Manifesto 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, Belgium**
Bart.Preneel@esat.kuleuven.be
2 **University of California, Davis, US**
rogaway@cs.ucdavis.edu
3 **University of Birmingham, Great Britain**
m.d.ryan@cs.bham.ac.uk
4 **University of Luxembourg, Luxembourg**
peter.ryan@uni.lu

Abstract

Before the Snowden revelations about the scope of surveillance by the NSA and its partner agencies, most people assumed that surveillance was limited to what is necessary and proportionate for these agencies to fulfil their prescribed role. People assumed that oversight mechanisms were in place to ensure that surveillance was appropriately constrained. But the Snowden revelations undermine these beliefs. We now know that nations are amassing personal data about people's lives at an unprecedented scale, far beyond most people's wildest expectations.

The scope of state surveillance must be limited by an understanding of its costs as well as benefits. The costs are not limited to financial ones but also include eroding personal rights and the degradation to the integrity, vibrancy, or fundamental character of civil society.

This manifesto stems from a Dagstuhl Perspectives Workshop held in late 2014. The meeting was a four-day gathering of experts from multiple disciplines connected with privacy and security. The aim was to explore how society as a whole, and the computing science community in particular, should respond to the Snowden revelations. More precisely, the meeting discussed the scope and nature of the practice of mass-surveillance, basic principles that should underlie reforms, and the potential for technical, legal, and other means to help stem or restore human rights threatened 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/DagMan.5.1.25

Executive Summary

While intelligence services play a role in protecting democratic societies against their enemies, their capabilities and methods must respect both human rights and the rule of law. Many people have assumed that intelligence agencies did indeed confine themselves to what was necessary to their task – for example, that surveillance was done only on "targeted" individuals, and that a variety of oversight mechanisms ensured this. But the Snowden revelations have made clear that the "Five Eyes" organisations, and by extension other national intelligence agencies, routinely go beyond what most would regard as proportionate and necessary for

Privacy and Security in an Age of Surveillance, *Dagstuhl Manifestos*, Vol. 5, Issue 1, pp. 25–37
Editors: Bart Preneel, Phillip Rogaway, Mark D. Ryan, and Peter Y. A. Ryan
DAGSTUHL MANIFESTOS Dagstuhl Manifestos
Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

the execution of their duties: they electronically surveil most inhabitants of the planet, and have been active in undermining the security of the internet. Oversight mechanisms have been ineffectual.

The Snowden revelations raise issues of immense significance to the information society: how can we resolve the tension that exists between maintaining the effectiveness of intelligence services in protecting society on the one hand, and the need to respect essential privacy rights on the other? The difficulty is aggravated by the impossibility of making the activities and capabilities of intelligence services totally transparent. More subtle approaches are required, and any solutions to this conundrum must involve a mix of legal and technical mechanisms.

To understanding the gravity of the problem one needs to realize that privacy is not just an individual right: it is essential to the health of a democratic society. Society benefits from the ability of people to exercise their rights and freedoms. It *needs* people to do so. Yet privacy rights, like most other rights, are not absolute. Someone for whom there are sound grounds for suspicion of involvement in a serious crime or terrorist activity might forfeit privacy rights with regard to investigations of the purported offences. Still, any such breaches of privacy, and the methods used to accomplish them, must be accountable and transparent.

How can society as a whole be provided strong assurance that intelligence services are "playing by the rules" while at the same time allowing them sufficient secrecy to fulfil their institutional role? It seems possible that technical mechanisms can contribute to solving this problem. One might imagine that something analogous to a zero-knowledge proof might help demonstrate that intelligence agencies are following appropriate rules while not revealing details of those activities. Or one might strive to make public and technically verifiable the total *amount* of surveillance done, but without revealing the targets. One might imagine that a specified limit is placed on the proportion of internet or telephone data and metadata made available to intelligence services. The effect would be to force the agencies to be selective in their choice of targets. In a different direction, the crypto and security communities can strive to make the internet much more secure, hoping to make population-wide surveillance technically or economically infeasible, understanding that modest amounts of targeted surveillance will always be technically and economically feasible.

The problems addressed here have vast implications for society. It would not be reasonable to expect a small group of people, not representative of society as a whole, to produce solutions in the course of less than four days. Our goal was to air technical, legal, and social issues connected to mass surveillance, and to propose a number of guiding principles and ways forward. In the following pages, we do so.

Table of Contents

1 Introduction

The world's communication infrastructure wasn't designed to be robust against nation-state adversaries – and it isn't. Working with industry or in secret, governments track who searches for what, who calls whom and says what, who emails what to whom, who buys what, who goes where, and so on. Using automated means, they can do this on a population-wide scale, surveilling virtually everyone. The surveillance is not entirely passive. When technology is being standardised, governments can exert such weight on standards bodies so as to virtually ensure that the ability to surveil is woven into our technological infrastructure.

The contours of contemporary governmental surveillance did not arise from the leaks of Edward Snowden: they began surfacing several years earlier, from the work of prior whistle blowers and journalists. Still, for many people – even researchers in computer security and cryptography – it was indeed the Snowden revelations that brought home the scope of contemporary surveillance. It was no longer feasible to regard mass surveillance as the fringe concern of conspiracy theorists.

It was in the wake of the Snowden revelations, then, that the organizers felt it important to gather a group at Schloss Dagstuhl. We assembled in September/October of 2014 for four days of discussion. We wanted to explore how society as a whole, and the computing science community in particular, should respond to the Snowden revelations. We aimed to discuss the scope and nature of mass-surveillance, basic principles that should underlie reforms, and potential means to address the problem of ubiquitous surveillance.

Surveillance is by no means limited to governments; industry too is an eager player. Industry and government surveillance are deeply intertwined: governments exploit the capabilities of industry to surveil the users of the ubiquitous electronic services that they provide, while industry exploits the laissez-faire regulatory environment that helps maximize both profits and information of governmental interest. Still, there are significant differences between governmental surveillance and industry surveillance, beginning with the fact that, presumably, only governments, employ surveillance data for assassinations and the suppression of dissent.

This Dagstuhl Manifesto gathers participant views expressed at a Dagstuhl Perspectives Workshop. We assembled a mix of people with expertise in the legal, social-scientific, and technological aspects of privacy and surveillance. We invited members of the intelligence services, but those invitees declined to attend (in most cases failing to even reply). We had more success getting positive replies from members of the technical community than members of the legal or regulatory communities. In the end, the makeup of the workshop was not as balanced as we had hoped. Nonetheless, we felt that we did achieve a healthy mix, which resulted in plenty of lively debate. Indeed the issues addressed by this workshop were unusually contentious for a Dagstuhl workshop, and discussions were, at times, highly animated, even heated. In editing this manifesto, we did not attempt or expect to get every workshop participant to agree to every view we set forth. That would not have been possible.

We have organized this manifesto in three sections. We begin with some basic principles we heard expressed. Our enumeration of principles is rather different from prior ones we have seen. Then we discuss some research problems in this space. It is a diffuse and multidisciplinary area, and the list of research areas we give is similarly diffuse. Finally, we propose some strategies to help redress the balance in favour of the rights to privacy.

Our workshop was the first gathering at Dagstuhl on this contentious topic. It was a relatively rare instance in which computer scientists and others come together to discuss something inherently political associated with our work. The starting point is the decision to take the problem seriously. “Communications surveillance should be regarded as a highly intrusive act that interferes with human rights” says the Necessary and Proportionate document [1]; therefore, one *should* treat the topic with corresponding seriousness. There is an inherently normative core to any serious consideration of privacy and surveillance.

2 Principles

There have been many attempts to enumerate basic principles associated with privacy and surveillance. Prominent examples include the Fair Information Practice (FIP) principles [2], versions of which underlie all information privacy legislation; the list of questions suggested by Gary Marx [3]; the Necessary and Proportionate principles [1]; and the Reform Government Surveillance principles [4]. Our own attempt to compile a list of principles is informed by such works, but includes principles with a more technical slant, as well as those with clear political overtones. Our list takes the form of short imperatives and maxims.

Like most rights, privacy rights are not absolute. For example, when we say that “Every person has the right to communicate privately and securely with every other person” we do not mean that there are *no* circumstances under which it would be legitimate for a state to abridge this right for a given pair of communicants. We mean that the right is the norm and that its abridgment would not be legitimate if carried out *en masse*, without warrant, or outside of a known legal framework.

We begin with high-level maxims on privacy, security, and surveillance (Principles 1–9). Next we list some imperatives that speak more specifically to the design, construction, and operation of privacy-relevant technological systems (Principles 10–15). We end with some imperatives directed to individuals and organisations on the conduct of their work (Principles 16–17).

Basic Privacy Principles

1. **Right to secure communication and services.** Every person has the right to communicate privately and securely with every other person, no matter where they are located. Every person has the right to interact securely and privately with electronic services.
2. **Universality.** With respect to privacy, security, and surveillance, all persons in any jurisdiction have the right to equal treatment without regard to citizenship.
3. **Privacy can enhance security.** Privacy and security are often construed as in conflict and zero-sum. But enhancing privacy often *enhances* security. Sometimes these goals are mutually antagonistic but, just as often, they are mutually supportive.
4. **Privacy is a social good.** Privacy is often positioned as a *personal* value while security is positioned as a *societal* need. But privacy is also a social value and a public good, not just an individual right.
5. **Metadata is data.** There is no significant distinction between *data* and *metadata* from a privacy perspective. Labeling bits as “metadata” does not change the privacy implications of collecting or analyzing it, nor the applicability of the principles enumerated in this document.
6. **Machine interception is interception.** The technology-driven shift from human-mediated to machine-mediated surveillance does not negate the applicability of surveillance principles. A communication is collected when it is captured, processed, or retained for intelligence or law-enforcement purposes even if no human is directly involved as an agent in these processes.

7. **Oversight.** Where targeted and proportionate surveillance is performed, there should be meaningful and independent oversight.
8. **No secret law.** Governments must eschew secret laws, secret interpretations of laws, and secret legal definitions.
9. **No proxy surveillance.** A government must not obtain information that its own laws would forbid it to collect by getting it from another entity not covered by those laws.
10. **Building privacy in.** Privacy protection should be built into technology. Good privacy defaults, including ubiquitous encryption and anonymity, will not prevent governments from spying on targeted individuals, but can inhibit mass surveillance.
11. **No backdoors.** Technical features to facilitate and routinize law enforcement or intelligence agency requests should not be built into computing and communication technology. Systems should not embed privacy-relevant features undesired by or unknown to users.
12. **Privacy impact assessments.** Governments should require that information technology with surveillance implications be subjected before deployment to an assessment of its implications for human rights and social values, including privacy. The assessment must be made public and potential adverse consequences mitigated. The sale and use of systems for population-wide phone or internet surveillance should be illegal.
13. **Fair Information Practices (FIP).** The FIP principles [2] are still relevant and important, but need updating to be applicable to contemporary conditions of technology, law, commerce, state action, and public policy.
14. **Reversed privacy policy.** People should be able to create a machine-readable privacy policy, and companies should be required to retrieve the policies and to comply with them (when they are legal and compliance is technically feasible).
15. **No race to the bottom.** In creating technological artefacts for the international market, privacy protections must not be reduced in order to enter markets where privacy rights or their enforcement are weaker.
16. **No vulnerability stockpiling.** Anyone who discovers a vulnerability in a computer system should engage in a coordinated disclosure as quickly as practically possible. Minimising the window of opportunity for exploitation should be the primary goal. The sale of exploits for use as cyberweapons should in most cases be illegal. Exceptions should be regulated and monitored with democratic oversight.
17. **Duty of care.** Companies and governments, as well as computer scientists and relevant researchers, have a duty of care to uphold, promote, and protect the rights expressed in this enumeration of principles.

3 Research Directions

This section explores some research topics identified during the discussions. They have been grouped under four categories: mass surveillance, communications security, big data and centralised cloud infrastructures, and nation-state compromise of systems and standards. Here *systems* is a broad concept that includes not only hardware and software in end-user devices and routers, but also cryptographic systems. These topics are clearly not independent.

3.1 Mass Versus Targeted Surveillance

Security agencies operate a “funnel” in which bulk data collection is done population-wide, and this is used to inform them of targets of interest. Then deeper, more resource-intensive analysis is done on those targets. But the initial, bulk surveillance raises serious concerns about abuse and the limitations of state power. Most people have done nothing that would justify a forfeiture of their basic privacy rights. One might ask:

- Can researchers agree on definitions of *mass surveillance* and *targeted surveillance*?
- Are there any kinds of mass surveillance that can be considered legitimate?
- What alternatives to bulk collection exist for security agencies to identify targets of interest?

Typically, bulk collection is done on metadata, because it is more readily available and easier to process than content data. Metadata is the data that arises as a side effect of a user’s intention. For example, a user wants to send a message (content), and as a side effect, records are created that a message was sent at a certain time, of a certain length, to a certain person (metadata). Metadata is just as privacy-sensitive as content data; in fact, because it is easier to collect and process, it can be considered more sensitive.

- How can we better protect metadata than is done by leading technologies such as Tor?

Some ways of making bulk collection more acceptable have been proposed. They aim to mitigate its bad effects, for example by trying to constrain the level of collection or processing, or make it accountable, or limit the possible outcomes. The *time capsule* approach gathers and stores everything but without processing it; the data can be opened at a later date if there are indications that crucial intelligence is buried in it. Another idea is to devise techniques that restrict the computations that can be done, for example, using functional encryption. It may be difficult to agree and specify the computations that are allowed; an alternative is to allow any computations, but limit their number or the amount of data they can access. Again, recognising the difficulty of agreeing any limit on the amount, one might just try to enforce that the amount will be known and verifiable. This would mean that there is no limit on how the data is used, but the nature and quantity of access to the data would be plain for all to see. In a democracy, one could imagine that discussion of the quantity becomes part of the political discourse, in a similar way to that taxation levels are debated.

- Are there ways of managing the collection of data so that *limitations on its use*, or *transparency of how it is used*, can be assured? Can technical means ever achieve that?
- What limitations or transparency measures are technically feasible?
- How could information about the nature and quantity of bulk surveillance carried out be presented to citizens in an *understandable and meaningful way*?

An asymmetry of the debate around mass surveillance arises because participants who are not “security cleared” are not allowed to know the details of surveillance carried out, and what, if any, are the tangible benefits that have accrued.

- Are there technical solutions that would enable auditors outside the intelligence community to audit surveillance outcomes, without viewing information that would compromise the purpose of the surveillance?
- In particular, can citizens be given access to verifiable quantitative correlation about the subjects of surveillance and the outcomes it has?

3.2 Communications Security

Securing communication content seems to be the "easy" problem, certainly in comparison to securing computations and devices. However, it has become apparent that, even if we have strong cryptography, most communications are unprotected and the threat models that have most often been considered so far are too weak. Moreover, protecting metadata – particularly who is communicating with whom – is challenging.

- Can we develop technical solutions that provide strong-end-to-end communications, offering protection of data against global adversaries that control part of the network, and control some of the endpoints?
- Can the protection of *metadata* be added to the solutions, resulting in *strongly-anonymous* communication systems? These systems should resist attackers that are able to eavesdrop on multiple points in the network, interfere with communication and control a significant number of the anonymising servers.
- Can we develop *key management* techniques that are easy to deploy and use and that offer support for forward secrecy, deniability, group sessions, multi-cast?
- Can we implement these solutions so that they interoperate seamlessly with complex network and IT environments, which include proxies, content-distribution networks, users and servers with multiple devices and instances, and so on?
- Can we develop *free and open-source software* for the above problems? A key element here is audit, usability and integration with existing applications.
- How can we encourage *universal deployment* of these solutions?

3.3 Big Data and Centralised Cloud Infrastructures

The separation between data collected by governments and private organisations is increasingly blurred. While it is the role of the government to regulate the collection of personal data/Personal Identifiable Information (PII) by private organisations, government agencies use a broad range of methods to get access to data collected by those organisations. Data in cloud infrastructure needs to be protected against mass surveillance by intelligence agencies.

- Can we deal with *compelled service providers?* The Snowden revelations tell us that Section 702 of the FISA Amendments Act of 2008 is used to compel US companies to grant access to data they hold on production of a court warrant. Is it technically possible for a service provider to provide a set of useful services, including mail, document storage, and search, while protecting themselves against a state that demands to see particular users' data?
- Can we enable citizens to exercise their rights? How can service providers offer more transparency about the economic benefits they derive from user's data and how they collect and use the data in an acceptable way? How can they enable users to exercise their rights (such as right of access and right to delete).
- How can privacy regulators mandate privacy-protective versions of services? What criteria would define "usable" or "privacy protective"? What are the economics of a privacy-protective set of offerings?
- Can we develop a better understanding of the *economics of privacy?* If the research community cannot find effective and efficient solutions to the above problem, can we find economic models under which privacy preserving solutions can thrive? What is the economic and social impact (the cost) of loss of privacy, and in particular of this

phenomenon (small number of corporations controlling huge collections of data)? What regulatory and financial/market mechanisms can protect against these concerns? Can we change liability rules for entities that store personal data/PII to create economic incentives to minimize personal data collection?

- Which services and infrastructure can we offer in a *decentralised mode with minimal centralised data collection and trust* and a high level of robustness?
- Can we develop *efficient cryptography for outsourced data?* Current practice in cloud environments is that most data is stored in cleartext form. Applications that only require storage allow for encryption, but this precludes any computation on this data. We have theoretical solutions enabling "computation on encrypted data", such as fully homomorphic encryption (FHE), secure multiparty computation (MPC), and functional encryption (FE).
  - Is it possible to enhance the *functionality* offered by currently deployed solutions (in terms of the computation that can be done "in the encrypted domain") whilst maintaining efficiency such that the overall cost to the service provider does not become exorbitant? This requires an exploration of tradeoffs.
  - Privacy preservation in the free service model: As a special case, are privacy-preserving *search, data mining and advertising* – at scale and with timing constraints – possible? This would be necessary to enable companies to be able to continue to provide their services for free whilst enhancing the privacy of users. For search, there is *Startpage*[1] , but because it deletes results immediately, it lacks certain capabilities (e.g., the ability to go back and continue the search). Does the lack of functionality matter?
  - One approach to deploy these technologies would be to perform computations on cleartext exclusively in the *browser*, and the service provider only sees ciphertext. *confichair.org* is a conference management system that aims to achieve this goal; can it be generalised?
  - What are the *limitations* of this approach? Is the idea of a privacy-protective version of *Google Now* even meaningful?
  - How do we make solutions, with all the attendant user interface and key management issues, *deployable?*

3.4 Nation-state Compromise of Systems and Standards

We have strong evidence that mass surveillance is not limited to passive eavesdropping. The NSA has compromised cryptographic standards (e.g., the Dual_EC_DRBG[2] random number generator), with an eye toward improving its ability to decrypt intercepted messages easily. Likewise, from the Snowden revelations, we understand that the NSA has a variety of capabilities to compromise computer hardware while it is being delivered from the manufacturer to an entity that would then be subject to surveillance. These issues are not exclusive to the NSA (e.g., similar accusations are leveled against a large router manufacturer). These issues raise a number of interesting research challenges:

- *Policy of software/hardware trapdoor operations.* What are the long-term implications of the current trend of exploitation of vulnerabilities, and even 'planting' of vulnerabilities,

[1] https://startpage.com
[2] http://en.wikipedia.org/wiki/Dual_EC_DRBG

by nation-states' offensive cyberwarfare organisations? Is there a better way, e.g., treaties or agreements on restrictions on such practices?

- *Re-architecting the Internet infrastructure.* How can we redesign and/or protect the Internet infrastructure (mainly routing and naming services) from sophisticated active attacks?
- *Supply chain integrity.* Outsourcing manufacturing leads to plants that might substitute malicious parts or components. Tools and techniques are required to detect this; it might include sampling techniques that would require disassembly and detailed analysis. Similar problems can occur during shipping of devices.
- *Base software integrity.* Techniques are needed to provide assurances that a platform is running "correct" software (i.e., software as distributed by the original vendor). These techniques often include "attestations" that can be verified by users or third parties, outside of the particular hardware device, that the software stack is "correct". These techniques must be extended to work under a stronger threat model, such as when the vendor itself might be compelled to produce customized software for a targeted attack against a specific individual.
- *Trustworthy user environment.* Investigate and develop trusted environment that allows handling sensitive operations, data etc., in a way which is secure even if the general operating system of the device is not secure. This is particularly relevant to mobile devices (smart phones).
- *Secure cryptography.* Having the current standards potentially compromised requires the research community to revisit currently deployed cryptographic systems and networking protocols and to devise new systems with public review.
- *Identifying the current obstacles to the widespread use of cryptography.* We need to facilitate mass use of cryptography by developing free and open-source, secure, user-friendly and free clients which bring cryptography closer to the ordinary citizens.
- The previous items have focused mostly on existing ICT environments and how they can be improved. One can expect that in the next decade the *Internet of Things* will become a reality: tens of billions of "smart" devices (i.e., equipped with a processor) will be connected to the Internet. One can think of sensors and actuators in buildings, cars, TVs, smart phones, and the human body. This creates a potential avenue for extremely invasive surveillance and presents enormous security and privacy challenges. How can we know (or regulate) who has access to data coming from the sensors (e.g., device manufacturers, app developers, cloud providers)? How can one define and enforce data sharing policies? How can users express consent for the data collection and processing by these sensors?
- Ways should be sought to prevent states from undermining the standardization processes for the security of the internet. These could include, as a minimum, the exclusion of members of intelligence agencies from the standards bodies.

4 Strategy

Having enumerated some privacy principles and research problems, we list some strategic possibilities towards realizing these aims. In the same sense that many of the enumerated principles were high-level and aspirational, so too are some of the strategic directions.

- We call on system developers to design easy-to-use cryptographic software to facilitate personal privacy and security.

- We call on funding agencies to fund research into hardware and software supporting security and privacy, as well as social, ethical and legal aspects of surveillance and counter-surveillance.
- We call on oversight and privacy regulatory bodies to develop sufficient technical expertise, in-house or on tap, to enable them to be effective in regulating and overseeing surveillance.
- We call on legislators to regulate more aggressively the collection and use of customer data by the private sector, and to regulate the exchange of data collected for monitoring purposes between public and private sectors, including the transfer of personal data from the private sector to law enforcement and intelligence agencies.
- We call on legislators to improve legal protections afforded to whistle-blowers.
- We call on governments and other stakeholders to devote immediate attention and resources to the negotiation, agreement and ratification of an international treaty on surveillance.
- We call on legislators to introduce laws that make it illegal for organisations to buy, sell or operate computing systems specifically designed to facilitate population-wide electronic surveillance.
- We call on countries and regions to help minimise the risk to personal data by promoting, encouraging and assisting companies offering national and regional privacy-friendly IT solutions, including cloud services.
- We call on cryptographers to attend more seriously to problems of anonymity, traffic analysis, and subversion.
- We call on governments to allocate funding for education about the value of privacy and the risks posed by surveillance, and about means of increasing personal privacy protection.
- We call on intelligence-agency insiders to "blow the whistle" if they are aware of illegal activities within their organisation and cannot find redress though other means.

5 Acknowledgements

Our deepest thanks to Matt Blaze, who co-organized this Dagstuhl Perspectives Workshop 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 release in cinemas.

6 In Memoriam

This report is dedicated to our late colleague Caspar Bowden, who worked tirelessly to protect universal human rights, including people's right to privacy regardless of nationality. Well before the Snowden disclosures caught the attention of the world, Casper raised the problem of protecting privacy in the cloud to the European Parliament [6]. His voice will be sorely missed.

7 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 Univ., Ramat Gan, IL
- Eleni Kosta
Tilburg University, NL
- Hugo Krawczyk
IBM TJ Watson Research Center, Hawthorne, US
- Susan Landau
Worcester Polytechnic Inst., US
- Tanja Lange
TU Eindhoven, NL
- Kevin S. McCurley
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 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

References

1 "Necessary and Proportionate Principles." International Principles on the Application of Human Rights to Communications Surveillance. Final version, May 2014. Available from https://necessaryandproportionate.org/

2 Federal Trade Commission (USA). Privacy Online: A Report to Congress. June 1998. Available from the FTC website.

3 Gary T. Marx. An Ethics for the New Surveillance. *The Information Society*, 14(3), pp. 171–186, 1998.

4 Global Government Surveillance Reform. Joint from AOL, Apple, Dropbox, Facebook, Google, Linkedin, Microsoft, Twitter, and Yahoo! https://www.reformgovernmentsurveillance.com/

5 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

6 Didier Bigo, Gertjan Boulet, Caspar Bowden, Sergio Carrera, Julien Jeandesboz, Armandine Scherrer, "Fighting Cybercrime and Protecting Privacy in the Cloud," Directorate General for Internal Studies, Policy Department C: Citizens Rights and Constitutional Affairs, Study for the European Parliament, Oct. 2012. Available from http://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/dv/study_cloud_study_cloud_en.pdf