HAL
archives-ouvertes.fr

Surveillance and Privacy

Yola Georgiadou, Simone Fischer-Hübner

▶ To cite this version:

Yola Georgiadou, Simone Fischer-Hübner. Surveillance and Privacy. Jacques Berleur; Magda David Hercheui; Lorenz M. Hilty. 9th IFIP TC9 International Conference on Human Choice and Computers (HCC) / 1st IFIP TC11 International Conference on Critical Information Infrastructure Protection (CIP) / Held as Part of World Computer Congress (WCC), Sep 2010, Brisbane, Australia. Springer, IFIP Advances in Information and Communication Technology, AICT-328, pp.175-177, 2010, What Kind of Information Society? Governance, Virtuality, Surveillance, Sustainability, Resilience. <10.1007/978-3-642-15479-9_16>. <hal-01054797>

HAL Id: hal-01054797
https://hal.inria.fr/hal-01054797

Submitted on 8 Aug 2014

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Distributed under a Creative Commons Attribution| 4.0 International License

Surveillance and Privacy

Yola Georgiadou[1] and Simone Fischer-Hübner[2]

[1] Faculty of Geo-Information Science and Earth Observation (ITC),
University of Twente, PO Box 6, 7500 AA Enschede - the Netherlands
[2] Karlstad University, Department of Computer Science,
Universitetsgatan 2, S 651 88 Karlstad / Sweden
georgiadou@itc.nl, simone.fischer-huebner@kau.se

Recent social and technical developments are expanding surveillance by the government and private sector and intensifying privacy concerns, resulting in a surveillance-privacy dilemma. Governments establish surveillance schemes to fight terrorism and crime. Private organizations use profiling and data mining techniques to target marketing endeavors, to analyze customer behavior and monitor the work practices of employees. Social networks bring to the fore new means for the surveillance of individuals, publishing intimate details about themselves. Individuals are usually unaware of the constant data collection and processing in their surroundings. They are effectively losing control over their personal spheres. The aim of the conference track "Surveillance and Privacy" is to discuss and analyze, from multi-disciplinary perspectives, the privacy risks of surveillance for individuals and society, as well as solutions for protecting an individual's right to informational self-determination.

As argued by Edwards et al. [1] the key question is "*whether we choose, for any given problem, a social or a technical solution, or some combination. It is the distribution of solutions that is the object of study. An everyday example comes from the problem of email security. How do I distribute my trust? I can delegate it to my machine, and use Pretty Good Encryption for all my email messages. Or I can work socially and organizationally to make certain that sysops, the government, and others who might have access to my email internalize a value of my right to privacy. Or I can change my own beliefs about the need for privacy – arguably a necessity with the new infrastructure*" (p.6).

The Track 3 on "Surveillance and Privacy" at HCC9 is introduced by a keynote presentation by Klaus Brunnstein on the future of Privacy and Surveillance in the Information Society.

In the four articles of this track, authors either inscribe privacy solutions in technical artifacts (Hoepman and Kuntze & Rudolph) or argue and advocate for a more social solution to the privacy-surveillance dilemma (Clarke and Verplanke et al.). In the panel, the members dissect and debate the future of privacy for the millennial generation.

In "Privacy enhanced fraud resistant road pricing", Hoepman presents an architecture for a road pricing system where privacy is achieved by implementing two technical design principles: (i) splitting of trips into short segments (so-called legs) that are non-linkable to each other and (ii) distributing the process steps needed to determine the overall road charge over several system components, so that no single

component has enough information to reconstruct a particular route travelled. Invoices contain aggregated information, while the charging details are available only to the vehicle driver. Fraud is avoided by integrating random spot checks in a novel enforcement protocol.

In “Privacy in distributed commercial applications”, Kuntze and Rudolph analyze the different and possibly conflicting security and privacy requirements of multiple stakeholders in distributed commercial applications. They propose pseudonymous or anonymous attestation of the state of a device installed in a user’s home as a building block towards privacy-preserving, secure, distributed commercial applications. They discuss two possibilities for pseudonymous and anonymous attestation. The first uses a generic approach of deep attestation through virtual machine to the hardware TPM. The second relies on the mutual attestation of nodes in the network.

In “Civil Society Must Publish Standards Documents”, Roger Clarke argues for social solutions to the privacy-surveillance dilemma, and puts the onus squarely on the shoulders of civil society. He advocates for public interest NGOs to invest more in 'practical activism' by establishing Standards and Process Descriptions, which clearly communicate their expectations and provide benchmarks against which the inadequacies of processes and the unacceptable dangers of projects and schemes can be delineated. Using examples of public interest standards development, he demonstrates that public interest NGOs can emulate industry and government in playing the standards game.

In “Citizen Surveillance of the State: A mirror for eGovernment?”, Verplanke and co-authors also advance a social solution to the privacy-surveillance dilemma, a case of what has come to be called “sousveillance.’ They outline an approach where citizens invert surveillance tools (e.g. Google Earth), made available by global corporations, to hold government accountable for the delivery of basic public services. Commercial virtual globes act as a mirror to the traditional eGovernment framework and make visible to all, in real time, both the performance of government services and localized citizens’ needs.

In the panel “Privacy...going, going, gone?” Ianella and other panelists show how social networks have put the media spotlight on privacy, as new and old web companies vie for the attention of an increasingly polarized global web community. The panel debates issues arising from the social web, including privacy dramas on social networks, technical challenges to privacy, the redefinition of privacy norms and solutions to address these issues in terms of law, enforcement, practice, design and technology and the future survival of privacy as a concept.

Acknowledgments. We want to thanks the track 3 programme committee very much, who contributed with helpful reviews, comments and who help us to select the papers for track 3. In this context, we especially want to acknowledge the programme committee contributions by Roger Clarke, George Danezis, Marit Hansen, Francis Harvey, David-Olivier Jaquet-Chiffelle, Eleni Kosta, Andreas Pfitzmann, Kai Rannenberg, Morton Swimmer, Jozef Vyskoc and Diane Whitehouse and well as the help by the sub reviewer Matthias Kirchner.

References

1. Edwards, P. N., Jackson, S. J., Bowker, G. C., Knobel, C. P.: Report of a Workshop on "History & Theory of Infrastructure: Lessons for New Scientific Cyberinfrastructures, NSF Grant 0630263, Human and Social Dynamics, Computer and Information Science and Engineering, Office of Cyberinfrastructure (January 2007), http://deepblue.lib.umich.edu/bitstream/2027.42/49353/3/UnderstandingInfrastructure2007.pdf.