The Context-Dependence of Citizens' Attitudes and Preferences Regarding Privacy and Security

Michael Friedewald, Marc van Lieshout, Sven Rung, Merel Ooms

M. Friedewald, S. Rung, Fraunhofer Institute for Systems and Innovation Research ISI, Breslauer Straße 48, 76139 Karlsruhe, Germany, e-mail: Michael.friedewald@isi.fraunhofer.de

M. van Lieshout, M. Ooms, The Netherlands Organisation for Applied Science (TNO), Strategy and policy department, P.O. Box 155, 2600 AD Delft, The Netherlands

Abstract This paper considers the relationship between privacy and security and, in particular, the traditional "trade-off" paradigm that argues that citizens might be willing to sacrifice some privacy for more security. Academics have long argued against the trade-off paradigm, but these arguments have often fallen on deaf ears. Based on data gathered in a pan-European survey we discuss which factors determine citizens' perceptions of concrete security technologies and surveillance practices.

Acknowledgments This work was carried out in the project "PRISMS: Privacy and Security Mirrors" co-funded from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement 285399. For more information see: http://prismsproject.eu

Friedewald, Michae et al., "The Context-Dependence of Citizens' Attitudes and Preferences Regarding Privacy and Security", in Serge Gutwirth, et al. (eds.), *Data Protection on the Move: Current Developments in ICT and Privacy/Data Protection*, Springer, Dordrecht, 2016, pp. 51-74.

1. Introduction

The relationship between privacy and security has often been understood as a zero-sum game, whereby any increase in security would inevitably mean a reduction in the privacy enjoyed by citizens. A typical incarnation of this thinking is the all-too-common argument: "If you have got nothing to hide you have got nothing to fear". This 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 surveillance technologies to be useful in terms of security but potentially harmful in terms of privacy.[1] Whilst some people consider privacy and security as intrinsically intertwined conditions where the increase of one inevitably means the decrease of the other. There are also other views: There are those who are very sceptical about surveillance technologies and question whether their implementation can be considered beneficial in any way. Then there are people who do not consider monitoring technologies problematic at all and do not see their privacy threatened in any way by their proliferation. Finally there are those who doubt that surveillance technologies are effective enough in the prevention and detection of crime and terrorisms to justify the infringement of privacy they cause.[2]

Insight in the public understanding of security measures is important for decision makers in industry and politics who are often surprised about the negative public reactions showing that citizens are not willing to sacrifice their privacy for a bit more potential security. On the back of this the PRISMS project aimed to answer *inter alia* the question: When there is no simple trade-off between privacy and security perceptions, what then are the main factors that affect public assessment of the security and privacy implications of specific security technologies, of specific security contexts and of specific security-related surveillance practices?

The PRISMS project has approached this question by conducting a large-scale survey of European citizens. This is, however, 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. For example, privacy and security may be experienced differently in different political and socio-cultural contexts. In this paper, however, our focus will be on the survey results, not their interpretation from different disciplinary perspectives.

2. Measuring people's perceptions of security technologies

Researchers investigating the relationship between privacy and security have to deal with the so-called privacy paradox: It is well known that while European citizens are concerned about how the government and private sector collect data about citizens and consumers, these same citizens seem happy to freely give up personal and private information when they use the

[1] Vincenzo Pavone and Sara Degli Esposti, "Public Assessment of New Surveillance-Oriented Security Technologies: Beyond the Trade-Off between Privacy and Security," *Public Understanding of Science* 21, no. 5 (2012). Daniel J. Solove, *Understanding Privacy* (Cambridge, Mass.: Harvard University Press, 2008).

[2] Reinhard Kreissl et al., "Surveillance: Preventing and Detecting Crime and Terrorism," in *Surveillance in Europe*, ed. David Wright and Reinhard Kreissl (London, New York: Routledge, 2015).

Friedewald, Michae et al., "The Context-Dependence of Citizens' Attitudes and Preferences Regarding Privacy and Security", in Serge Gutwirth, et al. (eds.), *Data Protection on the Move: Current Developments in ICT and Privacy/Data Protection*, Springer, Dordrecht, 2016, pp. 51-74.

Internet. This ”paradox” is not really paradoxical but represents a typical value-action gap, which has been observed in other fields as well.[3]

Measuring privacy and security perceptions thus has to deal with problems similar to ecopsychology at the beginning of the environmental movement in the 1970s: What is the relationship between general values and concrete (environmental) concerns and how do they translate into individual behaviour? In PRISMS we have been inspired by the “theory of planned behaviour” (TPB) that suggests that if people evaluate the suggested behaviour as positive (attitude), and if they think their significant others want them to perform the behaviour (subjective norm), this results in a higher intention and they are more likely to behave in a certain way.[4] TBP is a positivist approach as it assumes that there are rules structuring the way people think and these “social facts”, as Durkheim is calling them, can be verified by scientific observation and experimentation.[5] We are aware of the fact that this assumption has been critised by other epistemological perspectives such as critical school, cultural studies and STS, which are highlighting that attitudes and values may be situationally determined rather than stable dispositions and that a number of context factors may limit individual choice.[6] On the other hand a high correlation of attitudes and subjective norms to behavioural intention, and subsequently to behaviour, has been confirmed in many studies.[7]

Another issue to be considered is that people can (and do) understand concepts such as privacy and security in very different ways, and that they often only have a vague idea how security technologies work and what kind and how much information they collect. Nonetheless people often are voicing (even strong) opinions.

2.1 Operationalization of privacy

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. Although a widely accepted definition of privacy remains elusive, there has been more consensus on a recognition that privacy comprises multiple dimensions, and some privacy theorists have attempted to create taxonomies of privacy intrusions or problems – for instance Debbie Kasper or Daniel Solove.[8] However, the outlining of privacy problems or intrusions does little to provide an overarching framework that would ensure that individuals’ rights are proactively protected.

On the other hand operationalising privacy as a positive right focuses on preventing harms rather than providing redress. Roger Clarke outlined specific elements of individual privacy

[3] E.g. in the context of environmentalism consumers often state a high importance of environmental protection that is not reflect in their actual behaviour. See Anja Kollmuss and Julian Agyeman, "Mind the Gap: Why Do People Act Environmentally and What Are the Barriers to Pro-Environmental Behavior?," *Environmental Education Research* 8, no. 3 (2002).

[4] One of the most successful (and most criticized) application of TPB is the so-called “Technology Acceptance Model” and its extension, the “Unified Theory of Acceptance and Use of Technology”, which simplifies the TPB approach by eliminating the direct consideration of attitudes because they are difficult or impossible to measure. They are very popular methods in computer science assess the acceptance of human computer interface designs. Cf. Viswanath Venkatesh et al., "User Acceptance of Information Technology: Toward a Unified View," *MIS Quarterly* 27, no. 3 (2003); Fred D. Davis, "Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology," ibid.13 (1989).

[5] Emile Durkheim, *The Rules of Sociological Method [1895]*, trans. Steven Lakes (New York et al.: The Free Press, 1982).

[6] Cf. for instance Andrew J. Cook, Kevin Moore, and Gary D. Steel, "Taking a Position: A Reinterpretation of the Theory of Planned Behaviour," *Journal for the Theory of Social Behaviour* 35, no. 2 (2005).

[7] Icek Ajzen and Martin Fishbein, "The Influence of Attitudes on Behavior," in *The Handbook of Attitudes*, ed. Dolores Albarracin, Blair T. Johnson, and Mark P. Zanna (Mahwah, NJ: Erlbaum, 2005).

[8] Debbie V. S. Kasper, "The Evolution (or Devolution) of Privacy," *Sociological Forum* 20, no. 1 (2005); Solove, *Understanding Privacy*.

Friedewald, Michae et al., "The Context-Dependence of Citizens’ Attitudes and Preferences Regarding Privacy and Security", in Serge Gutwirth, et al. (eds.), *Data Protection on the Move: Current Developments in ICT and Privacy/Data Protection*, Springer, Dordrecht, 2016, pp. 51-74.

that ought to be protected. His very popular taxonomy distinguished four types of privacy, but is no longer adequate to capture the range of potential privacy issues, which must be addressed.[9] In PRISMS we are using an extensions of Clarke's typology developed by Finn et al. who suggest seven different types of privacy that ought to be protected and that receive different attention and valuation in practice. Such a detailed taxonomy helps to overcome the problem that privacy is too abstract as a concept and therefore helps to deal with the fact that people can (and do) understand the term in very different ways. The seven types of privacy comprise:[10]

1. *Privacy of the person* encompasses the right to keep body functions and body characteristics (such as genetic codes and biometrics) private. This aspect of privacy also includes non-physical intrusions into the body such as occur with airport body scanners.
2. *Privacy of behaviour* and action includes sensitive issues such as sexual preferences and habits, political activities and religious practices. However, the notion of privacy of personal behaviour concerns activities that happen in public space *and* private space.
3. *Privacy of communication* relates to avoiding the interception of communications, including mail interception, the use of bugs, directional microphones, telephone or wireless communication interception or recording and access to e-mail messages.
4. *Privacy of data and image* includes protecting an individual's data from being automatically available or accessible to other individuals and organisations and that people can "exercise a substantial degree of control over that data and its use".[11]
5. *Privacy of thoughts and feelings* is the right not to share ones thoughts or feelings or to have those thoughts or feelings revealed. Privacy of thought and feelings can be distinguished from privacy of the person, in the same way that the mind can be distinguished from the body.
6. *Privacy of location and space* means that individuals have the right to move about in public or semi-public space without being identified, tracked or monitored. This conception of privacy also includes a right to solitude and a right to privacy in spaces such as the home, the car or the office.
7. *Privacy of association* (including group privacy) is concerned with people's right to associate with whomever they wish, without being monitored.

For the PRISMS survey we have developed a battery of eight questions that are covering all these seven aspects. A factor analysis has shown that all the answers to all these questions are highly correlated and can therefor be grouped into one construct labelled "privacy attitude".[12]

2.2 Operationalization of security

The concept of security is at least as difficult to approach as privacy. Researchers have stated that the "multidimensional nature of security results in both a society and industry that

[9] Roger Clarke, "Introduction to Dataveillance and Information Privacy, and Definitions of Terms," Xamax Consultancy.

[10] Rachel L. Finn, David Wright, and Michael Friedewald, "Seven Types of Privacy," in *European Data Protection: Coming of Age*, ed. Serge Gutwirth, et al. (Dordrecht: Springer, 2013)., p. 7-9

[11] Clarke, "Introduction to Dataveillance and Information Privacy, and Definitions of Terms".

[12] Michael Friedewald et al., "Privacy and Security Perceptions of European Citizens: A Test of the Trade-Off Model," in *Privacy and Identity 2014, IFIP AICT, Vol. 457*, ed. Jan Camenisch, Simone Fischer-Hübner, and Marit Hansen (Heidelberg, Berlin: Springer, 2015).

Friedewald, Michae et al., "The Context-Dependence of Citizens' Attitudes and Preferences Regarding Privacy and Security", in Serge Gutwirth, et al. (eds.), *Data Protection on the Move: Current Developments in ICT and Privacy/Data Protection*, Springer, Dordrecht, 2016, pp. 51-74.

has no clear understanding of a definition for the concept of security. Moreover the current concepts of security are so broad as to be impracticable".[13]

According to Fischer and Green's reference work "security implies a stable, relatively predictable environment in which an individual or group may pursue its ends without disruption or harm and without fear of such disturbance or injury".[14] Such a definition is also picked up in the context of European policy makers. The European Committee on Standardisation's working group 161 defines that "security is the condition (perceived or confirmed) of an individual, a community, and organisation, a societal institution, a state, and their assets (such as goods, infrastructure), to be protected against danger or threats such as criminal activity, terrorism or other deliberate or hostile acts, disasters (natural and man-made)".[15] Security is thus negatively defined as the absence of insecurity. Perfect objective security thus implies the absence of any threat. Even if this was achieved today it remains open to societal negotiations of new threats in the future.

Over the years this view has partly been replaced by that of risk management and loss prevention. The latter does no longer focus on dangers and hazards and replaces them by risks, which have an (un)certainty to occur. They are based on the assumption that risks cannot totally be prevented and damages and losses will occur anyway. The focus of this approach is no longer directed towards the source of the damage but towards the management of the effects with the goal to minimise the adverse effects for those affected.

It is also difficult to delineate the content of "security". 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, organisations, companies and states, 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 any of these perspectives,.

We have identified seven general types of security contexts and the accompanying measures to safeguard and protect these contexts:[16]

1. *Physical security* deals with physical measures designed to safeguard the physical characteristics and properties of systems, spaces, objects and human beings
2. *Socio-economic security* deals with economic measures designed to safeguard the economic system, its development and its impact on individuals.
3. *Radical uncertainty* security deals with measures designed to provide safety from exceptional and rare violence/threats, which are not deliberately inflicted by an external or internal agent, but can still threaten drastically to degrade the quality of life.
4. *Information security* deals with measures designed to protect information and information systems from unauthorized access, use, disclosure, disruption, modification, perusal, inspection, recording or destruction.
5. *Political security* deals with the protection of acquired rights, established institutions/structures and recognised policy choices.
6. *Cultural security* deals with measures designed to safeguard the permanence of traditional schemas of language, culture, associations, identity and religious practices while allowing for changes that are judged to be acceptable

[13] David J. Brooks, "What Is Security: Definition through Knowledge Categorization," *Security Journal* 23, no. 3 (2009).

[14] Robert J. Fischer and Gion Green, *Introduction to Security*, 7th ed. (Amsterdam, Boston: Butterworth-Heinemann, 2004).

[15] European Committee on Standardisation (CEN), BT/WG 161, cited in Carlos Martí Sempere, "The European Security Industry: A Research Agenda," (Berlin: German Institute for Economic Research, 2010).

[16] Monica Lagazio, "The Evolution of the Concept of Security," *The Thinker*, September 2012.

7. *Environmental security* deals with measures designed to provide safety from environmental dangers caused by natural or human processes due to ignorance, accident, mismanagement or intentional design, and originating within or across national borders.

It has also to be taken into account that security can be an individual or a collective issue. As in the case of privacy we have designed two batteries of questions to address the wide spectrum of meanings. Again factor analysis has shown – though not as unambiguously as for privacy – that all the items within the two batteries correlated and can therefor be grouped into two constructs labelled "general security" and "personal security" attitudes. Finally we have shown elsewhere that there is no statistically significant correlation between the security and the privacy attitudes.[17]

2.3 Vignettes as a tool for contextualisation

To address this ambiguity and context dependence of the central concepts the PRISMS survey is working with so called anchoring vignettes that are used when survey respondents may understand survey questions in different ways, due to the abstractness of the presented concepts (privacy, security), their complexity (security technologies and practices) 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.[18]

In PRISMS we have developed eight different vignettes that are covering 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 are mainly covering applications such as the fight against public disorder, criminality and terrorism and additionally some commercial applications. We have also made sure that the vignettes cover virtual as well as physical applications, which are operated by public as well as private sector organisations (see Fig. 1).

[17] Friedewald et al., "Privacy and Security Perceptions of European Citizens: A Test of the Trade-Off Model."

[18] Andrey Pavlov, "Application of the Vignette Approach to Analyzing Cross-Cultural Incompatibilities in Attitudes to Privacy of Personal Data and Security Checks at Airports," in *Surveillance, Privacy, and the Globalization of Personal Information: International Comparisons*, ed. Elia Zureik, et al. (Montreal, Kingston: McGill-Queen's University Press, 2010). Gary King and Jonathan Wand, "Comparing Incomparable Survey Responses: Evaluating and Selecting Anchoring Vignettes " *Political Analysis* 15 (2007).

Friedewald, Michae et al., "The Context-Dependence of Citizens' Attitudes and Preferences Regarding Privacy and Security", in Serge Gutwirth, et al. (eds.), *Data Protection on the Move: Current Developments in ICT and Privacy/Data Protection*, Springer, Dordrecht, 2016, pp. 51-74.

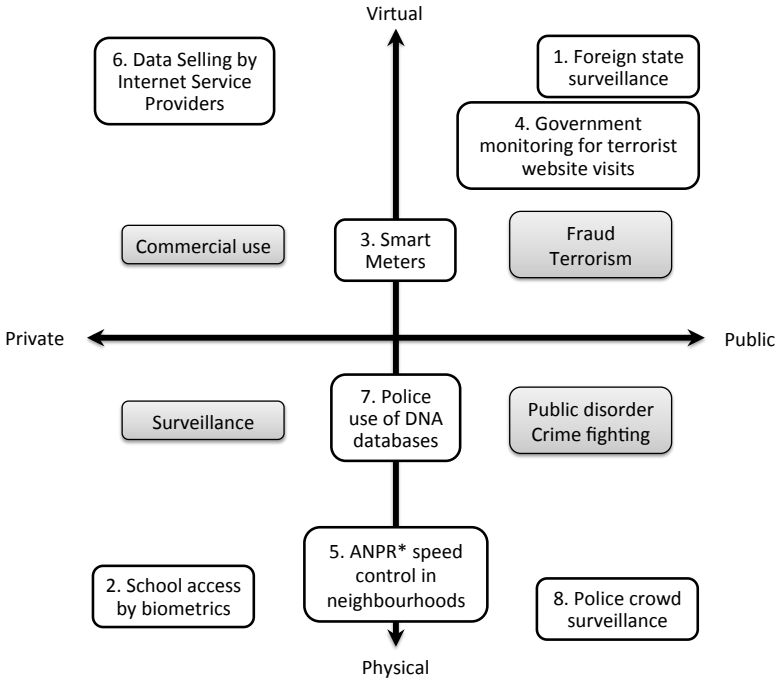


Fig. 1 Classification of the vignettes (*ANPR = Automatic Number Plate Recognition)

The PRISMS vignettes are very short narratives of 50 to 100 words. They have been validated and refined though sixteen focus groups in eight representative EU countries.[19] In this way it was ensured that the vignettes are understood uniformly in different languages and that they do not cause extreme reactions that would conceal the perceptions to be measured. Two of the vignettes also had (slightly) different wording to test if it makes a difference if citizens assess security practices that are directly affecting them or if they are asked to assess a practice in general (a company selling your data vs. a company selling customers' data). In the vignette about police monitoring crowds the situation was slightly varied, in one version surveillance takes place at a football match while in the other version participants of a political demonstration are monitored. For each of the vignettes citizens were asked two identical questions (the complete set of vignettes and questions can be found in the annex).

- *Question 1: "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", and
- *Question 2: "Do you think the [actor] doing this…*
  - *… helps to protect people's rights and freedoms*
  - *… threatens people's rights and freedoms*
  - *… has no impact on people's rights and freedoms"*
  - (don't know)

[19] Carolina Haita and Daniel Cameron, "Privacy or Security: A False Choice? European Citizens' Perceptions of Privacy, Personal Data, Surveillance and Security," *Understanding Society (*2014).

2.4. Data collection

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[20] (27,195 in total) amongst a representative sample (based on age, gender, work status and region) within each country (see table 1). For economic reasons each interviewee was presented only four randomly selected vignettes, resulting in approx. 13,600 responses for each vignette (500 per country).[21]

Table 1 Survey composition

		Responses	Per cent
Total		27.195	100 %
Gender	Male	12.566	46 %
	Female	14.629	54 %
Age	16-24	2.793	10 %
	25-34	4.006	15 %
	35-44	4.704	17 %
	45-54	4.960	18 %
	55-59	2.435	9 %
	60-64	2.305	8 %
	65-74	3.643	13 %
	75+	2.294	8 %
Work status	Working	13.775	51 %
	Unemployed or in education	5.788	21 %
	Retired	7.209	27 %
Geographic area[22]	Big city	6.535	24 %
	Suburban area or small city	12.833	47 %
	Rural area	7.748	28 %

3. Descriptive results

In an introductory question we asked citizens to what extent they think that an institutional actor should or should not implement the given security practice. The answers were measured on a 5-point Likert-scale ranging from „definitely should“ to „definitely should not“ (see Fig. 2).

[20] Croatia had not acceded to the EU at the time of the project planning.

[21] For those vignettes with alternative wording the sample was halved again to 6,800 responses in total or 250 responses per country.

[22] Self-assessment by interviewees (answer categories: 1a big city; 2a suburbs or outskirts of a big city, 2b town or small city, 3a country village, 3b farm or home in the countryside).

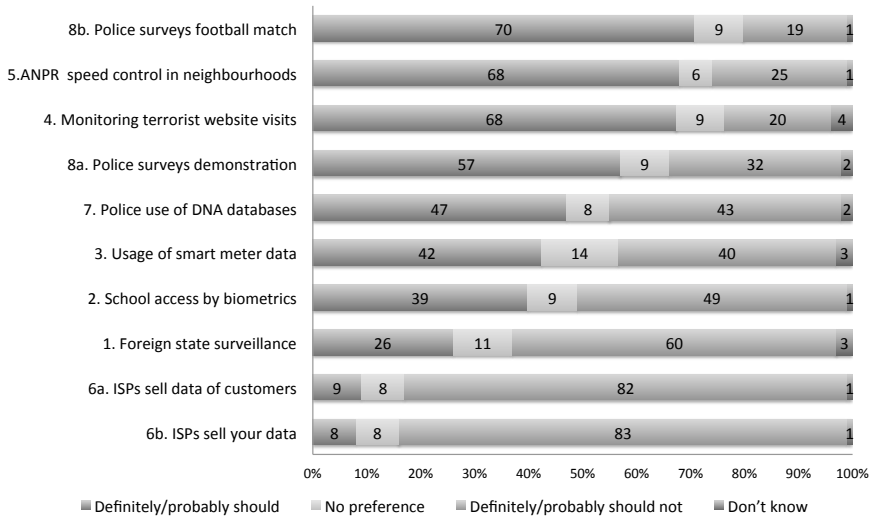


Fig. 2 Question 1. To what extent, if at all, do you think that [an institution] should or should not…?

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", "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 "ISPs selling customer data" should not take place.

The rest of the vignettes, however, did not produce equally clear results. While still a majority of respondents were 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.

In the second question citizens were asked if the practice described in a vignette is having an impact of people's rights and freedoms. This question was intentionally formulated in general terms since security practices do not only have an impact on the right to data protection but can also include other rights and freedoms such as freedom of decision, freedom of association or freedom of movement that citizens would not automatically regard as part of an extended privacy concept that is used in the PRISMS survey (cf. section 2.1).

Again the survey shows a wide spectrum of differences between the vignettes though the results are more evident than in the previous question (see Fig. 3). The first observation is that in all but one cases only a minority of the respondents (between 12 and 24 per cent) think that the described practice is helping to protect people's rights and freedoms.

On the other side of the spectrum citizens think that the practices describe in the vignettes about „ISPs selling customer data" are having the biggest negative impact on their personal freedoms. Many other vignettes, however, are not regarded as very momentous. For these vignettes only a minority (between 19 and 34 per cent) see a threat for people's rights and freedoms. A particularly interesting case is again the vignette on smart meters with almost 40 per cent of positive and 40 per cent of negative answers. It shows that there is no societal consensus about this technology yet and that citizens often do not trust that private companies operate responsibly towards their customers' interests (from those interviewees that think that energy companies should not collect smart meter data almost 50 per cent also stated that they do not trust businesses). Finally the assessment of „foreign state surveillance" shows that a majority of citizens feels this practice is harming, and only 14 per cent think it is helping

protect people's freedom. With ten per cent this vignette is having the highest number of „don't know" answers.

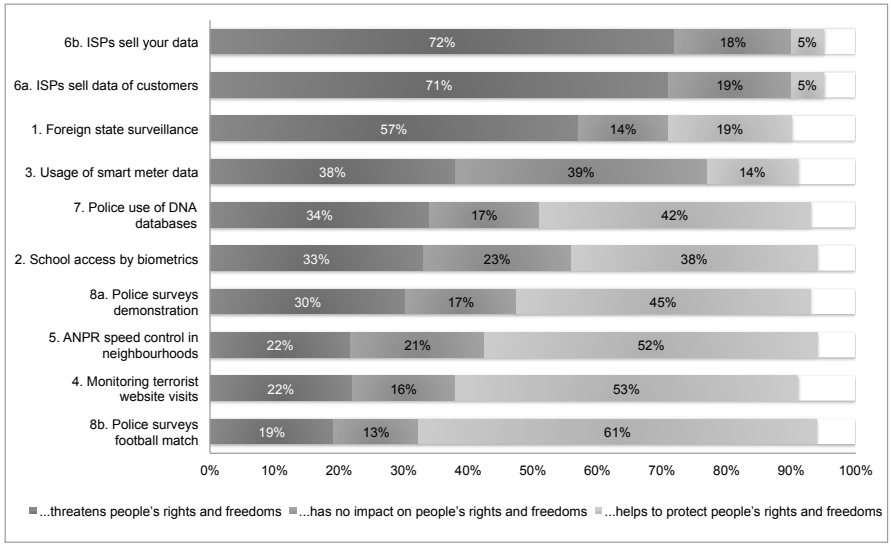


Fig. 3 Question 2. Do you think the _____ doing this [impacts people's rights and freedoms]?

All in all, European citizens are rather critical of surveillance oriented security measures in the sense that their assessment differs widely depending on the context, purpose and implementation of a specific measure.

Already on the basis of the descriptive statistics 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 intelligences 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 rather 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.

4. Determinant of citizen's acceptance of specific surveillance oriented security technologies

Elsewhere we have already demonstrated that there is no strong correlation between the privacy and security constructs and thus no simple trade-off between security and privacy attitudes of European citizens.[23] In the following section we are presenting the analysis of a selection of factors that determine citizens' assessment of the systems/practices outlined in the vignettes. It makes clear that there is no simple impact of specific factors in the assessment of concrete cases of security technologies and surveillance practices.

[23] Friedewald et al., "Privacy and Security Perceptions of European Citizens: A Test of the Trade-Off Model."

Friedewald, Michae et al., "The Context-Dependence of Citizens' Attitudes and Preferences Regarding Privacy and Security", in Serge Gutwirth, et al. (eds.), *Data Protection on the Move: Current Developments in ICT and Privacy/Data Protection*, Springer, Dordrecht, 2016, pp. 51-74.

4.1 Methodology

To answer the research questions and to empirically test our theoretical assumptions we conducted a series of ordered logistic regressions. The introductory question for each vignette was defined as the dependent variable and regressed by two different sets of independent variables. The list of independent categorical variables included 'age', 'gender', 'education', 'political orientation', 'level of privacy activism' [24] and 'experience with privacy infringements'.[25] For the virtual surveillance cases we used 'intensity of Internet use' as an additional variable. For the physical surveillance cases 'work status' and 'living environment' were added.[26]

Table 2 is a simple overview of our results. The first column shows the independent variables. The cells indicate the results of the regression analysis for all 8 (10) vignettes. We have not used numerical results as these would not be directly comparable across vignettes. Instead, we have opted for a visual indication of the direction and strength of the correlation:

- A single plus mark (+) indicates that respondents to which the marked factor applies are up to twice as likely to accept the respective surveillance practice as the reference group.
- A double plus mark (++) indicates that respondents to which the marked factor applies are more than twice as likely to accept the respective surveillance practice as the reference group.
- A single minus mark (-) indicates that that respondents to which the marked factor applies are between half as likely and as likely, to accept the respective surveillance practice as the reference group
- The double minus mark (--) indicates that respondents to which the marked factor applies are less than half as likely to accept the respective surveillance practice as the reference group.
- Finally, a grey cell shading indicates of a correlation of statistical significance ($p<0.05$). The variables relating to the cells shaded grey can be assumed to have a "significant influence" on the vignette.[27]

For instance: The likelihood that young adults (16-34) assess the practice of data selling by ISPs positively ("Actors should be doing this") has a [++] and is thus more than twice as high as for the reference group of the older adults (60+). For middle age (34-59) this likelihood [+] is still higher than for reference group of older adults but lower than for the young adults. In summary this means that the younger people are the more positive they are about this practice.

[24] To measure "privacy activism" we asked citizens if they had actively taken steps to protect their personal information. Answer categories included: refuse to give information, ask company to delete information, ask company not to disclose information, deliberatively give incorrect information etc. Citizens who answered they had taken at least two of the given possibilities were considered as "privacy active".

[25] Some of these items are, however, themselves determined by basic control variables (e.g. age or education level).

[26] Consequently the respective cells in the table are empty (n/a).

[27] More details on methodology can be found in Michael Friedewald et al., "Report on the Analysis of Survey Results," (2015).

Table 2: Factors influencing the personal perception of different security practices

Factor \ Vignette	Virtual surveillance					Physical surveillance				
	Public ---------->				Private	Public ---------->				Private
	1. Foreign government surveillance	4. Monitoring terrorist website visits	3. Usage of smart meter data	6b. ISPs sell your data	6a. ISPs sell data of customers	8b. Police surveys football match	8a. Police surveys demon-stration	5. ANPR speed control	7. Police use of DNA databases	2. School access by biometrics
Avg. acceptance level	3,6	2,28	2,92	4,27	4,22	2,28	2,72	2,17	2,97	3,26
More worried about personal security	+	++	+	++	+	++	++	++	++	++
More worried about privacy	--	-	--	-	--	--	--	--	--	--
High trust in institutions	+	+	++	++	++	+	++	++	+	+
Young adults (16-34)[a]	+	-	++	++	++	-	-	+	+	+
Middle age (35-59)[a]	+	-	+	+	+	-	-	+	+	+
Male[b]	-	-	+	+	+	+	+	-	+	-
Secondary education 1†[c]	+	+	-	+	+	+	+	+	+	+
Secondary education 2 and post secondary education†[c]	+	+	-	-	+	+	+	+	+	+
Unemployed and in education[d]	n/a	n/a	n/a	n/a	n/a	-	+	-	-	+
No Internet use[e]	+	+	+	n/a	++	n/a	n/a	n/a	n/a	n/a
Occasional Internet use‡[e]	-	-	-	+	+	n/a	n/a	n/a	n/a	n/a
Living in big cities[f]	n/a	n/a	n/a	n/a	n/a	+	+	+	-	+
Living in suburbs/small cities[f]	n/a	n/a	n/a	n/a	n/a	+	-	-	-	-
Political left[g]	-	-	-	-	-	-	--	-	-	-
Political center[g]	-	-	-	-	-	-	-	-	-	-
No privacy activism[h]	+	+	+	+	+	-	+	+	+	+
Low privacy activism[h]	+	-	+	+	-	+	-	+	-	+
Privacy never invaded	-	-	-	+	-	+	-	+	-	+

Avg. acceptance level: Scale from 1 (definitely should) to 5 (definitely should not)
Correlations and significance: ++ strong positive correlation / + positive correlation / - negative correlation / -- strong negative correlation. Grey-shaded cells indicate a significant correlations ($p<0.05$)
Reference groups: a Old age (60+) / b female / c Higher education (ISCED level >5) / d Retired / e Regular Internet use (once per week or more) / f Rural area (country villages, farms or countryside) / g Political right / h High privacy activism (people who have actively protected their privacy more than one time)
† Secondary education stage 1: ISCED-11 levels 1-2; Secondary education stage 2 and post secondary education: ISCED-11 levels 3-5
‡ Occasional Internet use: Less than once per week.

4.2 Results

The analysis shows that there are only a few factors, which play an important role in all cases. Not surprisingly these include the constructs describing citizens' *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*.[28] 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 recent discussions about the importance of trust for the assessment of risks and benefits and the acceptability of technologies.[29] 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,

[28] The importance of trust (or distrust) has been a familiar factor in explaining privacy attitudes since the earliest surveys by Alan Westin. See for instance: Susannah Fox et al., "Trust and Privacy Online: Why Americans Want to Rewrite the Rules," (Washington, DC: Pew Internet & American Life Project, 2001); Stephen T. Margulis, Jennifer A. Pope, and Aaron Lowen, "The Harris-Westin Index of General Concern About Privacy: An Exploratory Conceptual Replication," in *Surveillance, Privacy, and the Globalization of Personal Information: International Comparisons*, ed. Elia Zureik, et al. (Montreal, Kingston: McGill-Queen's University Press, 2010); Wainer Lusoli et al., *Pan-European Survey of Practices, Attitudes and Policy Preferences as Regards Personal Identity Data Management*, JRC Scientific and Policy Report EUR 25295 (Luxembourg: Publication Office of the European Union, 2012).

[29] Timothy C. Earle and George Cvetkovich, *Social Trust: Toward a Cosmopolitan Society* (Westport, Conn.: Praeger, 1995).

Friedewald, Michae et al., "The Context-Dependence of Citizens' Attitudes and Preferences Regarding Privacy and Security", in Serge Gutwirth, et al. (eds.), *Data Protection on the Move: Current Developments in ICT and Privacy/Data Protection*, Springer, Dordrecht, 2016, pp. 51-74.

although some studies seem to suggest that this is not always the case.[30]

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 public 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.[31] The assumption that this also leads to a more critical assessment of surveillance practices by youngsters 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. Based on qualitative research Pavone et al. and others suggest that a possible explanation might be that older citizens who made experience with European authoritarian regimes, are more distrustful, whereas younger people, who had not lived in surveillance states are less concerned.[32]

---

[30] Richard J. Bord and Robert E. O'Connor, "Determinants of Risk Perceptions of a Hazardous Waste Site," *Risk Analysis* 12 (1992).

[31] Mary Madden et al., "Teens, Social Media, and Privacy," (Washington, DC: Pew Research Center, 2013); Wainer Lusoli et al., "Young People and Emerging Digital Services: An Exploratory Survey on Motivations, Perceptions and Acceptance of Risks," (Luxembourg: Office for Official Publications of the European Communities, 2009).

[32] Vincenzo Pavone, Sara Degli Esposti, and Elvira Santiago, "Key Factors Affecting Public Acceptance and Acceptability of SOSTs," (The SurPRISE consortium, 2015), p. 139. Iván Székely, "Changing Attitudes in a Changing Society? Information Privacy in Hungary, 1989-2006," in *Surveillance, Privacy, and the Globalization of Personal Information: International Comparisons*, ed. Elia Zureik, et al. (Montreal, Kingston: McGill-Queen's University Press, 2010).

Friedewald, Michae et al., "The Context-Dependence of Citizens' Attitudes and Preferences Regarding Privacy and Security", in Serge Gutwirth, et al. (eds.), *Data Protection on the Move: Current Developments in ICT and Privacy/Data Protection*, Springer, Dordrecht, 2016, pp. 51-74.

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 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 vignette on "school access by biometrics". On the other side, their support for the police use of DNA databases is 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.[33] More important than the fear of crime seems to be the perceived usefulness and effectiveness of concrete measures.[34]

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.

It could not be shown that work status, intensity of Internet use and experience with privacy infringements is influencing citizens' assessment of surveillance based security technologies in a significant way.

---

[33] Kristof Verfaillie et al., "Public Assessments of the Security/Privacy Trade-Off: A Criminological Conceptualization," (PRISMS Project, 2013).

[34] Kreissl et al., "Surveillance: Preventing and Detecting Crime and Terrorism."

Friedewald, Michae et al., "The Context-Dependence of Citizens' Attitudes and Preferences Regarding Privacy and Security", in Serge Gutwirth, et al. (eds.), *Data Protection on the Move: Current Developments in ICT and Privacy/Data Protection*, Springer, Dordrecht, 2016, pp. 51-74.

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.

6. Discussion of results and 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 the essential factor for the acceptability of a security practice. The important role of trust, in people, institutions as well as the whole societal environment, is regularly confirmed in surveys.[35] The SurPRISE project, for instance, confirmed clearly that "the more people trust scientific and political institutions … the more acceptable a technology would be." In their explanatory model institutional trust is the strongest positive influence factor for acceptability of surveillance oriented security technologies.[36] The PACT project on the other side stresses the strong impact that distrust has on the likelihood that citizens' reject a given security measure.[37]
- Openness has a positive effect on the willingness of citizens to accept security practices. This can be understood on different levels:

[35] Baldo Blinkert, "Unsicherheitsbefindlichkeit als ‚sozialer Tatbestand'. Kriminalitätsfurcht und die Wahrnehmung von Sicherheit und Unsicherheit in Europa," *Monatsschrift für Kriminologie und Strafrechtsreform* 93, no. 2 (2010); Fox et al., "Trust and Privacy Online: Why Americans Want to Rewrite the Rules."; Dina Hummelsheim, "Subjektive Unsicherheit und Lebenszufriedenheit in Deutschland: Empirische Ergebnisse einer repräsentativen Bevölkerungsbefragung," in *Sichere Zeiten? Gesellschaftliche Dimensionen der Sicherheitsforschung*, ed. Peter Zoche, Stefan Kaufmann, and Harald Arnold (Münster: Lit Verlag, 2015).

[36] Pavone, Esposti, and Santiago, "Key Factors Affecting Public Acceptance and Acceptability of SOSTs," p. 135-6.

[37] Sunil Patil et al., "Public Perception of Security and Privacy: Results of the Comprehensive Analysis of PACT's Pan-European Survey," (Cambridge, UK: RAND Corporation, 2014), p. v.

  - Citizens tend to accept security practices when they are convinced that a security measure is necessary, proportional and effective.
  - This is easier when a security practice is embedded in a context that citizens are familiar with and where they understand who is surveying whom and how.
  - As a result the surveillance activity should not be covert but perceivable for the citizen and communicated in a responsible way by the operator.
  - Understanding and acceptance is also a question of proper knowledge and education - though not only in one way. While education contributes to understanding technicalities and complexity of a security practices it also drives critical reflections.[38]

- All these factors also involve an inherent risk for manipulation, since a security practice can be designed to create false trust among citizens to be accepted.
- On the downside it can also be stated that many citizens do not care about surveillance that does not negatively affect them personally but only others.[39]

For the design and introduction of security measures it is useful to consider some of the main determinants, since poorly designed measures can consume significant resources without achieving either security or privacy while others can increase security at the expense of privacy. However, since there is no natural trade-off between privacy and security, carefully designed solutions can benefit both privacy and security.

Law enforcement and government officials often heavily weight security.[40] On the other hand we have shown in our analysis of the

[38] SurPRISE also confirmed most these observations. Cf. Pavone, Esposti, and Santiago, "Key Factors Affecting Public Acceptance and Acceptability of SOSTs," p. 154-5.

[39] SurPRISE concludes “the more participants perceive SOSTs to be targeted at others rather than themselves, the more likely they are to find a SOST more acceptable“. Ibid., p. 138.

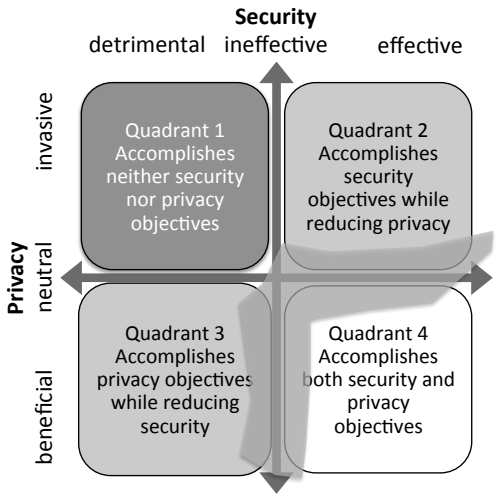
[40] It is quite telling that in the most recent Eurobarometer study on Europeans’ attitudes towards security the focus is strongly on terrorism, cybercrime, organized crime and insecurity of the EU’s external borders trustworthiness of security agencies and their measures are not even mentioned. Cf. TNS Opinion & Social, "Europeans' Attitudes Towards Security," (Brussels, 2015).

Friedewald, Michae et al., "The Context-Dependence of Citizens’ Attitudes and Preferences Regarding Privacy and Security", in Serge Gutwirth, et al. (eds.), *Data Protection on the Move: Current Developments in ICT and Privacy/Data Protection*, Springer, Dordrecht, 2016, pp. 51-74.

vignettes that citizens' opinions on security measures vary, and are influenced by some crucial factors. Apart from trust in the operating agency or company we could observe mainly four different types of reactions (cf. Fig. 4):

- Citizens may consider a measure as useless to enhance security, and at the same time invasive for their privacy (Quadrant 1). Such a situation has to be absolutely avoided.
- Citizens may consider a measure useless to enhance security but with no risk for their privacy (Quadrant 3)
- Citizens may consider a measure as useful in terms of security, but privacy invasive (Quadrant 2).
- Finally, citizens may consider a measure both useful to increase security and with no risk for their privacy (Quadrant 4).

Fig. 4: Mapping of the perceived risk-benefit for privacy and security (based on Conti et al. 2014)



.

As Fig. 4 classifies citizens' reactions it does not (always) have to reflect the real effectiveness of a security measure and its real impact on privacy. Considering the importance of trust for the acceptability and acceptance the responsible parties should aim to reconcile the perceived and real impacts. Potential for conflicts can be mainly found at the border to quadrants 2 and 3 where citizens fear an

Friedewald, Michae et al., "The Context-Dependence of Citizens' Attitudes and Preferences Regarding Privacy and Security", in Serge Gutwirth, et al. (eds.), *Data Protection on the Move: Current Developments in ICT and Privacy/Data Protection*, Springer, Dordrecht, 2016, pp. 51-74.

invasion of their privacy or perceive a technology as ineffective.[41] The diagram represents a logical ordering of responses of citizens towards security and privacy measures rather than being the result of empirical study. These responses are generally based upon perceptions rather than rational assessments. They are influenced by a multitude of factors as we found them in the survey. Trust in institutions is one, the perceived self-interest is another, the measure being overt or covert a potential third. In that sense the diagram quite neatly presents a kind of heuristics for elaborating decision-making processes that try to overcome the barriers we sketch (the boundaries between the quadrants).

Especially for these cases PRISMS has developed a participatory and discursive technique[42] that can help decision-makers in industry, public authorities and politics to implement security measures, which raise fewer concerns in the population and are thus more acceptable along the lines stated in many policy documents.[43]

Appendix: 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

[41] Pavone, Esposti, and Santiago, "Key Factors Affecting Public Acceptance and Acceptability of SOSTs."; Gregory Conti, Lisa Shay, and Woodrow Hartzog, "Deconstructing the Relationship between Privacy and Security," *IEEE Technology and Society Magazine* 33, no. 2 (2014).

[42] As the empirical basis PRISMS has defined 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. Cf. Friedewald et al., "Report on the Analysis of Survey Results."; Marc van Lieshout, Anne Fleur van Veenstra, and David Barnard- Wills, "The PRISMS Decision Support System," (2015).

[43] The most notable is maybe the European Union's "Stockholm programme" that states "[t]he challenge will be to ensure respect for fundamental freedoms and integrity while guaranteeing security in Europe" European Council, "The Stockholm Programme – an Open and Secure Europe Serving and Protecting the Citizens," *Official Journal of the European Union*, 4.5.2010 2010, p. 4.

Friedewald, Michae et al., "The Context-Dependence of Citizens' Attitudes and Preferences Regarding Privacy and Security", in Serge Gutwirth, et al. (eds.), *Data Protection on the Move: Current Developments in ICT and Privacy/Data Protection*, Springer, Dordrecht, 2016, pp. 51-74.

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 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 (ANPR) systems, which identify and track all vehicles and calculate their average speed. This allows those who drive too fast to be prosecuted.

6. ISP Data

Friedewald, Michae et al., "The Context-Dependence of Citizens' Attitudes and Preferences Regarding Privacy and Security", in Serge Gutwirth, et al. (eds.), *Data Protection on the Move: Current Developments in ICT and Privacy/Data Protection*, Springer, Dordrecht, 2016, pp. 51-74.

Companies offering services on the Internet want to sell information about [a) your b) 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, helicopters and drones, phone tapping, and try to find people on social media.

Version 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.

References

Ajzen, Icek, and Martin Fishbein. "The Influence of Attitudes on Behavior." In *The Handbook of Attitudes*, edited by Dolores Albarracin, Blair T. Johnson and Mark P. Zanna, 173-221. Mahwah, NJ: Erlbaum, 2005.

Friedewald, Michae et al., "The Context-Dependence of Citizens' Attitudes and Preferences Regarding Privacy and Security", in Serge Gutwirth, et al. (eds.), *Data Protection on the Move: Current Developments in ICT and Privacy/Data Protection*, Springer, Dordrecht, 2016, pp. 51-74.

Blinkert, Baldo. "Unsicherheitsbefindlichkeit als ‚sozialer Tatbestand'. Kriminalitätsfurcht und die Wahrnehmung von Sicherheit und Unsicherheit in Europa." *Monatsschrift für Kriminologie und Strafrechtsreform* 93, no. 2 (2010): 106-25.

Bord, Richard J. , and Robert E. O'Connor. "Determinants of Risk Perceptions of a Hazardous Waste Site." *Risk Analysis* 12 (1992): 411-16.

Brooks, David J. "What Is Security: Definition through Knowledge Categorization." *Security Journal* 23, no. 3 (2009): 225-39.

Clarke, Roger "Introduction to Dataveillance and Information Privacy, and Definitions of Terms." Chapman, Australia: Xamax Consultancy, 7 August 2006. http://www.rogerclarke.com/DV/Intro.html.

Conti, Gregory, Lisa Shay, and Woodrow Hartzog. "Deconstructing the Relationship between Privacy and Security." *IEEE Technology and Society Magazine* 33, no. 2 (Summer 2014): 28-30.

Cook, Andrew J., Kevin Moore, and Gary D. Steel. "Taking a Position: A Reinterpretation of the Theory of Planned Behaviour." *Journal for the Theory of Social Behaviour* 35, no. 2 (2005): 143-54.

Davis, Fred D. "Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology." *MIS Quarterly* 13, no. 3 (1989): 319-39.

Durkheim, Emile. *The Rules of Sociological Method [1895]*. Translated by Steven Lakes. New York et al.: The Free Press, 1982.

Earle, Timothy C., and George Cvetkovich. *Social Trust: Toward a Cosmopolitan Society*. Westport, Conn.: Praeger, 1995.

European Council. "The Stockholm Programme – an Open and Secure Europe Serving and Protecting the Citizens." *Official Journal of the European Union* C115, 4.5.2010, 1-38

Finn, Rachel L., David Wright, and Michael Friedewald. "Seven Types of Privacy." In *European Data Protection: Coming of Age*, edited by Serge Gutwirth, Ronald Leenes, Paul De Hert and Yves Poullet, 3-32. Dordrecht: Springer, 2013.

Fischer, Robert J., and Gion Green. *Introduction to Security*. 7th ed. Amsterdam, Boston: Butterworth-Heinemann, 2004.

Fox, Susannah, Lee Rainie, John Horrigan, Amanda Lenhart, Tom Spooner, and Cornelia Carter. "Trust and Privacy Online: Why Americans Want to Rewrite the Rules." Washington, DC: Pew Internet & American Life Project, 2001. http://www.pewinternet.org/files/old-media//Files/Reports/2000/PIP_Trust_Privacy_Report.pdf.pdf

Friedewald, Michael, Marc van Lieshout, Sven Rung, Merel Ooms, and Jelmer Ypma. "Privacy and Security Perceptions of European Citizens: A Test of the Trade-Off Model." In *Privacy and Identity 2014, IFIP AICT, Vol. 457*, edited by Jan Camenisch, Simone Fischer-Hübner and Marit Hansen, 39-53. Heidelberg, Berlin: Springer, 2015.

———. "Report on the Analysis of Survey Results." PRISMS Project, Deliverable 10.1, 2015. http://prismsproject.eu

Haita, Carolina, and Daniel Cameron. "Privacy or Security: A False Choice? European Citizens' Perceptions of Privacy, Personal Data, Surveillance and Security." *Understanding Society*, July 2014, 12-16.

Hummelsheim, Dina. "Subjektive Unsicherheit und Lebenszufriedenheit in Deutschland: Empirische Ergebnisse einer repräsentativen Bevölkerungsbefragung." In *Sichere Zeiten?*

Friedewald, Michae et al., "The Context-Dependence of Citizens' Attitudes and Preferences Regarding Privacy and Security", in Serge Gutwirth, et al. (eds.), *Data Protection on the Move: Current Developments in ICT and Privacy/Data Protection*, Springer, Dordrecht, 2016, pp. 51-74.

Gesellschaftliche Dimensionen der Sicherheitsforschung, edited by Peter Zoche, Stefan Kaufmann and Harald Arnold. Münster: Lit Verlag, 2015.

Kasper, Debbie V. S. "The Evolution (or Devolution) of Privacy." *Sociological Forum* 20, no. 1 (1 March 2005): 69-92.

King, Gary, and Jonathan Wand. "Comparing Incomparable Survey Responses: Evaluating and Selecting Anchoring Vignettes ". *Political Analysis* 15 (2007): 46-66.

Kollmuss, Anja, and Julian Agyeman. "Mind the Gap: Why Do People Act Environmentally and What Are the Barriers to Pro-Environmental Behavior?". *Environmental Education Research* 8, no. 3 (2002): 239-60.

Kreissl, Reinhard, Clive Norris, Marija Krlic, Leroy Groves, and Anthony Amicelle. "Surveillance: Preventing and Detecting Crime and Terrorism." In *Surveillance in Europe*, edited by David Wright and Reinhard Kreissl, 150-210. London, New York: Routledge, 2015.

Lagazio, Monica. "The Evolution of the Concept of Security." *The Thinker*, September 2012, 36-43.

van Lieshout, Marc, Anne Fleur van Veenstra, and David Barnard- Wills. "The PRISMS Decision Support System." PRISMS Preoject, Deliverable 10.2, 2015. http://prismsproject.eu

Lusoli, Wainer, Margherita Bacigalupo, Francisco Lupiañez, Norberto Andrade, Shara Monteleone, and Ioannis Maghiros. *Pan-European Survey of Practices, Attitudes and Policy Preferences as Regards Personal Identity Data Management*. JRC Scientific and Policy Report EUR 25295, Luxembourg: Publication Office of the European Union, 2012.

Lusoli, Wainer, Caroline Miltgen, Ramón Compañó, and Ioannis Maghiros. *Young People and Emerging Digital Services: An Exploratory Survey on Motivations, Perceptions and Acceptance of Risks*. IPTS Technical Report EUR 23765 EN, Luxembourg: Office for Official Publications of the European Communities, 2009.

Madden, Mary, Amanda Lenhart, Sandra Cortesi, Urs Gasser, Maeve Duggan, Aaron Smith, and Meredith Beaton. "Teens, Social Media, and Privacy." Washington, DC: Pew Research Center, 2013. http://pewinternet.org/Reports/2013/Teens-Social-Media-And-Privacy.aspx

Margulis, Stephen T., Jennifer A. Pope, and Aaron Lowen. "The Harris-Westin Index of General Concern About Privacy: An Exploratory Conceptual Replication." In *Surveillance, Privacy, and the Globalization of Personal Information: International Comparisons*, edited by Elia Zureik, L. Lynda Harling Stalker, Emily Smith, David Lyon and Yolande E. Chan, 91-109. Montreal, Kingston: McGill-Queen's University Press, 2010.

Martí Sempere, Carlos. *The European Security Industry: A Research Agenda*. Economics of Security Working Paper 29. Berlin: German Institute for Economic Research, February 2010.

Patil, Sunil, Bhanu Patruni, Hui Lu, Fay Dunkerley, James Fox, Dimitris Potoglou, and Neil Robinson. "Public Perception of Security and Privacy: Results of the Comprehensive Analysis of PACT's Pan-European Survey." PACT Project, Deliverable 4.2, Cambridge, UK: RAND Corporation, 2014. http://www.rand.org/content/dam/rand/pubs/research_reports/RR700/RR704/RAND_RR704.pdf

Pavlov, Andrey. "Application of the Vignette Approach to Analyzing Cross-Cultural Incompatibilities in Attitudes to Privacy of Personal Data and Security Checks at Airports." In *Surveillance, Privacy, and the Globalization of Personal Information: International Comparisons*, edited by Elia Zureik, L. Lynda Harling Stalker, Emily Smith, David Lyon and Yolande E. Chan, 31-45. Montreal, Kingston: McGill-Queen's University Press, 2010.

Friedewald, Michae et al., "The Context-Dependence of Citizens' Attitudes and Preferences Regarding Privacy and Security", in Serge Gutwirth, et al. (eds.), *Data Protection on the Move: Current Developments in ICT and Privacy/Data Protection*, Springer, Dordrecht, 2016, pp. 51-74.

Pavone, Vincenzo, and Sara Degli Esposti. "Public Assessment of New Surveillance-Oriented Security Technologies: Beyond the Trade-Off between Privacy and Security." *Public Understanding of Science* 21, no. 5 (July 2012): 556-72.

Pavone, Vincenzo, Sara Degli Esposti, and Elvira Santiago. "Key Factors Affecting Public Acceptance and Acceptability of SOSTs." SurPRISE project, Deliverable 2.4, 2015. http://surprise-project.eu/wp-content/uploads/2015/02/SurPRISE-D24-Key-Factors-affecting-public-acceptance-and-acceptability-of-SOSTs-c.pdf

Solove, Daniel J. *Understanding Privacy*. Cambridge, Mass.: Harvard University Press, 2008.

Székely, Iván. "Changing Attitudes in a Changing Society? Information Privacy in Hungary, 1989-2006." In *Surveillance, Privacy, and the Globalization of Personal Information: International Comparisons*, edited by Elia Zureik, L. Lynda Harling Stalker, Emily Smith, David Lyon and Yolande E. Chan, 150-70. Montreal, Kingston: McGill-Queen's University Press, 2010.

TNS Opinion & Social. *Europeans' Attitudes Towards Security*. Special Eurobarometer 432, Brussels, 2015.

Venkatesh, Viswanath, Michael G. Morris, Gordon B. Davis, and Fred D. Davis. "User Acceptance of Information Technology: Toward a Unified View." *MIS Quarterly* 27, no. 3 (September 2003): 425-78.

Verfaillie, Kristof, Evelien van den Herrewegen, Jenneke Christiaens, and Serge Gutwirth. "Public Assessments of the Security/Privacy Trade-Off: A Criminological Conceptualization." PRISMS Project, Deliverable 4.1 2013. http://prismsproject.eu

Friedewald, Michae et al., "The Context-Dependence of Citizens' Attitudes and Preferences Regarding Privacy and Security", in Serge Gutwirth, et al. (eds.), *Data Protection on the Move: Current Developments in ICT and Privacy/Data Protection*, Springer, Dordrecht, 2016, pp. 51-74.