Project acronym:	PRESCIENT
Project title:	Privacy and emerging fields of science and technology: Towards a common framework for privacy and ethical assessment
Project number:	244779
Programme:	Seventh Framework Programme for research and technological development
Objective:	SiS-2009-1.1.2.1: Privacy and emerging fields of science and technology: ethical, social and legal aspects.
Contract type:	Collaborative project
Start date of project:	1 January 2010
Duration:	39 months

Deliverable 5:
Privacy, data protection and ethical issues in new and emerging technologies: Final conference — Book of abstracts

Editor:	Michael Friedewald, Fraunhofer ISI
Dissemination level:	Public
Deliverable type:	Report
Version:	1.0
Due date:	None
Submission date:	30 November 2012

Terms of use

Fraunhofer
ISI

FRAUNHOFER INSTITUTE FOR SYSTEMS AND INNOVATION RESEARCH ISI

PRIVACY AND EMERGING SCIENCES AND TECHNOLOGIES

INTERNATIONAL CONFERENCE OF THE PRESCIENT PROJECT

27–28 November 2012
Berlin, Germany

SUPPORTED BY

SEVENTH FRAMEWORK PROGRAMME

Science in Society

ORGANISED BY

Fraunhofer

Trilateral Research & Consulting

LSTS
LAW, SCIENCE, TECHNOLOGY & SOCIETY STUDIES

CSSC
Centre for Science, Society and Citizenship

Contact
Dr. Michael Friedewald
Fraunhofer Institute for Systems and Innovation Research ISI
Breslauer Strasse 48 | 76139 Karlsruhe | Germany
Phone +49 721 6809-146 | Fax: +49 721 6809-315
michael.friedewald@isi.fraunhofer.de

Photo Credit | iStockphoto.com/TonisPan

PRESCIENT – Privacy and Emerging Science and Technologies

PRESCIENT is a three-year research project funded by the European Commission under its Seventh Framework Programme. The Project is part of the Science in Society activies of DG Research. It started in 2010 and will terminate in early 2013.

PRESCIENT aims to provide an early identification of privacy and ethical issues arising from emerging technologies and their relevance for EC policy. It will contribute to the quality of research in the field of ethics, by distinguishing between privacy and data protection and analysing the ethical, legal and socio-economic conceptualisations of each.

The PRESCIENT project has unfolded in four stages.

Work Package 1 – Current approaches to privacy and technology: The first stage is analysis: the partners provided a state-of-the-art analysis of privacy and data protection as conceptualised from an ethical, socio-economic and legal perspective.

Work Package 2 – Privacy, data protection and ethical issues in selected emerging technologies: The second stage were case studies wherein the partners have identified the privacy, data protection and ethical issues arising from five different emerging technologies and their applications.

Work Package 3 – Citizens' perception of privacy: The third stage focuses on citizens. The partners have analysed various existing surveys to assess citizen concerns and knowledge of the way in which their data are collected, stored and used and their concerns about new technologies and how their concerns have changed over time. The partners have also examine important websites and interview data collectors to assess how easy or difficult it is for citizens to access their information and to find out how it is being used.

Work Package 4 – Privacy and ethical impact assessments: The fourth and final stage focuses on development of a new framework for privacy and ethical impact assessments. The partners have developed scenarios as an element in this new framework, which is based on an integration of the results of this study and on privacy impact assessment guidelines such as those of the UK.

Organization

The PRESCIENT conference is organized by the partners of the PRESCIENT project: Fraunhofer Institute for Systems and Innovation Research ISI (Karlsruhe, Germany), Trilateral Research & Consulting (London, UK), Vrije Universiteit Brussels (Brussels, Belgium) and the Centre for Science, Society and Citizenship (Rome, Italy). The PRESCIENT project is funded under the European Commission’s 7th Framework Programme for research and technological development (SIS-CT-2009-244779).

Executive Committee

Program Chairs:	Michael Friedewald (Fraunhofer ISI) Serge Gutwirth (Vrije Universiteit Brussel)

Program Committee

Michael Friedewald	Fraunhofer ISI
Serge Gutwirth	Vrije Universiteit Brussels
Emilio Mordini	Center for Science, Society and Citizenship
David Wright	Trilateral Research and Consulting

Reviewers

M. Arnaud
R. Bellanova
R. Finn
M. Friedewald
R. Gellert
S. Gutwirth
B. Hüsing
D. Hallinan
G. Hornung
M. Langheinrich
E. Mordini
P. Schütz
S. Venier
D. Wright

List of invited talks

Philip Brey (University of Twente): *Anticipating and Evaluating Privacy Issues in Emerging Technologies*

Alexander Dix (Berlin Commissioner for Data Protection and Freedom of Information): *Closing Remarks*

Charles Raab (University of Edinburgh): *Governing the Safety State*

Iván Székely (Eötvös Károly Policy Institute): *Future technologies, future implications, future data subjects - can we regulate their relationships now?*

Bernd Carsten Stahl (DeMontfort University): *Responsible Research and Innovation: The Role of Privacy and Ethics in an Emerging Framework*

Table of Contents

Conference Schedule

Session 2: Ethical Challenges of Privacy and Emerging Technologies

Session 3: Technical Challenges of Privacy and Emerging Technologies

Session 4: Legal Challenges of Privacy and Emerging Technologies

Session 5: Societal Challenges of Privacy and Emerging Technologies

Annex

Program

Tuesday, 27 November 2012

13:30 – 14:00	Registration + Welcome coffee
Session 1	**Opening**
14:00	Opening remarks and introduction to the conference *Michael Friedewald, Fraunhofer ISI & PRESCIENT co-ordinator*
14:15	Welcome address *Karen Fabbri, European Commission*
14:25	Responsible Research and Innovation: The Role of Privacy and Ethics in an Emerging Framework *Bernd Carsten Stahl, DeMontfort University*
Session 2	**Ethical Aspects of Privacy and Emerging Technologies** *Chair: Emilio Mordini, CSSC*
14:45	Anticipating and Evaluating Privacy Issues in Emerging Technologies *Philip Brey, University of Twente*
15:15	The role of bioethics in public policy-making on new biotechnologies *Ruud Ter Meulen, Zuzana Deans and James Yeates, University of Bristol*
15:45	Biobank Privacy Regimes and the constitution of the ’bioinformed’ polity *Georg Lauß, University Vienna*
16:15 – 16:35	Coffee break
Session 3	**Technical Challenges of Privacy and Emerging Technologies** *Chair: Yair Sharan, University of Tel Aviv, PRACTIS project co-ordinator*
16:35	Privacy protection of biometric templates *Moazzam Butt, Olaf Henniger and Alexander Nouak, Fraunhofer IGD*
17:05	An Approach to Introduce Privacy-by-Design in Agile App-Development *Martin Degeling and Kai-Uwe Loser, Ruhr-University Bochum*

17:35 Accountability by Design for Privacy
Denis Butin, Marcos Chicote and Daniel Le Métayer, INRIA and University Lyon

18:05 Reception

Program

Wednesday, 28 November 2012

08:45	Late registration
Session 4	**Legal Aspects of Privacy and Emerging Technologies** *Chair: Serge Gutwirth, Vrije Universiteit Brussels*
09:00	Future technologies, future implications, future data subjects - can we regulate their relationships now? *Iván Székely, Eötvös Károly Policy Institute and Open Society Archives (OSA) Archivum*
09:30	Blurring the dimensions of privacy? Law enforcement and trusted traveler programs *Matthias Leese, University Tübingen*
10:00	The core content of personal data protection: A conceptual controversy *Gloria González Fuster and Serge Gutwirth, Vrije Universiteit Brussels*
10:30 – 11:00	Coffee break
11:00	Privacy and free speech on the Internet - taking the ’household exemption’ online *Zuzanna Warso, Helsinki Foundation for Human Rights*
11:30	Robots in the Cloud with Privacy A New Threat to Data Protection? *Ugo Pagallo, University of Torino*
12:00	Lunch
Session 5	**Societal Challenges of Privacy and Emerging Technologies** *Chair: Michael Friedewald, Fraunhofer ISI*
13:00	Governing the Safety State *Charles D. Raab, University of Edinburgh*
13:30	Smart Cities: the societal drivers and impact of smart environments *Gemma Galdon Clavell, University of Barcelona*

14:00 Towards a rhizomatic theoretical framework to understand the consequences of preemptive surveillance of children
Rosamunde van Brakel, Vrije Universiteit Brussels

14:30 Towards a multi-dimensional technology assessment: The introduction of security technologies at airports and public transport systems
Leon Hempel, Tobias Schaaf, Dagny Vedder, and Lars Ostermeier, Technical University Berlin

15:00 – 15:15 Coffee break

Session 6 **PRESCIENT project results: The way ahead**
chair: tbd

15:15 A new way of looking at privacy
Michael Friedewald, Fraunhofer ISI

The legal construction of privacy and data protection
Serge Gutwirth and Raphael Gellert, Vrije Universiteit Brussels

What is an ethical impact?
Emilio Mordini and Silvia Venier, CSSC

An integrated privacy and ethical impact assessment
David Wright, Trilateral Research & Consulting

16:15 Panel discussion

16:45 **Closing remarks**
Alexander Dix, Berlin Commissioner for Data Protection and Freedom of Information

17:00 End of event

The role of bioethics in public policy-making on new biotechnologies[*]

Ruud ter Meulen, Zuzana Deans, and James Yeates

Centre for Ethics in Medicine, University of Bristol,
39 Whatley Road, Bristol BS8 2PS, United Kingdom
e-mail: {r.termeulen,zusana.Deans,James.Yeates}@bristol.ac.uk

In our paper we want to present the outcomes of one aspect of our research into the contribution theoretical bioethics makes and can make to the ethical governance of science and technology, and whether bioethicists can be considered ethical experts. The rationale of the EPOCH project was that though EU policies often said to combine scientific insights with a framework for deciding the best ethical approach (i.e. a normative framework), it is not clear what this normative framework looks like, nor from which sources it should be derived. The project addresses the questions of what type of ethical 'expertise' is needed for the development of public policies on new technologies and how this expertise should be included in the governance of these new technologies. There are two main sections to the presentation. We start with a description of how bioethicists are formally integrated into public policy discussions and consultations before offering an evaluation of how useful these contributions can be with particular reference to ethics expertise.

The presentation starts with a brief overview describing the role bioethicists play in ethics committees. A very short summary is given of the different models in Europe, with focused attention on the UK as a detailed example. Generally, ethical decision-making regarding the governance of science and technology is a multi-professional, multi-disciplinary endeavour to which bioethicists contribute. Important instruments in this context are (national and international) ethics committees which can be seen as public bodies that try to bridge between academia and policy environments. Their main functions include: drawing attention to relevant ethical issues; making sense of the various positions; harmonising academic findings with public values; and suggesting practical governance solutions. The general means by which public policy bodies arrive at policy recommendations are: fact-finding, surveying possible positions and views, and subjecting these to group deliberation and (some form of) agreement. Different models of agreement (e.g. compromise and consensus) were discussed. The report suggests that reaching agreement is desirable on the grounds that governance policy can be made.

The presentation moves on to question the 'expert' status of the bioethicist, especially as compared with scientific or legal experts in the group. With reference to relevant literature, a distinction is made between a descriptive expert in ethics (one with skills in reasoning and detailed knowledge of the relevant moral issues) and a normative expert in ethics (one with knowledge of what the right course of action is), both of which will be explained in the presentation.

[*] This research was part of the EPOCH project funded by the European Commission.

These categories are paralleled with two types of authority: an authority and in authority, respectively. Some accounts of morality can accommodate normative ethical expertise, but in other versions of morality (that hold it matters who does the action) moral decision-making is non-transferable. There is, however, still good reason to suppose that bioethicists might be better equipped to arrive at sensible solutions to moral problems more quickly than the layperson, and therefore non-normative ethics experts, it is argued, are valuable for ethics committees.

The overall conclusions of this part of our study are that, in the realm of policy and practice, bioethics is one voice among many, being simultaneously representative and advocatory, independent and objective. We suggest a modest status for influencing public policy is appropriate, and conclude that although improvements could be made to how bioethics is done, no higher authoritative status of the discipline should be expected. We suggest that, owing to the nature of ethics and bioethical inquiry, there is a limit to expertise in bioethics. This, along with the socio-political structures of Western democratic societies, means that bioethics is not authoritative, but it does have a valuable contribution to make in reporting, representing, assessing and advancing debate.

About the author

Prof. Ruud ter Meulen (1952) is psychologist and ethicist. He is Chair for Ethics of Medicine and Director of the Centre for Ethics in Medicine at the University of Bristol. Previously he has worked as Professor of Philosophy and Medical Ethics and Director of the Institute for Bioethics at the University of Maastricht (The Netherlands). Ruud Ter Meulen has been working on a broad range of issues in medical ethics and has directed several international projects. He was principal co-ordinator of a range of European projects, including the ENHANCE project, funded within the Sixth Framework Program of the European Commission, dealing with the ethical, philosophical and social issues of enhancement technologies. He is currently co-ordinator of the European EPOCH project on the role of ethics in public policy-making on new biotechnologies, and of the European SYBHEL project on the ethical, legal and social issues of synthetic biology as applied to human health.

Biobank Privacy Regimes and the constitution of the ’bioinformed’ polity

Georg Lauß

Department of Political Science, University of Vienna
Universitätsstr. 7/2, A-1010 Vienna, Austria
e-mail: georg.lauss@univie.ac.at

The rise of molecular biology in the form of genetics, genomics and (post-) genomics has rendered the inherent information potential of human biological materials such as blood, saliva and tissues discernible. Together with associable information on lifestyle, genealogical data and health records these types of bioinformation are today assembled in largescale biobank projects, which are infrastructures for collecting, processing, storing and distributing such bioinformation in a systematic fashion for research purposes. Such projects that have been considered to be merely expensive visions two decades ago have now become an expansive reality. Albeit one that has been accompanied with quite intense privacy debates and constant attempts to come to grips with these pending issues in ‘ethically’ and legally sound ways.

Although, privacy has always been a constitutive concept for liberal political theory, modern biopolitical governmentality has been practically blurring any strict separation between a private sphere of (re-)production on the one hand and a public sphere of political deliberation about common matters on the other hand. The demarcation of private and public information or matter can’t be considered a straightforward task. Moreover, in the context of political programs to facilitate the creation of a ‘knowledge based bio-economy’ (KBBE) bioinformation acquired the status of a highly valued resource that is indispensible for the creation of knowledge, health and wealth. Consequently we are witnessing appeals for altruistic biocitizens to wave their privacy and contribute their personal bioinformation to the common thread of bioscientific development. Under such conditions privacy regimes practically constitute the bioinformed polity when they lay down legitimate access procedures to private matters in the name of biomedical innovation.

The paper discusses the ways in which the practical exchanges of biological research materials have been entangled in ethico-legal , and social scientific arguments. It examines the framework of the so called ‘communitarian turn in bioethics’ and shows how its discourse - which incorporated promissory scientific narratives and built on the assumption that ethics was predestined to respond to scientific development -became hegemonic. It then shows how this hegemony started to erode for several reasons, including the publication of a Eurobarometer survey and other research on citizens’ attitudes that demonstrated the ongoing significance of privacy narratives and showed that the idea of giving broad consent wasn’t warmly welcomed among most European constituencies. Leading protagonists of the biobank community, who had argued that broad consent was a condition sine qua non for biobank operation, reconsidered possible (technical) answers to ‘societal demands’, which would not hamper the progress of research. These reconsiderations resulted in recent proposals in which certain conceptions of privacy and autonomy materialized not only in technology based data protection methods like k-anonymity and l-diversity and technology based formats that are designed to facilitate scientific cooperation without conflicting with societal and regulatory privacy demands, like DataSHIELD, but also in ICT based concepts that offer donor choice, like disclosure filters or dynamic consent models.

The paper concludes by discussing status and function of ‘privacy’ in the bioinformed polity.

About the author

Georg Lauß was born in Vienna (Austria) in 1981. He started studying political science and science of communication at the University Vienna in 2001. From 2003- 2004 he was studying Public Administration at the Erasmus University in Rotterdam. After moving back to Vienna he finally finished his master theses on the biopolitics of neuroscientific research in the field of Attentiondeficit-/Hyperactivitydisorder (ADHD) in 2006. Since November 2006 Georg is a researcher at the GeneBanC project and a member of the Life Science Governance Research Platform.

Accountability by Design for Privacy[⋆]

Denis Butin, Marcos Chicote, and Daniel Le Métayer

Inria, Université de Lyon
INSA-Lyon, CITI-Inria
F-69621, Villeurbanne, France
e-mail: {denis.butin,daniel.le-metayer}@inria.fr;mchicote@dc.uba.ar

The growing scope of information and communications technologies (ICT) increases concerns regarding sensitive data. In particular, individuals share more personally identifiable information (PII) than ever before and demand accordingly stronger guarantees with respect to privacy. The first of these guarantees are provided by regulations (e.g. European Union directives [6, 7] regulating PII processing). However, because privacy and PII protection are very subtle and context-dependent notions, regulations have to be complemented with practical means to assess specific situations.

A first and foremost approach to evaluate risks is the application of Privacy Impact Assessment (PIA) procedures. Potential issues should be foreseen and analyzed in a collaborative and interactive way before the design and deployment of a new system. As such, PIAs can be seen as a form of risk assessment [14]. Risk management and mitigation is a continuous process though, and another, complementary, guarantee for individuals is the fact that controllers will be accountable for their actual use of the PIIs they have collected.

Our first point in this paper is that *PIA and accountability are dual* in some sense — PIA occurs before the deployment of a system whereas accountability applies, by definition, to a running system — and strongly tied, in the sense that PIAs should lead to measures to make accountability possible.

The second point we want to emphasize is that *accountability does not emerge spontaneously*. In other words, a system has to be designed with accountability requirements in mind and these requirement should arise from the PIA. Indeed, the feasibility of accurate and comprehensive a posteriori verifications depends directly on the architecture of the technical platform under consideration.

In this context, accountability [13, 9, 10, 4] refers to the *requirement on a data controller to produce evidence that previously agreed commitments were fulfilled*. Having that evidence available depends on design choices regarding events to be recorded and supplied to data subjects or third parties for verification.

Providing accountability by design, therefore, demands building ICT systems that can be audited in sufficient detail. In practice, the key aspect of ICT platforms that enable audit are traces taking the form of log files. Which PII usage events are logged and what contextual information is provided determines the level of accountability of the entire system.

While previous work has been done on frameworks for a posteriori compliance control [5, 3, 8] and log architecture design [12, 2, 11], *little attention has*

[⋆] This work was partially funded by the European FI-WARE[1] project / FP7-2012-ICT-FI.

been paid so far to the design of logs recording information about PII usage. We illustrate our "accountability by design" approach with the concrete example of a usage policy language, the Primelife Policy Language (PPL). Usage policy languages allow data subjects to specify precisely how their PII should be handled. For instance, a data subject may agree to the use of their email address by a data controller for the sole purpose of sending security alerts, and under the condition that the address may not be shared with third parties.

PPL allows the specification of a wide range of obligations for data controllers. Various categories of events define how data controllers must act when they perform specific actions with PII. For instance, a data controller may be required to notify a data subject when using their PII for a given purpose. The rules under which PII can be forwarded and used by third parties can also be set and analyzed. Data handling policies defined separately by data subjects and data controllers are matched automatically to generate so-called "sticky policies", representing agreements that suit both parties.

In the technical part of our contribution, we build on the pre-existing PPL specification by defining an abstract syntax and the set of events relevant for accountable logging. The purpose of the abstract syntax is to reduce ambiguity by defining how PPL elements can be combined meaningfully. We then define formal semantics for a compliance analyzer, which amounts to specifying the properties a log must satisfy to be compliant. As this is done formally, the compliance checks can be adapted for other policy languages than PPL. We then implement a compliance checker for logs of data controller events. This kind of tool enables partially automated accountability checking.

General insights about log design choices for accountability are then derived. Those principles are independent of the specific language chosen and are relevant for any system involving PII usage by a data controller. Since the conclusions are general, they can be adapted to other platforms and policy languages.

References

1. FI-WARE (Core Platform of the Future Internet). `http://www.fi-ware.eu`.
2. M. Bellare and B. Yee. Forward Integrity for Secure Audit Logs. Technical report, Computer Science and Engineering Department, University of California at San Diego, 1997.
3. J. G. Cederquist, R. Corin, M. A. C. Dekker, S. Etalle, J. I. den Hartog, and G. Lenzini. Audit-based compliance control. *Int. J. Inf. Sec.*, 6(2-3):133–151, 2007.
4. S. Eriksén. Designing for Accountability. In *Proceedings of the Second Nordic Conference on Human-Computer Interaction*, NordiCHI '02, pages 177–186. ACM, 2002.
5. S. Etalle and W. H. Winsborough. A Posteriori Compliance Control. In V. Lotz and B. M. Thuraisingham, editors, *SACMAT*, pages 11–20. ACM, 2007.
6. European Parliament and the Council of the European Union. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of such Data. *Official Journal of the European Union*, 23, 1995.
7. European Parliament and the Council of the European Union. Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 on the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector. *Official Journal of the European Union*, 201, 2002.
8. J. Feigenbaum, J. Hendler, A. Jaggard, D. Weitzner, and R. Wright. Accountability and Deterrence in Online Life (Extended Abstract). In *Proceedings of the 3rd International Conference on Web Science*, 2011.

9. D. Le Métayer. A formal privacy management framework. In P. Degano, J. D. Guttman, and F. Martinelli, editors, *Formal Aspects in Security and Trust*, volume 5491 of *Lecture Notes in Computer Science*, pages 162–176. Springer, 2008.
10. D. Le Métayer. Formal Methods as a Link between Software Code and Legal Rules. In G. Barthe, A. Pardo, and G. Schneider, editors, *SEFM*, volume 7041 of *Lecture Notes in Computer Science*, pages 3–18. Springer, 2011.
11. D. Le Métayer, E. Mazza, and M.-L. Potet. Designing log architectures for legal evidence. In J. L. Fiadeiro, S. Gnesi, and A. Maggiolo-Schettini, editors, *SEFM*, pages 156–165. IEEE Computer Society, 2010.
12. B. Schneier and J. Kelsey. Secure Audit Logs to Support Computer Forensics. *ACM Trans. Inf. Syst. Secur.*, 2(2):159–176, 1999.
13. D. J. Weitzner, H. Abelson, T. Berners-Lee, J. Feigenbaum, J. Hendler, and G. J. Sussman. Information Accountability. *Commun. ACM*, 51(6):82–87, 2008.
14. D. Wright, R. Gellert, S. Gutwirth, and M. Friedewald. Minimizing Technology Risks with PIAs, Precaution, and Participation. *IEEE Technol. Soc. Mag.*, 30(4):47–54, 2011.

About the authors

Denis Butin is a postdoctoral researcher at Inria (Lyon, France). His research currently focuses on access and usage policy languages and accountability by design. He holds a PhD in Computer Science from Dublin City University, where he worked on the application of formal methods to electronic voting protocol analysis. Earlier, he earned a Master’s degree in mathematics and computer science at the University of Tours.

Marcos Chicote is a research intern at Inria (Lyon, France). His areas of interest include software engineering, automatic program analysis and program verification and has broad experience in industrial software development. He holds a Master’s degree in Computer Science from the University of Buenos Aires.

Daniel Le Métayer is Research Director for INRIA (the French National Institute for Research in Computer Science and Control) and head of the Inria Project Lab CAPPRIS. CAPPRIS is an interdisciplinary initiative involving seven research teams working on various aspects of privacy. From 2000 to 2006, Daniel Le Métayer worked for Trusted Logic, a leading company in security and open middleware for embedded systems. Daniel Le Métayer has been involved in various international projects on IT security, software design and analysis, testing, etc. He has also served on programme committees of many IT international conferences and he has been the editor of special issues of computer science journals such as ACM Transactions on Software Engineering and Theoretical Computer Science.

Privacy protection of biometric templates

Moazzam Butt, Olaf Henniger, and Alexander Nouak

Fraunhofer Institute for Computer Graphics Research IGD
Fraunhoferstr. 5, D-64283 Darmstadt, Germany
e-mail: {moazzam.butt;olaf.henniger;alexander.nouak}@igd.fraunhofer.de

In modern times, many aspects of life have been or are becoming automated. Biometrics, i.e. the automated recognition of individuals based on their biological and behavioral characteristics, is a promising technology for automating authentication at human-machine interfaces. Recently, a significant raise has been seen in deployment of biometrics in domains like civil and criminal identification, travel and immigration, physical and logical access control, banking, and consumer electronics.

Unlike passwords, not all biometric characteristics are secrets. For instance, while vein patterns or handwritten-signature dynamics are hard to detect, anyone can rather easily take photographs of someone else's face. Nevertheless, biometric reference data (also known as biometric templates) are required to be stored securely and to be protected against unauthorized use. Many people are troubled by the risks associated with storing biometric templates in computer systems because biometric templates are highly sensitive personal data. Unlike the ubiquitous passwords, biometric templates cannot as often as desired be replaced with different biometric traits of the same person. Furthermore, they do not only contain information about the biometric features of a person, but may also contain personal information beyond what is needed for authentication (e.g. information about body conditions and diseases), which one would like to keep private. Removing such extra information may not be feasible, but the biometric templates can be stored in a fashion that superfluous information is hidden. The confidentiality of passwords is usually protected by cryptographic hash functions, and the hash value of a presented password is bit by bit compared with the hash value of the stored password. This approach cannot be applied to biometric data because biometric data from the same person are never completely the same due to their natural variability. For the protection of biometric templates special biometric template protection techniques have been developed utilizing cryptographic techniques. The biometric template protection techniques do not only prevent privacy leakage and provide confidentiality of the stored biometric templates, but address also problems like ID theft and cross-matching of biometric templates stored in different systems.

This paper summarizes challenges with respect to privacy and security and recent innovations in biometric template protection schemes. Privacy considerations are discussed for instance with respect to biometric access control for holders of season tickets to a public outdoor pool.

About the author

Moazzam Butt is a researcher at the competence center “Identification and Biometrics” of the Fraunhofer Institute for Computer Graphics Research IGD in Darmstadt, Germany. In December 2011, he received his Master of Science degree in Information and Communication Engineering from Technische Universität Darmstadt, Germany. During his graduate studies, he worked in the Fraunhofer Institute for Computer Graphics Research IGD and in the Fraunhofer Institute for Secure Information Technology SIT in the departments “Identification and Biometrics” and “Media Security” respectively. In Fraunhofer IGD, he worked in the field of template protection of fingerprints and iris templates. In Fraunhofer SIT, he worked in the area of audio watermarking using perceptual hashing. His main research interests lie in the fields of security of biometrics, template protection, and perceptual hashing.

An Approach to introduce Privacy by Design in Agile App-Development

Martin Degeling and Kai-Uwe Loser

Ruhr-University Bochum, Information and Technology Management
Universitätsstraße 150, 44780 Bochum
Germany
e-mail: {martin.degeling,kai-uwe.loser}@rub.de

This paper reports about experiences and an approach to integrate privacy-by-design (PbD) principles in an agile development project. Within small and distributed teams several prototypes and applications (apps) with a focus on learning support were developed. The approach included measures to ensure security and privacy awareness. Secondly more general guidelines were developed as a starting point for the appropriate development of specific solutions. Thirdly a process model gave advice on when and how to consider privacy requirements.

Often privacy assessments are made on large impact applications like electronic voting systems (Gürses et al. 2011) or the introduction of SAP. But nowadays also the “appification” results in a much more diverse landscape of software products. Small tools (apps) with limited capabilities are developed by distributed teams in short times spans. These apps running on smartphones, tablets and desktop PCs are designed to collect, use and distribute information to share them on social networks or with other apps.

Privacy by design (Schaar 2010) researchers on the other hand suggest a multi-level approach of analyzing privacy problems that may arise from software in development. Although there exist overall guidelines how to do privacy engineering (Gürses et al. 2011; Speikermann/Cranor 2009) and integrate Privacy Enhancing Technologies (PETs) on a more general level one open challenge is how to integrate PbD principles into current development practice (Spiekermann 2012). Especially in agile development projects with small iteration cycles with a focus on quick implementation of new features any privacy analysis, similar to security (Siponen et al. 2005) are often only added afterwards.

We have been working as privacy officers in a large scale research project that has the goal to develop multiple apps which should collect data about the work life of users and help them to learn and reflect on their everyday work practice. The apps were developed mostly for mobile devices and support reflective learning at the workplace by manual and automatic capturing of work situations. Due to the exploratory design process development took place in short time periods (between 3 and 12 month) with elements of agile development and rapid prototyping based on storyboards written in cooperation of developers and users.

During discussions we saw a high awareness for privacy problems on developers side as well as on the side of the users. Nevertheless when it came to building and evaluating them there was only little time left to make a deep privacy impact analysis neither for each developer nor for us as informal data protection officers. We therefore focused on privacy impact assessment of a smaller number of apps that served as examples for all developers. Guidelines where developed from existing resources but with a strong focus on the apps and on the context of their planned usage. The process model we developed for our approach included perspectives of user privacy, third party privacy, special requirements of mobile devices and organizational security. By this we fostered adoptions of the scenarios to include e.g. data minimization and maximum retention times that guided the app development and took advantage of the developers intrinsic motivation to avoid to develop features that might be to privacy invasive and instead encouraged “privacy by default”. Together with participatory design approaches we could make sure all apps protected privacy on a comparable level.

References

1. Gürses, F.S., Troncoso, C., Diaz, C.: Engineering Privacy by Design. Computers, Privacy & Data Protection. (2011).
2. Schaar, P.: Privacy by Design. Identity in the Information Society. 3, 267–274 (2010).
3. Siponen, M., Baskerville, R., Kuivalainen, T.: Integrating Security into Agile Development Methods. Proceedings of the 38th Annual Hawaii International Conference on System Sciences, 2005. HICSS ’05. p. 185a (2005).
4. Spiekermann, S.: The challenges of privacy by design. Communications of the ACM. 55, 38 (2012).
5. Spiekermann, S. and Cranor, L. F: “Engineering Privacy,” IEEE Transactions on Software Engineering, vol. 35, no. 1, pp. 67–82, Jan. 2009.

About the authors

Martin Degeling (M.Sc.) is research assistant at the Ruhr-University in Bochum. His research interests are privacy and data-protection in CSCW contexts as well as design of socio-technical systems. He is working in the MIRROR project on the work packages "Collaborative Knowledge Construction" and "Privacy".

Dr. Kai-Uwe Loser is data protection official at two universities, privacy consultant and a senior researcher in human computer interaction. Besides data protection and privacy he is interested in user experience, sociotechnical systems, appropriation of software systems and participatory design.

Blurring the dimensions of privacy?

Law enforcement and trusted traveler programs

Matthias Leese

International Centre for Ethics in the Sciences and Humanities,
University of Tübingen,
Wilhelmstraße 19, 72074 Tübingen, Germany
e-mail: matthias.leese@izew.uni-tuebingen.de

The debate on privacy has lately been influenced by Nissenbaum's (2010) notion of contextual integrity. Within aviation, as has been noted by Bennett (2005, 2008), the meaning of privacy is indeed highly dependent on contextual factors.

With new passenger screening concepts presented by the IATA[1] ("checkpoint of the future") and ACI/AEA[2] ("Better Security"), risk as the central paradigm for future developments in airport security is on the rise. Supposed to be a remedy for multiple challenges in aviation, the assignment of risk levels for passengers would potentially allow airport authorities to add or subtract layers of security measures, according to the assumed threat that a given passenger would pose to aviation. The computing of risk levels must be based on extensive coverage of passenger information, though. Thus, what does the introduction of risk mean in terms of privacy impact assessment?

Taking contextual factors into account, airports have been described as disciplinary spaces (Lyon 2003). Taking up the notion of Augé's (2006) "non-places", airports exist for the mere purpose of transit and for their lack of stable social relations, are mostly regulated via technology, especially when it come to ensuring security. Thus, an atmosphere of intimidation is created and as a matter of fact, individuals are more likely to accept cutbacks in terms of privacy claims within the contextual setting of the airport than in other environments.

Risk-based security frameworks aim at implementing assisted decision-making in order to offer custom- tailored screening for the enhancement of overall security. Thus, new screening concepts indeed enact what O'Malley (2006; see also Zedner 2006) has called a shift from rule-based to risk-based security. Risk struggles with the prediction of human behavior, though (Aradau, Lobo-Guerrero, and Van Munster 2008). In a preemptive approach to screening that focuses on intentions, mistakes can flag innocent individuals as potential threats and lead to serious and real consequences (more intrusive screening, questioning, considerable delay).

In order to avoid false negatives and false positives, risk-based screening approaches thus tend to make the database for risk-assessment as complete as possible. By converging information from law enforcement, homeland security and the private industry, "big data" is constructed and at the same time, the

[1] International Air Transport Association

[2] Airports Council International / Association of European Airlines

once distinct privacy dimensions of citizen-government and consumer-market (Westin 2003) become blurred.

But not only do risk-based screening approaches intend to make use of passenger information conducted by airlines (API, PNR[3]), but they also seek to exploit genuinely commercial programs like frequent-flyer-clubs or trusted traveler programs. Created for the purpose of facilitating air travel for the global elites, those programs have turned out to be a valuable source of additional information, as members have to undergo an additional background check in order to become trustworthy (Jackson, Chan, and LaTourrette 2012).

As a conclusion, my paper finds that passengers at the airport have little leverage in negotiating privacy. The context is dominated by the overwhelming paradigm of global security and increasingly converges data from commerce and law enforcement. Hence, passengers not only have no choice for an opt-out from full disclosure of personal data – the alternative would be not flying after all – but that on the contrary, risk-based concepts like the ones presented by IATA and ACI/AEA include an additional opt-in, requiring the surrender of even more information. In terms of privacy, this raises major concerns that call for regulation on the policy level.

References

1. Aradau, Claudia, Luis Lobo-Guerrero, and Rens Van Munster. 2008. "Security, Technologies of Risk, and the Political: Guest Editors’ Introduction." Security Dialogue no. 39 (2-3):147-154.
2. Augé, Marc. 2006. Non-places: Introduction to an Anthropology of Supermodernity. London: Verso.
3. Bennett, Colin J. 2005. "What Happens When You Book an Airline Ticket? The Collection and Processing of Passenger Data Post-9/11." In Global Surveillance and Policing. Borders, Security, Identity, edited by Elia Zureik and Mark B. Salter. Cullompton/Portland: Willan.
4. Bennett, Colin J. 2008. "Unsafe at Any Altitude. The Comparative Politics of No-Fly Lists in the United States and Canada." In Politics at the Airport, edited by Mark B. Salter. Minneapolis/London: University of Minnesota Press.
5. Jackson, Brian, Edward Chan, and Tom LaTourrette. 2012. "Assessing the Security Benefits of a Trusted Traveler Program in the Presence of Attempted Attacker Exploitation and Compromise." Journal of Transportation Security no. 5 (1):1-34.
6. Lyon, David. 2003. "Airports as Data Filters: Converging Surveillance Systems after September 11th." Journal of Information, Communication and Ethics in Society no. 1 (1):13-20.
7. Nissenbaum, Helen. 2010. Privacy in Context: Technology, Policy, and the Integrity of Social Life. Stanford: Stanford Law Books.
8. O’Malley, Pat. 2006. "Risks, Ethics, and Airport Security." Canadian Journal of Criminology and Criminal Justice no. 48 (3):413-421.
9. Westin, Alan F. 2003. "Social and Political Dimensions of Privacy." Journal of Social Issues no. 59 (2):431-453. Zedner, Lucia. 2006. "Neither Safe Nor Sound? The Perils and Possibilities of Risk." Canadian Journal of Criminology & Criminal Justice no. 48 (3):423-434.

About the author

Matthias Leese, is a research associate within the Section Security Ethics at the International Centre for Ethics in the Sciences and the Humanities (IZEW), University of Tuebingen. He is currently involved in the interdisciplinary research project KRETA, concerned with social and political implications of body scanner technology at the airport. Furthermore, he is a member of the ethical

[3] Advanced Passenger Information / Passenger Name Record

advisory board of the EU-FP7 research project Alert for All, concerned with ethical implications in the development of a new European alerting tool. Holding a masters degree in political science (University of Hamburg), his primary research interests are located in the fields of surveillance and security studies, as well as civil liberties, terrorism and securitization issues, especially within airport/aviation security.

Privacy and free speech on the Internet

Taking the ”household exemption“ online

Zuzanna Warso

Helsinki Foundation for Human Rights
ul. Zgoda 11, 00-018 Warsaw, Poland
e-mail: z.warso@hfhr.org.pl

The proposed EU law on personal data protection has been designed so as to enable users to remove their personal data from the Internet. While the proponents of the „right to be forgotten” hope it to be a remedy to the problem of the impossibility to escape one’s past once its records are published online, others refer to it as the “ticking time bomb” and regard the new right as the “biggest threat to free speech on the Internet in the coming decade”.

The need for a change in the legal framework results from a paradigmatic shift that made online remembering the norm, and forgetting the exception. This change was due to a number of technological drivers that apart from the digitalization of data included the development of cheap storage, easy retrieval and global search. The idea of the right to be forgotten grows out of the realization that preserving control over one’s identity has become a challenge in a world in which almost all that is said about an individual may go into permanent public files.

Although the right to be forgotten has been established in order to give back to Internet users control that they have been gradually loosing, it triggers a series of doubts. Enforcement of the new rules may result in a conflict of fundamental rights that will require striking a balance between the right to privacy and data protection on one hand, and the freedom of expression and the right to access information on the other. It is possible that not only courts will engage in the balancing exercise, but also private companies and individuals will need to apply the proportionality principle in their online activity. The opponents of the new right fear that the risk of financial sanctions for illegal processing of personal data may turn Internet service providers into censors and, in general, have a chilling effect on the free online expression. The debate triggered by the new European proposal also exposed the cultural and legal differences in attitudes to privacy and free speech in the EU and the US. While for practical reasons, legal regulations of data protection should be brought closer, different understanding of online privacy may create serious obstacles in establishing common standards.

The presentation will look closely at the controversies surrounding the right to be forgotten. It will argue that, while the discussion about the virtue of forgetting in digital age is animated by the conflict between privacy and free speech, a more nuanced understanding of these values is still needed in order to strike a “fair balance” between the conflicting rights in the online environment. The author will argue against the view of the Court of Justice of the European Union expressed in the Lindqvist case (C -101/01) concerning the so-called "household exemption", where the Court stated that the act of identifying a natural person on an Internet site, by name or other personal identifiers, automatically constitutes "processing" of personal data. A broader understanding of the “household exemption” applicable online will be proposed. The presentation hopes to prove that a methodological differentiation between data which is published seeking broad dissemination and that which although in the public space, is not intended for mass communication, as well as taking into consideration the context in which information is shared, the changing nature of information over time, and the intentions of the content’s producer, are necessary in order to adjust the legal framework resting on the concepts of privacy and data protection to the demands of digital age, while avoiding the risk of stifling freedom on the Internet.

About the author

Zuzanna Warso studied Law at the University of Warsaw, including a two-semester stay at the Humboldt University in Berlin. She also holds an MA in English studies. She wrote her master thesis on the relationship between technology, the body and the feminine in cyberpunk fiction.

She is currently working at the Helsinki Foundation for Human Rights, a Warsaw based NGO. She is responsible, among others, for reviewing the impact of EU legislation on human rights.

The core content of personal data protection
A conceptual controversy

Gloria Gonzalez Fuster and Serge Gutwirth

Research Group on Law Science Technology & Society (LSTS)
Vrije Universiteit Brussel (VUB)
Pleinlaan 2, 1050 Brussels Belgium
e-mail: {gloria.gonzalez.fuster,serge.gutwirth}@vub.ac.be

The existence of a fundamental right to the protection of personal data in European Union (EU) law is nowadays undisputed. Established in the EU Charter of Fundamental Rights in 2000, this new right is increasingly permeating EU secondary law, and is more and more frequently relied upon by the EU Court of Justice in its judgments. It is also expected to play a crucial role in the future EU personal data protection landscape, as advanced in the legislative package published by the European Commission in January 2012. The right's incipient presence in such package, however, has rendered manifest the co-existence of two possible and contrasting interpretations as to what it really means. Whereas it is often construed as a combination of subjective rights (granted to individuals, or 'data subjects') and obligations (imposed on those who process personal data) and an obligation of independent supervision, as jointly prescribed by the three paragraphs of Article 8 of the EU Charter, the right is sometimes portrayed as being constituted solely by the general reference of the EU Charter's Article 8(1) to everybody's right to have their personal data 'protected', a word understood then as 'kept free from processing'. If some envision the right to the protection of personal data as a positive right or a power, enabling the processing of such data under certain conditions, others picture it as a negative prescription, implying that any processing of data is a limitation of such 'protection' and, thus, a violation of the fundamental right. The identification of the right's core content is indeed crucial, as the respect of such core is precisely one of the requirements that any limitation must meet in order to be considered lawful according to the EU Charter.

This paper seeks to render visible the existing tensions between the understandings of the right to the protection of persona data, and to explore the assumptions and conceptual legacies underlying both approaches. It studies them from various angles. It first traces their historical lineages, locating their roots in the very origins of European data protection. Second, focusing on the right to personal data protection as established by the EU Charter, it analyses the different arguments that can ground contrasted readings of its Article 8: in particular, the drafting process of the article (which was only divided into three paragraphs at a final stage), and the Charter's structure (which appears to formally relegate the description of rights' limitations to its final horizontal provisions). Third, it reviews the conceptualisations of personal data protection as present in the literature, noting that some of them emphasise its continuities with the right to respect for private life, or right to privacy (and attribute to it, by analogy, a prohibitive nature), while others stress instead its discontinuities (for instance, in terms of ‘generations’ of rights, or as through the opacity v. transparency opposition), but that they are almost invariably built upon, or against, the right to privacy. Finally, it questions the pros and cons of the discussed approaches vis-a-vis the challenges of emerging technologies.

About the authors

Gloria González Fuster is a researcher at the Law, Science, Technology & Society (LSTS) Research Group of the Faculty of Law and Criminology of the Vrije Universiteit Brussel (VUB), where she is finalising a PhD thesis on the emergence of the right to the protection of personal data as a fundamental right of the European Union (EU). With work experience at different EU institutions, and an academic background in Law, Communication Sciences and Modern Literature, she has actively contributed to various EU-funded research projects, including Reflexive Governance in the Public Interest (REFGOV), Converging and Conflicting Ethical Values in the Internal/External Security Continuum in Europe (INEX) and Privacy and Security Mirrors (PRISMS).

Serge Gutwirth is professor of law at the Faculty of Law and Criminology of Vrije Universiteit Brussel and holder of a research fellowship in the framework of the VUB-Research Contingent. He is the Director of the research group on Law, Science, Technology & Society (LSTS).

Robots in the Cloud with Privacy

A New Threat to Data Protection?

Ugo Pagallo

Law School, University of Torino,
via s. Ottavio 54, 10124 Torino, Italy
e-mail: ugo.pagallo@unito.it

> "Newspaper taxis appear on the shore,
> Waiting to take you away.
> Climb in the back with your head in the clouds,
> And you're gone."
>
> *John Lennon & Paul McCartney*

There are a number of robots out there: military and civilian drones, driverless cars, hybrids of natural and artificial systems, unmanned underwater vehicles, reprogrammable and multipurpose manipulators in the industrial field, and even diva-bot pop star singers as the HRP-4C robot developed by the Institute of Advanced Industrial Science and Technology's media interaction group in Japan. The focus of this paper is on the class of robots connected to a networked repository on the internet that allows such machines to share the information required for object recognition, navigation and task completion in the real world. As a part of the *Cognitive Systems and Robotic Initiative* from the European Union seventh framework programme (FP7/2007-2013), this is, for instance, the aim of the RoboEarth project on a world wide web for robots, namely, a network and database repository where machines can share information and learn from each other about their behaviour and their environment. Avoiding shortcomings of traditional approaches, such as onboard computers for robots, the goal of the project is to complete a sort of cloud robotics infrastructure with all that is needed to close the loop between robots, RoboEarth, and robots.

There are however risks for people's informational privacy (Gogarty et al. 2009; Sharkey et al. 2010): a new generation of network-centric applications could collect data incessantly and in ways that are "out of control," because such machines are increasingly "autonomous," that is, they respond to stimuli by changing the values of their properties or inner states and, furthermore, they can improve the rules through which those properties change without external stimuli. Therefore, by collecting information in open or public environments and, moreover, bringing such environmental information to cloud servers, robots can severely impinge on current data protection, since these machines may replicate and spread all the data they collect beyond human control. Consider for example the class of robots for personal and domestic use: we already have, after all, a number of robot toys and robot nannies that are programmed to provide love and take care of children and the elderly. Likewise, think of new types of artificial assistants for university teachers, as a sort of i-Jeeves that could help us schedule a set of conferences, lectures and meetings: By checking the availability and convenience of logistics in accordance with a number of parameters like budget, time efficiency, or weather average conditions, these robots could report its findings back for a decision or, even, determine the steps of the academic tour by directly accepting invitations, booking hotel rooms, flights and so forth.

Yet, in addition to problems of data protection induced by the "autonomy" of these machines, personal and/or domestic robots will raise a number of psychological issues concerning feelings of subordination, attachment, trustworthiness, etc. (Veruggio 2006): it is also likely that these machines will know a lot of things about our private life. Consequently, a further set of problems should be taken seriously: Whereas issues of data protection mostly revolve around the transparency with which personal data are processed, people's privacy has often to do with the idea of "opaqueness" (Arendt 1958), i.e., privacy conceived of as a condition of "solitude," "exclusion," "secrecy," and so on (Westin 1967; Gavison 1980; Allen 1988; etc.). Of course, matters of data protection and privacy at times overlap, as it occurs with people unintentionally using network-centric machines that infringe data protection laws, i.e., regardless of human wrongdoing or mere negligence and, vice versa, people spying on other individuals through domestic robots, and even kidnapping such robots so as to get personal data. Here, some approaches to data protection, such as "privacy by design," appear particularly fruitful to protect people's "opaqueness" (Pagallo 2011, 2012). Still, individual interaction with personal machines, domestic robots, and so forth, will also affect what U.S. common lawyers call a reasonable "expectation of privacy." The traditional "right to be let alone" (Warren and Brandeis 1890) does not represent any automatic zero-sum game, because personal choices play a crucial role when individuals modulate different levels of access and control over information, depending on the context and its circumstances (Nissenbaum 2004). Accordingly, some approaches of the aforementioned principle of privacy by design may fall short in coping with issues that depend on the cultural context and the type of application with which we are dealing: robots as "lovers" (Levy 2007), as "human cubs" (Dautenhahn 2007), as "pets" (McFarland 2008), etc. These differentiations are critical to appreciate how robots bring about a set of constraints and opportunities that impact on norms of appropriateness, i.e., norms that determine whether it is appropriate to trace back information to an individual, and norms of flow, that is, how information should be distributed according to different standards in different contexts.

In light of these differentiations, a final convergence between privacy and data protection should be stressed. What "robots in the cloud" will ultimately affect concerns the "ontological friction" in the informational sphere, namely the forces that oppose the flow of personal information, as "the amount of work and efforts required for a certain kind of agent to obtain, filter and/or block information (also, but not only) about other agents in a given environment" (Floridi 2006). Whilst some "degrees of friction" are required to keep firm distinctions between agents and system, individuals and society, robots will affect such degrees in a twofold way, that is, via new expectations of privacy in the personal or domestic human-robot interaction that reverberate on the ways in which personal data ought to be processed through different types of network-centric applications, e.g., the conditions that make the processing of personal data legitimate through the informed consent of the individual. At the end of the day, we should be prepared to accept a new category of artificial behaviour, which is not simply mechanical or reducible to an aggregation of human beings as the only relevant source of their action, yet produces multiple relevant effects in the fields of privacy and data protection. Since robots are here to stay, the aim of the law should be to wisely discipline our mutual relationships (Pagallo, forthcoming).

References

1. Allen, Anita (1988) Uneasy Access: Privacy for Women in a Free Society. Totowa, N.J.: Rowman and Littlefield
2. Arendt, Hannah (1958) The Human Condition. Chicago: University of Chicago Press
3. Dautenhahn, Kerstin (2007) Socially Intelligent Robots: Dimensions of Human-Robot Interaction, Philosophical Transactions of the Royal Society B: Biological Sciences, 362(1480): 679-704
4. Floridi, Luciano (2006) Four Challenges for a Theory of Informational Privacy, Ethics and Information Technology, 8(3): 109-119
5. Gavison, Ruth (1980) Privacy and the Limits of the Law, Yale Law Journal, 89: 421-471
6. Gogarty, Brendan and Meredith Hagger (2008) The Laws of Man over Vehicle Unmanned: the Legal Response to Robotic Revolution on Sea, Land and Air, Journal of Law, Information and Science, 19: 73-145
7. Levy, David (2007) Love and Sex with Robots: The Evolution of Human-Robot Relationships. Harper, New York
8. McFarland, David (2008) Guilty Robots, Happy Dogs: The Question of Alien Minds. Oxford University Press, New York
9. Nissenbaum, Helen (2004) Privacy as Contextual Integrity. Washington Law Review, 79(1): 119-158
10. Pagallo, Ugo (2011) Designing Data Protection Safeguards Ethically. Information, 2(2): 247-265
11. Pagallo, Ugo (2012) On the Principle of Privacy by Design and its Limits: Technology, Ethics, and the Rule of Law. In European Data Protection: In Good Health?, Serge Gutwirth, Ronald Leenes, Paul De Hert and Yves Poullet (eds.), pp. 331-346. Springer, Dordrecht
12. Pagallo, Ugo (forthcoming) The Laws of Robots: Crimes, Contracts, and Torts. Springer, Dordrecht
13. Sharkey, Noel, Goodman, Marc and Nick Ross (2010) The Coming Robot Crime Wave, IEEE Computer Society, 114-116
14. Veruggio, Gianmarco (2006) Euron Roboethics Roadmap. In: Proceedings Euron Roboethics Atelier, February 27th-March 3rd, Genoa, Italy
15. Warren, Samuel D., and Louis D. Brandeis (1890) The Right To Privacy, Harvard Law Review, 4:193-220.
16. Westin, Alan F. (1967) Privacy and Freedom. New York: Atheneum

About the author

Ugo Pagallo is a Full Professor in Philosophy of Law at the University of Torino, Law School, since 2000, and Faculty at the Center for Transnational Legal Studies (CTLS) in London, U.K. He is editor of the Digitalica series published by Giappichelli in Turin and co-editor of the AICOL series by Springer: Since 2008 member of the Programme Committee of ETHICOMP. In addition to numerous essays in scholarly journals like Journal of Business Ethics, AI & Society, Journal of Information, Communication and Ethics in Society, Hobbes Studies, Journal of Chinese Philosophy, Apuntes filosóficos, and so forth, he is the author of eight monographs. His main interests are AI & Law, Network theory, Robotics, and Information Technology Law (specially data protection law and copyright).

(Not So) Smart Cities
The societal drivers and impact of smart environments

Gemma Galdon Clavell

Department of Sociology and Organizational Analysis,
Universitat de Barcelona,
Av. Diagonal 696, 08034 Barcelona, Spain
e-mail: gemma.galdon@ub.edu

The term ’smart city’ is becoming pervasive in the urban agenda of the 21st Century. City halls and local decision-makers fill their discourses with references to the promise of smart technology for increased efficiency and quality of life. The industry offers funding, ready-made technological solutions and the promise of a quick fix to all current and future urban challenges. Local SMEs strive to find the formula that will make them relevant and useful in this new scenario. While the appeal of technologies is understandable, and part of the enthusiasm for the contribution that technology can make to better cities is fully justified (e.g. open data, urban computing, integrated operations centres, RFID, sensors and system integration have endless possibilities), many of the policies, approaches, discourses and technologies that fall under the ’smart’ umbrella have yet to take into account the social, ethical and privacy risks associated with smart environments. However, cities around the world continue to buy into the ’smart city’ paradigm put forward by the industry, which has labeled as smart solutions a series of technology applications which have the potential of improving urban mobility and efficiency (from garbage collection to improved parking solutions, sensors, etc.) but which so far do not constitute a working, useful paradigm or urban solution.

Parallel to this proliferation of the term and the associated technologies, the debate around their desirability and usefulness is being raised from different perspectives. Some suggest that there is a need to escape or complement the top-down approaches promoted by the industry with bottom-up, citizen technologies that connect solutions to ’actually-existing problems’ (Schaffers et al. 2012). Others argue in favour of escaping the market-driven approach to promote effective empowerment and participation though urban technologies (Hollands 2008). And, in the midst of all this, the number of media reports and EU rulings on the risks of smart solutions such as ’smart meters’ and ’big data’ suggest there are still many aspects that have not properly been dealt with.

This paper presents a summary of smart solutions applied to urban environments, in order to provide a picture of what are the different solutions that make up what constitutes a ‘smart city’ and their actual potential to significantly alter the way urban environments are run and experienced. The argument is organized around three main points:

- Technological determinism: while many are demanding that smart city solutions start to take into account citizens, informal dynamics and bottom-up innovative solutions, many of the current critiques of smart cities take for granted the earth-changing possibilities of smart technologies. This approach underestimates risks, instances of failure, false positives or the effects of the industry-promoted ‘hype’ around such solutions, and continues to rely on the possibility of a ‘technological fix’ (Ceyhan 2006) to social and urban problems. Understanding technology as part of a political assemblage and not a silver bullet could thus be useful in terms of escaping both technological determinism and technophobia.

- Smart technologies as surveillance: all smart solutions have surveillance capabilities, as they are pervasive into people’s daily life and into the social infrastructure and can track, record and match people’s activities, movements, biometric data, etc. This raises a number of ethical, legal and social issues that need to be taken into account by policy makers, technology developers and all those involved in the value chain of smart environments at an early stage. In this respect, many of the issues raised by the EU in relation to the need for responsible innovation in the field of ICT development and for a careful assessment of the societal impact of new technologies are very relevant to smart cities.
- The pull factors behind smart cities: There seems to be a consensus that smart technologies are ’vendor pushed’. However, the enthusiasm for technological solutions is deeply felt in urban policy, as smart technologies are seen as a key ally in the improvement of efficiency in service provision and communication. The ’pull’ role of local and regional governments suggests a need to better understand the dynamics of policy transfer, the role of cities in global governance, the impact of technology in decision-making processes and internal government and government-to-citizens dynamics, and the relationship between the economic configurations that emerge to foster smart cities (Public-Private Partnerships) and broader issues related to urban governance.

References

1. Ceyhan, A. (2006). ‘Téchnologie et sécurité: une gouvernance libérale dans un context d’incertitudes’. Cultures & Conflits, 64 (hiver). Pgs. 11?32.
2. Hollands, R.G. (2008) Will the real smart city please stand up? Intelligent, progressive or entrepreneurial?. In City. Analysis of urban trends, culture, theory, policy, action 12 (3): 303.320.
3. Schaffers, H., Komninos, N., Pallot, M. (2012) ’Smart Cities as Innovation Ecosystems Sustained by the Future Internet’. FIREBALL White Paper. Available at `http://www.fireball4smartcities.eu/wp-content/uploads/2012/05/FIREBALL-White-Paper-Final2.pdf`

About the author

Dr. Gemma Galdon Clavell is a policy analyist working on surveillance, the social, legal and ethical impact of technology, smart cities and public space, privacy, security policy, resilience and policing. She is currently working as a researcher at the Sociology Department at the Universitat de Barcelona (UB), where she is a leading partner and member of several FP7 and COST research projects (IRISS, LiSS, RESPECT, SMART, SOURCE, CP-UDP). She completed her PhD on surveillance, security and urban policy in early 2012 at the Universitat Autònoma de Barcelona (UAB) and was later appointed Director of the Security Policy Programme at the Universitat Oberta de Catalunya (UOC). Previously, she worked at the Transnational Institute (TNI), the United Nations' Institute for Training and Research (UNITAR) and the Catalan Institute for Public Security (ISPC). She is a member of the international advisory board of Privacy International and a regular analyst on TV, radio and print media. Her recent academic publications tackle issues related to the proliferation of surveillance in urban settings, urban security policy and community safety, security and mega-events and the relationship between privacy and technology.

Towards a rhizomatic theoretical framework to understand the consequences of preemptive surveillance of children

Rosamunde van Brakel

Research Group on Law Science Technology & Society (LSTS)
Vrije Universiteit Brussel (VUB)
Pleinlaan 2, 1050 Brussels Belgium
e-mail: rosamunde.vanbrakel@gmail.com

Considering that surveillance of children can be seen as the oldest and most “banal” form of surveillance and taking into account all the measures and technologies that have been developed to surveill children from the 20th century onwards in Western society, it is striking how little research has been done on surveillance of children and the consequences flowing from it. Scholars have consigned children to the margins or, even more commonly, entirely excluded children as a political (Wagnsson, Hellman & Holmberg, 2010) or social actor category. This lack of attention is strange especially as Marx & Steeves (2011) remark “kids are literally the poster children for surveillance”; children illustrate a broader array of central surveillance concepts and dynamics and confront one with issues that do not come to light when focusing on the general ‘adult’ population.

Furthermore although increasingly surveillance technologies are designed to predict future crimes, and within criminological research a shift has been emphasised from a post-crime to a pre-crime society, which is "“characterised by calculation, risk and uncertainty, surveillance, precaution, prudentialism, moral hazard, prevention and which has the overarching goal of the pursuit of security” (Zedner, 2007), very little in-depth research has been conducted on the nature of preemptive surveillance and its consequences. As a result of this shift, earlier and earlier interventions are seen as necessary to reduce criminal opportunity and to increase surveillance before harm is done. ‘ShareCare for children’ which is implemented in several councils in England is one of the results of this ‘pre-emptive turn.’ ‘ShareCare for children’ is an integrated assessment and case management system of which the key focus is to facilitate the secure sharing of health, youth justice, social care and education systems data with the goal of targeting children and young people before they get into trouble.

The main purpose of this paper is, by using ’ShareCare for children’ as a case study, to propose a rhizomatic theoretical framework to understand the (unintended) consequences of preemptive surveillance of children which goes further than a discussion of privacy and data protection issues to which discussions about the unintended consequences of such systems are often reduced to. This proposal will use the notion of the ’surveillant assemblage’ as proposed by Haggerty & Ericson (2000) as starting point to provide a better understanding of how these technologies are governed and implemented.

By looking at the governance and practice of these types of system as assemblages, which are characterised by a rhizomatic structure, surveillance dynamics, power relations and unintended consequences come to light that otherwise would have stayed in the dark. Moreover, by looking at surveillance technologies as an assemblage, it is possible to go beyond the traditional understanding of surveillance as an exclusive relationship between the surveillance authority and the subject of the surveillance and it becomes clear how other actors, like technology play an important role too and need to be taken into account when exploring the unintended consequences of the implementation of these technologies.

References

1. Haggerty, K.D. & R.V. Ericson (2000) The surveillant assemblage, British Journal of Sociology, 51(4): 605-622.
2. Marx, G.T. & V. Steeves (2011) From the beginning: Children as subjects and agents of surveillance, Surveillance & Society, 7 (3/4): 192-230.
3. Wagnsson, C., Hellman, M. & A. Holmberg (2010) The centrality of non-traditioal groups. Security in the globalized era: the case of children, International Political Sociology, 4(1): 1-14.
4. Zedner, L. (2007) Pre-crime and post-criminology?, Theoretical Criminology, 11 (2): 261-281.

About the author

Rosamunde van Brakel has studied at the Katholieke Universiteit Leuven and University of Ottawa and obtained degrees in both educational sciences and criminology. She has been a visiting researcher at the Surveillance Studies Centre at Queens University in Canada, is an expert in the EU COST-LISS project and is Associate Member Representative on the Network and Editorial Board of the Surveillance Studies Network. Currently she is involved in the FP7 SIAM project. The doctoral research focuses on the social, ethical and legal issues involved in the implementation of pre-emptive surveillance technologies in the context of crime prevention. She is also part of the programming committee of the annual Computers, Privacy and Data Protection Conference, which is co-organised by LSTS and has recently co-authored an article in the international interdisciplinary journal Surveillance & Society, on Understanding resistance to digital surveillance: Towards a multi-disciplinary, multi-actor framework (2009).

Towards a multi-dimensional technology assessment[*]

The introduction of security technologies at airports and public transport systems

Leon Hempel, Tobias Schaaf, Dagny Vedder, and Lars Ostermeier

Centre for Technology and Society, Technical University Berlin,
Hardenbergstrasse 16-18, 10623 Berlin, Germany
e-mail: {hempel,schaaf,vedder,ostermeier}@ztg.tu-berlin.de

The paper presents a conceptual approach to build a multi-dimensional Security Technology Assessment Support System and discusses the societal dimensions of technology assessment procedures.Today diverse assessment approaches exist, often focusing on one dimension without regarding the interrelations to other assessment dimensions. Security Technology Assessments frequently measure the functionality and efficiency against the promised security gain, neglecting that there is a privacy and trust impact that needs to be considered. Other approaches emphasize the impact on privacy, neglecting not only efficiency but also trust considerations (Privacy Impact Assessment - PIA). Personal perception and experiences of the scrutinized are being mitigated or ignored, even though they have major impacts on the perception towards SMTs.

Beside the choice of assessment approaches, the time of involvement of relevant actors implies the current difficulties of decision makers. At an early stage, when irreversibilities have not yet emerged and influence on the technology acquisition process is still possible, the decision makers have to define who has to participate at which time and which assessment criteria should be used in order to assess the technology. At the same time, decision makers have to cope with the situation that very little is known about the technology and the involved processes.

The paper addresses those problems by rendering a multidimensional holistic approach for security technology assessment. On the highest aggregation level the paper presents a model integrating four assessment dimensions: Security, Trust, Efficiency and Freedom Infringements (STEFI model). These four assessment dimensions are the result of empirical investigations conducted in four case studies about how the actors themselves decide about technology criteria, how they prioritise them and thereby construct the realty of SMTs. A major focus was set on an airport case study to acknowledge its role as both

[*] The paper is produced in the context of a EU-funded research project coordinated by the authors, called SIAM (Security Impact Assessment Measures). SIAM aims to develop an Assessment Support System that helps to increase inclusiveness of security technology assessment procedures for airports and public transport systems. Besides technological functionalities and economic requirements, SIAM analyses methods and criteria to assess the effectiveness in countering threats and reducing risks; regulative issues; freedom infringements; cultural issues; accountability and acceptance of Security Measures and Technologies.

being the subject to a highly restricted security regime and being a test field for evolving new SMTs.

The STEFI assessment procedure encompasses a set of questions related to the assessment criteria that provide decision makers with a guideline that allows them to plan and conduct a comprehensive security technology assessment. In a guided assessment procedure, the user will be presented with a pre-defined sequence of questions corresponding to his or her role in the assessment procedure. As a result, the user will receive some indication of open issues that are related to other assessment perspectives. This will be realized as a work list or in the manner of a ticketing system where open tickets represent issues that require further attention. The assessment procedure will most certainly require further expertise and information to be successfully completed. In order to facilitate these subsequent steps, the system will provide access to additional information which may be relevant for the decision-making process. Such information is often publicly available (e.g. threat assessments, crime statistics, legal documentation, etc.), yet not drawn together in a single source. The SIAM tool will provide a library of these kinds of documents and make its repository easily accessible through advanced indexing, ranking and search tools. The final output of the Assessment Suppport System will be an Assessment Report that summarises the information collected and gives an overview of issues that still have to be addressed. The paper provides an example illustrating a security technology assessment procedure based on the STEFI model.

The paper concludes that STEFI could be a possibility to overcome the dilemma of exclusion and the lack of common assessment criteria. It calls for multi-dimensional technology assessment procedures in order to facilitate reflexivity and social learning as early as possible in the technology development.

About the authors

Leon Hempel is a senior researcher and head of the research unit Security – Privacy – Risk at the Centre for Technology and Society, Technical University Berlin. He is involved in a number of national an international (FP6, FP7) security research projects and coordinating the SIAM project.

Dagny Vedder holds a Degree in Science and Technology Studies and is a researcher in the Security – Privacy – Risk research unit at the Centre for Technology and Society, Technical University Berlin. She is currently working in the SIAM project. Her research interests are the Social Shaping of Technology (SST) and Constructive Technology Assessment (CTA) programmes, risk communication and risk perception, technology assessment of security technologies, nanotechnologies, information- and communication technologies.

Tobias Schaaf earned his MA in Contemporary European Studies at the University of Bath and is a researcher in the Security – Privacy – Risk research unit at the Centre for Technology and Society, Technical University Berlin. He is currently working in the SIAM project. His research interests are security policy making, the normativity of security, and security technology implementation.

Lars Ostermeier studied Political Science and Criminology and is a researcher in the Security – Privacy – Risk research unit at the Centre for Technology and Society, Technical University Berlin. He is currently working in the SIAM project. His research interests are security and control, police studies, risk- and crime scenarios, science studies and the sociology of knowledge.

Participants

A

Abels, Ruben (DesignArbeid, Amsterdam, NL)

B

Bach, Nicolas (Nexus Institute, Berlin, DE)
Bahtiyar, Serif (Technical University Berlin, DE)
Bartelová, Pavlína (Czech Ministry of the Interior, Prague, CZ)
Bartolucci, Valentina (University of Bradford, UK)
Baumann, Pierre-Yves (Federal data protection and information commissioner, Bern, CH)
Borking, John J. (Borking Consultancy, Wassenaar, NL)
Boulanin, Vincent (École des Hautes Études en Sciences Sociales, Paris, FR)
Brey, Philip (University of Twente, Enschede, NL)
Burnik, Jelena (Information Commissioner Republic of Slovenia, Ljubljana, SI)
Butin, Denis (Inria, University of Lyon, FR)

C

Calzarossa, Maria Carla (University of Pavia, IT)
Casper, Carsten (Gartner, Privacy & Security, Berlin, DE)
Cruz, José (Universität Lusofona do Porto, PT)

D

Debeuckelaere, Willem (Commissioner for the Protection of Privacy, Brussels, BE)
Degeling, Martin (Ruhr University Bochum, DE)
Dix, Alexander (Commissioner for Data Protection and Freedom of Information, Berlin, DE)
Dumortier, Franck (University of Namur, BE)

F

Fabbri, Karen (European Commission, Brussels, BE)
Friedewald, Michael (Fraunhofer ISI, Karlsruhe, DE)

G

Galdon Clavell, Gemma (Universitat de Barcelona, ES)
Gellert, Raphael (Vrije Universiteit Brussels, BE)
Gonzalez Fuster, Gloria (Vrije Universiteit Brussels, BE)
Grunewald, Dennis (Technical University Berlin, DE)
Guagnin, Daniel (Technical University Berlin, DE)
Gutwirth, Serge (Vrije Universiteit Brussels, BE)

H

Hallinan, Dara (Fraunhofer ISI, Karlsruhe, DE)
Hempel, Leon (Technical University Berlin, DE)

J

Just, Miriam (Fraunhofer ISI, Karlsruhe, DE)

K

Karhula, Päivikki (Tampere University , FI)
Koch, Heiner (University of Tübingen, DE)
Köhl, Stefanie (IfG.CC - The Potsdam eGovernment Competence Center, Potsdam, DE)
Krempl, Stefan (heise.de)
Kurtze, Hannes (VDI/VDE Innovation + Technik GmbH, Berlin, DE)

L

Lauß, Georg (University of Vienna , AT)
Leese, Matthias (University of Tübingen, DE)
Llongueras, Adrianna (Instituto Universitario General Gutiérrez Mellado, Madrid, ES)
Lodge, Juliet (University of Leeds, UK)

M

Martens, Tobias (30dna Web + People, Bremen, DE)
Matzner, Tobias (University of Tübingen, DE)
Mordini, Emilio (CSSC, Rome, IT)

N

Nagenborg, Michael (University of Tübingen, DE)
Nwankwo, Iheanyi (University of Hannover, DE)

O

Ostermeier, Lars (Technical University Berlin, DE)

P

Pagallo, Ugo (University of Torino, IT)
Pöchhacker, Nikolaus (University of Vienna, AT)
Pohle, Jörg (Technical University Berlin, DE)
Pubalová, Miloslava (Czech Ministry of the Interior, Prague, CZ)
Püschel, Florian (University of Passau, DE)

R

Raab, Charles D. (University of Edinburgh, UK)
Ragnedda, Massimo (University of Northumbria, Newcastle, UK)
Rauls, Alexander (University of Bremen, DE)
Rettke, Annett (Technical University Berlin, DE)
Rommetveit, Kjetil (University of Bergen, NO)
Rouvroy, Antoinette (University of Namur, BE)

S

Sadikin, Mohammad Fal (Technical University Berlin, DE)
Samatas, Minas (University of Crete, Rethymno, GR)
Schaaf, Tobias (Technical University Berlin, DE)
Schartau Lara (University of Maastricht, NL)
Schaub, Florian (Ulm University, DE)
Schäufele, Fabia (Technical University Berlin, DE)
Schlehahn, Eva (Independent Centre for Privacy Protection Schleswig-Holstein, Kiel, DE)
Schraudner, Martina (Technical University Berlin, DE)
Schuppan, Tino (IfG.CC - The Potsdam eGovernment Competence Center, Potsdam, DE)
Schütz, Philip (Fraunhofer ISI, Karlsruhe, DE)
Seitz, Florian (University of Hamburg, DE)
Sharan, Yair (University Tel Aviv, IL)
Stahl, Bernd Carsten (DeMontfort University, Leicester, UK)
Székely, Iván (Eötvös Károly Policy Institute, Budapest, HU)

T

ter Meulen, Ruud (University of Bristolm, UK)
Tielemans, Laura (Vrije Universiteit Brussels, BE)
Thomé, Sarah (University of Kassel, DE)
Timmerhoff, Tom (newthinking communications GmbH, Berlin, DE)
Töpfer, Eric (German Institute for Human Rights, Berlin, DE)

U

Ulbricht, Max R. (Technical University Berlin, DE)
Unverricht , Kristina (DIN Deutsches Institut für Normung e.V., Berlin, DE)

V

van Brakel, Rosamunde (Vrije Universiteit Brussels, BE)
Vedder, Dagny (Technical University Berlin, DE)
Venier, Silvia (CSSC, Rome, IT)

W

Wagner, Ben (European University Institute, Florence, IT)
Warso, Zuzanna (Helsinki Foundation for Human Rights, Warsaw, PL)
Weimerskirch, Pierre (National Commission for Data Protection, Luxembourg, LU)
Whitehouse, Diane (The Castlegate Consultancy, Malton, UK)
Wiele, Johannes (TÜV Rheinland i-sec GmbH, Cologne, DE)
Wright , David (Trilateral Research & Consulting, London, UK)

Z

Zimmer-Helfrich, Anke (Verlag C.H. Beck, München, DE)

Useful information

Dates

27 - 28 November 2012

Conference venue

Fraunhofer Forum Berlin, Spreepalais, Anna-Louisa-Karsch-Straße 2, 10178 Berlin.
`http://www.forum.fraunhofer.de`

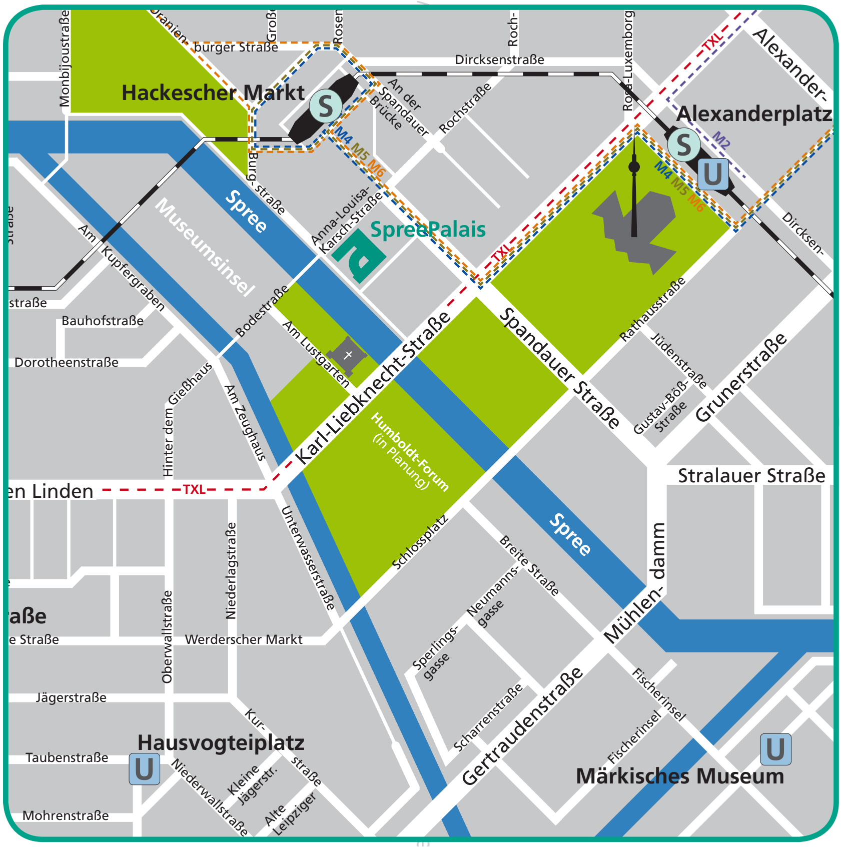
How to get there

By rail – Hauptbahnhof, Zool. Garten and Friedrichstraße: S-Bahn lines S 5, S 7, S 75, S 9 as far as the Hackescher Markt. Leave the station,towards Burgstraße/ Museumsinsel. At the Burgstraße go towards the cathedral as far as the Anna-Louisa-Karsch Strasse, and cross this street. The main entrance of the Spreepalais is 20 m along on the left-hand side.

By rail – Ostbahnhof and Alexanderplatz: S-Bahn lines S 5, S 7, S 75, S 9 as far as the Hackescher Markt. Leave the station,towards Burgstraße/ Museumsinsel. At the Burgstraße go towards the cathedral as far as the Anna-Louisa-Karsch Strasse, and cross this street. The main entrance of the Spreepalais is 20 m along on the left-hand side.

By air – Airport Tegel: The Spreepalais is approx.10 km from Berlin-Tegel airport. The TXL bus route, going towards Mollstr./Prenzlauer Allee, departs directly outside the main concourse of the terminal. The journey time is approx. 35 minutes. Travel to Spandauer Str./Marienkirche and cross the Karl-Liebknecht Strasse. Then proceed approx.150 m towards the Berliner Dom and turn right onto the embankment footpath just before the Spree. The main entrance of the SpreePalais am Dom is on the right-hand side just before the Anna-Louisa-Karsch Strasse, positioned slightly back from the road.

By air – Airport Schönefeld: The Spreepalais is approx. 23 km from Berlin-Schönefeld airport. Take the S-Bahn line 9, towards Spandau, from the S-Bahnhof at Berlin-Schönefeld airport. The journey time is approx. 45 minutes to Hackescher Markt station. Leave the station, going towards the Burgstraße/ Museumsinsel. At the Burgstraße go towards the cathedral,as far as the Anna-Louisa-Karsch Strasse, cross this street. The main entrance of the Spreepalais is 20 m along on the left-hand side.



Contacts

Conference Chair: Michael Friedewald (michael.friedewald@isi.fraunhofer.de)

Secretariat: Silke Just (silke.just@isi.fraunhofer.de)

Host Institution: Fraunhofer-Institute for Systems and Innovation Research, Breslauer Strasse 48, 76139 Karlsruhe, Germany. Telephone: +49.721.6809-146

Information: coordinator@prescient-project.eu

Fraunhofer
ISI

FRAUNHOFER INSTITUTE FOR SYSTEMS AND INNOVATION RESEARCH ISI

PRIVACY AND EMERGING SCIENCES AND TECHNOLOGIES

SUPPORTED BY

SEVENTH FRAMEWORK PROGRAMME

Science in Society

ORGANISED BY

Fraunhofer

Trilateral Research & Consulting

LSTS
LAW, SCIENCE, TECHNOLOGY & SOCIETY STUDIES

CSSC
Centre for Science, Society and Citizenship

INTERNATIONAL CONFERENCE OF THE PRESCIENT PROJECT

27–28 November 2012
Berlin, Germany

Contact
Dr. Michael Friedewald
Fraunhofer Institute for Systems and Innovation Research ISI
Breslauer Strasse 48 | 76139 Karlsruhe | Germany
Phone +49 721 6809-146 | Fax: +49 721 6809-315
michael.friedewald@isi.fraunhofer.de

Photo Credit | iStockphoto.com/TonisPan

Co-ordinator:
Dr. Michael Friedewald
Fraunhofer Institute for Systems and Innovation Research ISI
Breslauer Straße 48 | 76139 Karlsruhe | Germany
Phone: +49 721 6809-146 | Fax +49 721 6809-315
michael.friedewald@isi.fraunhofer.de

Fraunhofer
ISI