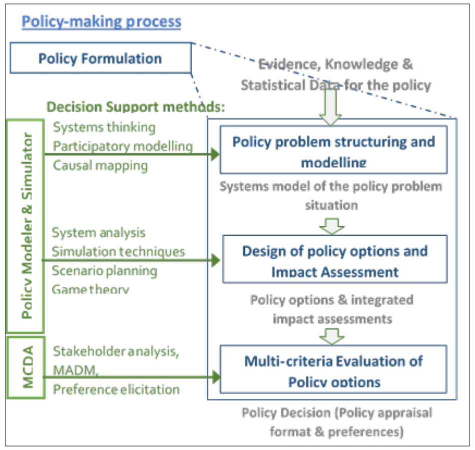

Policy-making process
Policy Formulation
Evidence, Knowledge & Statistical Data for the policy
Decision Support methods:
Policy Modeler & Simulator
Systems thinking
Participatory modelling
Causal mapping
Policy problem structuring and modelling
Systems model of the policy problem situation
System analysis
Simulation techniques
Scenario planning
Game theory
Design of policy options and Impact Assessment
Policy options & integrated impact assessments
MCDA
Stakeholder analysis,
MADM,
Preference elicitation
Multi-criteria Evaluation of Policy options
Policy Decision (Policy appraisal format & preferences)

Figure 17: Integration of operations research (OR) modelling and decision-support methods for the three steps of policy formulation

Conclusion

Within this paper we presented information and communication technologies that are part of the Framework 7 European research project Sense4us. The tools' goal is to enable stakeholders within the political sphere to identify online available data related to their policies.

Concerning our research regarding the semantics of Twitter posts, we investigated the use of contextual and conceptual semantics for calculating sentiment. Results showed that using conceptual semantics (e.g. gleaned from term co-occurrence or entities extraction using AlchemyAPI) the sentiment accuracy could be increased over several baselines. Regarding the conceptual semantics, we looked at stop words where the best results were achieved when using an automatically generated dataset-specific set of stop words. Furthermore, we experimented with a new approach to automatically extend sentiment lexicons to render them more adaptable to domain change on social media, and generated and published a new gold-standard dataset for social media sentiment analysis.

The proposed policy modelling and simulation approach allows simplifying and summarising the decision maker's knowledge (notions and causal beliefs) and information gathered from different sources about a social, socioeconomic or sociotechnical system and visually simulates the system behaviour and responses to interventions over time. Large-scale causal maps can be used to model complex policy problems, representing what a government decision maker thinks about the drivers, barriers, instruments and consequences of change achieved by a certain policy proposal. It is obvious that such maps can be useful for analysing, developing and sharing views and understanding among key actors also for creating some preconditions for intervention.

References: Page 436

Factors Influencing Citizens' Attitudes Towards Surveillance-Oriented Security Technologies

Michael Friedewald and Marc van Lieshout

Abstract

This paper deals with the question which factors have an influence on citizens' attitudes towards surveillance-oriented security technologies and their privacy implications. Based on data gathered in a pan-European survey, we discuss which factors determine citizens' perceptions in concrete surveillance practices. We argue that the perceived usefulness of the security practices and the trust in those actors that are promoting and operating security systems are paramount for citizens' acceptance. In addition, individual factors and experiences play an important role for the assessment.

Introduction

The relationship between privacy and security has often been understood as a zero-sum game, whereby any increase in security would inevitably result in a reduction of the privacy enjoyed by citizens. A typical representation of this thinking is the all-too-common statement: "If you have nothing to hide, you have nothing to fear". This trade-off model has, however, been criticised because it approaches privacy and security in abstract terms and reduces public opinion to one specific attitude, which considers surveillance technologies to be useful in terms of security, but potentially harmful in terms of privacy (Pavone/Esposti 2012). In any case insight into the public understanding of security measures is important for industry and politics to make informed decisions and to avoid negative public reactions. Since we have already shown elsewhere that there is no simple trade-off between privacy and security perceptions (Friedewald et al. 2015a), this chapter deals with the question what, then, are factors that affect public assessment of specific surveillance-based security practices?

The PRISMS project[1] has approached this question by conducting a large-scale survey of European citizens. Fieldwork took place between February and June 2014. The survey company Ipsos MORI conducted around 1,000 telephone interviews in each EU member states except Croatia[2] (27,195 in total) amongst a representative sample (based on age, gender, work status, and region) within each country.

Measuring People's Opinions About Security Technologies

Citizens usually understand concepts such as privacy and security in very different ways and often only have a vague idea how security technologies work and what kind and how much information they collect. Thus we first have to operationalize the central terms accordingly.

Privacy is a concept that is not only hard to measure but also difficult to define. It is, however, a key lens through which many new technologies, and most especially new surveillance or security technologies, are critiqued. For the PRISMS work we have used a taxonomy developed by Finn et al. (2013, p. 7-9) who suggest seven different types of privacy that ought to be protected and that receive different attention and valuation in practice. The seven types of privacy comprise: (1) privacy of the person, (2) privacy of behaviour, (3) privacy of communication, (4) privacy of data and image, (5) privacy of thoughts and feelings, (6) privacy of location and space, and (7) privacy of association (including group privacy).

The concept of security is at least as difficult to approach. According to the European Union, "security" can be defined as "protecting people and the values of freedom and democracy, so that everyone can enjoy their daily lives without fear" (General Secretariat of the Council 2010) and is negatively defined as the absence of insecurity. Perfect objective security thus implies the absence of any threat. The discourse in the media and among (EU) policy makers is often narrowed down to issues of terrorism, crime and, increasingly, border security. For the general public, however, security is usually much more, including socio-economic conditions, health or cultural security. Therefore we are using a broad definition, in order not to exclude interesting perspectives. We have identified seven general types of security contexts and the accompanying measures to safeguard and protect these contexts (cf. Lagazio 2012): (1) physical security, (2) socio-economic security, (3) radical uncertainty security, (4) information security, (5) political security, (6) cultural security, and (7) environmental security.

To address the ambiguity and context dependence of the central concepts, the PRISMS survey is working with so-called vignettes that are used when survey respondents may understand survey questions in different ways, due to the abstractness of the presented concepts, their complexity, and because they come from different cultures. Vignettes translate theoretical definitions of complicated concepts in presenting hypothetical situations and asking respondents questions to reveal their perceptions and values (King/Wand 2007).

In PRISMS we have developed eight different vignettes that cover all seven types of privacy. Since our aim is to scrutinize how citizens assess the implications of specific security technologies, our focus is limited to those types of security that are technologically supported, in particular by surveillance-oriented security technologies. This implies that vignettes mainly cover applications such as the fight against public disorder, criminality and terrorism, and also some commercial applications. We have made sure that the vignettes cover virtual as well as physical applications, which are operated by public as well as private sector organisations (see Figure 18).

The vignettes are short narratives of no more than 100 words (the complete text of the vignettes can be found in the annex on the page 437). The vignette about police monitoring crowds was used in two different versions, in the first one surveillance takes place at a football match while in the other participants of a political demonstration are monitored. For each of the vignettes citizens were asked the question: "To what extent, if at all, do you think that [actors] should or should not [do this]" with answer options on a 5-point Likert scale ranging from "definitely should" to "definitely should not".[3]

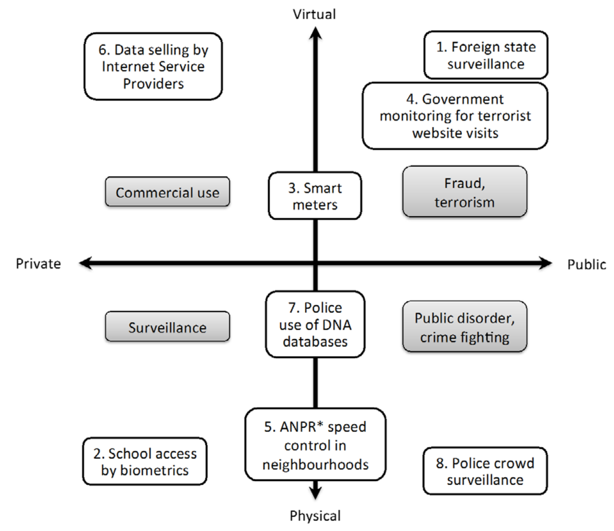

Virtual
6. Data selling by Internet Service Providers
1. Foreign state surveillance
4. Government monitoring for terrorist website visits
Commercial use
3. Smart meters
Fraud, terrorism
Private
Public
Surveillance
7. Police use of DNA databases
Public disorder, crime fighting
5. ANPR* speed control in neighbourhoods
2. School access by biometrics
8. Police crowd surveillance
Physical

Figure 18: Classification of the vignettes (*ANPR = Automatic Number Plate Recognition)

Descriptive Results

All in all, European citizens are rather critical in their assessment of the security technologies and practices covered by the vignettes. The spectrum of opinions, however, differs widely between the vignettes (see Figure 19).

About half of the vignettes produced a rather clear positive or negative assessment. For instance, more than two thirds of the respondents agreed that "Police surveilling football match", "Automatic number plate recognition (ANPR) speed control in neighbourhoods", and "Monitoring terrorist website visits" should be used to protect security. On the other side of the spectrum, more than 80 per cent of the respondents thought that "Internet Service Providers (ISPs) selling customer data" should not take place.

The rest of the vignettes, however, did not produce equally clear results. While a majority of respondents were still in favour of "Police surveillance at demonstrations" and against "Foreign state surveillance", the remaining three vignettes had about as many supporters as opponents. Especially the usage of smart meter data did not only have almost as many positive as negative votes, it also had the highest number of undecided respondents.

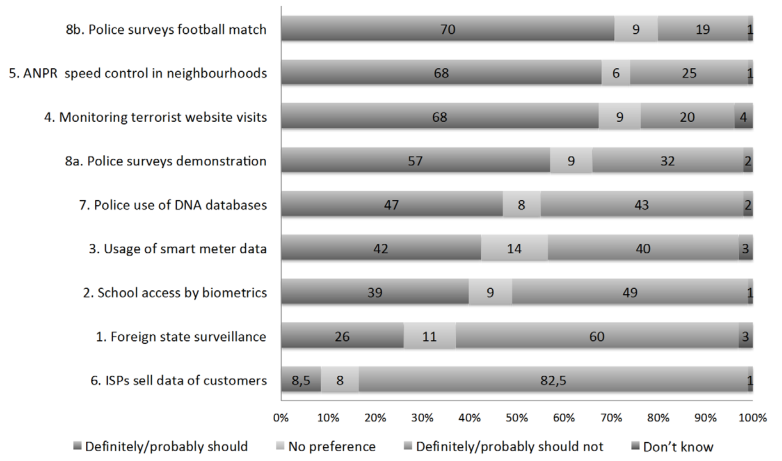


Figure 19: "To what extent, if at all, do you think that [an institution] should or should not…?"

Already on the basis of this basic statistic it becomes clear that there is a distinction between security technologies and practices operated by public and private sector institutions. Even in spite of the obscure role that European authorities (mainly intelligence services) have played in the NSA spying scandal, citizens still have more trust that public authorities do respect their rights to privacy and data protection than profit-oriented companies (which are often branches of multinational corporations).

The figures also show that citizens are especially critical with regard to purely virtual forms of surveillance. There is opposition against covert surveillance practices and secondary use or disclosure of data, especially for commercial purposes.

Identifying Determinants of Citizens' Acceptance

In this section we present results from the analysis of a selection of factors that determine citizens' assessment of the systems/practices outlined in the vignettes. It will show that there is no simple impact of specific factors in the assessment of concrete cases of security technologies and surveillance practices. To answer the research questions and to empirically test our theoretical assumptions, we conducted a series of ordered logistic regressions (a detailed presentation of the regression results can be found in Friedewald et al. 2015b).

The analysis shows that there are only a few factors which play an important role in all cases. Not surprisingly these include citizens' general privacy and security attitudes. Firstly, in most cases there is a strong positive correlation between worries about personal security and support for a security practice. The support is stronger for the cases of physical surveillance than for virtual surveillance practices, which means that people tend to accept security practices when they come close to personal concerns, are understandable, and do not affect them personally. Secondly, there is an even stronger correlation between privacy worries and the non-acceptance of a security practice.

The third factor that has a significant positive correlation with citizens' support for a security practice is their trust in institutions. It is clearly visible that the perceived trustworthiness of an authority, organisation, or company operating a security system has a positive effect on citizens' acceptance. This supports discussions about the importance of trust for the assessment of risks and benefits and the acceptability of technologies. According to these discussions, trust reduces the complexity people need to face. Instead of making rational judgements based on knowledge, trust is employed to select actors who are trustworthy and whose opinions can be considered accurate and reliable. People having trust in the authorities and management responsible for the technology perceive less risk than people who lack that sense of trust in those members, although some studies seem to suggest that this is not always the case (Bord/O'Connor 1992).

Other factors do not show an equally clear picture and are more difficult to interpret, either because the correlations with the assessment of the vignettes are not always statistically significant or even have effects in different directions.

Gender for instance has a significantly positive correlation in three and a significantly negative correlation in four of the cases. Men tend to reject surveillance practices by public authorities more than those of private sector. This is in line with the fact that, according to our survey, men have less trust in public authorities than in the private sector and less trust in institutions in general than women.

Age is an interesting factor inasmuch as it has been recently shown that the younger generation is not generally valuing privacy differently from older citizens. The assumption that this also leads to a more critical assessment of surveillance practices by younger citizens is not supported by the survey results. Rather, the likelihood that young adults (16-34) found a surveillance practice acceptable is higher than that of middle-aged people and much higher than that of older citizens. This correlation, however, is not significant for all the vignettes. Young adults only found the monitoring of websites in search of terrorists a less acceptable practice. Qualitative research by Székely (2010) suggests that a possible explanation might be that older citizens, who experienced European authoritarian regimes, are more distrustful, whereas younger people, who had not lived in surveillance states, are less concerned.

In general, the survey has shown that the educational level is positively correlated with the valuation of privacy and negatively correlated with the valuation of security. In concrete cases, however, education only seems to have a weak influence on the acceptance of a surveillance measure. For most of our vignettes one can state that the higher the education level, the less likely it is that one is willing to accept a surveillance practice. This indicates that the more knowledge and understandings of the context people have, the more critical they are. These observations, however, are only significant in some of the cases. This is an interesting complement to the findings about privacy since people with a higher education have a significantly higher appreciation for their privacy than those with an intermediate or low level of education.

It has sometimes been suggested that people living in big cities are more worried about their security and thus more supportive to physical security measures than citizens living in small cities, suburbs, or even in rural areas. Our survey results do not fully confirm this hypothesis. Residents of big cities are only significantly more supportive to the vignette on "school access by biometrics". Their support for the police use of DNA databases is even significantly lower. For all other cases we could not show a significant correlation. The situation is similarly mixed for smaller cities and suburbs. It is in line with the observation that the people least in danger are most afraid. More important than the fear of crime seems to be the perceived usefulness and effectiveness of concrete measures (Verfaillie et al. 2013).

Political orientation has a weak effect on the assessment. Citizens with a left-wing or liberal orientation are less likely to accept surveillance than those who consider themselves conservatives or right wing.

In summary, one can say that people who are not worried at all about being monitored (do not mind being under surveillance) have lower education, are relatively young, and prefer conservative over liberal thinking.

Conclusions

Our analysis of the questions that aimed to measure European citizens' attitudes towards specific examples of surveillance technologies and practices had the following main results:

- Trust in the operating institution is an essential factor for the acceptance of a surveillance-oriented security technology.
- Openness has a positive effect on the willingness of citizens to accept security practices. This can be understood on different levels: (1) The surveillance activity should not be covert but perceivable for the citizen. (2) Citizens tend to accept security practices when they are addressing their personal concerns. Thus, they need to be convinced that a security measure is necessary, proportionate, and effective. A nuanced and critical view on them is also a question of proper education.
- On the downside it can be stated that many citizens do not care about surveillance measures that do not negatively affect them personally.

Starting from these more general findings, the next step is to define a structural model that describes the relationship of the main constructs in greater detail. This will be a translation of the theory of planned behaviour into a survey-based empirical model. Such an enriched model may then support decision-makers in industry, public authorities, and politics to implement security measures that raise fewer concerns among the population and are thus more acceptable (Friedewald et al. 2015b).

References: Page 436

The Security/Privacy Trade-off

Citizens' Perspectives on a Politically and Scientifically Contested Concept

Johann Čas

Abstract

The relationship between security and privacy is usually treated as a trade-off. A central premise of the research presented in this paper is that framing the relationship between privacy and security in terms of a trade-off is only one among several potential interpretative frames, and also that it may not be the most common way of approaching the security issue among European citizens. The SurPRISE project developed and applied an innovative research approach to explore these issues, involving about 2000 citizens from nine European countries in participatory technology assessment activities. Qualitative and quantitative methods were used to ensure that citizens not only had a chance to express their preferences among a set of predetermined options, but that they also had an opportunity to voice their own views, ideas, knowledge and proposals. SurPRISE provided a deep scientific understanding of the rationale behind the rejection or acceptance of security solutions and recommendations to increase the appropriateness and effectiveness of security measures embedded in complex social realities.

Introduction

The objective of this paper is to sketch in a condensed form core elements of the research methodology applied in the SurPRISE[1] project and to summarise the main results of this large-scale participatory technology assessment of surveillance technologies (SurPRISE Consortium 2015). It presents recommendations for security measures and technologies that respect human rights and European values and summarises the main factors and criteria influencing the acceptability of surveillance-oriented security technologies (SOSTs).

One of the central objectives of SurPRISE was to question the trade-off approach between privacy and security which largely dominates security policy making and the development and implementation of surveillance-orientated security technologies. SurPRISE challenged this approach from different perspectives: from a theoretical one, which was subsequently

Policy Making in a Complex World, p. 253.

Acar, W.; Druckenmiller, D., 2006: Endowing cognitive mapping with computational properties for strategic analysis, Futures 38:993-1009

Cornwall, A., 2002: Making spaces, changing places: Situating participation in development. Institution of Development Studies, IDS Working Paper 170

Fernandez, M.; Wandöfer, T.; Allen, B.; Elisabeth Cano, A.; Alani, H., 2014: Using Social Media To Inform Policy Making: To whom are we listening?. In Proceedings of the European Conference on Social Media (ECSM). UK

Fung, A., 2006: Varieties of Participation in Complex Governance, Public Administration Review, Vol. 66, 2006, pp. 66-75

Gaventa, J.; Barrett, G., 2012: Mapping the outcomes of citizen engagement. World Development 40 (12), 2399-2410

Lindblom, C., 1968: The Policy-making Process, Prentice-Hall, Englewood Cliffs NJ

Franco, L. A. and Montibeller, G. (2010). Facilitated modelling in operational research. European Journal of Operational Research 205: 489-500

Reed, 2008: Stakeholder participation for environmental management: a literature review, Biol. Conserv., 141 (10) (2008), pp. 2417–2431

Saif, H.; Fernandez, M.; He, Y.; Alani, H., 2013: Evaluation datasets for twitter sentiment analysis a survey and a new dataset, the sts-gold. In Proceedings, 1st Workshop on Emotion and Sentiment in Social and Expressive Media (ESSEM) in conjunction with AI*IA Conference, Turin, Italy, 2013

Saif, H.; Fernandez, M.; He, Y.; Alani, H., 2014a: On Stopwords, Filtering and Data Sparsity for Sentiment Analysis of Twitter. In Proc. 9th Language Resources and Evaluation Conference (LREC), Reykjavik, Iceland, 2014

Saif, H.; Fernandez, M.; He, Y.; Alani, H., 2014b: SentiCircles for Contextual and Conceptual Semantic Sentiment analysis of Twitter. Extended Semantic Web Conference (ESWC), Crete, 2014

Saif, H.; Fernandez, M.; He, Y.; Alani, H., 2014c: Adapting Sentiment Lexicons using Contextual Semantics for Twitter Sentiment Analysis. In Proceeding of the first semantic sentiment analysis workshop: conjunction with the eleventh Extended Semantic Web conference (ESWC). Crete, Greece

Saif, H.; Fernandez, M.; He, Y.; Alani, H., 2014d: Semantic Patterns for Sentiment Analysis of Twitter, The 13th International Semantic Web Conference (ISWC), Riva del Garda - Trentino Italy

Turnhout, E.; van Bommel, S.; Aarts, N., 2010: How participation creates citizens: Participatory governance as performative practice. Ecology and Society, 15(4), 26

Footnotes:

1) Cp. URL: http://www.sense4us.eu/ (Retrieved on 01/07/2015)

Factors Influencing Citizens' Attitudes Towards Surveillance-Oriented Security Technologies, p. 259.

Bord, R.J.; O'Connor, R.E., 1992: Determinants of risk perceptions of a hazardous waste site. In: Risk Anal. 12 (1992), pp. 411-416

Finn, R.L.; Wright, D., et al., 2013: Seven types of privacy. In: Gutwirth, S. et al. (eds.): European Data Protection: Coming of Age. Dordrecht, pp. 3-32

Friedewald, M.; van Lieshout, M., et al., 2015a: Privacy and Security Perceptions of European Citizens: A Test of the Trade-off Model. In: Camenisch, J. et al. (eds.): Privacy and Identity 2014, IFIP AICT, vol. 457. Heidelberg, Berlin, pp. 39-53

Friedewald, M.; van Lieshout, M., et al., 2015b: Report on statistical analysis of survey results. PRISMS Deliverable 10.1. http://prismsproject.eu (download 15 September 2015)

General Secretariat of the Council, 2010: Internal security strategy for the European Union: Towards a European security model. Luxembourg

King, G.; Wand, J., 2007: Comparing Incomparable Survey Responses: Evaluating and Selecting Anchoring Vignettes In: Politic. Anal. 15 (2007), pp. 46-66

Lagazio, M., 2012: The evolution of the concept of security. In: Thinker 43/9 (2012), pp. 36-43

Pavone, V.; Esposti, S.D., 2012: Public assessment of new surveillance-oriented security technologies: Beyond the trade-off between privacy and security. In: Public Underst. Sci. 21/5 (2012), pp. 556-572

Székely, I., 2010: Changing Attitudes in a Changing Society? Information Privacy in Hungary, 1989-2006. In: Zureik, E. et al. (eds.): Surveillance, Privacy, and the Globalization of Personal Information: International Comparisons. Montreal, Kingston, pp. 150-170

Verfaillie, K.; van den Herrewegen, E., et al., 2013: Public assessments of the security/privacy trade-off: A criminological conceptualization. PRISMS Deliverable 4.1. http://prismsproject.eu (download 15 September 2013)

Footnotes:

1) PRISMS is co-funded from the European Union's 7th Framework Programme under grant agreement 285399.

2) Croatia had not acceded to the EU at the time of the project planning.

3) Apart from the vignette-related questions, the survey also collected a large number of demographic variables (age, sex, education, geographic region, political orientation, internet experience, and many more) that were used to extract the defining factors.

Annex: The vignettes:

1. Foreign government surveillance. An international disaster relief charity has been sending a monthly newsletter by email to its supporters. The people who run the charity find out through the media that a foreign government has been regularly capturing large amounts of data on citizens of other countries by monitoring their emails. The foreign government says it needs to monitor some communications to help keep its citizens safe and that the main purpose is to focus on terrorism. The charity's officials are unsure whether this means their supporters' personal information is no longer confidential.

2. School access by biometrics. At a local primary school a new system for getting into the school has been installed. All pupils, teachers, parents, other family members, and other visitors have to provide their fingerprints on an electronic pad to identify themselves in order to enter or leave the school.

3. Usage of smart meter data. A power company has decided to offer smart meters to all its consumers. Smart meters enable consumers to use energy more efficiently by allowing them to see how much they are using through a display unit. The data recorded by smart meters allows power companies to improve energy efficiency and charge lower costs. They also enable power companies to build up a more detailed picture of how their customers use energy. It also enables the companies to find out other things, like whether people are living at the address, or how many people are in the household.

4. Monitoring terrorist website visits. A student is doing some research on extremism and as part of his work he visits websites and online forums that contain terrorist propaganda. When his parents find out they immediately ask him to stop this type of online research because they are afraid security agencies such as the police or anti-terrorism bodies will find out what he has been doing and start to watch him.

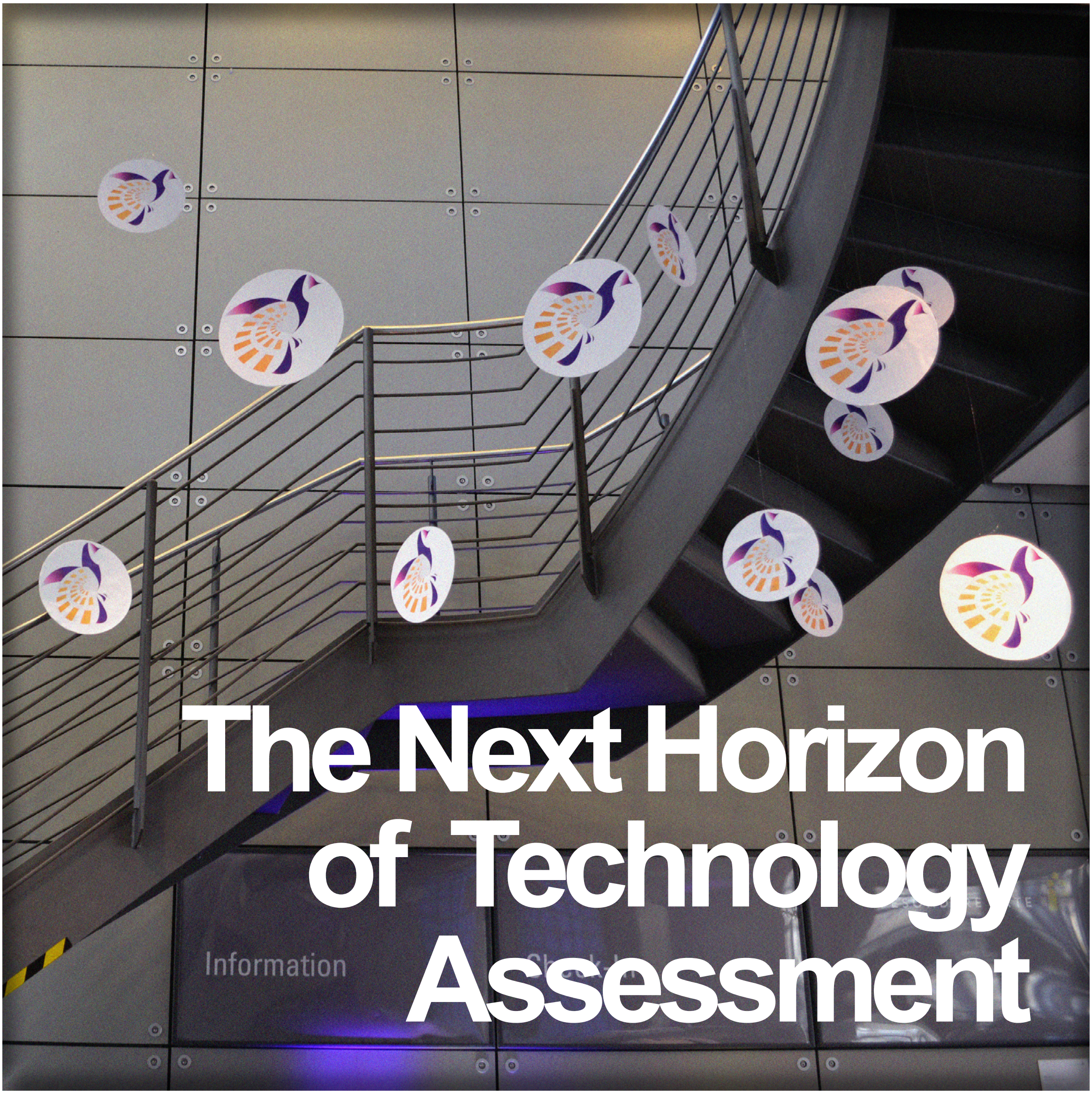
5. Speed control in neighbourhoods by automatic number plate recognition (ANPR). Michael lives in a suburban neighbourhood where his children like to play outside with their friends. However, his street is a short cut for commuters who drive faster than the speed limit. In response to complaints from residents, the local authority decides to install automatic number plate recognition systems, which identify and track all vehicles and calculate their average speed. This allows those who drive too fast can to be prosecuted.

6. Internet Service Provider (ISP) Data. Companies offering services on the Internet want to sell information about their customers' Internet use to advertisers and other service providers so the information can be used to create more personal offers and deals. This would include the searches you conduct and the websites you visit. Your provider says the information they sell will be anonymous.

7. Use of DNA databases by police. James voluntarily provided a sample of his DNA to a company that carries out medical research. DNA contains the genetic pattern that is uniquely characteristic to each person. He then learns that the research company has been asked to disclose all their DNA samples to police for use in criminal investigations. Samples of DNA can be used to understand potential health problems but also to identify people and to make inferences about who they are related to.

8. Crowd surveillance by police. Version a "Demonstration": Claire is an active member of an environmental group, and is taking part in a demonstration against the building of a new nuclear plant. The police monitor the crowd in various ways to track and identify individuals who cause trouble: they use uniformed and plain-clothes police, CCTV (closed circuit television, i.e. video surveillance), helicopters and drones, phone tapping, and try to find people on social media. V***ersion b "Football":*** David is a football fan who regularly attends home matches. The police monitor the crowd in various ways to track and identify individuals who cause trouble: through uniformed police and plain-clothes police, CCTV, by using helicopters and drones, tapping phones, and by trying to find people on social media.

Proceedings from the PACITA 2015 Conference in Berlin



The Next Horizon of Technology Assessment

Edited by
Constanze Scherz, Tomáš Michalek,
Leonhard Hennen, Lenka Hebáková,
Julia Hahn and Stefanie B. Seitz

PACITA

THE NEXT HORIZON OF TECHNOLOGY ASSESSMENT

PROCEEDINGS FROM THE PACITA 2015 CONFERENCE IN BERLIN

PACITA

TECHNOLOGY
CENTRE ASCR

ITAS Institute for
Technology Assessment
and Systems Analysis

The Next Horizon of Technology Assessment
Proceedings from the PACITA 2015 Conference in Berlin

Edited by
Constanze Scherz, Tomáš Michalek, Leonhard Hennen,
Lenka Hebáková, Julia Hahn and Stefanie B. Seitz

Graphic Design by
Iván Barreda and Tomáš Michalek

Cover Photo by
Tomáš Michalek

Printed by
INFORMATORIUM

ISBN 978-80-7333-121-4

Prague: Technology Centre ASCR, 2015

CAPACITIES

European Research Area

This publication was prepared as a part of the framework of the EU-funded
Parliaments and Civil Society in Technology Assessment (PACITA) project.
www.pacitaproject.eu