems – this is the actual problem, not the one they think they have. The second is to understand their equities, the third, to speak their language. This talk will discuss successfully dancing with governments, improving law, policy, and – sometimes – even privacy in the process.

## 3.13 Dual EC and what it taught us about vulnerabilities of the standardization ecosystem

*Tanja Lange (TU Eindhoven, NL)*



**Joint work of** S. Checkoway, R. Niederhagen, A. Everspaugh, M. Green, T. Lange, T. Ristenpart, D. J. Bernstein, J. Maskiewicz, H. Shacham, M. Fredrikson

**Main reference** S. Checkoway, R. Niederhagen, A. Everspaugh, M. Green, T. Lange, T. Ristenpart, D. J. Bernstein, J. Maskiewicz, H. Shacham, M. Fredrikson, "On the Practical Exploitability of Dual EC in TLS Implementations," in Proc. of the 23rd USENIX Security Symposium, pp. 319–335, USENIX Association, 2014.

**URL** https://www.usenix.org/conference/usenixsecurity14/technical-sessions/presentation/checkoway

**URL** https://projectbullrun.org/dual-ec

This talk describes how the back door in Dual EC works and how it can be exploited in TLS implementations. It also gives some historical background on how the standards including Dual EC came to live and when knowledge of the back door became public.

## 3.14 Security of Symmetric Encryption against Mass Surveillance

*Kenneth G. Paterson (Royal Holloway University of London, GB)*


**Joint work of** Bellare, Mihir; Paterson, Kenneth G.; Rogaway, Phillip
**Main reference** M. Bellare, K. Paterson, P. Rogaway, "Security of Symmetric Encryption against Mass Surveillance," in Proc. of the 34th Annual Cryptology Conf. (CRYPTO'14), LNCS, Vol. 8616, pp. 1–19, Springer, 2014; pre-print available as report 2014/438 from Cryptology ePrint Archive.
**URL** http://dx.doi.org/10.1007/978-3-662-44371-2_1
**URL** http://eprint.iacr.org/2014/438

Motivated by revelations concerning population-wide surveillance of encrypted communications, we formalize and investigate the resistance of symmetric encryption schemes to mass surveillance. The focus is on algorithm-substitution attacks (ASAs), where a subverted encryption algorithm replaces the real one. We assume that the goal of "big brother" is undetectable subversion, meaning that ciphertexts produced by the subverted encryption algorithm should reveal plaintexts to big brother yet be indistinguishable to users from those produced by the real encryption scheme. We formalize security notions to capture this goal and then offer both attacks and defenses. In the first category we show that successful (from the point of view of big brother) ASAs may be mounted on a large class of common symmetric encryption schemes. In the second category we show how to design symmetric encryption schemes that avoid such attacks and meet our notion of security. The lesson that emerges is the danger of choice: randomized, stateless schemes are subject to attack while deterministic, stateful ones are not.

## 3.15 Privacy as a Social Value and as a Security Value

*Charles Raab (University of Edinburgh, UK)*


**Main reference** Charles D. Raab, "Privacy as a Security Value,", pp. 39–58, in: Dag Wiese Schartum, Lee Bygrave and Anne Gunn Berge Bekken (eds.), "Jon Bing: En Hyllest / A Tribute", Oslo: Gyldendal, 2014.

- Privacy and security (national security, public safety) have no agreed singular meanings.
- Law and conventional wisdom: Privacy is only an individual right.
- But the social and public interest value of privacy is insufficiently recognized: it can be construed as a constitutive public good and as part of the public interest as well as being an individual right.
- Across and within societies, different people construe, and value, privacy differently, and privacy has to be seen contextually.
- Security is also a slippery term, and can refer to different levels of social scale: individual, neighbourhood, local community, a whole country or society, a region, the world. 'Safety' is a related concept (and in today's world, has become a pre-eminent value, along with 'security').
- These definitional and conceptual ambiguities and variations are not necessary a problem, except when – in legal, political, social, and medial parlance-it is said that (e.g.) 'privacy' conflicts with 'security' and must be 'balanced'.
- The concept of 'balance' is conceptually and empirically flawed; 'balancing' (individual) privacy and (national) security is a rhetorical and tendentious proposition.

- We need to think more imaginatively about the relationship between privacy and security, especially if we are to avoid security (almost always) trumping privacy in public policy, surveillance practice, and in popular parlance.
- It is helpful to consider that privacy and security have closer affinities than the 'versus' rhetoric allows. An important part of the value of privacy is that it affords a zone of security or safety. If so, the relationship between the two values is much more interesting and complex, and points to a need for a creative policy discourse.
- In addition, if privacy is an element of the public interest and a foundational principle of social relationships, for which there is considerable psychological and sociological support, then a relationship between privacy and security (or safety) as also public-interest values, becomes more complex and requires more subtle public-policy approaches.

## 3.16 End-to-end encrypted mail made easy for users

*Mark D. Ryan (University of Birmingham, GB)*


**Main reference** M. D. Ryan, "Enhanced certificate transparency and end-to-end encrypted mail," in Proc. of the 21st Annual Network and Distributed System Security Symposium (NDSS'14), 14 pages, The Internet Society, 2014.
**Main reference** http://www.internetsociety.org/doc/enhanced-certificate-transparency-and-end-end-encrypted-mail
**URL** https://www.cs.bham.ac.uk/~mdr/research/papers/pdf/14-ndss-cert.pdf

The certificate authority model for authenticating public keys of websites has been attacked in recent years, and several proposals havebeen made to reinforce it. We develop and extend *certificate transparency*, a proposal in this direction, so that it efficiently handles certificate revocation. We show how this extension can be usedto build a secure end-to-end email or messaging system using PKI with no requirement to trust certificate authorities, or to rely on complexpeer-to-peer key-signing arrangements such as PGP. This makesend-to-end encrypted mail possible, with apparently few additional usability issues compared to unencrypted mail (specifically, users donot need to understand or concern themselves with keys or certificates). Underlying these ideas is a new attacker model appropriate for cloud computing, which we call "malicious-but-cautious".

## 3.17 Data Obfuscation/Pollution: adapting TrackMeNot to counter surveillance

*Vincent Toubiana*


**Joint work of** Toubiana, Vincent; Howe, Daniel; Nissenbaum, Helen
**URL** http://cs.nyu.edu/trackmenot/

TrackMeNot is a browser extension designed to pollute the web search profile and web search history of users. Initial design of TrackMeNot considered search engines as the main adversaries. However, recent revelation about the NSA program XKeyScore highlights that surveillance can be triggered by specific search queries. This revelation raises the question "Could data pollution be used to make bulk collection inefficient?". Addressing this question implies to adapt the threat model to consider an adversary that use less accurate profiles. Furthermore, in order to adapt to this type of adversary it is necessary to find new sources of keywords like the list released by DHS in 2012. The open question is could data pollution have a positive outcome and could it be extended to other services than search.

### 3.18 The Velocity of Censorship: High-Fidelity Detection of Microblog Post Deletions

*Dan S. Wallach (Rice University, US)*


**Joint work of** Zhu, Tao; Phipps, David; Pridgen, Adam; Crandall, Jedidiah R.; Dan S. Wallach
**Main reference** T. Zhu, D. Phipps, A. Pridgen, J.',R. Crandall, D. S. Wallach, "The Velocity of Censorship: High-Fidelity Detection of Microblog Post Deletions," in Proc. of the 22th USENIX Security Symposium, pp. 227–240, USENIX Association, 2014; pre-print available from the author's webpage.
**URL** https://www.usenix.org/conference/usenixsecurity13/technical-sessions/paper/zhu
**URL** http://www.cs.unm.edu/~crandall/usenix13.pdf

Weibo and other popular Chinese microblogging sites are well known for exercising internal censorship, to comply with Chinese government requirements. This research seeks to quantify the mechanisms of this censorship: how fast and how comprehensively posts are deleted. Our analysis considered 2.38 million posts gathered over roughly two months in 2012, with our attention focused on repeatedly visiting "sensitive" users. This gives us a view of censorship events within minutes of their occurrence, albeit at a cost of our data no longer representing a random sample of the general Weibo population. We also have a larger 470 million post sampling from Weibo's public timeline, taken over a longer time period, that is more representative of a random sample.

We found that deletions happen most heavily in the first hour after a post has been submitted. Focusing on original posts, not reposts/retweets, we observed that nearly 30% of the total deletion events occur within 5–30 minutes. Nearly 90% of the deletions happen within the first 24 hours. Leveraging our data, we also considered a variety of hypotheses about the mechanisms used by Weibo for censorship, such as the extent to which Weibo's censors use retrospective keyword-based censorship, and how repost/retweet popularity interacts with censorship. We also used natural language processing techniques to analyze which topics were more likely to be censored.

## 4 Acknowledgements

Our deepest thanks to Matt Blaze, who co-organized this Dagstuhl event with us, but who was unable to attend for reasons beyond his control. Many thanks to Johana Hamilton for making available to us her documentary film *1971*, which we were delighted to screen during our workshop prior to its theatrical release.

## 5 References

- "Necessary and Proportionate Principles." International Principles on the Application of Human Rights to Communications Surveillance. Final version, May 2014. Available from https://necessaryandproportionate.org/.
- Federal Trade Commission (USA). Privacy Online: A Report to Congress. June 1998. Available from the FTC website.
- Gary T. Marx. An Ethics for the New Surveillance. *The Information Society*, 14(3), pp. 171–186, 1998.

- Global Government Surveillance Reform. Joint from AOL, Apple, Dropbox, Facebook, Google, LinkedIn, Microsoft, Twitter, and Yahoo! – https://www.reformgovernmentsurveillance.com/
- Frank la Rue. Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression. Report to the United Nations General Assembly, Human Rights Council. A/HRC/23/40.

## Participants

- Jacob Appelbaum
The Tor Project – Cambridge, US
- Daniel J. Bernstein
Univ. of Illinois – Chicago, US
- Caspar Bowden
GB
- Jon Callas
Silent Circle – San Jose, US
- Joseph Cannataci
University of Malta, MT & University of Groningen, The Netherlands
- George Danezis
University College London, GB
- Pooya Farshim
RHUL – London, GB
- Joan Feigenbaum
Yale University, US
- Ian Goldberg
University of Waterloo, CA
- Christian Grothoff
TU München, DE
- Marit Hansen
ULD SH – Kiel, DE
- Amir Herzberg
Bar-Ilan University – Ramat Gan, IL
- Eleni Kosta
Tilburg University, NL
- Hugo Krawczyk
IBM TJ Watson Res. Center – Hawthorne, US
- Susan Landau
Worcester Polytechnic Inst., US
- Tanja Lange
TU Eindhoven, NL
- Kevin S. McCurley
Google – San Jose, US
- David Naccache
ENS, Paris, FR
- Kenneth G. Paterson
Royal Holloway University of London, GB
- Bart Preneel
KU Leuven and iMinds, BE
- Charles D. Raab
University of Edinburgh, GB
- Phillip Rogaway
Univ. of California – Davis, US
- Mark D. Ryan
University of Birmingham, GB
- Peter Y. A. Ryan
University of Luxembourg, LU
- Haya Shulman
TU Darmstadt, DE
- Vanessa Teague
The University of Melbourne, AU
- Vincent Toubiana
CNIL – Paris, FR
- Michael Waidner
TU Darmstadt, DE
- Dan Wallach
Rice University, US