Modelling the Relationship Between Privacy and Security Perceptions and the Acceptance of Surveillance Practices

Michael Friedewald[1(✉)], Marc van Lieshout[2], and Sven Rung[1]

[1] Fraunhofer Institute for Systems and Innovation Research ISI, Breslauer Straße 48, 76139 Karlsruhe, Germany
{michael.friedewald,sven.rung}@isi.fraunhofer.de
[2] The Netherlands Organisation for Applied Science (TNO), Strategy and Policy Department, P.O. Box 155, 2600 AD Delft, The Netherlands
Marc.vanLieshout@tno.nl

Abstract. The relationship between privacy and security is often but falsely understood as a zero-sum game, whereby more security can only be achieved by sacrifice of privacy. Since this has been proven as too simplistic this chapter explores what factors are influencing people's perceptions of privacy and security in the context of security-oriented surveillance practices. We are presenting a model showing that structural elements such as trust in the institutions that are implementing and operating surveillance systems are crucial for the acceptability while individual factors such as age, gender or region of living are less important than often assumed.

Keywords: Privacy · Public opinion · Security · Trade-off

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 [23,25]. 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

D. Aspinall et al. (Eds.): Privacy and Identity 2015, IFIP AICT 476, pp. 1–18, 2016.
DOI: 10.1007/978-3-319-41763-9_1

way by their proliferation. Finally there are those who doubt that surveillance technologies are effective enough in the prevention and detection of crime and terrorism to justify the infringement of privacy they cause [17].

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 the perception and finally acceptance 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. In [12] we have shown that privacy and security attitudes of European citizens are largely independent from one another. Now we are exploring what factors are influencing citizens' perception towards surveillance-based security practices. 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 chapter, however, our focus will be on the survey results, not their interpretation from different disciplinary perspectives.

2 Theoretical Approach

Researchers investigating the relationship between privacy and security have to deal with the so-called privacy paradox [8]: 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 Internet. This "paradox" is not really paradoxical but represents a typical value-action gap, which has been observed in other fields as well [12].[1]

2.1 Social Facts

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 (Fig. 1).

[1] E.g. in the context of environmentalism consumers often state a high importance of environmental protection that is not reflected in their actual behaviour [16].

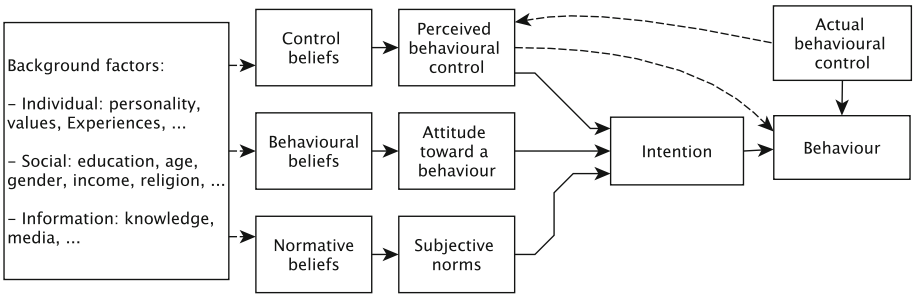

Fig. 1. Model of "planned behaviour" [1, p. 194]

TBP is a positivist approach as it assumes that there are rules structuring the way people think and these "social facts", as Emile Durkheim has been calling them, can be verified by scientific observation and experimentation [9]. We assume that privacy and security perceptions of human being are such social facts and that they can be explained by other attributes (variables) on an aggregated level. We are aware of the fact that this assumption has been criticised 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 [7]. 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 [1].

2.2 Operationalisation of Central Concepts

As a consequence the PRISMS survey comprises of questions exploring respondents' perceptions of privacy and security issues as well as values questions including political views, attitudes to rights and perceptions of technology. For the operationalisation of the central concepts we rely on the privacy typology by Finn et al. [10] and a security typology by Lagazio [18], each distinguishing seven different dimensions. These typologies could be used to design batteries of questions to address the wide spectrum of meanings of privacy and security.

To address this 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 (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 [22]. We have developed eight different vignettes (very short narratives of 50 to 100 words) presenting different types of security

situations and surveillance technologies.[2] They are also covering all dimensions of privacy and security. For each of the vignettes citizens were asked if they think that the respective security-oriented surveillance practice should be used ("acceptance") and to what extend these practices threaten people's rights and freedoms ("intrusiveness").

2.3 Questionnaire and Variables

For our research question we have modified and extended the general TBP model (see Fig. 2) that includes demographic and structural factors and already suggests some interrelationships between the model elements, [cf. 4,20,24, for similar attempts].

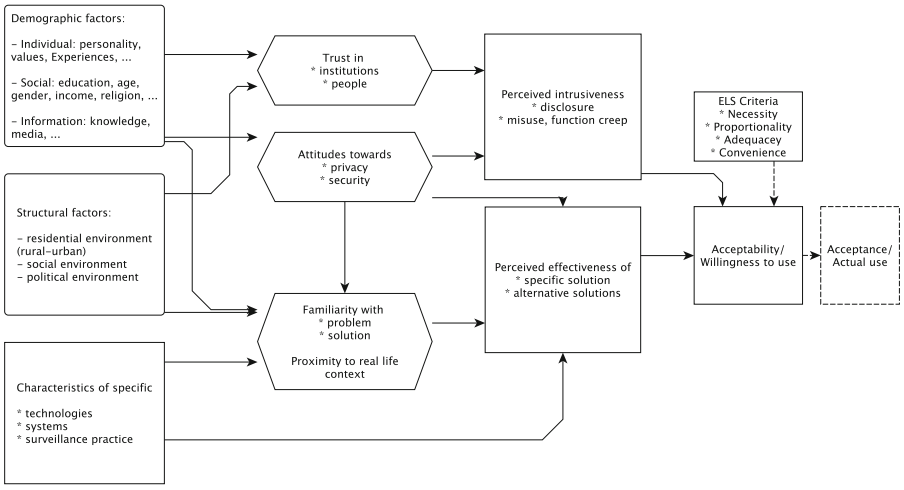

Fig. 2. Suggested relationships between variables explaining privacy and security perceptions and acceptance of security practices

The questionnaire used for the fieldwork thus did not only ask for an assessment of the central concepts privacy and security and of the acceptability and perceived intrusiveness of different security oriented surveillance practices but also those variables needed for the model:

Individual characteristics: Age, gender, education, political orientation, geographic area (country, region), employment status, trust in people, attitude

[2] The vignettes depicted situations of (1) foreign government (NSA type) surveillance, (2) school access by biometrics, (3) usage of smart meter data, (4) monitoring of terrorist website visits, (5) speed control in neighbourhoods by automatic number plate recognition (ANPR), (6) selling of Internet Service Provider (ISP) data, (7) use of DNA databases by police and (8) smart video surveillance of crowds.

towards the benefits and risks of science and technology, member of a minority (self assessment)

Experience, behaviour: Intensity of Internet use, experience with privacy invasions, experience with privacy preserving measures, perceived intrusiveness of security practice

Knowledge: Privacy and data protection knowledge

Interim target variables: Trust in institutions, security perceptions, privacy perceptions

Final target variable: Vignette acceptance

2.4 Fieldwork

Fieldwork took place between February and June 2014. The survey company Ipsos MORI conducted around 1,000 30-min phone interviews in all EU member states except Croatia (27,195 in total) amongst a representative sample (based on age, gender, work status and region) within each country. For economic reasons each interviewee was presented only four randomly selected vignettes, resulting in approx. 13,600 responses for each vignette (500 per country).[3]

3 Empirical Results

3.1 Concept and Methodology

Structural equation modelling (SEM) is a method used to study the relationship among multiple outcomes involving latent variables. In this respect SEM is similar to the regression models that were used to test if linear correlations exist between the different variables. However, SEM allows to estimate and test direct and indirect effects in a more complex system of regression equations and verify (or falsify) theories about the absence of relationships among latent variables [15]. For instance, for the development of the SEM we tested the direct influence of demographics variables such as age on the constructs such as privacy and security perceptions and on the acceptance of the vignettes but also the indirect influence of the demographic variable on the acceptance via the constructs.

The main task in the development of a SEM is to reduce the large number of possible connections between the variables by deleting connections that do not show a statistically significant impact on the target variable. This is done iteratively until a number of benchmarks indicate a good model fit.[4]

[3] The full questionnaire, technical details of the fieldwork and detailed analyses of the survey can be found in [13].

[4] For estimating fit and coefficients we have used the asymptotic distribution free (ADF) function for SEM. The main advantage of ADF is that it does not require multivariate normality. The estimation of the parameter is done by minimizing the discrepancy between the empirical covariance matrix, and a covariance matrix implied by the model [5].

The model explores the relationship between the different variables to explain which variables influence the acceptance or rejection of surveillance based security practices as outlined in the scenarios. On the highest level the model does no longer distinguish between the vignettes, neither between virtual and physical forms of surveillance nor between public and private operators. Even with these generalisations or simplifications the resulting model is rather complex; it includes 17 variables with more than 40 significant correlations. However, the coefficient of determination R^2, that indicates that the fraction by which the variance of the errors is smaller than the variance of the dependent variable. In our case the target variable "acceptance of surveillance oriented security measure" shows $R^2 = 0.484$, which means that almost half of the variability can be explained though the other variables in the model. This is a good value comparable to similar studies such as [4] or [24].

Due to the complexity of the model it will be presented in four parts or sub-models to single out important influence factors. Three of the sub-models focus on the main constructs (security perceptions, privacy perceptions and trust in institutions) while the last one discusses the "acceptance of security practices" as the target variable. The data used for the model can be found in Table 1.

The nodes in the following diagrams are representing those (influencing) variables that have a significant influence on the other (target) variable ("acceptance of a concrete security practice"). Elliptic nodes represent general demographics variables such as age, gender or education. Rectangular boxes stand for variables that are closely related to the context of surveillance and security practices. These include knowledge about data protection rights, experiences with privacy invasions etc. Hexagonal nodes stand for the main constructs that are also important mediating variables. The trapezoidal nodes finally stand for the target variable(s).[5] The coefficients listed in the second column of Table 1 can also be found next to the edges.

3.2 Factors Influencing "Security Concerns"

Figure 3 shows the influences that constitute citizens' personal security perception (in the context of surveillance oriented security practices). In contrast to the other constructs the security perception is strongly influenced by a number of factors.

Experience with prior privacy infringements has a strong positive effect on the security perception – this is in line with the notion that privacy and security are not perceived as competing values, but that privacy is rather seen as an element of security. On the other hand there are three factors that have a negative influence on the security perception. The higher the education the less worried citizens are about their security. The other negative influence factors are related to trust. The more people trust their fellow citizens and in particular institution the less their security concerns. Apart from these strong influence factors, age,

[5] For reasons of simplicity and readability we are not using the normal notation in the following SEM path diagrams. Error terms are not displayed either.

gender and rural-urban classification have a weaker influence on the formation of security perceptions.

Security perceptions in turn have a strong influence on privacy perception (in concrete security contexts!) and finally on the target variables.

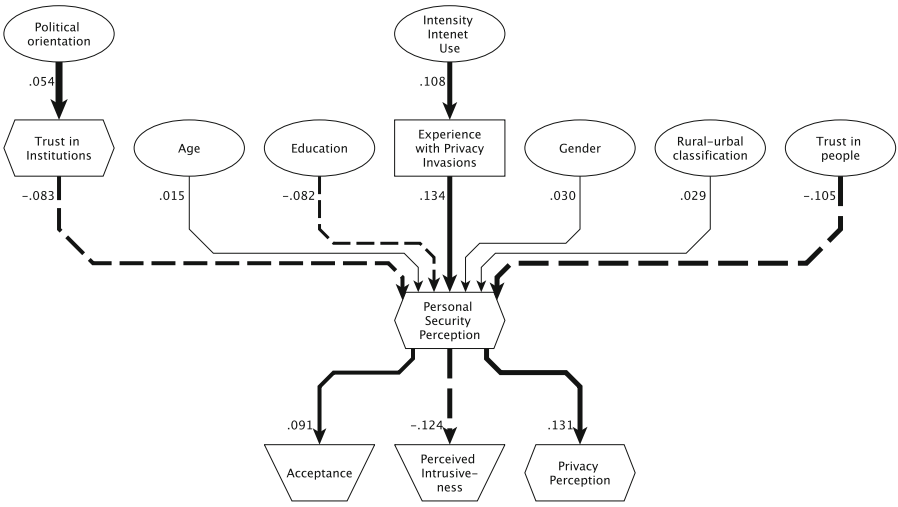

Fig. 3. Sub-model for security concerns. Dotted lines = negative influence, solid lines = positive influence, thickness of the line = strength of the influence

3.3 Factors Influencing "Privacy Concerns"

The influence factors on privacy perceptions as the second important construct is shown in Fig. 4. Privacy perception is constituted from a large number of influence factors without very dominant ones. The rather strong influence of the personal security perception was already mentioned before. Experience with privacy infringements and with privacy protecting measures (privacy activism) have a similarly strong influence on privacy perceptions. Minor influence factors include trust, political orientation and privacy knowledge. The educational level is having a relatively strong indirect influence moderated by trust and intensity of Internet use. In summary the formation of privacy perceptions depends on experience in the context where surveillance takes place and on general knowledge. These two elements help citizens to comprehend the complexity and rationale of surveillance measure and to assess the possibilities of safeguards.

Privacy perceptions are the most important influence factor for citizens' acceptance or rejection of concrete surveillance oriented security measures either directly or indirectly via the assessment of the intrusiveness.

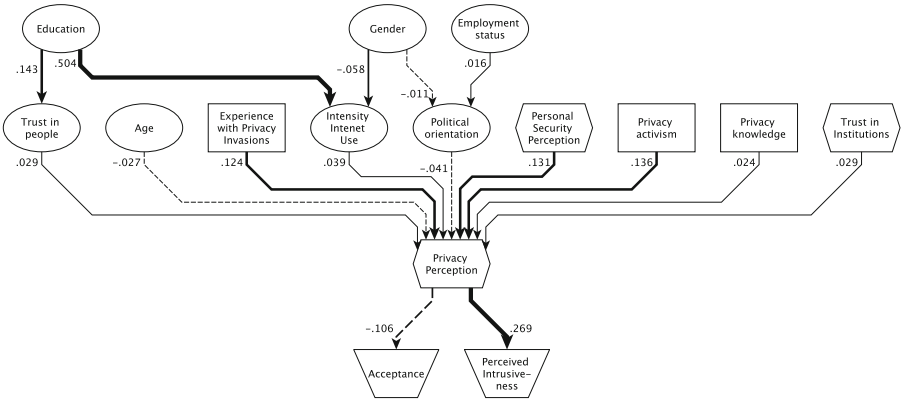

Fig. 4. Sub-model for privacy concerns. Dotted lines = negative influence, solid lines = positive influence, thickness of the line = strength of the influence

3.4 Factors Influencing "Trust in Institutions"

As already mentioned before trust in institutions is another important moderating factor in citizens' assessment of security technologies and practices. Figure 5 shows how the trust construct is influenced by other factors. The most dominant influence is the other dimension of trust, the trust in persons which shows to be highly correlated with trust in institutions. Other more important factors include a person's political orientation, where more conservative (right-winged) persons have a higher trust in institutions such as state agencies, companies and the press. On the other hand trust – in concrete surveillance/security situations – is also influenced by experiences that citizens have had. People who found their privacy invaded are less trusting towards institutions in general. The direct influence of education, gender and rural-urban classification is less important on the formation of trust in institutions. Blinkert has pointed out that this is related to the "relative structural effectiveness", which he defines as a combination of the effectiveness of the state's monopoly on legitimate use of force and the extent of social welfare and distributive justice, that varies greatly between countries and regions [4].

Trust in institutions has no immediate influence on the acceptance of a specific security measure but plays a strong role for people's assessment if such a measure is intrusive, i.e. if it threatens or protects people's fundamental rights. It also has minor effects on the perception of personal security and the perception of privacy, which in turn have a strong effect on acceptance.

3.5 Factors Influencing Acceptance of Surveillance-Oriented Security Technologies

Figure 6 finally shows which variables and constructs influence European citizens' acceptance or rejection of security practices. The most striking result is that the

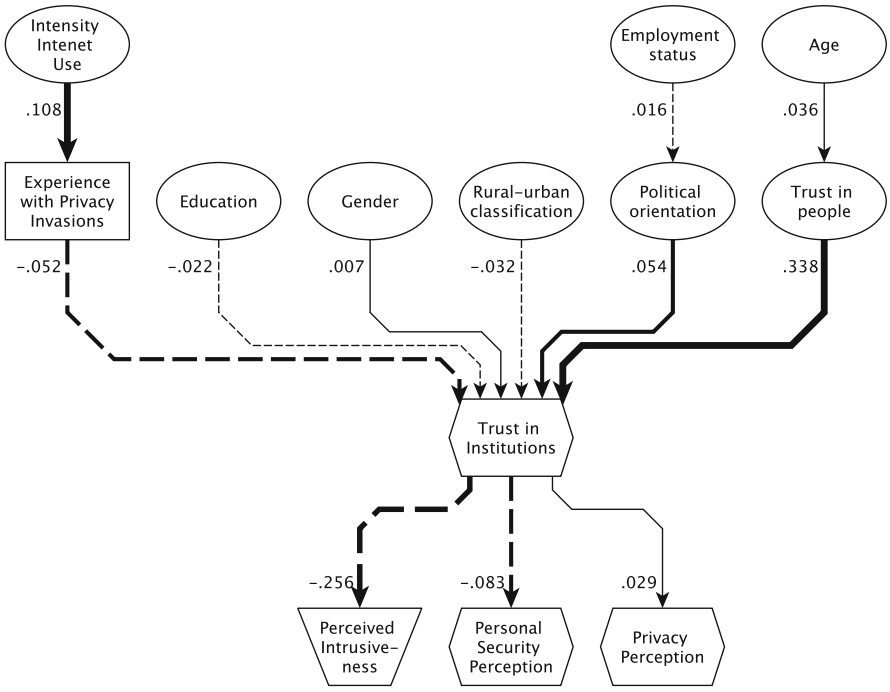

Fig. 5. Sub-model for citizens' trust in institutions. Dotted lines = negative influence, solid lines = positive influence, thickness of the line = strength of the influence

perceived impact of the practice on citizens' rights (here called intrusiveness) is the most critical factor for their acceptance or rejection that itself is strongly influenced by trust in institutions. Privacy and security perceptions follow as the next important factors, however, with a much smaller coefficient. Apart from these three factors most of the other variables play a direct or indirect role, but with a rather small contribution. The only new demographic variable that has a significant (but still small) influence on acceptance is the general attitude towards science and technology where people with a more positive assessment of their benefit have a greater acceptance.

3.6 The Full Picture

The combination of these sub-models does not only show the impacts described before but also the indirect and cumulative effects. Figure 7 is giving a comprehensive picture of the different factors influencing people's perceptions of privacy and security in the context of concrete applications of surveillance based security technologies. In this picture each of the variables (boxes) also includes the share that it contributes to the manifestation of the target variable. The higher this contribution, the bigger the size of the respective node.

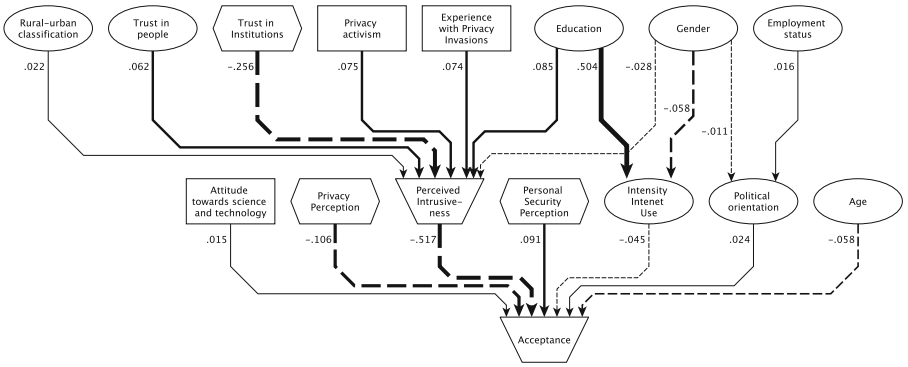

Fig. 6. Sub-model for acceptance of surveillance-oriented security technologies. Dotted lines = negative influence, solid lines = positive influence, thickness of the line = strength of the influence

Apart from the importance of the perceived intrusiveness, trust in institutions and the general perception of privacy and personal security that have already been discussed play a significant role in the acceptance of security oriented surveillance practices. The picture also gives a better impression of the relevance of different personal characteristics.

Among the individual characteristics education plays the most important role: the higher the education level the lower the acceptance of security technology. The influence of education is moderated mainly over three channels: (1) More educated people have a higher level of trust with an influence on the perception of intrusiveness; (2) more educated people usually use the Internet more intensively and have thus more experiences with the possibilities of online surveillance and (3) more educated people have less worries about their personal security.

The other influential personal characteristic is political orientation: More conservative people have a higher level of trust in institutions, also those operating surveillance oriented security technology and thus tend to accept them to a higher degree than more left-winged persons.

Noteworthy is also that age is playing a significant role in the model; the influence, however, on acceptance of surveillance based security technologies is small.

4 Discussion of Results

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

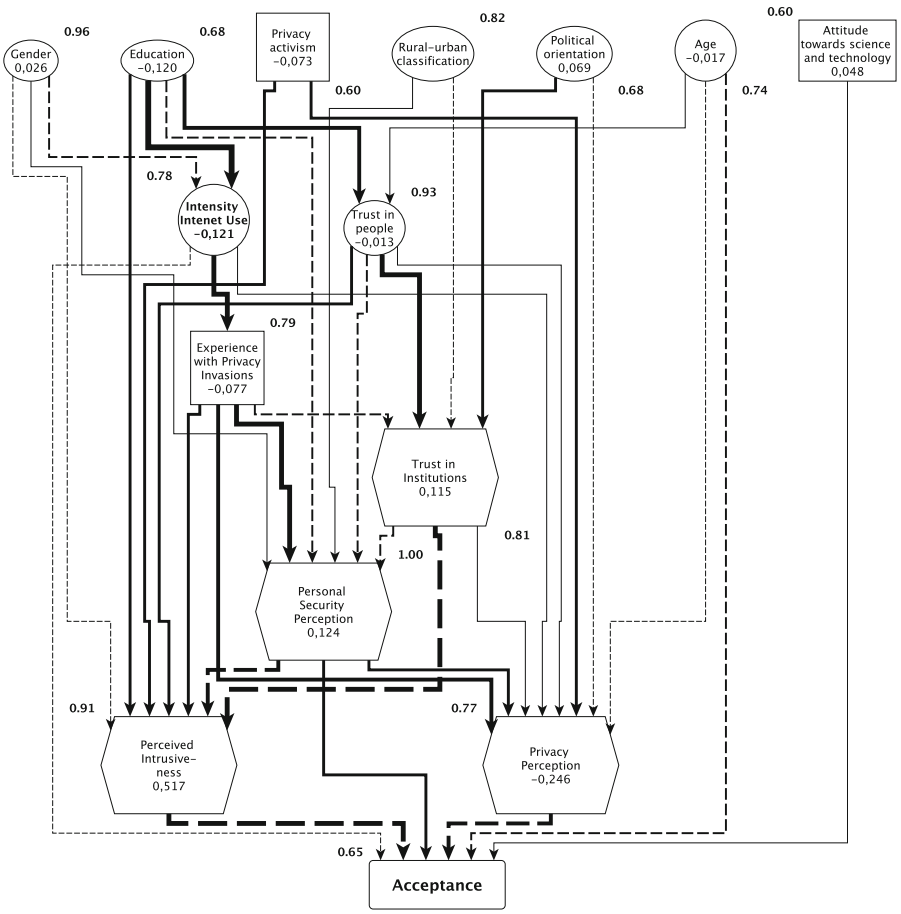

Fig. 7. Model of factors influencing acceptance of SOSTs (simplified). Dotted lines = negative influence, solid lines = positive influence, thickness of the line = strength of the influence, size of nodes = overall influence of a factor on acceptance

Trust in the operating institution is the essential factor for the acceptability of a security practice. The important role of trust, in people, in institutions as well as in the whole societal environment, is regularly confirmed in surveys [4,11,14].

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 [24, p. 135f.].

The PACT project on the other side stresses the strong impact that distrust has on the likelihood that citizens reject a given security measure [21, p. v].

Table 1. Structural equation model data. Estimation Method = ADF; Number of obs = 12,196; Discrepancy = 0.1244

Target variable ← Influencing variables	**Coef.**	**Std. err.**	**z**	**P>|z|***	**95% Confidence Interval****	
Perceived Intrusiveness ←						
Personal Security Perception	0.125	0.013	9,450	0.000	0.099	0.151
Trust in Institutions	0.257	0.015	17,420	0.000	0.228	0.286
Intensity Internet Use	-0.074	0.009	-7,910	0.000	-0.093	-0.056
Trust in people	-0.062	0.011	-5,430	0.000	-0.085	-0.040
Privacy Perception	-0.269	0.011	-25,220	0.000	-0.290	-0.248
Political orientation	0.053	0.010	5,350	0.000	0.034	0.072
Privacy activism	-0.076	0.010	-7,290	0.000	-0.096	-0.055
Experience with Privacy Invasions	-0.074	0.011	-6,480	0.000	-0.097	-0.052
Education	-0.086	0.011	-7,520	0.000	-0.108	-0.064
Age	-0.061	0.009	-6,790	0.000	-0.078	-0.043
Rural-urban classification	-0.023	0.008	-2,920	0.004	-0.038	-0.007
Gender	0.028	0.005	5,940	0.000	0.019	0.037
Attitude towards science and technology	0.063	0.008	7,480	0.000	0.047	0.080
_cons	0.602	0.017	36,130	0.000	0.569	0.635
Acceptance ←						
Perceived Intrusiveness	0.518	0.006	89,060	0.000	0.506	0.529
Personal Security Perception	0.092	0.008	11,350	0.000	0.076	0.108
Intensity Internet Use	-0.045	0.005	-9,010	0.000	-0.055	-0.035
Political orientation	0.025	0.006	3,850	0.000	0.012	0.037
Privacy Perception	-0.107	0.007	-15,100	0.000	-0.121	-0.093
Age	-0.058	0.006	-10.510	0.000	-0.069	-0.048
Attitude towards science and technology	0.015	0.005	2,890	0.004	0.005	0.026
_cons	0.320	0.009	33,800	0.000	0.301	0.338

continued on next page

Table 1. (*Continued*)

Target variable ← Influencing variables	Coef.	Std. err.	z	P>|z|*	95% Confidence Interval**	
Personal Security Perception ←						
Trust in people	-0.106	0.009	-11,840	0.000	-0.123	-0.088
Trust in Institutions	-0.083	0.012	-7,150	0.000	-0.106	-0.060
Experience with Privacy Invasions	0.135	0.008	16,800	0.000	0.119	0.150
Education	-0.083	0.008	-10.770	0.000	-0.098	-0.068
Age	0.015	0.005	2,870	0.004	0.005	0.026
Rural-urban classification	0.029	0.006	5,230	0.000	0.018	0.040
Gender	0.031	0.003	9,170	0.000	0.024	0.037
_cons	0.376	0.009	44,150	0.000	0.359	0.393
Intensity Internet Use ←						
Education	0.504	0.013	40.220	0.000	0.480	0.529
Age	-0.534	0.009	-57,600	0.000	-0.552	-0.516
Gender	-0.058	0.005	-10.700	0.000	-0.069	-0.048
_cons	0.778	0.009	83,430	0.000	0.760	0.797
Political orientation ←						
Employment status	0.017	0.006	2,800	0.005	0.005	0.028
Gender	-0.012	0.004	-2,720	0.007	-0.021	-0.003
_cons	0.511	0.005	98,230	0.000	0.500	0.521
Trust in people ←						
Education	0.144	0.009	15,210	0.000	0.125	0.163
Age	0.037	0.007	5,310	0.000	0.023	0.050
_cons	0.425	0.007	58,640	0.000	0.411	0.439
Privacy Perception ←						
Personal Security Perception	0.131	0.011	12,120	0.000	0.110	0.153
Trust in Institutions	0.029	0.013	2,330	0.020	0.005	0.054

continued on next page

Table 1. (*Continued*)

Target variable ← Influencing variables	Coef.	Std. err.	z	P>|z|*	95% Confidence Interval**	
Intensity Internet Use	0.040	0.007	5,660	0.000	0.026	0.054
Trust in people	0.029	0.010	2,960	0.003	0.010	0.048
Political orientation	-0.041	0.009	-4,730	0.000	-0.058	-0.024
Privacy activism	0.137	0.008	16,410	0.000	0.120	0.153
Experience with Privacy Invasions	0.125	0.009	13,570	0.000	0.107	0.143
Age	-0.027	0.007	-3,710	0.000	-0.042	-0.013
Privacy knowledge	0.024	0.007	3,260	0.001	0.010	0.039
_cons	0.397	0.014	29,170	0.000	0.370	0.424
Privacy activism ←						
Intensity Internet Use	0.266	0.005	50.330	0.000	0.255	0.276
Experience with Privacy Invasions	0.253	0.010	24,300	0.000	0.232	0.273
_cons	0.105	0.004	24,950	0.000	0.097	0.113
Trust in Institutions ←						
Trust in people	0.338	0.007	47,770	0.000	0.324	0.352
Political orientation	0.055	0.007	7,830	0.000	0.041	0.068
Experience with Privacy Invasions	-0.053	0.007	-7,980	0.000	-0.066	-0.040
Education	-0.022	0.007	-3,440	0.001	-0.035	-0.010
Rural-urban classification	-0.033	0.005	-6,680	0.000	-0.042	-0.023
Gender	0.008	0.003	2,740	0.006	0.002	0.014
_cons	0.364	0.007	52,560	0.000	0.350	0.378
Experience with Privacy Invasions ←						
Intensity Internet Use	0.109	0.006	19,480	0.000	0.098	0.120
_cons	0.080	0.005	16,700	0.000	0.071	0.089

* A z-score is a measure of how many standard deviations below or above the population mean a raw score is. The value of the test P > |z| indicates the probability that the z-score is random. Zero values in this test indicate that the influence of the factor is not random, i.e. it has a significant influence. It does not give evidence about the strength of the influence.
** The true value of coefficient can be found with a 95% probability in the range given by the 95% Confidence Interval.

Finally also a recent Eurobarometer study on Europeans' attitudes towards security found that institutions' respect for fundamental rights and freedoms is a strongly impacting the perception of security [26, p. 15f.].

Transparency or openness has a positive effect on the willingness of citizens to accept security practices. This can be understood on different levels:

- Citizens tend to accept security practices when they are convinced that a security measure is necessary, proportionate and effective.
- People are more easily convinced 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 complexities of a security practices it also drives critical reflections. The SurPRISE project also confirmed most of these observations [24, p. 154f.].
- Current security practices, however, often do not seem to take this lesson seriously. In a Eurobarometer survey a majority of European citizens said they think that the security technologies and practices in the fight against terrorism and crime have restricted their rights and freedoms, which then is negatively impacting citizens' trust [26, p. 45ff.].

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 [3].

On the downside our empirical results also showed that many citizens do not care about surveillance that does not negatively affect them personally but only others. The SuPRISE project similarly concludes that "the more participants perceive SOSTs to be targeted at others rather than themselves, the more likely they are to find a SOST more acceptable" [24, p. 138].

5 Conclusions

For the design and introduction of security measures it is useful to consider some of the main socio-demographic determinants for acceptance of these measures, 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. On the other hand we have shown in our analysis of the 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 [6]:

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

However, citizen perceptions do 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 between reaction types 2 and 3 when citizens fear an invasion of their privacy or perceive a technology as ineffective. Citizens' reactions are mostly based upon perceptions rather than rational fact-based assessments. As we have shown before these are influenced by a multitude of factors. Trust in institutions is one, the perceived self-interest is another, the measure being overt or covert a potential third. These three elements should be taken into account in the design of new security technologies and in specific security investments. For these cases PRISMS has developed a participatory and discursive technique that can help decision-makers in industry, public authorities and politics to implement security measures that raise fewer concerns in the population and are thus more acceptable along the lines stated in many policy documents [2,19].

Acknowledgement. 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.

References

1. Ajzen, I., Fishbein, M.: The influence of attitudes on behavior. In: Albarracin, D., et al. (eds.) The Handbook of Attitudes, pp. 173–221. Erlbaum, Mahwah (2005)
2. Barnard-Wills, D.: Security, privacy and surveillance in european policy documents. International Data Priv. Law **3**(3), 170–180 (2013)
3. Barnard-Wills, D., et al.: Possible dual use of the decision support system. PRISMS Deliverable 10.3, June 2015
4. Blinkert, B.: Unsicherheitsbefindlichkeit als 'sozialer Tatbestand'. Kriminalitätsfurcht und die Wahrnehmung von Sicherheit und Unsicherheit in Europa. In: Erkundungen zur Zivilgesellschaft, pp. 119–146. Lit-Verlag, Münster (2013)

5. Browne, M.W.: Asymptotically distribution-free methods for the analysis of covariance structures. Br. J. Math. Stat. Psychol. **37**(1), 62–83 (1984)
6. Conti, G., et al.: Deconstructing the relationship between privacy and security. IEEE Technol. Soc. Mag. **33**(2), 28–30 (2014)
7. Cook, A.J., et al.: Taking a position: a reinterpretation of the theory of planned behaviour. J. Theory Soc. Behav. **35**(2), 143–154 (2005)
8. Dienlin, T., Trepte, S.: Is the privacy paradox a relic of the past? An in-depth analysis of privacy attitudes and privacy behaviors. Eur. J. Soc. Psychol. **45**, 285–297 (2015)
9. Durkheim, E.: The Rules of Sociological Method [1895]. Trans. by Lakes, S. The Free Press, New York et al. (1982)
10. Finn, R.L., et al.: Seven types of privacy. In: Gutwirth, S., et al. (eds.) European Data Protection: Coming of Age, pp. 3–32. Springer, Dordrecht (2013)
11. Fox, S., et al.: Trust and privacy online: Why Americans want to rewrite the rules. Washington, D.C.: Pew Internet & American Life Project, August 2001. http://www.pewinternet.org/files/old-media//Files/Reports/2000/PIP_Trust_Privacy_Report.pdf
12. Friedewald, M., van Lieshout, M., Rung, S., Ooms, M., Ypma, J.: Privacy and security perceptions of european citizens: a test of the trade-off model. In: Camenisch, J., Fischer-Hübner, S., Hansen, M. (eds.) Privacy and Identity 2014. IFIP AICT, vol. 457, pp. 39–53. Springer, Heidelberg (2015)
13. Friedewald, M., et al.: Report on the analysis of the PRISMS survey. PRISMS Deliverable 10.1. PRISMS project, October 2015. http://prismsproject.eu
14. Hummelsheim, D.: Subjektive Unsicherheit Lebenszufriedenheit in Deutschland: Empirische Ergebnisse einer repräsentativen Bevölkerungsbefragung. In: Zoche, P., et al. (ed.) Sichere Zeiten? Gesellschaftliche Dimensionen der Sicherheitsforschung, pp. 67–89. Lit Verlag, Münster (2015)
15. Kaplan, D.: Structural Equation Modeling: Foundations and Extensions. SAGE, Thousand Oaks (2000)
16. Kollmuss, A., Agyeman, J.: Mind the Gap: why do people act environmentally and what are the barriers to pro-environmental behavior? Environ. Educ. Res. **8**(3), 239–260 (2002)
17. Kreissl, R., et al.: Surveillance: preventing and detecting crime and terrorism. In: Wright, D., Kreissl, R. (eds.) Surveillance in Europe, pp. 150–210. Routledge, London (2015)
18. Lagazio, M.: The evolution of the concept of security. Thinker **43**(9), 36–43 (2012)
19. van Lieshout, M., et al.: The PRISMS Decision Support System. PRISMS Deliverable 11.3, July 2015. http://prismsproject.eu
20. Morton, A.: Measuring inherent privacy concern and desire for privacy: a pilot survey study of an instrument to measure dispositional privacy concern. In: Proceedings of the 2013 ASE/IEEE International Conference on Social Computing, 8–14 September 2013, pp. 468–477. IEEE Computer Society, Washington, D.C. (2013)
21. Patil, S., et al.: Public Perception of Security and Privacy: Results ofthe comprehensive analysis of PACT's pan-European Survey. PACT Deliverable 4.2. RAND Corporation, June 2014. http://www.rand.org/content/dam/rand/pubs/research_reports/RR700/RR704/RAND_RR704.pdf

22. Pavlov, A.: Application of the vignette approach to analyzing cross-cultural incompatibilities in attitudes to privacy of personal data and security checks at airports. In: Zureik, E., et al. (eds.) Surveillance, Privacy, and the Globalization of Personal Information: International Comparisons, pp. 31–45. McGill-Queen's University Press, Montreal (2010)
23. Pavone, V., Degli Esposti, S.: Public assessment of new surveillance-oriented security technologies: beyond the trade-off between privacy and security. Public Underst. Sci. **21**(5), 556–572 (2012)
24. Pavone, V., et al.: Key factors affecting public acceptance and acceptability of SOSTs. SurPRISE Deliverable 2.4. SurPRISE project, January 2015. http://surprise-project.eu/wp-content/uploads/2015/02/SurPRISE-D24-Key-Factors-affecting-public-acceptance-and-acceptability-of-SOSTs-c.pdf
25. Solove, D.J.: Understanding Privacy. Harvard University Press, Cambridge (2008)
26. TNS Opinion & Social, Europeans' attitudes towards Security, Special Eurobarometer 432. doi:10.2837/41650. http://ec.europa.eu/public_opinion/archives/ebs/ebs_432_en.pdf