Abstract Booklet

Citizens' Perspectives on Surveillance, Security and Privacy: Controversies, Alternatives and Solutions

Joint Conference of SurPRISE, PRISMS and PACT
Austrian Academy of Sciences, Vienna
November 13th-14th, 2014

The PACT, PRISMS and SurPRISE projects have received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreements no. 285635, 285399 and 285492 respectively.

Citizens' Perspectives on Surveillance, Security and Privacy: Controversies, Alternatives and Solutions

Joint Final Conference of the SurPRISE, PRISMS and PACT Projects

Recent revelations of mass surveillance programmes clearly demonstrate the ever-increasing capabilities of surveillance technologies. The lack of serious reactions to these activities shows that the political will to implement them appears to be an unbroken trend. The resulting move into a surveillance society is, however, contested for many reasons. Are the resulting infringements of privacy and other human rights compatible with democratic societies? Is security necessarily dependent on surveillance? Are there alternative ways to frame security? Do surveillance technologies address the most pressing security needs, and if yes, are they the most efficient means to do so? Is it possible to gain in security by giving up civil liberties, or is it even necessary to do so? Do citizens adopt this trade-off and, if yes, are they willing to enter into this trade?

Three FP7 Security Research projects have addressed these and related questions, putting the perspective of European citizens in the very centre of the research focus. Major aims are to better understand the relationship between surveillance, security and privacy, to inform policymaking and to support decision making with the gained insights. The revelation of practically unlimited surveillance activities of the NSA by Snowden, the rejection of the Data Retention Directive by the European Court of Justice and the recently adopted Opinion on Ethics of Security and Surveillance Technologies by the European Group on Ethics (EGE) are unambiguous signals that such decisions are urgently needed.

Conference

This two-day conference is jointly organised by the EU FP7 research projects SurPRISE, PRISMS and PACT. The three projects aim at integrating the citizens' perspective into the investigation of controversial topics such as surveillance, security and privacy. Hence, this joint conference will offer a unique occasion to both present and discuss the results of the projects, but also to integrate them into a wider spectrum of social, academic and political debates. It will involve speakers from different scientific disciplines - social sciences, law, computer sciences, etc. – as well as practitioners – policy makers, NGOs, law enforcement officers, etc.

Organization

The conference is organized by the partners of the PACT, PRISMS, and SurPRISE projects:

PACT (Public Perception of Security and Privacy: Assessing Knowledge, Collecting Evidence, Translating Research into Action):
- VITAMIB, France
- ATOS Spain S.A., Spain
- Centre for Irish and European Security, Ireland
- Ipsos MORI, Belgium
- Center for Security Studies, Greece
- The Hebrew University of Jerusalem, Israel
- Demokritos, National Center of Scientific Research, Greece
- RAND Europe, United Kingdom
- Peace Research Institute Oslo, Norway
- University of Westminster, United Kingdom

PRISMS (The PRIvacy and Security MirrorS: Towards a European framework for integrated decision making):
- Fraunhofer Institute for Systems and Innovation Research ISI, Germany
- Trilateral Research & Consulting, United Kingdom
- Vrije Universiteit Brussel, Belgium
- TNO, The Netherlands
- University of Edinburgh, United Kingdom
- Eőtvős Károly Policy Institute, Hungary
- Hogeschool Zuyd, The Netherlands
- Ipsos MORI, United Kingdom

SurPRISE (Surveillance, Privacy and Security: A large scale participatory assessment of criteria and factors determining acceptability and acceptance of security technologies in Europe):
- Institute of Technology Assessment of the Austrian Academy of Sciences, Austria
- Agencia de Protección de Datos de la Comunidad de Madrid, Spain
- Instituto de Politicas y Bienes Publicos/Agencia Estatal Consejo Superior de Investigaciones Científicas, Spain
- The Danish Board of Technology, Denmark
- European University Institute, Italy
- Verein für Rechts-und Kriminalsoziologie, Austria
- Median Opinion and Market Research Limited Company, Hungary
- The Norwegian Board of Technology, Norway
- The Open University, United Kingdom
- TA-SWISS, Centre for Technology Assessment, Swiss Academies of Arts and Sciences, Switzerland
- Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein, Germany

Funding

The PACT, PRISMS and SurPRISE projects have received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreements no. 285635, 285399 and 285492 respectively.

Program Committee

Johann Čas	Austrian Academy of Sciences, Institute of Technology Assessment
Rocco Bellanova	Peace Research Institute Oslo
J. Peter Burgess	Peace Research Institute Oslo
Michael Friedewald	Fraunhofer ISI
Marc van Lieshout	TNO - Netherlands Organisation for Applied Scientific Research
Walter Peissl	Austrian Academy of Sciences, Institute of Technology Assessment

Table of Contents

Session 8: In search of alternative policy solutions

Citizens' Privacy Concerns: Does National Culture Matter?

Jelena Budak and Edo Rajh

Institute of Economics, Zagreb
Trg J. F. Kennedyja 7, 10000 Zagreb, Croatia
e-mail: {jbudak,erajh}@eizg.hr

This study is an integral part of a large research project aiming to develop a comprehensive integrated model of privacy concerns in the online environment and to empirically test it to provide deeper understanding of various interactions between antecedents, concerns and consequences of online privacy. The research objectives will initially be achieved by identifying and developing (i) a comprehensive list of antecedents such as demographic factors (e.g. gender, education), experience factors (e.g. internet use experience, web expertise) and social-psychological factors (values, attitudes, culture norms), and (ii) a comprehensive list of consequences of online privacy concern on individual-user level.

Within this wider research framework, our intuition is that the cultural characteristics of a society determine the level of privacy concern. Such soft indicators are often used in studies explaining individual set of values, working habits, and other behaviour patterns of individuals. However, it has not been observed if the cultural attributes of a nation shape citizens' perceptions on privacy related issues.

We will empirically test dimensions of national culture as antecedents of privacy concern. For this purpose we will construct an index of privacy concerns and national cultural dimensions indicators and examine their interrelations. Both set of indicators will be created using the data collected in two public surveys in Croatia. Testing the model on the Croatian population is seen as an appropriate way to empirically test the concept and interrelations, especially as it concerns a middle-developed EU country that constitutes a part of the digital society.

The privacy concern index will be obtained from survey data exploring public attitudes towards privacy and behaviour patterns when taking different roles and actions related to the privacy infringement, surveillance and data protection in Croatia (Budak et al., 2013).

Hofstede's (1980) seminal work points to the way in which certain national cultures determine the way in which businesses in different countries and parts of the world are organised and operate. Our empirical research will employ survey data collected in accordance with the Hofstede methodology on national cultural dimensions (http://geert-hofstede.com) at the large net sample of 1500 citizens. Indicators for defined five dimensions of national cultures (Power Distance, Individualism vs. Collectivism, Masculinity vs. Femininity, Uncertainty Avoidance and Long-Term Orientation) will be constructed. In the next step, national culture indicators will be compared to privacy concern index on a regional level.

Our empirical study will examine if (and which) national culture dimensions would impact the privacy concern, and therefore should be included in the set of socio-psychological factors in the extended model of privacy concern.

Academic literature recognizes privacy concern as a growing issue in the digital age, especially for new EU member states and post-transition countries. The impact of a rather traumatic transformation, marked by considerable distrust in institutions, speaks to a number of Hofstede's national cultural dimensions, notably regarding the distribution of power and resources, the balance between individualist and collectivist values, and the threat felt when facing uncertain or unknown situations. The research will contribute to the final definition of an integrated theoretical framework of online privacy concern. The additional project outcomes are policy implications and recommendations for regulatory control, internet users, policy and business strategies.

References

1. Budak, Jelena, Ivan-Damir Anić, and Edo Rajh, "Public attitudes towards privacy and surveillance in Croatia", Innovation: The European Journal of Social Science Research, Vol. 26, No. 1-2, 2013, pp. 100-118.
2. Hofstede, Geert, Culture's Consequences – Comparing Values, Behaviors, Institutions and Organizations Across Nations, Sage, Thousand Oaks, London, Neu Delhi, 1980.

About the authors

Dr. *Jelena Budak* is a Senior Research Fellow with the Institute of Economics, Zagreb. She had participated in research projects on various aspects of Croatia's accession to the EU, such as institutional convergence, public sector policies and regional development issues. Her research interests are institutions and applied institutional analysis, and most recent publications are in economics of corruption and privacy issues.

Dr. *Edo Rajh* is a Senior Research Fellow with the Institute of Economics Zagreb, Croatia, the Department for Industrial Economics, Innovations and Entrepreneurship. He received his PhD at the University of Zagreb, Faculty of Economics and Business. His primary research areas are consumer behaviour, market research methodology and measurement scales development. Recent publications are related to his work on the survey-based research projects.

Citizens' Perception on Surveillance, Security and Privacy: A Psychosocial Perspective*

María Del Carmen Hidalgo, Fernando Casado Castro, and Antonio Maña

University of Málaga, 29071 Málaga, Spain
e-mail: {mchidalgo,fcasado}@uma.es; amg@lcc.uma.es

Privacy, security and surveillance have become important elements in current societies. In the last years, security systems and video surveillance technologies have been widely adopted and have evolved, adapting to new infrastructures and ICTs. From a psychosocial point of view, it is necessary to know how individuals and the society can adapt to such changes.

Surveillance has started to expand in an international response to ensure the security of citizens. Security systems and video surveillance technologies are becoming increasingly prevalent in individuals' lives. These technologies provide effective tools for recognizing or verifying the identity and behavior of a person based on physical or behavioral characteristics.

On the other hand, many people are deeply concerned about the uncontrolled proliferation of surveillance systems. As surveillance systems expand their number, scope and capabilities, it becomes difficult for individuals to maintain their privacy. There are well-established psychological consequences to being watched, which have been observed consistently in many studies.

The PARIS project has the goal of developing mechanisms to ensure that surveillance systems are designed and developed to be respectful with privacy issues.

In this context, we have developed a study to analyse the citizens' acceptance of security and surveillance technologies and their relationship with privacy. The overall goal of this study is to serve as a basis for the development of a generic methodology to perform studies about the psychosocial perception of privacy in relation to surveillance in different environments, which in turn will be used by system designers to create privacy-respectful surveillance systems.

We have designed a questionnaire which includes the following variables: perception of security in the city and the neighbourhood, feelings when being observed by video surveillance technologies, desired levels of privacy and security by citizens at different places, acceptance level of the implementation of security and surveillance technologies and general attitudes toward security and surveillance technologies. The questionnaire was completed through an online survey.

102 people, 56% women and 44% men, from Malaga, Spain, participated in the study and answered the questionnaire. The average age is 33 years old.

The perception of security is quite high in Malaga. Most participants declare always feeling safe in their neighbourhood and in their city. We also found that most citizens feel comfortable and safe when being observed by

* This work was funded by the EC through the PARIS research project

surveillance technologies, and rarely nervous or angry. The only place where people clearly consider surveillance unacceptable is at home. Pearson's correlation analysis revealed a positive relationship between acceptance level of surveillance and desired levels of security in private spaces. We can see that there are some places where people wish high levels of privacy, security and surveillance (bank, hospital or schools). Likewise, there are other places such as supermarkets or streets where privacy is not so important. Finally, there are some places (e.g. home) where privacy and security are very important but surveillance is considered unacceptable. We also explored the acceptance of specific surveillance technologies. In general, we can see that the ones that receive higher acceptance are: the less invasive technologies; the ones most directly related with security; the best known and the most understood. In general, it appears that identification technologies are perceived as less privacy-threatening than technologies that relate to personal activities.

Regarding the acceptance of the deployment of security and surveillance technologies in relation to public safety, participants feel safer in a controlled environment with video surveillance technologies and security systems, but they think that it is desirable to establish a balance between citizens' privacy and surveillance technologies.

About the authors

María Del Carmen Hidalgo received her MSc in Psychology from the Universidad Autónoma of Madrid in 1990 and her PhD degree in Psychology from the University of La Laguna (Tenerife) in 1998. In 1996 she joined the Department of Social Psychology of the University of Málaga where she is currently Professor of Social Psychology. She has publications in national and international journals such as Anales de Psicología, Psyecology, The Journal of Environmental Psychology or Journal of Community Psychology. She has participated in several projects funded by the Ministry of Science and Technology and the Regional Government of Andalusia. She is reviewer of several international journals such as Journal of Environmental Psychology or Climate Policy and has participated in the organization of Conferences (e.g. VIII Conference on Social Psychology, XI Conference on Environmental Psychology). Her current research interest focus on Environmental Communication: which type of information is most efficient to make people awareness of environmental problems/to adopt environmental responsible behaviour; Volunteerism: Studying how to promote volunteerism, the physical, social and psychological benefits of being a volunteer; Place attachment/place identity: the affective bonds people establish with their place of residence: homes, neighbourhoods or cities. How these places can contribute to the wellbeing of citizens. Recently, she has joined a new research line: users' reactions to technology; how users perceive technology and devices, and how they affect them, especially, how to use these technological advances in IT for educating citizens in different aspects (quality of life, environment preservation, social behaviour, etc.).

Fernando Casado Castro has a degree in Communication Sciences (Journalism) and Master's degree in Social and Community Psychology from the University of Málaga. He is currently developing his PhD on the advertising as a tool in the fight against climate change. His current research interest focus on Environmental Communication, Environmental Psychology and Social Psychology of Security and Privacy. At present, he is working in a new research line: users' reactions to technology; how users perceive technology and devices, and how they affect them, especially, how to use these technological advances in IT for educating citizens in different aspects (quality of life, environment preservation, social behavior, etc.). Other aspects are focused on professional business communication, design, training and online environment.

Antonio Maña received his PhD degree in Computer Engineering from the University of Malaga, where he is currently Associate Professor of Software Engineering in the Computer Science Department. His current research activities include security and software engineering, information and network security, ubiquitous computing and ambient intelligence, application of smart cards to digital content commerce, software protection, DRM and mobile applications.

Citizens' Attitude and Preferences Regarding Privacy and Security*

Marc van Lieshout[1] and Michael Friedewald[2]

[1] TNO, Strategy and Policy Department; P.O. Box 155, 2600 AD Delft, The Netherlands
e-mail: marc.vanlieshout@tno.nl
[2] Fraunhofer Institute for Systems and Innovation Research ISI,
Breslauer Strasse 48, 76139 Karlsruhe, Germany
e-mail: michael.friedewald@isi.fraunhofer.de

The relationship between privacy and security has traditionally been seen as a trade-off, whereby any increase in security would inevitably curb the privacy enjoyed by the citizenry. The trade-off model has, however, been criticised, because it approaches privacy and security in abstract terms, and because it reduces public opinion to one specific attitude, which considers these technologies as useful in terms of security but potentially harmful in terms of privacy. This is especially important for decision makers in industry and politics who are often surprised about negative public reactions showing that citizens are not willing to sacrifice their privacy for a bit more potential security. Consequently the PRISMS projects is dealing with two central questions:

- Do people actually evaluate the introduction of new security technologies in terms of a trade-off between privacy and security?
- What are the main factors that affect public assessment of the security and privacy implications of a given security technology?

Addressing these questions is not simply a matter of gathering data from a public opinion survey, as such questions have intricate conceptual, methodological and empirical dimensions. Citizens are influenced by a multitude of factors. Privacy and security may be experienced differently in different political and socio-cultural contexts. Therefore PRISMS has not only conducted a survey of public opinion, but has also explored the relationship between privacy and security from different disciplinary perspectives (see the other PRISMS presentations at this conference).

The PRISMS project has approached the main questions by a large-scale survey among European citizens. Between February and June 2014 Ipsos MORI has conducted around 1 000 telephone interviews in each EU member states except Croatia (27 195 in total) amongst a representative sample (based on age, gender and work status) within each country.

The survey comprised questions exploring respondents' perceptions of privacy and security issues and values questions including political views, attitudes to rights and perceptions of technology. The core of the questionnaire, however, was a series of eight vignettes aimed to understand public opinion towards different privacy and security scenarios. The questions for each vignette included whether the practices described should be allowed; the impact

* This research has received funding from the European Union in the PRISMS project under grant agreement No. 285399

on people's rights and freedoms; and a series of specific statement questions about each vignette.

In our presentation we will focus on the analysis of the vignettes, exploring differences between general attitudes towards privacy and security and citizens' valuation of these values in concrete situations. We will show to what extend the type of security situation is affecting the degree people value privacy and security. Finally we will also cover differences between countries or clusters of countries.

About the authors

Marc van Lieshout MSc, is senior scientist at TNO. He is working within the TNO department Strategy & Policy on privacy and identity management issues, combining technological, user oriented and policy perspectives on privacy and identity management. He is the linking pin of TNO with the Privacy and Identity Lab, a knowledge centre of TNO with Dutch universities Tilburg and Nijmegen and Dutch organization SIDN (responsible for release of domain names). He has been acting as Programme Manager of TNO's programme on Societal impact of ICT in the period 2005–2012. He is vice-chair of IFIP Working Group 9.2 on Social Accountability. He has been visiting scientist at JRC-IPTS in 2008/09. He has been engaged in several international projects related to the assessment and evaluation of national and international activities related to privacy and data protection, for the European Commission, the European Parliament and national departments.

Michael Friedewald is a Senior Research Fellow at the Fraunhofer Institute for Systems and Innovation Research (ISI) in Karlsruhe, Germany, and heads the ICT research group. His recent work focuses on privacy and data protection challenges of future and emerging information and communication technologies. He is also working in the field of foresight and technology assessment. He has been co-ordinating several FP7 projects including PRESCIENT, SAPIENT and PRISMS. He is co-editor (together with R.J. Pohoryles) of *Privacy and Security in the Digital Age* (Routledge, 2014).

Involving Citizens in Security Policy Making*

Jacob Skjødt Nielsen[1] and Szénay Márta[2]

[1] Danish Board of Technology Foundation, Toldbodgade 12 1253 København K, Denmark
e-mail: jsn@tekno.dk
[2] Medián Opinion and Market Research, Szent István Krt. 23., 1055 Budapest, Hungary
e-mail: szenay@median.hu

The SurPRISE Decision Support System (DSS) was developed and used in the five citizen meetings integrating questionnaires and deliberative methodologies. The DSS guides a structured procedure making it possible to conduct comparable citizen meetings exploring laypeople's acceptance levels of Security Oriented Surveillance Technologies (SOSTs).

The DSS is based on a modified methodology of participatory activities in the large-scale events, but adjusted in order to explore citizens' concerns about security challenges in smaller participatory settings. The SurPRISE DSS produces a summary of the small-scale citizen meetings including the main points of the dialogue, results of individual and group votes and recommendations towards decision makers and politicians.

The citizen meetings involved about 30 participants per country divided into five groups each discussing a different SOST. The five groups in each country worked with security challenges and options that were selected for further investigation after completing the large-scale participatory events.

- Security
  - Perception of security
  - Main perceived security challenges
- Surveillance
  - Overall evaluation of surveillance based security technologies
  - Awareness of information collected by surveillance technologies
  - Effect of surveillance on everyday life
- Privacy and Data Protection
  - Perception of privacy and data protection
  - Effect of surveillance oriented security technologies on privacy
  - The inviolable core of privacy
- Regulation and Control
  - Awareness of the regulation and control
  - Information request
  - Involvement of citizens
  - Legal safeguards

In the second session, each group was assigned one of the following SOSTs: Deep Packet Inspection (DPI), CCTV, Drones, Biometrics, Smartphone Location Tracking (SLT). All groups then assessed the technologies using the following structure:

* This research has received funding from the European Union in the SurPRISE project under grant agreement No. 285492

- Main Positives and Negatives
- Effectiveness
- Intrusiveness
- Acceptability
- Security Agencies and Legal Safeguards
- Trade-off
- Alternatives

After the meetings, the results of all the small-scale meetings were analysed, and the main outcome of the deliberative processes was incorporated into the recommendations to the European Parliament.

About the authors

Jacob Skjødt Nielsen is Head of DBT Participation at the Danish Board of Technology Foundation. He holds a master degree in Social Science and History of Science and Technology from Roskilde University. Jacob has worked for DBT for 9 years and is well advised in numerous methods of Technology Assessment and participatory theory and practice. Jacob has managed projects in ICT, security, privacy and innovation. He was research coordinator of the FP7 security project DESSI and in charge of the development of multi criteria, deliberative TA tools. As partner in SurPRISE he coordinated citizen summits on European level and work with integration of ICT in TA.

Márta Szánay is a senior research executive at Medián Opinion and Market Research Institute, Hungary. She is M.A. in Economics and also holding an MBA diploma. She has been working in opinion and market research for more than 15 years. Previously she worked as statistical analyst for the Department of Social Statistics at the Hungarian Central Statistical Office. In addition to her strong background in quantitative research and statistics, she has extensive experiences in qualitative research methodologies. Currently, she leads a work package in project SurPRISE that involves the conduction of participatory research in five European countries.

Moving away from the Security-Privacy Trade-Off: The Use of the Test of Proportionality in Decision Support?

Bernadette Somody[1], Máté Dániel Szabó[2], and Iván Székely[1]

[1] Előtvős Károly Policy Institute, Ulászló utca 43, 1113 Budapest, Hungary
e-mail: somodyb@alkotmanyjog.hu;szekelyi@ceu.hu
[2] University of Miskolc, Department of Informational and Media Law,
3515 Miskolc-Egyetemváros, Hungary
e-mail: szabomat@szabomat.hu

The introduction of security measures often infringes the privacy of the people concerned, and the legitimacy of such measures are often presented as the result of an inevitable trade-off between the two fundamental claims, rights or interests. In the legal domain two traditions have evolved for handling such conflicts: balancing of fundamental rights in the US, and the test of proportionality in the EU. Although the two traditions have different argumentation and philosophical background, at the practical level both approaches result in similar outcomes in the practice of the courts. This practice has been reinforced by the globalizing trends of constitutional law, and this, implicitly, further strengthens the legitimacy of the security-privacy trade-off concept.

However, the test of proportionality, as an original European standard, contains several steps which are based on facts and require factual decisions, and only in its final phase provides room for balancing on a moral basis, thus for an implicit trade-off between fundamental rights and interests. The test contains four stages or sub-tests: the legitimate aim test, the suitability test, the necessity test, and, finally, the proportionality test in the narrow sense. Each stage has its own aspects and decision criteria, and only if the case passes the sub-test concerned, may the following sub-tests be conducted during the procedure. This characteristic of the test of proportionality makes it possible to take its methodology seriously and, stepping out of the legal domain, integrate it into security-related decision-making processes.

Since the original concept of the test of proportionality reflects the vertical relationship between the citizen and the state, its use in a decision-support environment necessitates the modifying of the order of steps and the emphasis laid on certain phases of the test. After providing a brief critical overview of the practice of the European Court of Human Rights in cases where the legitimate aim of restricting the right to respect for private life is the interest of national security, public safety or prevention of disorder or crime, showing that certain steps of the test are often taken as mere formalities, the authors develop a detailed list of questions adjusted to situations when decisions need to be made about the deploying, maintaining or developing of surveillance or other security technologies, and the use of such technologies may have an impact on the privacy of the affected people.

The whole procedure of such a test is illustrated on a complex flowchart, which contains all questions to be answered and the possible branching points

and additional steps resulting from the answers. The application of this methodology would significantly reduce the weight of trade-off-based argumentation in the decision-making process; furthermore, this methodology may set the course for strengthening the application of the test of proportionality in the legal domain, too.

References

1. Robert Alexy, *A Theory of Constitutional Rights*. Oxford University Press, 2002.
2. Aharon Barak, *Proportionality. Constitutional Rights and their Limitations*. Cambridge University Press, 2012.
3. Cohen-Eliya, Moshe; Porat, Iddo: American Balancing and German Proportionality: The Historical Origins. *International Journal of Constitutional Law*; Apr2010, Vol. 8 Issue 2, p. 263.
4. Čas, Johann et al., "Social and economic costs of surveillance", in David Wright and Reinhard Kreissl (eds.), *Surveillance in Europe*, Routledge.
5. Raab, Charles, "From balancing to steering: new directions for data protection", in Colin J. Bennett and Rebecca Grant (Eds.), V*isions of Privacy: Policy Choices for the Digital Age*, Toronto: University of Toronto Press, 1999, pp. 68-93.
6. Wright, David and Paul De Hert (eds.), *Privacy Impact Assessment*, Dordrecht: Springer, 2012.

About the authors

Dr. *Bernadette Somody*, constitutional lawyer, researcher at the Eotvos Karoly Policy Institute, senior lecturer at the Constitutional Law Department of ELTE University (Budapest). She is specialised in the mechanisms and methods of fundamental rights protection, obtained her PhD degree based on a thesis on ombudsman institutions.

Dr. *Máté Dániel Szabó* is a lawyer specializing in the protection of fundamental freedoms and informational rights. His main field of interest focuses on the constitutional borders of the rights for informational self-determination. Currently he works as the Director of Programs at Hungarian Civil Liberties Union, and as senior lecturer at University of Miskolc's Department of Informational and Media Law.

Dr. *Iván Székely*, social informatist, senior research fellow of the Open Society Archives at Central European University, associate professor at the Budapest University of Technology and Economics, and board member of the Eotvos Karoly Policy Institute. His research interests are focused on information autonomy, openness and secrecy, privacy, identity, memory and forgetting, and archivistics.

The PACT Decision Support Tool for Privacy, Ethics and Social Impact Assessment of Surveillance Technology Investments*

Dimitris Kyriazanos, Olga Segou, Anastassios Bravakis, and Stelios Thomopoulos

National Centre for Scientific Research "Demokritos", Institute of Informatics and Telecommunications, Patriarchou Grigoriou and Neapoleos Street, 15310, Aghia Paraskevi, Athens, Greece
email: {dkyri,osegou,abravakis,scat}@iit.demokritos.gr

The PACT Decision Support System (DSS) is a tool for assessing the impact of future security technology investments and deployments in terms of privacy, ethics, social acceptance and public perception. It aims at assisting the decision making process of experts through efficient visualisation and interaction powered by the software implementation of PACT's theoretical and empirical findings.

The PACT DSS is a core tangible output of PACT research activities and it implements as a software tool the Privacy Reference Framework for Security Technologies (PRFST) toolbox described in PACT deliverable D5.2. The PRFST methodology which is implemented in the DSS begins with the surveillance technology scenario and use case analysis, identifying in the process the assets to protect. As a next step, legal requirements as well as ethical and societal considerations (the latter being based on the PACT empirical results) are analysed and correlated in order to produce threat and impact assessment metrics. The metrics are then consulted in order to build relevant decision trees which will support the user in his/her decision making for the selected security investment.

The PACT DSS is context-specific and it is based on the three contexts specified in the PACT survey, namely the Travel, Healthcare and Internet contexts. However, the PACT DSS is modular and extensible, having the ability to integrate future empirical studies in other contexts, or enrich the existing contexts without overhead or need for extended offline time for the PACT DSS system. To achieve this, the tool is powered by an extensible data model and data management algorithms which can adapt the analytical and prediction DSS functionalities to new use cases and datasets.

PACT DSS aims at the following user-perspective success criteria:

1. Reduction of average decision process time (including collaboration with other users)
2. Improving decision specific context visibility and access to necessary knowledge for related security technologies decision making
3. Reduction of average time for compiling a privacy impact assessment report

* This research has received funding from the European Union in the PACT project under grant agreement No. 285635

4. Convenience and acceptance of the produced PACT impact assessment report
5. Usability and User friendliness
6. Cost effectiveness (value for money)

It should be clearly noted that the PACT DSS is not a legal instrument responsible for validating the legality of the user's decisions. The user is the expert responsible for taking decisions, and the PACT DSS is a convenient and user-friendly tool to help him reach to the decision faster and with a better view of associated parameters, knowledge and arguments.

It is important to highlight that the design of the PACT DSS is user-driven, and decisions are taken by the users themselves, with the system supporting the process through multiple modalities and presenting quantitative and qualitative information regarding the impact of each decision path.

References

1. Pérez, Jaime Martín, Adem Yasar Mulayim, Gulden Yilmaz, Sadhbh McCarthy, Daniel Deering, Dimitris Kyriazanos, Olga Segou, Stelios Thomopoulos, Elida Jacobsen, Rocco Bellanova, Prokopis Drogkaris, and Lilian Mitrou, "PACT Privacy Reference Framework for Security Technology", Deliverable 5.2, The PACT Project, 2014. http://www.projectpact.eu/deliverables/wp5-new-conceptualization-and-framework/d5.2

About the author

Dr Dimitris M. Kyriazanos holds a PhD Degree and a Dipl.-Ing. Degree in Electrical and Computer Eng. from National Technical University of Athens (NTUA), Greece. He is an experienced research associate, collaborating with the Integrated Systems Laboratory (ISL) and National Centre for Scientific Research "Demokritos" (NCSRD) since 2006, in charge of project and technical management, performing also lead Software Engineering in EU ICT, Security and AAL projects, including design and implementation of large scale integration systems. His PhD dissertation included innovations for safeguarding privacy in context aware personal communications systems. He is an experienced researcher in the area of Privacy by design, data protection, trust and ethics: FP6-IST-MAGNET BEYOND leader of the trust and privacy task, FP7-SEC-TASS Privacy & Ethics committee member, FP7-SEC-PACT (ongoing) Decision Support System Work Package Leader.

Dr. Olga E. Segou holds a joint PhD in Electrical and Computer Engineering (2014) from the NTUA and the NCSRD, under a fellowship granted by the Hellenic General Secretariat of Research and Technology and NCSRD (2009), and a Diploma of Electrical and Computer Engineering (Dipl.Eng.) from the University of Patras (2008). Since 2009, she has been employed as a Research Associate in ISL. Her research focuses on architecture design, performance estimation and privacy implications of Location Based Services and Pervasive Computing.

Anastassios Bravakis is a Research associate in the NCSRD for the ISL Laboratory. He received his degree in Digital Systems from the University of

Pireaus, department of Digital Systems. His current research activities include software engineering and database design, mobile applications and related infrastructure, and the applied security of such infrastructure.

Dr. Stelios C. A. Thomopoulos holds a Diploma in Electrical & Mechanical Engineering (NTUA) and M.S & Ph.D. degrees in Electrical & Computer Engineering (SUNYAB). He is the Director of the Institute of Informatics & Telecommunications (IIT) of NCSRD, Director of Research and Head of the ISL at NCSRD and has served also as Director of IIT from 1998-2003. He has served as a faculty with the Departments of Electrical Engineering of Penn State University and the Southern Illinois University. Dr. Thomopoulos is credited with over 200 publications in peer reviewed professional journals and conference proceedings, scientific chapters in 8 books, and over 1100 citations. He has been a consultant and advisor to the US Air Force Predetection Fusion Program, and the governments and private industry of USA, France and Greece. He holds patent US Patent No. 5,978,495 for the design and implementation of a fingerprint recognition system. Dr. Thomopoulos has led as Coordinator and/or Scientific Coordinator in over 47 European, US and nationally funded projects, including the EU flagship and award winning projects OPTITRANS (FP7-GALILEO-228382) and PERSEUS (http://www.perseus-fp7.eu/).

Privacy, Security and Surveillance Preferences of European Citizens: Overview of PACT's Empirical Findings*

Sunil Patil

RAND Europe, Cambridge, UK
e-mail: spatil@rand.org

This presentation is a high-level summary of empirical findings of a three year FP7 project 'Public Perception of Security and Privacy: Assessing Knowledge, Collecting Evidence, Translating Research into Action (PACT)'. The study includes analysis of stated preference data collected from over 26 000 respondents across 27 European Member States to inform our understanding of the perception of security, privacy, and surveillance. The study also explores links between these perceptions and socio-economic factors, which include age, gender, education, work status and income. The survey specifically explores three real-life settings: (a) travel on the rail/metro, (b) choosing an Internet service provider and (c) choice of a personal health-data device or service. The results show that preferences for security and privacy are context dependent and do vary across countries and individuals. The collected data further provide robust evidence base that brings the citizens' voice into the privacy vs. security debate and better informs public policy.

The results for travel, Internet and healthcare highlight how dependent preferences for privacy, security and surveillance are on context. Most respondents across the EU are found to prefer some level of data storage on CCTV cameras or on a health device; the preference for CCTV cameras also indicates a preference for surveillance. However, they dislike any storage of information on Internet usage or monitoring of their Internet activities by the police, except when there is a genuine need (a warrant having been issued by a judge/court). Indeed they prefer that their ISP offers some services to improve online privacy.

Respondents' attitudes significantly affect their preferences in relation to privacy, security and surveillance. For example, the more distrustful (to business, voting, government and technology) respondents are, the greater their concern for privacy.

Despite the different preferences between contexts, the results are quite consistent across the 27 EU Member States surveyed, although there are some country-specific effects. These particularly concern the presence of security personnel and security checks in the Travel context and viewing of data by different groups other than medical practitioners in the Health setting.

Socio-economic effects were also found to play a role. In terms of surveillance, older people (65+) are generally less averse to the presence of CCTV cameras or Internet surveillance and had stronger preferences for services to

* This research has received funding from the European Union in the PACT project under grant agreement No. 285635

improve online privacy. Younger people (18-24), on the other hand, are more open to storage of their Internet and health data, but are more averse to physical security checks.

Overall, the results indicate that respondents' preferences relating to security and privacy are much more nuanced than the simplistic inverse relationship between security and privacy that is often assumed; this is an important finding from a policy-making perspective.

About the author

Dr. Sunil Patil is an Analyst at RAND Europe's Cambridge office. His areas of expertise include discrete choice modelling and application of advanced statistical methods. He routinely uses a variety of quantitative methods to inform public policy issues in the UK and across Europe. He is currently the scientific lead for RAND Europe's contribution on a three year FP7 project 'Public Perception of Security and Privacy: Assessing Knowledge, Collecting Evidence, Translating Research into Action (PACT)'. Dr. Patil holds a Ph.D. in Civil Engineering from the Texas A&M University.

Framing Effects on the Acceptance of Surveillance-Oriented Security Technologies

Evelien De Pauw and Hans Vermeersch

VIVES University College, Kortrijk, Belgium
e-mail: {evelien.depauw,hans.vermeersch}@vives.be

Background: New surveillance-oriented security technologies are increasingly implemented in contemporary safety and security policy to address a wide range of reducing risks challenges, for example, as a means to prevent crime and to increase the capacity for rapid detection and response. Safety, security and privacy which are all highly valued in Western societies. As most of these technologies are relatively new, it is unclear if and how 'framing' these technologies as a crimefighting instrument or as a potential 'threat to privacy' may affect public acceptance of their use.

Goals: This study is a pilot-study, and a first step towards a larger study on privacy, fear of crime and the public acceptance of SOSTs. It addresses the questions (i) whether and to what degree the use of security and/or privacy frames affect public acceptance of these SOSTs (ii) whether these frames affects acceptance differently in individuals with low versus high generalized privacy conerns, fear of crime and 'knowledge and understanding about technology'.

Methods: Undergraduate students were asked to participate in a study, by means of an online survey. Participants (n=410) were randomly selected into one of the four 'arms' of the study, answering questions on 4 SOSTs (intelligent CCTV, behavioral profiling, RIFT, and DNA databanks) accompanied, respectively, with a security frame, a privacy frame, a mixed frame and a neutral frame. Additionally we measured for all participants socio-demografic variables (age, gender, socio-economic background) and theoretically important variables like fear of crime and privacy concerns. Average acceptance scores in the four arms of the experiment were compared. In addition data were analysed to assess whether framing interacted with individual's traits – such as fear of crime and privacy concern – to predict to predict acceptance of SOSTs.

Results and conclusions: Small effects of frames on acceptance of some SOST's were found, but not for all SOST's. Significant interaction effects were found indicating that the effects of frames depended largely on the individual's pre-existing attittudes and characteristics.

About the authors

Hans Vermeersch has a PhD in sociology and is a researcher at the research group 'Society and Safety' of the Centre of Social Innovation (Vives University College, Kortrijk)

Evelien De Pauw has a M.A. in Criminology and is a researcher at the research group 'Society and Safety' of the Centre of Social Innovation (Vives University College, Kortrijk)

Aligning Security and Privacy: En Route Towards Acceptable Surveillance*

Sara Degli Esposti[1], Vincenzo Pavone[2], and Elvira Santiago-Gómez[2]

[1] Open University, Centre for Research into Information Surveillance and Privacy (CRISP)
Walton Hall, Milton Keynes MK7 6AA, United Kingdom
e-mail:e-mail: s.degliesposti@open.ac.uk
[2] Spanish National Research Council (IPP-CSIC), C/Albasanz 26-28, Madrid 28037 (Spain)
e-mail: {vincenzo.pavone,elvira.santiago}@cchs.csic.es

When surveillance functionalities are embedded into security tools and systems the risk of facing a backlash, due to widespread privacy concerns, increases dramatically. Yet, at the time of deploying a new surveillance-based security measure, developers struggle to imagine end-users' reactions. To help fill in this gap, this study investigates key factors determining public acceptance of surveillance-orientated security technologies (SOSTs). By analysing quantitative data gathered in nine European countries as part of the FP7 SURPRISE project, the article provides sound evidence of the detrimental effects that a technology's perceived degree of intrusiveness exercises on its perceived effectiveness, and of the negative effects caused by the adoption of blanket-surveillance security strategies on end-users' perceptions.

The interplay between technological attributes, such as accuracy and effectiveness, and non-technological considerations related to system operators' level of competence and integrity, is also examined. Operators' trustworthiness seems to play a particularly important role in reducing SOSTs' perceived intrusiveness and young people's inclination to resist these measures. Furthermore, apprehension caused by the way the technology might evolve in the future contributes to raise privacy concerns, which increases the perception of intrusiveness, which in turn decreases public support. Public understanding of SOSTs contributes to diminish public acceptance, as it raises public awareness of SOSTs' perceived intrusiveness. These findings have been obtained by testing the same path analysis model on data gathered in six EU countries on three specific SOSTs, which are Smart CCTV, Deep Packet Inspection, and Smartphone Location Tracking. Despite the fact that each of these technologies has different characteristics and it is perceived differently across countries, results still hold.

Security solutions are meant to foster public safety both in objective terms, by reducing crime, and in subjective terms, by helping people feeling secure and protected. With this article we hope to contribute to the shift from the old privacy-security trade-off model, to the development of a new win-win security paradigm, where surveillance is minimised and privacy and security are perfectly aligned.

* This research has received funding from the European Union in the SurPRISE project under grant agreement No. 285492

About the authors

Sara Degli Esposti is Research Assistant for the Surprise project at the Centre for Research into Information Surveillance and Privacy (CRISP) at the Open University (UK). She is also a PhD candidate at the Open University where she has investigated organisational information security strategies and compliance with EU data protection principles in the era of big data (`www.bigdataprotection.co.uk`). Sara is Privacy-by-Design Ambassador and an active member of the International Association of Privacy Professionals (IAPP). She has a BSc in Sociology and a MSc in Business Economics and Quantitative Methods. For the Surprise project she has been in charge of testing hypotheses and analysing the quantitative data gathered in the large scale events.

Vincenzo Pavone is Permanent Research Fellow at the Institute of Public Policies of the High Research Council in Spain (CSIC), and member of the SPRI Research Group. With a background in Politics and International Relations, his current area of expertise is science and technology studies, and his research specifically addresses public engagement and public assessment of science and technology as well as the ethical, social and legal aspects of emerging technologies. He is especially interested in the relationship between neoliberal modes of knowledge production and the emergence of new bioeconomies. In the field of security, he has been recently working on the FP7 SURPRISE project, not only developing a theoretical model on the criteria and factors likely to affect acceptability of surveillance-oriented security technologies (SOSTs) but also elaborating an empirically informed study of the changes and implications of the shifting trajectory of the concept of security in the EU from the end of the Cold War to present days.

Elvira Santiago is Postdoctoral Research Assistant at the Institute of Public Policies of the High Research Council in Spain (CSIC). With a background in Sociology, her doctoral research was aimed at finding a collaborative model in decision-making in the field of maritime security. Specifically applying the mapping tool proposed by ANT methodology, she explored the links between the different actors in the controversy and the frames in the discourse of civil society, politicians and experts looking for acceptable solutions for refuge ports in Spain. Her current area of expertise is science and technology studies, and her research specifically addresses public engagement and public assessment of science and technology as well as new approaches for collaborative risk management S.XXI societies new approaches for collaborative risk management in S.XXI societies. In the field of security, she has been recently working on the FP7 SURPRISE project, developing a theoretical model on the criteria and factors likely to affect acceptability of surveillance-oriented security technologies (SOSTs); organizing participatory events with over 200 people in Spain to discuss in an informed way about SOSTs and also elaborating an empirically informed study of the changes and implications of the shifting trajectory of the concept of security in the EU and the specific controversies that have erupted in Europe regarding use of these technologies.

Assessing Security Technologies: A Methodology for Societal Impacts on Diverse Stakeholders

Gemma Galdon Clavell and Philippe Mamadou Frowd

Department of Sociology and Organizational Analysis,
Universitat de Barcelona,
Av. Diagonal 696, 08034 Barcelona, Spain
e-mail: gemma@eticasconsulting.com; p.frowd@gmail.com

The development of security and surveillance technologies produces externalities both positive and negative - but how can these be measured and how can impacts on different stakeholders - such as citizens - and their perspectives be taken into account? This paper proposes a four-part societal impact assessment (SIA) methodology for the assessment of security and surveillance technologies that is sensitive as much to the economic concerns of designers as to societal values and the perspectives of citizens. To make the case, the paper draws on ongoing research from FP7 project ABC4EU.

Societal impact assessment is the evaluation of the risks, externalities and consequences of technologies, policies, programs, and systems. As a result, it must account for a wide range of concerns and stakeholders. The paper?s first main contribution is to suggest a four-part approach to SIA that can help to assess security and surveillance technologies. This framework based on desirability, acceptability, ethics, and data management provides a means of operationalizing assessment of security technologies to anticipate and compare a range of economic, data and values impacts for various stakeholders.

The *desirability* of a project or technology refers to the very need for a solution, and can be achieved through clear problem definition, good project governance but also cost-benefit analysis. This paper proposes a methodology through which the costs and benefits, economic and beyond, of a security project or technology can be assessed. This methodology, though not always quantifying costs, is a key decision-making support for designers as well as a measure of the value of what is often a public good.

The role of *acceptability* builds on the assessment of the social and public value of a technology or project. Acceptability accounts for the crucial role of how citizens (but also staff such as engineers) consent to and perceive a technology. This accounts for context and helps to assess proportionality. Drawing on literature on technology acceptance as well as a focus group-based methodology, this paper shows the stakes of accounting for citizens? perspectives and provides a methodology for doing so.

Ethics relates to the values and moral standards guiding a project. These include fundamental rights, inclusivity, the notion of a social contract of state and citizen, as well as what vision of ?security? is sought by a project or technology. Although ethics is one of the most challenging factors to measure, this paper includes such concerns in a cost-benefit matrix and weights them appropriately.

While *data management* does refer to the legal framework of privacy and data protection, it also encompasses much broader considerations relating to individual control and consent, methods of anonymization, and how privacy issues can be designed into technologies and projects. In this framework, the definition of ?privacy? itself is nuanced, and the gap between law and technology justifies additional assessment and safeguards.

Using this methodology, the paper deploys this four-part framework in relation to the ABC4EU project, which seeks a harmonized automated border control solution for the EU in anticipation of entry-exit and registered traveller programs. This paper suggests ways that the SIA framework might assess or question elements of the project, such as the role of convenience justifications in shaping acceptability and consent, or the role of biometrics on ethics and data management. To conclude, the paper produces some specific recommendations based on these findings, and reflects on improvements to the SIA model itself.

About the author

Gemma Galdon Clavell, PhD, is a policy analyst working on surveillance, the social, legal and ethical impact of technology, smart cities, privacy, security policy, resilience and policing. She is a founding partner at Eticas Research & Consulting and a researcher at the Universitat de Barcelona's Sociology Department. She is currently involved in several EC-funded projects, including IRISS, RESPECT, SMART, GRAFFOLUTION and ABC4EU. 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, the relationship between privacy and technology, and smart cities. She is an op-ed columnist in the Spanish newspapers *El País* and *El Diario*.

Philippe M. Frowd is a Postdoctoral Researcher at Eticas Research & Consulting. He will complete his PhD in international relations in December 2014 at McMaster University, Hamilton, Ontario, Canada. He is currently working on the ABC4EU and GIFT FP7 projects and is primarily interested in issues at the interface of security, technology and privacy. His dissertation research examines the security professionals and knowledge politics involved in border security measures in West Africa. His research appears in *Security Dialogue* and *Millennium* and he has contributed to "Research Methods in Critical Security Studies" (2012) and "The State of Surveillance" (2012).

Overview of the PACT Privacy Reference Framework for Security Technology (PRFST)*

Jaime Martín Pérez

ATOS Research and Innovation, Madrid, Spain
e-mail: Jaime.martinp@atos.net

The Privacy Reference Framework for Security Technology PRFST is a framework, which attempts to describe in a comprehensive manner the following:

- The main cultural, social, ethical factors (which vary across national cultures and contexts of application) to be taken in consideration during the assessment of the security and privacy implications of given security technology,
- Trade-off and non-trade-off elements that affects public perception of security investments, and
- The role played by trust and concern in addressing public concern in this policy area.

The main objective of PRFST is to assist decision and policy makers to consider privacy and fundamental rights when they evaluate the pros and cons of specific security investments.

The framework covers the following six steps:

Step 1 – Analysis of the scenario/use case: This step focuses on defining the context that is particular to each specific case of the security system that is being designed, and for which technology security investments will be made. Depending on the requirements and the level of maturity of scenario analysis, an initial description for the particular scenario in the form of a high-level use case should be provided (i.e. a short description of the scenario and scope), following a convenient and familiar use case template.

Step 2 – Assets to protect: The identification of assets that given security technology investments or policies (particularly in the area of Freedom, Security and Justice) should protect is of paramount importance in the initial characterization phase. In this regard, privacy and data protection frameworks are not the only means by which one protects assets. Furthermore, these frameworks often cover and imply much more than 'just' privacy and data protection. As a general rule, all personal data should be considered an asset to protect. Apart from the general privacy and data protection frameworks, it is also necessary to take into account fundamental rights, including the right to human dignity, right to integrity, right to freedom of movement, etc

Step 3 – Assessment of technological solutions: To assess the strengths and weaknesses of selected technologies in the context of security and

* This research has received funding from the European Union in the PACT project under grant agreement No. 285635

impact on privacy, mapping of the technologies is required with regards to (i) potential for privacy intrusion, including all types of privacy, (ii) relation to the main Privacy Targets according to the European Data Protection Directive and (iii) listing main connected Privacy Risks.

Step 4 – Privacy Threat Index (PTI): The privacy threat index (PTI) will act as a tool for security developers to identify a (non-exhaustive) range of privacy threat scenarios associated with taking a particular security policy/measure decision. The PTI is intended to identify a list of the privacy threats that may arise from a security policy, and categorise them according to their potential impact on citizens. A potential negative impact on citizens' privacy can, as a result, lead to a potential economic cost from taking the security technology that caused that privacy impact. This step is designed to assist the policy and decision makers collect the necessary privacy threat information associated with the prospective technology. The PTI is characterised by the following three elements: threat, likelihood, and impact.

Step 5 – Identification of the controls to apply: When identifying controls to apply, the PRFST user should first of all check which controls are mandatory, according to national, European and international regulations. Besides mandatory controls, a good rule to keep in mind is (data) minimization: both from scratch (e.g. no unnecessary data are collected) and on-going (data are erased as soon as possible). This has several implications in terms of technical controls, and permits to prevent or reduce a wide array of data-related harms

Step 6 – Reporting, guidelines and recommendations: The final step of the PRFST concerns the reporting of the overall process, as well as the formulation of guidelines and recommendations for development and deployment of the chosen technology (if any). The exercise of reporting about each previous step of the PRFST process, as well as the decisions taken and their rationale, permits to acquire an overview of the on-going decision making process. Moreover, a step-by-step report offers the occasion to assess the solution finally identified and may provide new insights on its overall impact on a given setting. It can be used as background material for an eventual Privacy and Data Protection Impact Assessment or for a Surveillance Impact Assessment.

References

1. Crespo García, A.; Ituarte Aranda, N.; Quesada Pérez, I. et al. (2013). Report on the Definition and Design of the Privacy Reference Framework for Security Technology (PRFST). Deliverable 5.1. The PACT Project. http://www.projectpact.eu/deliverables/wp5-new-conceptualization-and-framework/d5.1/D5.1.pdf/view.
2. Martín Pérez, J.; Yasar Mulayim, A.; Yilmaz, G. et al. (2014). PACT Privacy Reference Framework for Security Technology. Deliverable 5.2. The PACT Project. http://www.projectpact.eu/deliverables/wp5-new-conceptualization-and-framework/d5.2.

About the author

Jaime Martín holds a Bsc degree in Computer Science Engineering from Deusto University, Spain. He is research project manager in Atos Research & Innovation (R&D arm of Atos). He has both strong managerial and technical skills which he has proven in several European projects in the Secure Identity Technologies Lab and the Homeland Security and Defence sector such as STORK 2.0, DRIVER, PACT, SEMIRAMIS and VALUESEC, focusing on privacy, crisis management, security means, eID, risk analysis and managing consortia teams across different countries within the scope of specs, architectures, development, integration, piloting, dissemination and explotation. Before joining Atos he worked for Telefonica R&D, mainly in telecommunications country-scale network management and B2C services. He has also experience in the banking area, where he worked for several years in B2B and B2C projects of the Royal Bank of Canada Dexia Investor Services.

Between Participation and Securitization? A Bottom-up Perspective on Urban Security

Matthias Leese and Peter Bescherer

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

Cities are dense spaces in which societal friction can be experienced in an unmediated fashion, and thus urban politics is a powerful magnifying glass for questions of security and surveillance. Cities have long been conceptualized as epitomes for programs of surveillance and dataveillance, for the privatization and hybridization of policing, and for the roll-out of new technologies (Abrahamsen et al., 2009; Coward, 2009). However, more recently, there have been calls for a re-appropriation of urban space (Harvey, 2008; Revol, 2014) that, among others, put forward the need to include citizens in security policies (Connolly and Steil, 2009).

Such a participatory account arguably incorporates multiple advantages: (1) the scale of the city is large enough to provide meaningful governmental power, but still small enough to enable participatory impacts; (2) participatory programs foster political legitimacy; and (3) policy makers can incorporate citizens' needs to match political programs and requirements, thus leading to improved efficacy and reduced costs. However, so the argument we put forward, this logic is a compelling yet dangerous one. Citizens' perceptions of insecurity have been shown to be subjective and detached from actual threats (Leese, 2013). While most people in fact appear to disapprove of large-scale surveillance programs, 'more' security in terms of increased policing or video surveillance is cherished. Thus, can participatory security politics actually catalyze processes of securitization that put ever more aspects of everyday life under a paradigm of emergency and exceptionalism (Wæver, 1995)?

Within the VERSS project, we conduct empirical research in two German cities (Stuttgart, Wuppertal) in order to catalogue which forms of citizens' movement with a scope on security can be encountered in the first place, and to analyze how their work unfolds in urban policies and beyond. Questions we seek to address in this context are: To which extent do citizens' movements exist dependent or independent of political incentives? To which extent do they resist and counter; or support and foster urban security politics? And where can participation be placed among the continuum between genuine democratic input and a political 'trap' that reduces discourse to presumably technical choices that need to be affirmed by the population?

References

1. Abrahamsen R, Hubert D and Williams M C (2009) Guest Editors' Introduction. Security Dialogue 40(4-5): 363-372.

2. Connolly J and Steil J (2009) Introduction: Finding Justice in the City. In Marcuse P, Connolly J, Novy J, Olivo I, Potter C & Steil J (eds.) Searching for the Just City: Debates in Urban Theory and Practice. Milton Park/London: Routledge, 1-16.
3. Coward M (2009) Network-Centric Violence, Critical Infrastructure and the Urbanization of Security. Security Dialogue 40(4-5): 399-418.
4. Harvey D (2008) The Right to the City. New Left Review 53: 23-40.
5. Leese M (2013) The Perceived Threat. Determinants and Consequences of Fear of Terrorism in Germany. In Flammini F, Setola R & Franceschetti G (eds.) Effective Surveillance for Homeland Security: Balancing Technology and Social Issues. London: Chapman and Hall, 71-86.
6. Revol C (2014) English-Speaking Reception of "Right to the City": Transpositions and Present Meaning. In Erdi-Lelandais G (ed.) Understanding the City: Henri Lefebvre and Urban Studies. Newcastle upon Tyne: Cambridge Scholars, 17-36.
7. Wæver O (1995) Securitization and Desecuritization. In Lipschutz R D (ed.) On Security. New York/Chichester: Columbia University Press, 46-86.

About the authors

Matthias Leese is a researcher at the International Centre for Ethics in the Sciences and Humanities (IZEW), University of Tübingen. His primary research interests lie in the fields of critical security studies, surveillance studies, STS and privacy/data protection, more recently with a focus on aviation security.

Dr. Peter Bescherer is a researcher at the International Centre for Ethics in the Sciences and Humanities (IZEW), University of Tübingen. He is member of a research group dealing with justice in the realm of urban (in)security. His research interests lie in the fields of critical theory of society, precariousness of employment relations, right-wing populism and social movements.

The Dangers of Boundless Surveillance in a Democratic Society

Georg Markus Kainz and Christian Jeitler

quintessenz – Verein zur Wiederherstellung der Bürgerrechte im Informationszeitalter
quartier21 / MQ, Museumsplatz 1 (Electric Avenue), A-1070 Wien, Austria
e-mail: {kainz,chris}@quintessenz.at

Surveillance is based on the false promises of salvation that freedom and safety would directly depend on each other, and that safety could be purchased with the loss of just a few civil liberties. An analysis of both the costs and the benefits indicates that monitoring results can be achieved only for a short term, but that the harm to society is permanent, and in addition different population groups are affected to different degrees

On the one hand there is the small number of those who can set it up. As holder of a ’Carte Blanche’ they are not subject to the risk of data retention, because storage and analysis is suppressed or prohibited. Even today, it is possible that lawyers influence the constructed virtual representation search engine giant of a person.

Similar achievements can be obtained by groups that are technically capable of minimizing their digital footprint and who are capable of maintaining their digital personality while staying under the radar. Even the data that should be collected as part of data retention can be manipulated with simple technical arrangements. Therefore the group of criminals, who should be unmasked by data retention were easily able to protect themselves. Precisely these aspects were crucial in the ECJ and VGH prohibition of data retention.

What remains is the great mass of those who have neither the resources nor the technical know-how to protect themselves. This group falls fully in the case of the surveillance state. The more obviously the control and its negative impact on each individual is the more pronounced are phenomena such as the "spiral of silence". In a society in which everyone has the feeling of living in a panopticon, in which each of his steps and thoughts are monitored this inevitably leads to defensive reactions.

Just as discussions about mandatory real names show, how low the European Charter of Human Rights with its fundamental rights are enshrined in this group. For numerous actors in the political arena the fundamental rights seem not to represent the basis of their community and therefore they seem not to be a measurement for their actions. But when these rules are only an abstract statement of intent, they can be sacrificed at any time for individuals’ interests and goals. It may not be the target of policy to constantly undermine the fundamental rights only to achieve a short-term economic success just because monitoring is usually associated with massive investment. Fundamental rights which form the basis of a democratic society cannot be sacrificed just to achieve singular interests or to discipline the discussion culture in cyberspace.

About the author

Mag. Georg Markus Kainz is the President of quintessenz – an NGO for the restoration of civil rights in the information age.

After studies at the Johns Hopkins University, Baltimore, USA and the University of Vienna he entered professional life at the Northwest Zeitung, Oldenburg. After the fall of the German wall he was delegated to the Märkische Allgemeine in Potsdam to build up the ad sales and advertising department. The Holtzbrinck Publishing Group appointed him to the Südkurier, Konstanz for designing, conceptualizing and establishing an IT infrastructure for the advertising department. With the arise of the internet he became responsible for the web presence of the newspapers of the group and in particular of the Tagesspiegel in Berlin. At the time the German Telekom started their internet branch he became responsible for the content business of T-Online.

Today CEO of an Austrian Internet Service Provider, with a focus on e-commerce and content distribution. Board member of the "Linuxwochen Austria" and President of "quintessenz", the event organizer of the "Austrian Big Brother Awards".

Legal and Social Aspects of Surveillance Technologies: CCTV in Greece*

Lilian Mitrou[1,2], Prokopios Drogkaris[2], and George Leventakis[2]

[1] Laboratory of Information and Communication Systems Security, Department of Information and Communication Systems Engineering, University of the Aegean, Samos, GR-83200, Greece
e-mail: L.mitrou@aegean.gr
[2] Center for Security Studies (KEMEA), Ministry of Public Order and Citizen Protection, P. Kanellopoulou str. 4, Athens, GR-10177, Greece
e-mail: p.drogkaris@kemea-research.gr; gleventakis@kemea.gr

Video surveillance in public and/or publicly accessible places is not exceptional any more, rather it is notably increased - becoming sometimes a "panacea" - to promptly deal with security concerns. CCTV (systems) seem(s) to be deployed and perceived more as ad hoc "safety and security tools" for "protection" and "crime prevention and enforcement" and less as a form of surveillance, i.e. as process of monitoring, collecting of information and systematic classification and social sorting.

Even if CCTV is becoming a part of everyday-life, it still interferes with personality, privacy and data protection rights that are embedded in the Greek Constitution (in Art. 5, 9 and 9A) and law. According to Greek legal theory and jurisprudence people enjoy also "privacy in public" and audio/image data are considered to be personal data, if they refer to identified or even identifiable persons. One the other side, security is, in general, accepted as a restriction to fundamental rights, despite the divergent views about its nature (individual good, public good or pre-condition of exercising other rights). The "right to security", does not have a distinct, self-existent ground in the Greek Constitution, but constitutes the resultant of the demand for the state to undertake positive obligations and actions for the protection of rights such right to life, ownership, personality etc.

Following the public controversy concerning the legal ground and the use of CCTV by police authorities a specific law (Art. 14 of Law 3917/11 as modified by Law 3994/11), has defined terms and conditions for deployment of CCTV for the protection of state security, public safety and security, prevention of crime and law enforcement. Video-surveillance by individuals and private bodies is regulated by a "Directive" issued by the Greek Data Protection Authority, which lays down legal and technical restrictions (limits of equipment, limitations, "privacy zones", notification requirements), the core elements of the provision being lawfulness, purpose specification and proportionality.

The maturity of CCTV technology, the wide availability of (cheap) CCTV or biometric/face recognition systems, and respectively their widespread use (also in the private sector and by private citizens) change slightly but steadily the social perception of what is acceptable or excessive in relation to security

* This research was performed with the financial support of EU Seventh Framework Programme for research, technological development and demonstration under PACT project No. 285635 and under P-REACT project No. 607881.

measures, while influencing inevitably the regulatory content of core principles such as the principle of proportionality. Public perception and acceptance of such systems is oriented mostly around the conflict-balance relation of security or/and living and movement without being monitored.

Research into public support for CCTV has produced mixed results with many studies finding widespread support for CCTV. Especially in an environment of economic and social crisis, when uncertainty is rising on multiple levels, the prevention and removal of risks has become a social and political expectation, if not imperative. Acceptance and/or tolerance of CCTV mirror risk perceptions and fears and the sense that "somebody has to look after you". In this environment CCTV systems manifest the state’s concern about security and its fight against crime.

On the other hand it is difficult to define a dominant perception, as in Greece there is a popular sensitivity and vigilance against any state monitoring and filling. Due to their historic experiences under dictatorships and authoritarian regimes and the respective lack of trust in state-public institutions many Greek citizens have reproduced a "negative surveillance culture". At the same time social analysis, surveys and media reports confirm a "Greek surveillance paradox": While there is mistrust towards even legitimate "institutional surveillance" (Lianos, 2012), Greeks are generally unconcerned with non-state, private video surveillance and data collection. A position that is to be understood in the light of "privacy paradox": Collecting and aggregation of information by private parties "fits well into a society where most things are marketable" (G. Marx, 2013) and people are inclined to expose their life and activities to social media and leave data traces by every electronic interaction. However, we should consider that information gained through privately deployed CCTV systems can also be placed at the disposal of the State, which may result in systematic data sharing between the public and the private sector such as in the case of communication data retention.

References

1. Lianos, Michalis, The New Social Control: The Institutional Web, Normativity and the Social Bond, Red Quill Books, Ottawa, 2012.
2. Marx, Gary T., "The Public as Partner? Technology Can Make Us Auxiliaries as Well as Vigilantes", IEEE Security and Privacy, Vol. 11, No. 5, 2013, pp. 56-61.

About the authors

Dr. Lilian Mitrou is Associate Professor at the University of the Aegean-Greece She has served as a Member of the Hellenic Data Protection Authority (1999-2003). From 1999 till 2001 she was representative of the Hellenic Data Protection Authority at the Art. 29 Data Protection Working Group and from 2001-2004 national representative in the EC- Committee on the Protection of Individuals with regard to the Processing of Personal Data. She has served as Advisor to the former Prime Minister K. Simitis in sectors of Information Society

and Public Administration (1996 - 2004). She served and still serves as member of many Committees working on law proposals in the fields of privacy and data protection, communications law, e-government etc. Since January 2014 she serves as Chair of DAPIX (Working Group on Information Exchange and Data Protection). Her professional experience includes senior consulting and researcher positions in a number of private and public institutions on national and international level.

Dr. Prokopios Drogkaris has extensive research experience in areas pertaining Privacy Enhancing Technologies (PET), Digital Authentication, Public Key Infrastructures (PKI) and Federated Identities Management and is currently a teaching assistant at Postgraduate Programme in Techno-economic Management & Security at University of Piraeus, Greece. He is an author of several scientific publications and has served as a member on program and organizing committees at several scientific International and European conferences. As a researcher he has been involved in more than 10 National and EU funded research programmes and studies in the greater area of Information Security, Legal and Ethical issues management.

Dr. George Leventakis is Senior Advisor in European Programmes, former member to the BoD of European Organization for Security (EOS) and member to the European Research and Innovation Forum (ESRIF). He is a qualified Security Expert with more than 18 years of experience in Security Management. His key professional experience include, Civil Protection / Homeland Security technology & operations, Expert Security Systems including Command & Decision Support, physical security, command centre systems & port security systems across two Organizing Committees of Olympic Games for a duration of 6 years (SYDNEY 2000 and ATHENS 2004) and five years in the Hellenic Ministry Of Public Order. Since 2006 he is responsible (technical coordinator) for KEMEA'S participation in the various European Funding Programmes of the European Commission.

Privacy and Security Through Technical Solutions and their Regulation: Will the Law of the Future be Written in Code?

Florian Idelberger

European University Institute, Florence, Italy
e-mail: florian.idelberger@eui.eu

Due to the developments in the privacy and security world in the last two years (for example major security and privacy breaches and confirmation of mass surveillance campaigns) the incentive for the development of new and improved decentralized networking systems increased massively.

These systems have in common that they try to establish the next generation of networking technology, using the current infrastructure to create a technology that goes beyond what we have today by being private and secure by design.

Instead of traditional institutions it relies on itself to provide agreements ('soft law') and adequate governance. A great influence on the development of these new technologies was certainly the steady development and growth of bitcoin, which proved that even things that no one ever thought of before can still be improved or 'disrupted' by the digital world. This applies even more to more recent contenders. These are all systems that focus very much on 'privacy (or security) by design' as discussed in SURPRISE deliverable D 3.1 (Schlehahn et al. 2013) so that it becomes impossible or as good as impossible to spy on communication or storage or control a distributed application or company.

Where SURPRISE deliverable D3.4 (Kreissl et al. 2013) tries to find a new approach to reconcile privacy and security, many new systems currently under development go a different direction by inherently focusing on privacy and security, relying on code as law both for digital 'contracts' between virtual and natural entities and for self-governance. Thus, there is a strong technical drift towards much increased privacy and security, or at least that is the goal of these projects. Qabel for example focuses on communication, Maidsafe focuses on storage and Ethereum for the time being focuses on 'contracts' and autonomous, decentralized programs that tie everything together.

What all these systems have in common is that they are enabling users to create a system where parts of the internet and of society that were so far unable to lose their ties to the 'real world' become much more decentralized and independent than ever before. Ideally, these projects try to create networks where not only storage and communication, but also the algorithms that run the systems are distributed among all users.

The goal is that this could lead to applications that are much more sophisticated in their decentralization, privacy and security than ever before, which then could be the basis for the next generation of online banking, digital asset management (smart property) or contracts and digital autonomous

organizations (smart law). This will pose new challenges for regulators, legal professionals and society. Assuming an inability for international governments to agree on comprehensive regulation, the technologies in development are designed to work according to the rules of their code and the code of the 'contracts' and autonomous organizations that are established on them. This paper tries to show where conflict between the new technologies and regulators might arise, gives them a place in the current regulation and the research of SURPRISE and aims to provide an outlook towards the future of privacy, security and technology enabled governance and law.

References

1. Kreissl, Reinhard, Regina Berglez, Maria Grazia Procedda, Martin Scheinin, Matthias Vermeulen, and Eva Schlehahn, "Exploring the Challenges - Synthesis Report", Deliverable 3.4, The SurPRISE Project, 2013. http://surprise-project.eu/wp-content/uploads/2013/06/SurPRISE-D3.4-Exploring-the-Challenges-Synthesis-Report.pdf
2. Schlehahn, Eva, Marit Hansen, Jaro Sterbik-Lamina, and Javier Sempere Samaniego, "Report on surveillance technology and privacy enhancing design", Deliverable 3.1, The SurPRISE Project, 2013. http://surprise-project.eu/wp-content/uploads/2013/06/SurPRISE-D3.1-Report-on-surveillance-technology-and-privacy-enhancing-design.pdf

About the author

Florian Idelberger, LL.M is currently a Researcher at the European University Institute (EUI) in Florence, Italy, working on the fringe between law and technology. Previously he studied at Maastricht University for his LL.B in European Law with a thesis about the contemporary prospect of a European Cartel Office and at Lund University for an LL.M in European Business Law with a thesis about the concept of interoperability in EU competition law and EU intellectual property law. He is a contributor to the German Institute for legal issues in free and open source software (ifrOSS), participated in research pertaining to Contributor Licensing Agreements (`contributoragreements.org`) and in early years considered a career in computer science.

Judging Public Perceptions of Privacy: Should Law Actually Care about what People Think?*

Gloria González Fuster

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

This presentation discusses the legal significance of public perceptions of privacy, questioning the role that people's attitudes towards privacy and personal data protection shall play in the effective legal upholding of those rights– if any. To do so, it reviews different paths through which law can integrate and/or actively disregard public opinions on what deserves to be protected as private or as personal. It starts by reminding us that human rights and fundamental rights target the protection of individuals in general, and thus also of those with potentially extra-ordinary, or a-normal privacy concerns. It then describes the general limitations to the possible waiver of rights, and the relevance of these limitations in the context of the rights to privacy and personal data protection. Against this background, it analyses how public's attitudes might surface in the judicial construction of the scope of those rights, as well as the way in which the Court of Justice of the European Union has refused to reduce its conception of individuals to any pictures sketched out by statistical data. Finally, it considers the peculiar role of consent in European personal data protection laws, giving particular attention to how the sum of individual consent decisions might problematically be forced to account for a general acceptance of some data protection practices, notably through controversial appraisals of the economic value of personal data.

About the author

Gloria González Fuster is a senior researcher at the Law, Science, Technology and Society (LSTS) Research Group of the Vrije Universiteit Brussel (VUB). Author of a monograph on the emergence of the right to the protection of personal data as a fundamental right of the European Union, she has carried out extensive research on privacy and personal data protection law. Before joining the *Privacy and Security Mirrors* (PRISMS) project she had notably contributed to *Reflexive Governance in the Public Interest* (REFGOV) and *Converging and conflicting ethical values in the internal/external security in continuum in Europe* (INEX). She is also member of several advisory boards, including the Advisory Panel accompanying the *Surveillance, Privacy and Security: A large scale participatory assessment of criteria and factors determining acceptability and acceptance of security technologies in Europe* (SURPRISE) project.

* This research has received funding from the European Union in the PRISMS project under grant agreement No. 285399

Can Dynamic Groups be Protected under the Data Protection Regulation?

Dara Hallinan

Fraunhofer Institute for Systems and Innovation Research ISI
Breslauer Strasse 48, 76139 Karlsruhe, Germany
e-mail: dara.hallinan@isi.fraunhofer.de

Data processing can take as its primary focus, rather than individuals, groups of individuals. Such data processing may have an effect on those groups, but may also have an effect on the individual members of those groups.

It has been long established that individuals have rights impacted when their 'personal data' are processed. However, groups have also been considered to have rights – even privacy rights. If groups can hold rights, then surely these rights could also be impacted by the processing of data relating to these groups.

There have been a number of types of groups which have been traditionally recognised in European law – corporate groups and collections of individuals. These groups have tended to be made up of clearly definable collections of individuals who shared a specific, lasting, characteristic, or goal. Furthermore, the individuals in such groups were likely aware of their membership of the group and the identities of other members – allowing communication and collaboration. Data processing operations, however, may create groups with very different characteristics. Individuals may not be aware of their membership in such groups, the other members of the group, or the characteristic/s they have been grouped around. Furthermore, the groups may be highly dynamic – criteria for group membership may be subject to change on a rapid basis, as, thus, are the members of the group. As data protection law is the area of law aiming to protect rights at risk when data are processed, we might ask what possibilities the Regulation offers in protecting rights impacted by processing activities based on such dynamic groups. This contribution seeks to consider the possibilities which exist in the Regulation for the protection of such dynamic groups.

On the one hand, there seems facility to extend certain protection mechanisms – such as prior checking, procedural, organisational and technical mechanisms. On the other hand, however, the Regulation completely excludes the possibility to include such dynamic groups as rights holders. Indeed, such an exclusion seems quite justified and could not easily be remedied under current law.

About the author

Dara Hallinan, studied law with German law at the University of Birmingham and human rights and democratization at the European Inter-University Centre and at the University of Tartu. He has worked at Fraunhofer Institute for

Systems and Innovation Research ISI since 2011 on a number of projects investigating the interaction between ICT and society, including SAPIENT, PRESCIENT and IRISS. He is a doctoral candidate at the Vrije Universiteit Brussel, focusing on the relationship between data protection law and the use of genetic data in medical research.

Citizens' Recommendations on Law and Privacy at the SurPRISE Summits: A Litmus Test for Current Policy Initiatives?*

Maria Grazia Porcedda

European University Institute, Department of Law,
Villa Schifanoia, Via Boccaccio 121, 50133 Florence, Italy
e-mail: Maria.Porcedda@EUI.eu

The presentation will introduce the foundations of the SurPRISE legal recommendations based on the theoretical (WP3 'exploring the challenge'), empirical (WP 5 'participatory data gathering' and WP7 'decision support testing') and analytical (WP6 'analysis and synthesis') phases completed in the SurPRISE project.

The SurPRISE project challenges the so-called trade-off, whereby greater security can allegedly only be achieved based on the sacrifice of the rights to respect for private and family life and the protection of personal data.

SurPRISE investigates alternatives that can engender a positive-sum relationship between security and privacy. To do so, it has complemented legal and sociological (WP3), as well as political science (WP2) research with a deliberative methodology that involved 2000 European citizens by means of 12 large-scale participatory events ('citizen summits', WP5) and 5 small-scale ones ('citizen meetings', WP7). The goal of these events was twofold. First, to understand if and under what circumstances citizens are prepared to accept policies and the use of technologies that intrude into their fundamental right to privacy for the sake of increased security, thus effecting surveillance. Second, to advise possible solutions to what they saw as the most pressing issues concerning security, privacy and surveillance.

Citizens' recommendations converge in part with scholarship's theoretical findings. Based on such fruitful exchanges, we are elaborating a set of legal recommendations to concerned stakeholders: policy-makers, technology developers, data protection authorities, law enforcement authorities and civil society organizations.

Citizens' active engagement in the events shows that it is possible to submit complex policy issues, not least legal ones, to the general public by committing reasonable resources. While citizens were not consulted directly about current policy initiatives, some of their contributions provide striking insight into proposed measures, an insight worth exploring. The enthusiastic drafting of recommendations also suggests that direct consultation may prove useful in the face of problematic choices.

* This research has received funding from the European Union in the SurPRISE project under grant agreement No. 285492

About the author

Maria Grazia Porcedda is a researcher at the European University Institute, where she works for the projects SurPRISE and SURVEILLE (co-funded by the EU's FP7), on surveillance, privacy and security. Within the SurPRISE EUI team, Maria Grazia has been responsible for the legal research and the organization of both the Italian large-scale participatory event and the Experts Workshop. Maria Grazia is also a PhD candidate working on the relationship between cybersecurity and data protection. Maria Grazia previously worked at the Centre de Recherche Informatique et Droit (CRID), University of Namur. She was also a trainee within the privacy and information security unit at the Organization for Economic Cooperation and Development (OECD, Paris) and the European Data Protection Supervisor (EDPS, Brussels). She holds an LL.M. from the European University Institute, an M.A. in International Relations from the University of Bologna – where she was a member of Collegio Superiore (honours degree) – and a B.A. in Political Science from the University of Cagliari. She is a member of the Italian Information Security Association (CLUSIT).

Beyond the Trade-off between Privacy and Security? Individual Strategies at the Security Check*

Francesca Menichelli

Vrije Universiteit Brussel (VUB), Research Group on Law Science Technology & Society (LSTS), Pleinlaan 2, 1050 Brussels, Belgium
e-mail: francesca.menichelli@vub.ac.be

This presentation discusses the strategies developed by frequent flyers when going through security checks at the airport, and frames them within the wider remit of PRISMS. It is part of the work carried out at VUB for the criminological work package of that project and is based on research conducted on-site at Brussels airport, comprising interviews with passengers, non-participant observations at the barriers, interviews with screeners and airport management, in conjunction with the analysis of relevant legislation. The research sought to investigate how people experience security checks, in which terms they understand their participation to the screening process and how they relate to screeners; in turn, this helped to shed light on the notions of security and privacy that people practically develop while they are at the airport and, crucially, on the thresholds of acceptability that they use to draw the line for their involvement in security control.

The first part of the presentation will detail the themes that emerged in the course of the interviews with passengers, using quotes to show how a tension exists in how passengers understand security checks. While interviewees agreed that security checks are necessary, reservations were raised on a number of issues, particularly in terms of the accuracy of security controls and the unbalanced nature of the interaction between screeners and passenger. The second part will critically examine these findings, to try to understand how security procedures have become normalised over time, yet are problematized on two different levels; individually, in terms of the discomfort and anxiety they raise in passengers, collectively, because of their opacity and perceived arbitrariness. Finally, the presentation will discuss whether the data support or challenge the notion of a trade off between privacy and security, and will then conclude with some policy recommendation.

About the author

Francesca Menichelli is a postdoctoral researcher at the Faculty of Law and Criminology of the Vrije Universiteit Brussel, where she is part of the research team working on the FP7 project PRISMS - Privacy and Security Mirrors. She obtained a PhD in urban studies from the university of Milano-Bicocca

* This research has received funding from the European Union in the PRISMS project under grant agreement No. 285399

in May 2012 after carrying out research on police-run open-street CCTV systems in Italy. Before joining VUB, she worked as a research fellow for the regional government of Umbria, where she conducted research on cultural industries, equal opportunities in the workplace and youth, and spent a year at the Surveillance Studies Centre, based at Queen's University in Canada.

She has published on the use of urban security as a discursive device for the reconfiguration of sovereignty in Italy and on the role surveillance cameras play within wider strategies for the control of urban space. She is interested in mechanisms of social control, urban regulatory regimes and models of governance, policing and comparative research and she draws her theoretical references from political sociology and political geography, surveillance studies and science and technology studies.

The Deployment of Drones Technology in Border Surveillance and the Challenges to Privacy

Luisa Marin

University of Twente, Institute of Innovation and Governance Studies, Enschede, The Netherlands
e-mail: l.marin@utwente.nl

This paper focuses on the deployment of drones-technology (DT) in border surveillance and aims at assessing its perception and impact on privacy.

In the last years, we have witnessed and we are witnessing the deployment of all sorts of technological equipment in the different policies of the AFSJ. SIS, VIS, EURODAC, and most recently, ABC (Automated Border Controls), Smart Borders (EES and RTP), EUROSUR. The literature has captured these developments with images of the EU as dominated by "greedy information technology" (Besters), or, looking at the impact of those surveillance systems, cyber-fortress Europe (Guild) and high-tech fortress Europe (Marin). The deployment of DT in the domain of border surveillance seems part of a never-ending process, where the focus lies on using all the technologies available, in order to 'defend' borders from the 'threat' represented by migration, without an open public debate on the desirability, costs and benefits.

The paper focusses on the deployment of UAV (Unmanned Aerial Vehicles) or RPAS (Remotely Piloted Aircraft Systems), simply known as drones, in the context of border surveillance. After introducing the background of the paper (1), the article will first present the recent developments in border surveillance, namely EUROSUR and the shift toward intelligence it represents (2). In this context, it will examine (3) also the recent debate on the deployment of drones in border surveillance operations, a context pioneered by the US since 2004. In the EU, drones have been used during the Italian-led Mare Nostrum operation (4). The analysis of the current practices aims, first, at providing ethnographic information on the deployment of drones in practice and, second, at elaborating on the impact on privacy of DT. Which challenges for privacy arise from the current regulation on surveillance at the borders? how will the practices and policies change thanks to the deployment of DT in border surveillance? (5) The paper concludes by commenting on security and privacy in the context of border surveillance.

References

1. Besters, Michiel, and Frans Brom, "'Greedy' Information Technology: The Digitalization of the European Policy.", *European Journal of Migration and Law*, Vol. 12, No. 4, 2010, pp. 455-470.
2. Guild, Elspeth, Sergio Carrera, and Florian Geyer, "The Commission's New Border Package: Does It Take Us One Step Closer to a 'Cyber Fortress Europe'?", CEPS Policy Brief No. 154, 2008. http://www.ceps.eu
3. Marin, Luisa, "Is Europe Turning into a 'Technological Fortress'? Innovation and Technology for the Management of EU's External Borders: Reflections on Frontex and Eurosur", in Michiel A. Heldeweg, and Evisa Kica (eds.), *Regulating Technological Innovation: A Multidisciplinary Approach*, Palgrave Macmillan, London, 2011, pp. 131-151.

About the author

Dr. Luisa Marin is Assistant Professor of European Law at the University of Twente, School of Management and Governance. Formerly she has been a post-doctoral researcher and lecturer at the University of Helsinki and, previously, at the University of Verona, where she also defended her PhD on the principle of mutual recognition in criminal matters, as implemented in the European Arrest Warrant. Luisa teaches EU law at both undergraduate and Master level. Her research interests cover several policies of the Area of Freedom, Security and Justice, from judicial cooperation in criminal matters, to irregular migration and border surveillance. In this context she is looking at the deployment of technologies, such as UAVs, and their impact on the policies. She has co-edited a book and published a number of articles and book chapters on the European Arrest Warrant, and its impact on fundamental rights, and, on border surveillance and Frontex, UAVs. She is also a member of the Meijers Standing Committee, a network of independent experts, in the areas of international law, migration law, criminal law.

Digital Citizenship after Snowden: Self-Regulation and the Need for Critical Education Strategies

Dimitris Tsapogas

University of Vienna, Department of Political Science, Universitätsstrasse 7, 1010 Vienna, Austria
e-amil:dimitrios.tsapogas@univie.ac.at

An explosion of new Information and Communication Technologies (ICTs) has transformed the way in which people have access to information, communicate with each other, and engage civically and politically. A growing body of commentators suggests that there is indeed an emergence of new, online forms of political communication and participation. New ICTs have been claimed to revolutionise the way political activists, groups and organisations mobilise, protest and recruit, to bring the ability to bypass the established mediated channels of the public sphere and, in generally, to support the creation of new democratic spaces and processes that did not exist before. On the other hand, critics claim that these new technological affordances cannot radically modify the existing patterns of political communication, participation and governance, but instead, may even increase the gap of participation between the advantaged and disadvantaged parts of the population. Most importantly, there is the concern that ICTs may potentially harm democratic structures and processes by providing even more power of social control and repression over those who are dominated and discriminated, by using for instance, sophisticated means of electronic surveillance, propaganda, Internet filtering, data-mining and profiling.

Due to the work of researchers, journalists, hactivists, advocacy groups and individual leakers, the latter argument seems to be gaining significant substance. For instance, Edward Snowden, an American former intelligence agency member, with the collaboration of the *Guardian*, the *Washington Post*, *Der Spiegel* and a number of other media outlets revealed – and most importantly attested – the extent of the American, British and other intelligence agencies surveillance activities. These activities include mass online, mobile and landline telephone surveillance, covering nearly all-possible communicative transactions.

Such stories around contemporary surveillance practices are being covered by different kinds of mainstream and alternative media and play a significant role in modifying citizens' level of awareness, understanding and perceptions around privacy, data protection, security and surveillance (Coleman and Sim, 2000; Doyle, 2003; Nellis, 2007). One of the main concerns here is that surveillance may influence negatively important societal values, as individual freedom, autonomy, privacy, solidarity, equality, trust and the rule of law. These values are of paramount importance for the structure of democracy and the support of key democratic processes, such as the creation of associations, political interests, constructive and alternative ideas and the raising of

criticism (Habermas 1989; Solove 2007; Mitrou 2008; Haggerty and Samatas 2010). Surveillance is, thus, becoming damaging to (digital) citizenship.

The broader question this paper seeks to answer is how and to what extend do electronic state surveillance perceptions modify citizens' willingness and behaviour in the context of electronic participation. The country of Greece was used as a case study and all empirical data was acquired from respondents who lived there in late 2013. Due to the complexity of the central problem, a mixed-method was designed and operationalised, which collected both quantitative and qualitative data through a survey on the one hand, and a series of semi-structured interviews and focus groups on the other, with experts, academics, members of the police cybercrime unit, IT managers, activists, university students and citizens with different positioning upon the political spectrum.

The empirical data reveal that citizens are developing various self-regulation strategies with self-censorship and apathy occupying the two different ends of the spectrum of attitudes towards state surveillance. In addition, this process is influenced by a number of factors such as political education, regime type, quality of democracy, personal ideology, and knowledge/perceptions regarding the legal framework, surveillance and ICTs technologies. The findings also suggest that the simple raising of citizens' awareness regarding electronic surveillance developments – as with the case of Snowden's revelations – do not necessarily translate to individual cyber security mobilisation. The paper concludes by suggesting that new, critical education strategies need to be created that will empower citizens and key stakeholders of the relationship between state surveillance and (digital) citizenship.

References

1. Coleman, R. and J. Sim (2000) "You'll Never Walk Alone: CCTV Surveillance, Order and Neo-Liberal Rule in Liverpool City Centre", *British Journal of Sociology*, 51(4): 623-639.
2. Doyle, A. (2003) *Arresting Images: Crime and Policing in Front of the Television Camera*, Toronto: University of Toronto Press.
3. Habermas, J. (1989 [1962]) *The Structural Transformation of the Public Sphere: An Inquiry Into a Category of Bourgeois Society*, Burger, T. and Lawrence F. (Trans.), Cambridge, MA: The MIT Press.
4. Haggerty, K. D. & Samatas, M. (2010) "Surveillance and Democracy: An Unsettled relationship", in K.D. Haggerty and M. Samatas (Eds.) *Democracy and Surveillance*, New York, NY: Routledge, pp. 1-16.
5. Mitrou, L. (2008) "A Pandora's box for rights and liberties", in A. Acquisti, S. De Capitani di Vimercati, S. Gritzalis and C. Labrinoudakis (Eds.) *Digital Privacy: Theory, Technologies and Practices*, Boca Raton, FL: Auerbach Publications, pp. 409-433.
6. Nellis, M. (2007) "Electronic monitoring and the creation of control orders for terrorist suspects in Britain", in T. Abbas (Ed.) *Islamic political radicalism*, Edinburgh: Edinburgh University Press, pp. 263-278.
7. Solove, D. J. (2007) *The future of reputation: gossip, rumor, and privacy on the Internet*, New Haven, CT: Yale University Press.

About the author

Dimitris Tsapogas is a researcher, lecturer and PhD candidate at the University of Vienna in Austria and a digital rights activist. His interdisciplinary re-

search focuses on the relationship between surveillance and electronic citizenship and its results have been presented at numerous international conferences. Dimitris previously studied Philosophy and History of Science at the University of Athens in Greece and earned an MSc in Interactive Technologies at the University of Brighton in the UK.

The Discreet Charm of Impact Assessments: Contesting the Evidence Base for Security Research Policy

Georgios Kolliarakis

University of Frankfurt/EXC, Grüneburgplatz 1, 60323 Frankfurt am Main, Germany
e-mail: kolliarakis@soz.uni-frankfurt.de

Public policy resembles large-scale, real-time experiments with uncertain. This applies particularly to research policy, and, even more, to security research policy, which serves a value-laden, contested reference object: Security. Despite the complexity of the societal environment, the ambiguity in values and principles, and the uncertainty of outcomes – or rather because of it – evaluation and assessment of the impacts of security research policies is necessary in order to check whether they deliver on their objectives in service of the public interest. The generalized trend since the past decade, originating in public health and in environmental politics, toward evidence-based public policies aims at providing scientific tools for their assessment and evaluation in order to make them less vulnerable to ideological arbitrariness and to particularistic interests.

Security policy and, by default, security research policy, are "wicked" problems in that they are embedded in a nexus of contested concepts such as welfare, freedom, or civil rights, which are themselves moving targets. Such problems habitually attract "clumsy", piecemeal solutions, which they can misfire or even backfire. The core challenge this paper addresses is how to put in place and strengthen mechanisms for evaluation and impact assessment in the relatively young research field of civil security. More specifically, the attention is directed toward two key stages of the policy process in the European Security Research Programme (ESRP): Those of problem identification/prioritization and of evaluation/impact. The pursuit of surveillance, pattern recognition and detection technologies as innovative solutions for comprehensive societal challenges has yielded considerable criticism due to unbalanced stakeholder participation, and to a high-tech-biased agenda. Given the documented mismatch between set objectives and produced outcomes so far, the paper argues that strengthening the evidence base for those two policy stages along the conduct of policy regulatory impact assessments (RIAs) should align principle and practice of the ESRP with demands for responsiveness, accountability, and effectiveness.

In terms of governance, security research is embedded into a threefold context: Into a political context, which may shift following opportunistic waves of national and EU-level commitment, into a policy context, which seeks to establish compatibility and coherence among various legislative and non-legislative measures, and, last, into a technical/scientific evidence context, which aims at providing consistent empirical measurement anchors for evaluation and assessment. While little expert influence can be exercised within the former con-

text, there is potential to do so in the two latter ones. This paper will position the ESRP along a number of EU policy lines other than the currently predominant industrial-leadership one: The EU Internal Security Strategy (ISS) and the Stockholm Programme, the Responsible Research and Innovation (RRI) policies, and the EU Good Governance and Smart Regulation guidelines.

First, following European Commission's *Final Implementation Report of the Internal Security Strategy* from June 2014, which highlights the relevance of security research in the five priority areas for the future ISS policy, this paper takes the ESRP to be a key proactive form of security policy. Accordingly, it examines the lack, or (in-)adequacy of the existing evaluation and assessment instruments to guarantee that the ESRP delivers on the ISS primary objectives.

Secondly, predominant framings of innovation in security research as a growth-oriented and market-driven endeavour, preoccupied with a faster research-to-market process, blend out requirements for responsive, demand-driven understandings of public security. Furthermore, security research is unquestionably conflated with security technology research from the very start of the ESRP. Despite the fact that civil security features as a "societal challenge", it is evaluated and assessed along econometric indicators, rather with regard to its societal impact. Stakeholders from civil society are thereby practically absent from the policy formulation and evaluation process.

Thirdly, the paper will analyse the importance of the EU Regulatory Impact Assessments (adopted 2005, revised 2009, update pending in 2014) for establishing necessity, appropriateness, and efficacy of the current security research. Originating in the EU White paper on "Good Governance", the "Smart Regulation" programme, and anchored in the TFEU §191 (precautionary principle), policy development in contentious high-potential fields (e.g. renewable energy, GMO authorisation, shale gals, endocrine-disrupting chemicals, nanotechnologies) should undergo impact assessments in order to ensure that both legislative and non-legislative measures for an EU policy are (i) fit for purpose, (ii) proportional (cost-benefit balance), (iii) informed by scientific evidence, and (iv) value-adding to EU overarching goals. The RIA guidelines must additionally take account of the Charter of Fundamental Rights (since May 2011), and sustainable development (since February 2012).

As an illustrative example, the paper showcases the salience of the above considerations for high-gain/high-risk investments in "dual-use" security technologies R&D. As identified in a 2012 foresight report, infrared cameras, C4I (Command, Control, Communications, Computer, Intelligence) technologies, and UAVs (Unmanned Aerial Vehicles) technologies are the fields with the highest military-security technology synergy. The utility of the Technology Readiness Level classifications will be questioned with regard to providing evidence about non-anticipated and non-intended civil/military use of security technologies when ripe.

The present paper asks about access to adequate evidence, besides quantitative macro-data, sources of evidence beyond econometric ones, and transparency of evidence, particularly with regard to the civil security policy do-

main. Notwithstanding a number of challenges, the argument goes that streamlining of RIAs opens up the space for inclusion of citizens' perspectives as being the ultimate beneficiaries/affected parties by security (research) policies. This implies that stakeholders' diverging needs and concerns, together with the uneven distribution of costs and benefits, have to be weighed and accounted for in the evaluation and future planning of security research policy. What is more, linking technological, ethical, privacy, etc. impact assessments with the overarching regulatory assessments, would leverage them into evidence-providing tools for the design of security policy. Such a procedure is more likely to generate sensitivity for alternative problem definitions and prioritisations, clarify the ESRP objectives, and raise awareness for 2nd-order undesirable effects of the current security research and policy frameworks.

About the author

Georgios Kolliarakis is a Senior Research Fellow at the University of Frankfurt (Cluster of Excellence 'Formation of Normative Orders'), where he conducts research in the fields of security, society and conflict. Currently he focuses upon evaluation and impact assessment mechanisms in contentious fields, particularly for the analysis of non-intended and non-anticipated effects of public policy. Georgios has experience in engaging practitioners, scholars, and decision makers in order to promote transfer of knowledge, and valorize research results for policy. After studying Engineering at the National Technical University of Athens, Georgios earned a Master's degree in Political Geography from the Friedrich-Wilhelms University of Bonn, and a PhD in International Politics and Strategic Studies from the Ludwig-Maximilians University of Munich.

Latest publication: Daase, C., Engert, S. and Kolliarakis, G. (Eds.) 2014: *Politik und Unsicherheit. Strategien in einer sich wandelnden Sicherheitskultur* (Politics and Insecurity. Strategies in a changing Security Culture). Frankfurt, New York (Campus).

Privacy vs. Security – A Given Trade-Off?*

Stefan Strauß

Austrian Academy of Sciences, Institute of Technology Assessment
Strohgasse 45/5, 1030 Vienna, Austria
e-mail: sstrauss@oeaw.ac.at

The complex relationship between privacy and security is not significantly affected by the rapid dynamic of technological progress. In order to cope with a wide range of security challenges that to some extent include novel threats, security policies increasingly rely on the employment of technological means, i.e. surveillance-oriented security technologies (SOST). Despite (and to some extent also because) of the different roles and meanings of security, the call for a holistic security concept has increased over the years as part of a "securitization", where security becomes a permanent process seducing with a seemingly predictive view of threats fostering the effectivity of security measures. This development is mirrored in security policies at national as well as European level and entails the implementation and use of SOSTs which is mostly grounded in a model that frames privacy and security as a trade-off based on the assumption that a degree of privacy intrusion is required in order to achieve a higher level of security.

Already the term "trade-off" implies that one value has to be upheld at the expense of the other, i.e. that to improve security one has to accept a certain limitation of privacy. This model entails a sort of "all-or-nothing position" where privacy and security are framed as concepts with permanent contradictions inherently entailing the constant need to choose between these values. Such a framing leads to the neglect of the value of data protection and privacy because it is seen as burden to security. This entails a lack of consideration of the costs (economic and social) and effects of security measures. The trade-off is accompanied and shaped by the wrong questions: instead of asking the crucial question of how privacy should be protected, it is frequently asked whether privacy should be protected. Inherent in this logic is that privacy intrusions caused by security measures enable and foster security, which is often underlined by the argument that "those who have nothing to hide have nothing to fear". As a consequence the fact that both values, privacy and security are essential for well-being and social development is often neglected.

Challenges to overcome the fallacy of trading one against the other demand the development of new approaches that consider options where privacy and security are complementary concepts. The SurPRISE project contributes to the exploration of to what extent a complementary approach are feasible and which the relevant factors for such an approach would be. This not least is grounded on the re-examination of the privacy-security interplay incorporating the views of European citizens. This contribution sheds some light on the privacy-security tradeoff and presents the perceptions of European cit-

* This research has received funding from the European Union in the SurPRISE project under grant agreement No. 285492

izens which had been analysed in the SurPRISE project. The results of the SurPRISE citizen summits show that participants do not follow a trade-off argumentation: citizens neither want to fear security measures nor lose their privacy. Hence, they deem the tradeoff between privacy and security inappropriate, both with regards to the effectiveness of security measures as well as the protection of privacy. Instead of a tradeoff, alternatives are needed with respect to the effective protection of their privacy which was seen as a sine qua non for the acceptability and effectiveness of security measures.

About the author

Stefan Strauß is a researcher at the Institute of Technology Assessment (ITA) at the Austrian Academy of Sciences, he has a degree in business informatics/information systems. He focuses on the steering mechanisms of information technologies (e-governance) and their impacts on political processes, identity construction, surveillance and privacy protection. Further research interests include information- and computer ethics and the philosophy of information. He has been involved in different European research projects e.g. on privacy, security and surveillance, cloud computing, e-democracy and identity; currently in the project SurPRISE (surveillance, privacy and security).

A Window into the Reality of Post-9/11 Intelligence Surveillance: The Media Discourse on Privacy and Security before and after the NSA Revelations*

Jana Weitkamp

Fraunhofer Institute for Systems and Innovation Research ISI
Breslauer Strasse 48, 76139 Karlsruhe, Germany
e-mail: jana.weitkamp@isi.fraunhofer.de

In this presentation, we provide results from an analysis of the European media's coverage of privacy and security issues done in the context of the PRISMS project. The PRISMS project examines how technologies aimed at enhancing security are subjecting citizens to an increasing amount of surveillance and, in many cases, causing infringements of privacy and fundamental rights. By doing so, the project aims at investigating the traditional trade-off model – having more security leads to less privacy and vice versa – and providing a more evidence-based model for the complex relationship between privacy and security. Through the media, the public's perception of security and privacy is reflected and reinforced. Their role in reconstructing images, perceptions and beliefs is crucial; media express and at the same time shape public opinion. Especially when it comes to highly abstract topics such as privacy and security, which are bound to global and interdisciplinary developments and thus first hand experience is not available for many people, the media are the main source of information and their influence on people's agendas is expected to be high. A media analysis as carried out in our work package thus offers important information on what people actually are able to know about privacy and security, on which issues the two concepts are bound, their respective notions and instances of use and their framing.

The presentation provides insights into the results of an automated content analysis that covers the years 2008 to 2011, but focuses on the shift of discourse after the NSA revelations as disclosed by Edward Snowden. As a disruptive event that is highly relevant for our research, its influence on the media coverage of privacy and security issues is crucial, which will be shown by comparing the two very different settings of Germany and the UK.

About the author

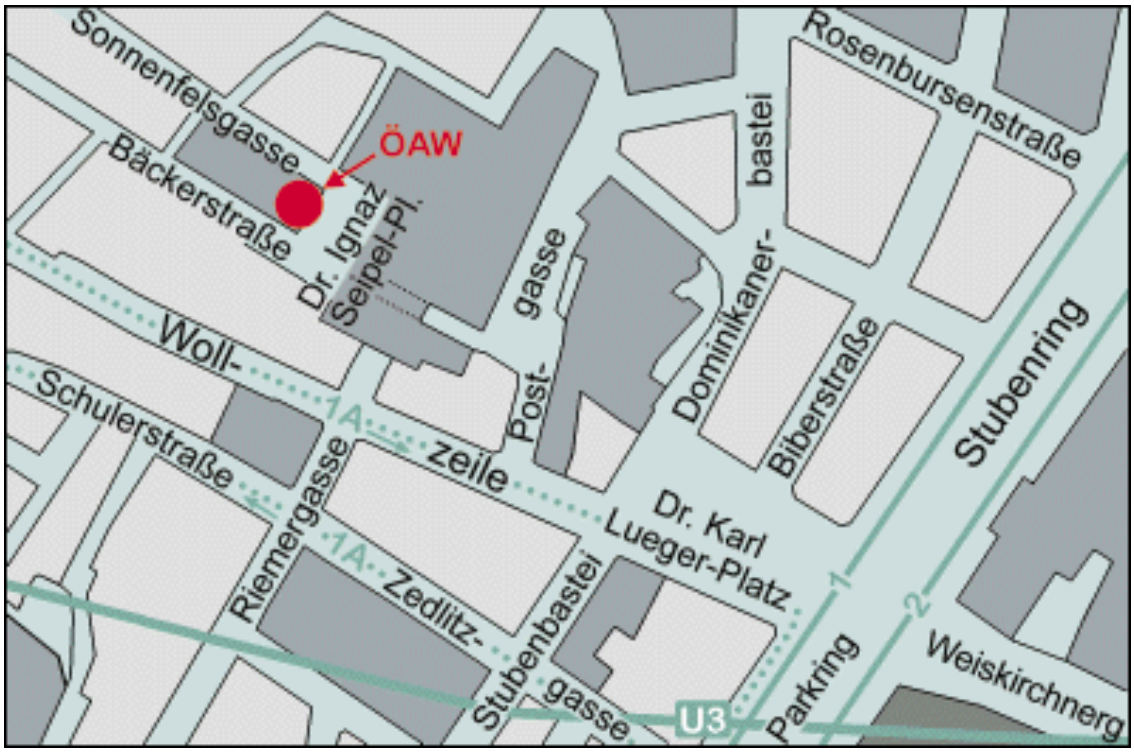
Jana Weitkamp holds a diploma in media science from the University of Paderborn. She has been working in publishing from 2006 to 2011, mainly on concepts of electronic and hybrid publishing for university presses. Since 2011 she works as a researcher at the Competence Center Emerging Technologies

* This research has received funding from the European Union in the PRISMS project under grant agreement No. 285399

at Fraunhofer Institute for Systems and Innovation Research ISI. Her main project is a long-term media analysis within the FP7-funded project PRISMS– The privacy and security mirrors, that examines the media coverage on privacy and security issues in a European context. Her dissertation project focuses on the question how the media's framing was influenced by the NSA revelations from June 2013.

Conference Venue and Directions

The conference will be held at the central building of the Austrian Academy of Sciences (ÖAW), Dr. Ignaz Seipel-Platz 2, 1010 Vienna.



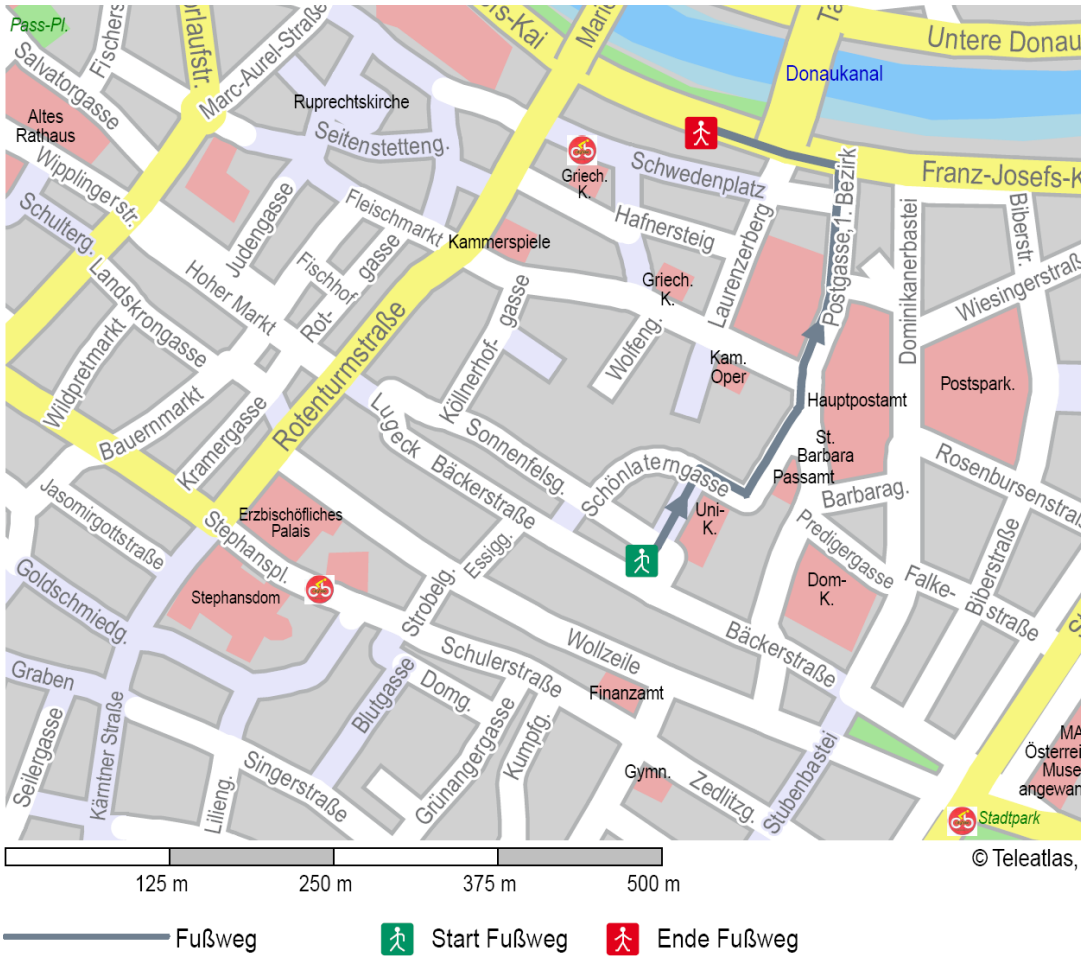
How to get there from the train station

From Süddbahnhof just take the Schnellbahn to Wien-Mitte, and from Westbahnhof take the U3 Subway to Stubentor, exit Wollzeile (or U4 Schwedenplatz).

How to get there from the Airport

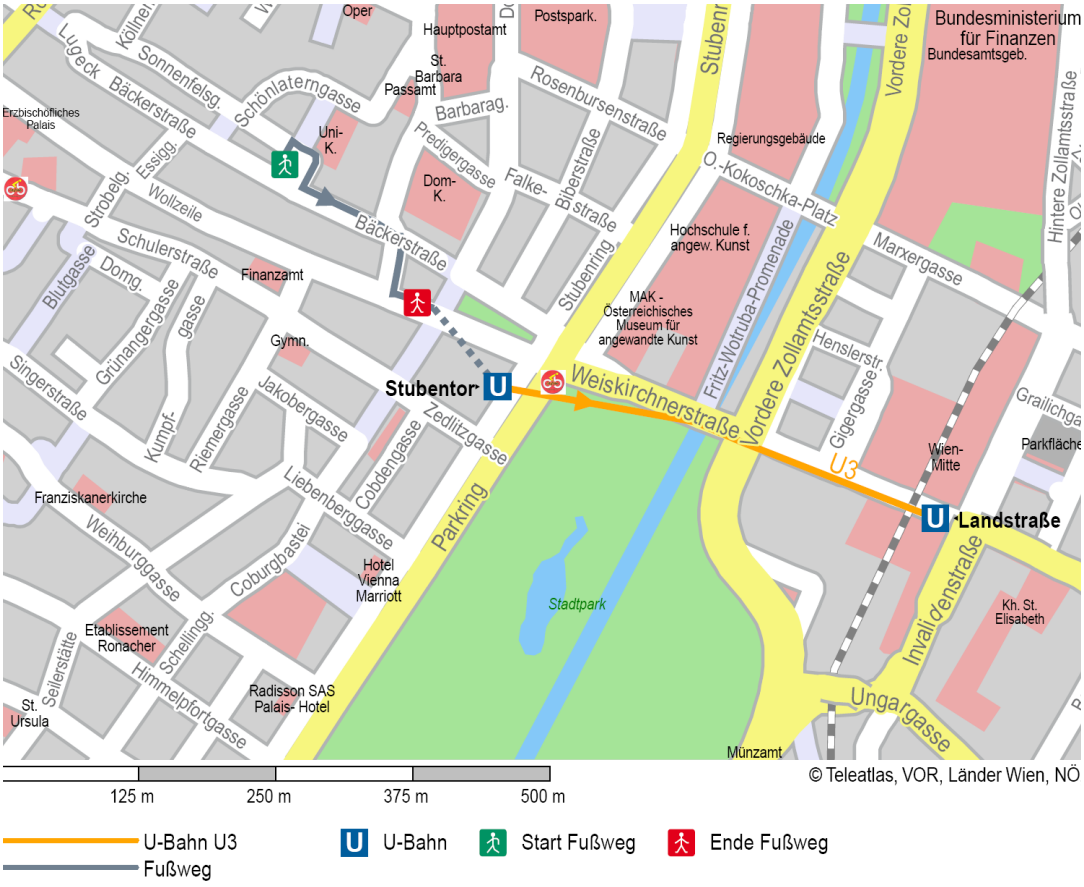
By Taxi: Travel time to or from the meeting venue is at least 20 minutes, depending on the traffic situation.
Please order an airport taxi (Flughafentaxi) to get the fixed price. We suggest the company "Airport Driver" where you can order your cab online in advance (€32 one direction) `http://www.airportdriver.at`

By Vienna Airport Lines (bus service): The closest bus terminal is at Schwedenplatz/Morzinplatz. Travel time from Schwedenplatz/Morzinplatz to the airport is about 40 minutes, depending on the traffic situation.
Price for one direction is €8. Departure: every 30 minutes. `http://www.postbus.at/de/Flughafenbus/Vienna_AirportLines/`
The walking distance from the conference venue to Morzinplatz/Schwedenplatz is app. 600 meters/10 minutes.


Pass-Pl.
Salvatorgasse
Marc-Aurel-Straße
Ruprechtskirche
Altes Rathaus
Seitenstetteng.
Wipplingerstr.
Schulterg.
Judengasse
Fleischmarkt
Kammerspiele
Hoher Markt
Fischhofgasse
Rot-
Landskrongasse
Wildpretmarkt
Bauernmarkt
Kramergasse
Rotenturmstraße
Kölnerhofgasse
Wolfeng.
Lugeck
Sonnenfelsg.
Bäckerstraße
Jasomirgottstraße
Stephanspl.
Erzbischöfliches Palais
Stephansdom
Goldschmiedg.
Strobelg.
Essigg.
Graben
Schulerstraße
Wollzeile
Blutgasse
Domg.
Finanzamt
Seilergasse
Kärntner Straße
Singerstraße
Grünangergasse
Kumpfg.
Lilieng.
Gymn.
Zedlitzg.
Stubenbastei
Donaukanal
Untere Donau
Franz-Josefs-K
Schwedenplatz
Griech. K.
Hafnersteig
Laurenzerberg
Griech. K.
Kam. Oper
Postgasse
1. Bezirk
Dominikanerbastei
Biberstr.
Wiesingerstraß
Postspark.
Hauptpostamt
St. Barbara Passamt
Schönlaterngasse
Uni-K.
Barbarag.
Rosenbursenstraß
Predigergasse
Dom-K.
Falke-
Biberstraße
Bäckerstraße
Stadtpark
125 m
250 m
375 m
500 m
© Teleatlas,
Fußweg
Start Fußweg
Ende Fußweg

By City Airport Train (CAT): The CAT leaves the Airport and City Air Terminal at "Wien-Mitte" railway station every half-hour, the non-stop drive takes 16 minutes. A Single-Ticket costs €11, a Return-Ticket €17. Departure: every 30 minutes.

The way from the meeting venue to the railway station "Wien-Mitte": You can take the underground line U3 from Stubentor, app. 200 meters from the meeting venue (one stop to Landstraße/Wien Mitte). The full walking distance to "Wien-Mitte" railway station is app. 700 meters/10 minutes. Please allow for some additional minutes to find your way in the railway station.



Citizens' Perspectives on Surveillance, Security and Privacy Controversies, Alternatives and Solutions