Report from Dagstuhl Perspectives Workshop 11061

Online Privacy: Towards Informational Self-Determination on the Internet

Edited by

Simone Fischer-Hübner[1], Chris Hoofnagle[2], Kai Rannenberg[3], Michael Waidner[4], Ioannis Krontiris[5], and Michael Marhöfer[6]

1 **Karlstad University, Sweden,** simone.fischer-huebner@kau.se
2 **UC Berkeley, USA,** choofnagle@law.berkeley.edu
3 **Goethe University Frankfurt, Germany,** Kai.Rannenberg@m-chair.net
4 **TU Darmstadt, Germany,** michael.waidner@sit.fraunhofer.de
5 **Goethe University Frankfurt, Germany,** ioannis.krontiris@m-chair.net
6 **Nokia Siemens Networks – München, Germany,** michael.marhoefer@nsn.com

Abstract

The Dagstuhl Perspectives Workshop "Online Privacy: Towards Informational Self-Determination on the Internet" (11061) has been held in February 6-11, 2011 at Schloss Dagstuhl. 30 participants from academia, public sector, and industry have identified the current status-of-the-art of and challenges for online privacy as well as derived recommendations for improving online privacy. Whereas the Dagstuhl Manifesto of this workshop concludes the results of the working groups and panel discussions, this article presents the talks of this workshop by their abstracts.

Seminar 6.–11. February, 2011 – www.dagstuhl.de/11061
1998 ACM Subject Classification D.4.1 [Computers and Society: Public Policy Issues: Privacy]; H.4 [Information Systems Applications: Miscellaneous: Personalized Services, Business Processes, Web 2.0, (mobile) Internet]; K.6.5 [Computing Milieux: Management of Computing and Information Systems: Security and Protection]
Keywords and phrases Online privacy, Data protection, Data security, Data loss prevention, Informational self-determination, Web 2.0, (mobile) Internet
Digital Object Identifier 10.4230/DagRep.1.2.1
Edited in cooperation with Sven Wohlgemuth

1 Executive Summary

Simone Fischer-Hübner
Chris Hoofnagle
Kai Rannenberg
Michael Waidner

While the collection and monetization of user data has become a main source for funding "free" services like search engines, on-line social networks, news sites and blogs, neither privacy-enhancing technologies nor its regulations have kept up with user needs and privacy preferences.

The aim of this Dagstuhl Perspectives Workshop is to raise awareness for the actual state of the art of on-line privacy, especially in the international research community and

Online Privacy: Towards Informational Self-Determination *[...]*, *Dagstuhl Reports*, Vol. 1, Issue 2, pp. 1–15
Editors: S. Fischer-Hübner, C. Hoofnagle, K. Rannenberg, M. Waidner, I. Krontiris, M. Marhöfer
Dagstuhl Reports
Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

in ongoing efforts to improve the respective legal frameworks, and to deliver soon after the workshop a Dagstuhl Manifesto providing recommendations to industry, regulators, and research agencies for improving on-line privacy. In particular we have examined how the basic principle of informational self-determination, as promoted by European legal doctrines, could be applied to infrastructures like the Internet, Web 2.0 and mobile telecommunication networks.

It was deemed necessary and timely to bring together a *broad spectrum of key contributors* in order to promote both legally and commercially viable foundations for a balanced on-line privacy:

- *Academia* (specifically data security, privacy, cyber-law, and privacy-influential technologies & services),
- *Public sector* (data protection officers, organizers of relevant research programs, relevant civil rights organizations), and
- *Industry* (providers of communication solutions, browsers and apps; data aggregation and web analytics companies; providers of major Internet and mobile Internet services)

This workshop and its planned Dagstuhl Manifesto have four goals, aside from galvanizing an emerging research community:

1. *Provide a big picture of on-line privacy, which can be understood widely*
   Because of swift progress in the mobile Internet, on-line social networks, and on-line advertisements, it is a challenge for non-experts (and perhaps even experts themselves) to understand the current state of on-line privacy including the technologies and systems to collect personal information on-line.
2. *Compile the industry and engineering options to improve on-line privacy*
   On-line privacy depends on the technologies and systems used to access Internet/Web 2.0 services as well as on the services provided to users. Therefore industry has a strong influence.
3. *Update the respective legislative and regulative authorities on their options for enforcing practical, commercially viable informational self-determination of users in global infrastructures (e.g. EU's Privacy Directive to be revised in 2011)*
   Access to personal information is critical to self-determination; it is also seen as a right that serves a policing function among information-intensive firms. However, legal and business structures have often foreclosed rights of access, or made them impracticable for consumers to exercise.
4. *Foster industry's and academia's research for creating effective on-line privacy technologies, components, and systems that promote informational self-determination*
   Corresponding to additional risks for on-line privacy, new approaches are required in research to again establish adequate levels of on-line privacy.

This workshop has been structured into four parts, for each part, a topic responsible has been assigned:

- Part 1: Current S-o-A of on-line privacy w.r.t. to informational self-determination
  Responsible: Alma Whitten, Google Research, Great Britain
- Part 2: Industry & engineering options to improve on-line privacy
  Responsible: Michael Waidner, ex-IBM CTO Security, then TU Darmstadt, Germany
- Part 3: Recommendations for improving regulations of online privacy
  Responsible: Caspar Bowden, Microsoft WW Technology Office, Great Britain

- Part 4: Recommendations for research to improve the S-o-A of online privacy
  Responsible: Kai Rannenberg, Goethe University Frankfurt, Germany

A Dagstuhl Manifesto will conclude this workshop according to http://www.dagstuhl.de/en/program/dagstuhl-perspectives/.

2 Table of Contents

3 Overview of Talks

3.1 Shining Light on Leakage of Private Information via the Web

Craig E. Wills (Worcester Polytechnic Institute, USA)

This talk seeks to shine light on the leakage of private information via the Web. We first examine longitudinal results showing the size of users' privacy footprints continues to grow as presence of third-party trackers increases on first-party sites. We then examine the leakage of private information about users to these third parties via traditional and mobile social networking sites. We conclude with directions of current and future work.

3.2 Online Privacy – "The Mobile Aspect" Privacy in Mobile Applications and Beyond

Kai Rannenberg (Goethe University Frankfurt, Germany)

Location Information enables or at least supports many mobile applications such as pollen warning, children tracking, location based advertising, and mobile communities. At the same time processing of location information either by providers or by community peers creates sensitive issues, such profiling and dangers on personal safety. As mobile applications usually involve consortia with at least two providers, privacy and information flow issues are relevant and a sensitive matter. Often mobile telecommunications providers are in a key position and exposed to the privacy issues, as they maintain the customer relationship and their mobile communications systems (e.g. GSM, UMTS) hold the location information. However with the development of mobile sensors such as GPS receivers location information can be sensed widely and is available to more players in the value chain. Enabling privacy without disabling essential parts of the applications requires the users to make decisions on information flows.

This presentation reports on the data gathered in mobile communication systems and the activities of mobile phones to this regard, e.g. collecting data, reporting data to 3rd parties, and leaving traces. Solution approaches from projects such as the PRIME and PICOS are introduced, e.g. the PRIME LBS application prototype and the PICOS mobile angling and gaming community applications to demonstrate how users can be enabled to protect their privacy considering the tension between restricting information flows and their respective application interests.

3.3 Trust and Privacy: What is missing?

Claire Vishik (Intel – London, Great Britain)

In the last 10-15 years, significant advances were achieved in the area of trust and privacy. In the area of trust, understood as obtaining proof of expected behavior, new metrics and attestation protocols as well as technical trust elements in other technologies were added to the list of available approaches. The area of online privacy is much harder to define, but those engaged in privacy by design processes adopt specific parameters that reflect level of privacy in various types of technologies.

The presentation covers advances in bringing more privacy to data handling processes, hardware and software design as well as advances in building legal framework in regulatory frameworks. But the progress made thus far is not sufficient for modern computing environments. The study of levels of privacy **across domains** remains an emerging area at the time when most electronic processes and data sharing cut across domains. The **evidence of trust and privacy** that could work in cross-domain environments is in the very early stages of definition. **Policy enforcement** as opposed to policy interpretation is still in its infancy. **Truly multidisciplinary studies** are needed in trust and privacy where technical solutions are necessary, but not sufficient for progress. Greater pragmatism is also required to develop deployable and adoptable approaches to online privacy. A lot of work needs to be done, and a multidisciplinary group like the one that has gathered in Dagstuhl are necessary to make rapid and lasting progress.

3.4 What can Engineers and Industry do to improve Online Privacy?

Alma Whitten (Google Research, Great Britain)

Engineers and industry have a great deal of valuable work to do to improve online privacy. There is much progress still to be made on offering better transparency and clarity in our products and in our communications, and on employing innovative techniques to enhance understanding. Similarly, there is still much that can be done to offer people improved choice and control that better aligns with their needs and concerns. Finally, progress is steadily continuing on strengthening the safety of online systems through cryptography, sandboxing, more efficient patching, and more.

3.5 Privacy in Online Social Networks – Past Experiences, Future Challenges

Andreas Poller (Fraunhofer SIT – Darmstadt, Germany)

In their study in 2008, Fraunhofer SIT evaluated seven online social networks for measures to protect the privacy of their users [1]. The analysis and evaluation was based on a criteria catalogue which considers the very risks of social network platforms and state of the art privacy concepts. None of the tested platforms fully convinced the testers. In many cases Fraunhofer SIT dissuaded from using several platform functions.

Since then, the platforms solved most of their teething problems like missing TLS encryption for whole user sessions. However, several issues remain: Up to now, there exists no convincing business model which can respect the users' privacy, external audits take place rarely, and access control concepts are difficulty to use. In addition, the platforms are becoming more complex by integrating third-party applications. Particularly biometric and augmented reality functions foster new privacy threats.

To meet the further challenges, it is necessary to identify the several stakeholders like the individual data subject, the other platform users, non-members, platform provider and third-party application provider. It is required to analyze their relationships, the data or information flow among them, and their individual privacy needs. For example, the users' privacy concerns about the flow of their personal information to other users differ from privacy concerns towards the service provider as a data collector. Further research shall distinguish these problems and propose pertinent solution, be it new regulations or new usable privacy mechanism.

References

1 A. Poller. Privatsphärenschutz in Soziale-Netzwerke-Plattformen. Fraunhofer Institute for Secure Information Technology. Technical Report. 2008. http://www.sit.fraunhofer.de/Images/SocNetStudie_Deu_Final_tcm501-35966.pdf

3.6 Technology and Privacy: A lost Battle!?

Jan Camenisch (IBM Research – Zürich, Switzerland)

Engineers have and are building lots of devices and tool for people to communicate with each other and for tapping into the digital world. The way these have been built makes them leaving lots of traces that endanger the users' privacy. This is despite there being lots of technologies available that would allow one to build such tools and devices in a privacy respective and enhancing way. Of course, doing so will come at some cost in performance similarly as when building-in security. Thus: we need to consider and find an answer to why are engineers are today not doing privacy by design although they could?

3.7 Online Privacy: Reflections on the Regulatory Aspects

Jos Dumortier (K.U. Leuven, Belgium)

The provision of personalised services is an essential element of the Internet business model. Personalised service offering is not possible without processing personal information. Some people estimate that the best solution for protecting the individual in this context consists in asking this individual's consent before registering his personal data and using him for the provision of personalised online services. Obtaining such consent in an online environment is usually very easy. Consequently so-called "informational self-determination" is very popular in the commercial profiling and direct marketing business.

In Europe, however, the law doesn't consider privacy exclusively as an individual's business but rather as a societal good. Privacy is in the first place necessary as a condition for maintaining democracy. This viewpoint is clearly reflected in the European Convention of Human Rights (ECHR) and in the jurisprudence of the European Court of Human Rights. Privacy is closely connected to diversity since it is the contrary of societal control and conformity. Privacy protection is mainly necessary to guarantee free self-expression, which is a condition sine qua non for a democratic society. This is the reason why we consider privacy as a fundamental right, a right which cannot be given away by the individual. Regulation to protect online privacy should therefore not primarily focus on informational self-determination but on the prevention of the societal risks connected to the large "oceans of data" that are created in the context of the Internet business model.

3.8 On Regulations of Online Privacy

Caspar Bowden (Microsoft WW Technology Office, Great Britain)

The EU Data Protection Directive 95/46/EC addresses personal data as information relating to an identified or identifiable natural person (data subject). The principles of protection shall not apply to data rendered anonymous in such a way that the data subject is no longer identifiable. However, scientific discoveries about data privacy and de-anonymization attacks, e.g. k-anonymity, show that data subjects can be re-identified even though their data have been anonymized. Currently, data is considered "atomically" and there is no proportionality according to scale. However, systems increasingly collect identifiable transactional data with the "side-effect" that a database of all transactions is retained. This talk addresses the questions by whom data subjects are identifiable and how to define the concept of data to be regulated. This talk stresses the importance to consider data sets and not atomic data. A proposal is to establish "red line" limits (absolute rules) against new threats, e.g. storage of e-mails and "life logs" as well as to eliminate consent as an "escape clause" towards a "right to lie". It also addresses the question how a regulator can carry out a meaningful inspection of , e.g., cloud computing and how does one certify a privacy system.

3.9 Regulating Online Privacy: Why, What, and Where

Omer Tene (Israeli College of Management School of Law, Israel)

When assessing the regulation of online privacy we must answer three fundamental questions [10], namely **why** should we regulate cyberspace? **What** exactly should be regulated? And **where** will privacy regulation apply geographically?

Why Privacy regulation can be justified by one of two basic hypotheses: First, from a law and economic perspective, regulation (any regulation) is justified where there is a **market failure** [5]. Arguably, this is the case for online privacy, given consumers' relative ignorance of privacy policies and weak bargaining position *vis-á-vis* online service providers. Conversely, if the online market is sufficiently competitive (as it is widely considered to be), it can be expected to clear any informational and bargaining discrepancies to obtain an efficient equilibrium. The second basis for regulation in this sphere is the conception of **privacy as a fundamental human right**, tightly linked to human dignity and autonomy, and not subject to market forces [9]. Under this view, privacy regulation is justified regardless of the market equilibrium, and may be effected by paternalistic decisions concerning individuals' welfare.

What The two thorny issues for online privacy regulation are the definition of personal data and the scope of consent. First, the **definition of personal data**, the basic building block of any privacy regime, has come under stress recently based on researchers' demonstrations of the ability to re-identify or de-anonymize the people hidden in anonymized data sets. "Re-identification science disrupts the privacy policy landscape by undermining the faith that we have placed in anonymization." [4] Second, **consent** has proven to be a weak basis for processing data in an online environment which is increasingly complex, involves multiple parties (many of which are invisible to the consumer), and is largely based on the American "notice and choice" model of regulation, which has largely failed. Indeed, in its recent Preliminary Staff Report, Protecting Consumer Privacy in an Era of Rapid Change, the Federal Trade Commission states: "the notice-and-choice model, as implemented, has led to long, incomprehensible privacy policies that consumers typically do not read, let alone understand." [2] This view is echoed in the Department of Commerce "Green Paper" on privacy and innovation in the Internet economy: "From the consumer perspective, the current system of notice-and-choice does not appear to provide adequately transparent descriptions of personal data use, which may leave consumers with doubts (or even misunderstandings) about how companies handle personal data and inhibit their exercise of informed choices." [3] Yet consent cannot be entirely done away with as it is inexorably linked with the definition of privacy itself. We must therefore find a way to reinvigorate transparency and allow consumers to make meaningful choices with respect to the collection and use of their personal data.

Where Choice of law and jurisdiction (which law applies and who is to apply it) have always raised dense problems in the online ecosystem. This is due to the fact that choice of law and jurisdiction are typically determined according to geographical markers, whereas cyberspace transcends national borders [7]. In addition, the paradigm shift to cloud computing and storage of personal data in the cloud pose risks to privacy, as data changes hands, crosses borders, and may be accessed and used without the knowledge and meaningful consent of individuals [1, 8]. The European Union Justice Commissioner Viviane Reding recently announced that legislation proposed next summer will call for "four pillars", including the

extraterritorial application of the EU Data Protection Directive to entities in the United States collecting information online from European data subjects [6]. This solution (namely, a "targeting" test initially introduced in the United States in the *Zippo case* [11]) has benefits and costs, given that increased scope may add pressure on enforcement resources which are already scarce and yield suboptimal results.

References

1 A. Cavoukian. Privacy in the Clouds: A White Paper on Privacy and Digital Identity – Implications for the Internet. May 28, 2008. http://www.ipc.on.ca/images/Resources/privacyintheclouds.pdf

2 Preliminary FTC Staff Report. Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers. December 2010. http://www.ftc.gov/os/2010/12/101201privacyreport.pdf

3 The Department of Commerce Internet Policy Task Force. Commercial Data Privacy and Innovation in the Internet Economy: A Dynamic Policy Framework. At page 22. December 2010. http://www.ntia.doc.gov/reports/2010/iptf_privacy_greenpaper_12162010.pdf

4 P. Ohm. Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization. 57 UCLA Law Review 1701. 2010.

5 R. A. Posner. The Right to Privacy. 12 Ga. L. Rev. 393. 1978.

6 V. Reding, Vice-President of the European Commission EU Justice Commissioner. Your data, your rights: Safeguarding your privacy in a connected world Privacy Platform. The Review of the EU Data Protection Framework. Brussels. March 16, 2011. http://europa.eu/rapid/pressReleasesAction.do?reference=SPEECH/11/183

7 J. Reidenberg. Technology and Internet Jurisdiction. 153 Penn. L. Rev. 1951. 2005.

8 W. Robison. Free at What Cost?: Cloud Computing Privacy Under the Stored Communications Act. 98 Geo. L. J. 1195. 2010.

9 S. Simitis. Reviewing Privacy in the Information Society. 135 Penn. L. Rev. 707. 1987.

10 O. Tene. Privacy: The New Generation, 1 International Data Privacy Law 15. url-http://idpl.oxfordjournals.org/content/1/1/15.full. 2011.

11 Zippo Manufacturing Co. v. Zippo Dot Com, Inc., 952 F. Supp. 1119 (W.D. Pa. 1997). 1997.

3.10 Online Privacy – a European Commission Perspective

Jesus Villasante (European Commission – Brussels, Belgium)

The European Commission's initiatives in the field of online privacy consist of several strands including policy and regulatory initiatives, the involvement of end-users and society as well as support for research and innovation. The objective of the talk by Jesus Villasante is to put the technological innovation in the field of online privacy into context with the EU's privacy policies and its research activities.

The Digital Agenda for Europe of May 2010 summarises the European Commission actions in the area of ICT. One of its pillars is dedicated to "Trust and Security" focusing in particular on the safety and privacy of online content and services. The actions foresee among others the implementation of privacy and personal data protection, where research results and innovative solutions could provide crucial support to tackle the burning issues of online privacy.

Due to the dynamic changes of digital society, privacy issues gain in importance and policy must keep up to date with emerging technological challenges. In order to enable the user to control his privacy online, the current open issues include privacy by design, the right to be forgotten and emerging privacy issues in cloud computing and the Internet of Things.

Research and Development is one way of the European Commission to address these open issues and this summer the opening of FP7-ICT Call 8 will provide an excellent occasion for researchers to receive substantial funding for projects in the field of Trust, eID, and Privacy Management Infrastructures.

At the same time, 2011 will see intensive discussions on the future European Research Framework Programme "FP8". Consultations will try identifying the remaining technological challenges for Privacy, ID management, and trustworthy ICT, which need to be prioritised in the coming years to enable the application of European principles of privacy in the Future Internet.

3.11 Recommendation on Structure and Form of Manifesto

Jacques Bus (Digitrust EU – Brussels, Belgium)

This presentation does not intend to give proposals for a Manifesto text. That would be the task of the participants in the discussions to follow. I will only raise questions and make suggestions on issues that are in my view important when writing a Manifesto that intends to give recommendations to politicians and researchers about the problems and possible research agenda for solutions in the field of privacy in the digital environment. Following the organizational structure we expect the following parts in the Manifesto, where of course parts three and four depend on the results of the first two parts:

- Part 1: Current S-o-A of online privacy w.r.t. to informational self-determination, including background and relevance
- Part 2: Industry & engineering options to improve online privacy, including the existing challenges
- Part 3: Recommendations for improving regulations of online privacy
- Part 4: Recommendations for research to improve the S-o-A of online privacy

Who do we want to address and influence?

When writing the Manifesto, the main question is who we want to address and influence. If we aim at politicians, privacy commissioners, lawyers, regulators etc., then we must ask the question how can technology play its role in creating transparency, privacy assurance, auditing. What is the societal and industrial motivation for protecting and strengthening privacy and the arguments for doing research in this field. How do governments and citizens react to the digital world?

If we aim mostly on those who will have to fund the research in government and industry we must think about political and societal arguments, as well as arguments of industrial competitiveness and innovation. This holds at the EU level as well as at the Member State level. If we aim at the researchers in academia it is mainly about interesting research and potential publications, patents, and generally recognition.

A terminological minefield

Let us just address a few terms in the field that we discuss in this workshop.

Security: We may have many different things in mind when we use the word "security", even if we would only restrict its use to information. We can mean the protection of the secrecy of information, by hiding it away or encrypt it. We can also mean the safety and protection of people and relate it to data protection and informational privacy of citizens, but also to secrecy of information avoiding that sensitive information gets in the hands of criminals or terrorists. We may think of the protection of critical infrastructures and the control structures with data that can be infiltrated. And we can think about national security as protected by intelligence agencies, armies, police, within the state, at its borders and beyond. All these aspects lead to different solutions and the debate on the perceived balance between privacy and public security through surveillance is only one example of the difficulties we get involved in.

Identity: Davis [2] distinguishes three concepts:

1. Metaphysical identity: what are the essential qualities of a person that makes him unique
2. Physical identity: the carrier in flesh and blood of all the roles and qualities
3. Epistemological identity: created by relations to institutions; or existing because of various practices connected to our culture, language, ...

We can also talk about multiple (partial) identities if we consider every creation of a relation or an existence of practice that form together the epistemological identity, as one (partial) identity. In general we can say that an "identity" in a certain context is a particular set of credentials (attributes), called a partial identity. FIDIS [3] distinguishes (1) the structural perspective (ID as set of attributes) and the (2) process perspective (ID as set of processes of disclosure and usage of ID data, i.e. authentication). Many more perspectives are given in literature, demonstrating the complexity and fuzziness when we use the term "identity".

Privacy: Maybe it started with Warren and Brandeis [7] in 1890 and their plea for privacy as the "right to be left alone". Allen [1] considers:

1. Physical privacy (seclusion, solitude)
2. Informational privacy (confidentiality, secrecy, data protection and control over personal information)
3. Proprietary privacy (control over names, likeliness and repositories of personal information)

Helen Nissenbaum [6] gives an excellent account and framework of contextual informational integrity, demonstrating the dependence of privacy per/Users/sven/Desktop/Dagstuhl - abstract Jesus Villasante.docception on context and social norms. Privacy is laid down as a human right and the Data Protection Regulation of the EU as well as the so-called Privacy Regulation (on data protection in digital services) are reflections of that. Privacy and Identity are closely related subjects and proper identity management is a pre-requisite for privacy, but not sufficient.

Confidence, Trust, and Trustworthiness: Confidence can be had in institutions, organizations, technology to do what it is expected to do, although we often say we trust (or not) the government, a company, etc. However, trust has a positive connotation and technology can do what is expected, which might be negative. For example we can be confident that viruses are harmful to our system. Hardin [5] uses therefore "confidence" instead of "trust" in institutions (the latter he reserves for interpersonal relations). But Fukuyama [4] talks about trust in government, society (societal trust as a measure of opinion). Trust can be seen as a context-dependent (also culture, character or psychology) – relation between entities (often reserved for persons) to have a certain benign behavior or acting.

Trustworthiness is the quality of an entity, as believed by the truster, to behave in a certain way (One can trust an entity without the entity being trustworthy!)

It is clear that we must in this workshop and in the Manifesto it produces be careful in the use of the terms mentioned above. What type of entities do we consider? How do these terms relate? What terminology do we use in particular in the context of technology?

The choices depend on the audience (policy, industry, researchers), and in general we must avoid abstract and rigid use of language (unless it is meant solely for researchers). It must be understood that people want to recognize their thinking and preaching and be able to integrate new ideas in their normal talking. In general it is difficult for politicians to change language once they have presented their basic vision and policy documents for their job period. It is often better if we address a larger public to use various words and meanings and explain them by metaphors. Finally, in general, research program language is vague and abstract to avoid strong prescription, potential errors and the risk of being already out-of-date when it is published. It should also leave creativity to the proposers (some years later !!).

Confidence in Technology

The main requirements for users to get confidence in the technology they are offered are:

1. Technology providers must be open and transparent about how it works, how they make profit from it, and how they provide redress in case of harm done.
2. Government must develop effective regulation and law, which is as much as possible technology neutral and enforceable (also globally).
3. The technology application must give users the feeling that its use is compliant with their norms, that they understand the general picture and dangers and that they have ways of controlling such dangers.

Research Directions in Privacy?

When proposing research directions in privacy we must take account of:

1. It is about informational privacy and takes account of the essential factors: context; social norms; potential of data inference; and the need for data security.
2. The developments in industry and society (ad-nets, targeted advertisement, profiling, location data collection, data in the cloud, social networks).
3. It takes account of developments in the regulatory environment (focus on Privacy by Design, privacy assurance methodology, auditing, reproducibility).
4. Take account of societal developments: increasing general worries with seemingly little relation to the actual behavior.
5. Ensuring attention for confidence building during the whole product life-cycle from design till customer service.
6. The need for real multi-disciplinary research.

And in doing so we must consider the timing. What need to be done in the short (1-2 yr) term, what in 3-5 years and what beyond 5 years. For example, the expected revision of the EU Data Protection Framework might in particular need research on Privacy by Design, assurance and certification, modular and transparent data management processes and auditing.

Conclusions

Summarizing, in writing the Manifesto we must:

1. Think from the world of the audience
2. Be tolerant with their language and understanding

3. Accept their worries, understand their goals
4. Be rational with timing

But the real barriers to make long term progress in online privacy technology are:

1. Including the dynamicity, diversity and cultural and normative essence of life.
2. To achieve essential multi-disciplinarity in all future work.

References

1 A. Allen. Uneasy Access, Totowa, NJ, Rowman & Littlefield. 1998.
2 S. Davis. A conceptual analysis of identity. In Kerr, Steeves and Lucock (eds) Lessons from the identity trail. Anonymity, Privacy and Identity in a Networked Society, Oxford. 2009.
3 FIDIS. Future of Identity in the Information Society. 2009. http://www.fidis.net
4 F. Fukuyama. Trust: the social virtues and the creation of prosperity. Free press, NY. 1995.
5 R. Hardin. Trust & Trustworthiness. Russel Sage Foundation, NY. 2002.
6 H. Nissenbaum. Privacy in Context: Technology, Policy and the Integrity of Social Life. Stanford Univ Press. 2010.
7 S. Warren & L. Brandeis. The right to Privacy. In F.D. Schoeman (ed) Philosophical dimensions of Privacy: an Anthology, Cambridge, MA. 1890.

Participants

- Andreas Albers
Goethe University Frankfurt, Germany
- Caspar Bowden
Microsoft WW Technology Office, Great Britain
- Sonja Buchegger
KTH Stockholm, Sweden
- Johannes A. Buchmann
TU Darmstadt, Germany
- Jacques Bus
Digitrust EU – Brussels, Belgium
- Jan Camenisch
IBM Research – Zürich, Switzerland
- Fred Carter
IPC – Toronto, Canada
- Ingo Dahm
Deutsche Telekom AG, Germany
- Claudia Diaz
K.U. Leuven, Belgium
- Jos Dumortier
K.U. Leuven, Belgium
- Simone Fischer-Hübner
Karlstad University, Sweden
- Dieter Gollmann
TU Hamburg-Harburg, Germany
- Marit Hansen
ULD SH – Kiel, Germany
- Jörg Heuer
Deutsche Telekom AG Laboratories, Germany
- Stefan Köpsell
TU Dresden, Germany
- Ioannis Krontiris
Goethe University Frankfurt, Germany
- Michael Marhöfer
Nokia Siemens Networks – München, Germany
- Andreas Poller
Fraunhofer SIT – Darmstadt, Germany
- Kai Rannenberg
Goethe University Frankfurt, Germany
- Thomas L. Roessler
W3C, France
- Kazue Sako
NEC, Japan
- Omer Tene
Israeli College of Management School of Law, Israel
- Hannes Tschofenig
Nokia Siemens Networks – Espoo, Finnland
- Claire Vishik
Intel – London, Great Britain
- Michael Waidner
TU Darmstadt, Germany
- Rigo Wenning
W3C / ERCIM, France
- Alma Whitten
Google Research, Great Britain
- Craig E. Wills
Worcester Polytechnic Institute, USA
- Jesus Villasante (Observer)
European Commission – Brussels, Belgium
- Sven Wohlgemuth
National Institute of Informatics – Tokyo, Japan