Towards a theoretical framework of acceptance for surveillance systems at airports

Gabriel Bartl
Freie Universität Berlin
gabriel.bartl@fu-berlin.de

Lars Gerhold
Freie Universität Berlin
lars.gerhold@fu-berlin.de

Matthias Wählisch
Freie Universität Berlin
m.waehlisch@fu-berlin.de

ABSTRACT

In this paper we illustrate (a) the background and goals of the interdisciplinary research project SAFEST and (b) first insights from the socio-scientific part within the project. Technical systems are often established without considering explicitly ethical, legal, and social implications. This frequently leads to a lack of acceptance. This paper aims at compiling an analytical scheme that tries to demonstrate the relevance of the social context for the emergence of different modes of acceptance in reference to surveillance systems at airports. It is intended to guide the technical experts to deal with and reflect acceptance issues in the process of technical development.

Keywords

acceptance, acceptability, privacy by design, privacy in context, technical surveillance systems, public infrastructures

INTRODUCTION: THE INTERDISCIPLINARY PROJECT SAFEST – CHALLENGES AND GOALS

Security and safety in the context of critical infrastructures are located in a tense relationship between human action and technological systems. Mutual dependencies between these two variables exist and have to be evaluated together with overall ethical, legal, and social conditions in order to prevent and handle crises at an optimum for all stakeholders involved. As the implementation of technical systems might generate conflicts and implications on different levels, for example with regard to the balance between security and freedom or issues of equitableness and privacy, these goods have to be weighed and related carefully to each other in order to take reasonable and fair decisions (Ammicht Quinn 2012: 62).

In the context of civil security, technological solutions usually focus on two functionalities: The prevention of crises through early detection approaches and the support of the crisis management itself are supported by making use of technical systems. In both cases data may be required that potentially touches privacy. Thus, innovative ways for privacy preserving techniques are needed instead of focusing solely on technical requirements because "public perception and social acceptance are important elements in technology implementation" (Sanquist et al. 2008: 1132). The SAFEST project takes account of this aspect when addressing the problems of crowd control and area surveillance at airports applying a privacy by design approach. Hence, the socio-scientific part of SAFEST concentrates on the question how privacy relates to other dimensions of acceptance. To mitigate acceptance problems, we established a theoretical model that tries to explain the emergence of certain kinds of acceptance patterns in a social context. The results are incorporated in the design of the SAFEST architecture and the implementation of the surveillance system. Our study of acceptance for these kinds of technical systems is not only based on the perspectives of safety and security experts at the airport but rather concentrates on the preferences and assessments of passengers.

The remainder of this short paper is structured as follows: The next section describes the background of both approaches, privacy by design and privacy in context. Based on that, the localization of privacy in the theoretical and empirical field of acceptance will be discussed. Section 4 presents our empirical design to establish an acceptance framework including expert interviews, qualitative interviews with passengers, and a quantitative survey. Section 5 reflects our preliminary results towards a framework for acceptance. Finally, we give a conclusion and an outlook.

THEORETICAL BACKGROUND

Whereas acceptance refers to the individual level of social action, acceptability is understood as ethical reflection on the macro level. Surely both constructs are linked in a non-arbitrary manner but relate to different issues and levels of analysis. So it has to be distinguished if, for example, new forms of social control, social inequalities, the definition of deviant behavior, or the intrinsic normativity of algorithms and scenarios (McPhail et al. 2009: 745; Zurawski 2012: 247-249) are analyzed in the sense of social behavior or as manifestation of ethical guidelines of a society as a whole. The social perspective therefore focuses on human behavior and deals with the question of social construction processes that lead to acceptance; the ethical perspective examines issues of legitimacy and acceptability.

This already indicates that acceptance and privacy should only be understood as small segments of more general ethical, legal and social implications that safety and security technologies provoke. Hence, acceptance should be discussed in a wider context to reveal also non-intended effects of technological innovations because these effects are not restricted to violations of personal rights: „In dealing with surveillance, scholars have widely agreed to refute privacy as an analytical concept and defining theme […] because it is regarded as too narrow to grasp the entirety of the social consequences resulting from surveillance practices“ (Möllers/Hälterlein 2013: 57). Nonetheless, privacy preservation remains an important aspect in the whole set of challenges technological surveillance systems have to meet. The goal must be to deal with privacy issues in regard to the social context and relate the findings to questions of acceptance and acceptability.

Privacy by design, as the new buzzword in technology implementation discourses, means to embed privacy proactively in the design process of a technical system by data minimization techniques. This implies the use of encrypted or coded information whenever possible and targets at minimizing the collection and analysis of personal information (Schaar 2010: 267-274). Additionally, privacy by default describes that the standard settings are adjusted in favor of data protection. In the corresponding literature, both terms are mostly treated as business issues, and not as compliance issues (e.g., Cavoukian 2012). Whereas the first perspective describes an economical user perspective by revealing the individual resentments in more detail to adapt the toolbox of technical development to the passengers‟ needs („Technology Acceptance Models“) the second approach intends to assess subjective patterns of acceptance, not only on the micro user level, but also on the macro and the context level. At this point the concept of privacy in context comes into operation which states that the context is decisive for the quality and quantity of data gathering purposes. Hence, asymmetries of power – who collects and analyzes information of whom? – can only be justified by the specificity of the context (Brunton & Nissenbaum 2012). The concept is based on the idea that the flow of information has to be appropriate depending on the variability of rules in certain social contexts within pluralistic societies. Combining the privacy by design approach with the concept of privacy in context seems to be a promising way of analyzing both challenges: acceptance and acceptability.

To which extent the increased deployment of security measures, especially surveillance technologies in public spaces affects the acceptance is still an open question. Adey, for example, observes that “surveillance is increasingly focused upon mobility” (Adey 2004: 500). Airports can be considered as gates of global mobility, thus the perception of surveillance is also an elementary ethical aspect for the evaluation of acceptance in terms of discrimination: „Surveillance has become a feature not of specific monitoring of suspects but of generalized social sorting of populations, in this case in relation to their perceived levels of dangerousness“ (Lyon 2006: 398). On the one hand, the strategy of categorical suspicion, for example on the basis of ascriptive attributes (e.g., skin colour), could be critically questioned by certain airport passengers and change the individual acceptance. In contrast to that, effects of habituation in the context of surveillance technologies have an impact on subjective acceptance patterns (Töpfer 2008). Hence, the quality of the connection between acceptance and acceptability with respect to security measures and surveillance technologies has to be clarified.

One approach to bridge the gap between the individual level of acceptance and the collective level of acceptability is trust. For Giddens trust is a key term for the description and analysis of increasingly complex and diverse societies (Giddens 1996). Referring to Luhmann trust arises from the demand of a “reduction of complexity” (Luhmann 2000) and is based on the delegation of decisions and responsibilities. On the one hand trust is experience-based and reflects an individual perspective, whereas on the other hand acceptability is based on the historical developments of cultures with specific collective values. By linking these two levels trust can serve as multilevel instrument in regard to the analysis of acceptability and acceptance of governance in general and privacy in particular. Institutional trust thus is also considered to have an impact on acceptance because institutions are responsible for the arrangement and the organization of security at airports. “Good governance” in terms of trustworthy and legitimate decision processes was also observed as factor of acceptance in some empirical studies (e.g. acatech 2011: 17). Moreover, trust is closely connected with risk perception (Siegrist & Cvetkovich 2000, Sjöberg 2001, Viklund 2003) in a world where a lack of control results from contingent scientific observations and interpretations. This also implicates “that the outcomes and effects that science seeks

to know and regulate are better regarded as contingent, than as the ostensibly determinate predictions represented by sound scientific knowledge" (Felt/Wynne 2007: 82).

Acceptance is usually considered as affirmative value of a specific dependent variable, even though acceptance is a very context dependent construct. Lucke conceptualizes acceptance as affirmative attitude (Lucke 1995: 94; 124). She defines acceptance as the chance to reach consent in an identifiable social group that agrees under assignable conditions (ibid.: 104). Moreover, Lucke describes acceptance as continuum stretching from reflective acceptance to opposition, including discrete modes of acceptance. Within the context of security technologies at the airport four modes are relevant: (1) informed consent, (2) ignorance, (3) forced compliance, and (4) opposition. The first mode could be considered as explicit acceptance because affirmation is based on reflective information whereas the second and the third mode describe rather passive forms of acceptance. Finally, opposition is equal to an active form of non-acceptance.

In addition to these four different modes, which model acceptance can be achieved, various subdimensions of acceptance have to be distinguished. Sanquist et al., for example, found empirical evidence for the assumption that acceptance „is highly correlated with attributes such as validity, personal benefit, national security benefit, and accuracy, suggesting that these attributes contribute to the overall perception of security system acceptability" (Sanquist et al. 2008: 1128). In the same study they also emphasize the importance „to evaluate the impact of demographics, political attitudes, and trust in government" (ibid.: 1132). This observation is confirmed by other studies, in which education was found to be a factor of acceptance, i.e., more knowledge on certain technologies resulted in more critical attitudes and less acceptance (acatech 2011: 16). Overall, the research on acceptance should differentiate between modes and dimensions of acceptance. Whereas the first one represents the formation of acceptance, the second one points to single factors of the construct of acceptance.

EMPIRICAL DESIGN

The structure of the study of acceptance can be divided into three larger steps.

In the first step, security experts from the Flughafen Berlin Brandenburg (FBB) are interviewed on technical and social aspects of implementing a new sensor-based security system at the airport. Experts represent an organizational unit because they have specific experiences or knowledge in their field that others do not have (Meuser/Nagel 2002). The results of the interviews provide the project team input from people who have been working in the field of safety and security for years.

In the second step, the socio-scientific study deals with the question of acceptance of security measures by airport passengers at the airport Berlin Schönefeld, Germany. Problem-centered interviews (Witzel/Reiter 2012) with passengers aim at developing a preliminary model of acceptance in regard to safety and security measures at airports. Methodically, a structured content analysis (Mayring 2000) is applied. This method reduces the material to its central entities. The results of this analysis lead to our theoretical model of acceptance and are then used for the thematic structuring and construction of a standardized questionnaire for flight passengers.

In the third step this questionnaire will be used for a quantitative survey with airport passengers. The empirical results of this data may reveal individual differences in the perception and acceptance of security measures with particular attention on privacy issues. To comply with Sanquist et al.'s request, the questionnaire contains socio-demographic (age, gender) and socio-economic (education, income, profession) variables. Moreover the explanatory power of trust, values and subjective perception in regard to individual acceptance patterns will be explored. The outcomes of the statistical analyses are discussed with the technical developers of SAFEST.

PRELIMINARY RESULTS

The expert interviews clearly identified the importance of a holistic approach. Experts emphasized that new technical systems that are implemented in existing technical setup always change organizational structures and responsibilities. This can be considered as sociotechnical aspect which cannot be observed in isolation because the implications are both technical and social. On the one hand, the implementation of a new technical system leads to technical questions such as compatibility and adaptability. On the other hand, the passengers and the security staff at the airport have to use these systems that bring social and legal inferences for them. Thus, organizational structures of an airport seem to act on the interface between these two extremes.

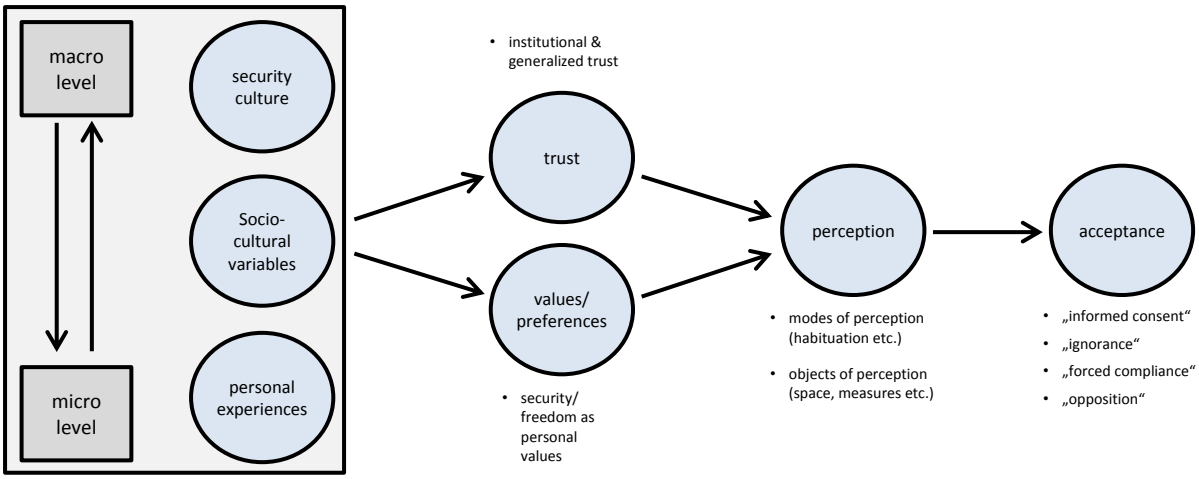
The epistemological motivation of the passenger interviews was to directly ask flight passengers themselves in order to improve the procedure of building systems for the public and get an idea about patterns acceptance or possible side effects that security measures provoke. Firstly, the analysis of the interviews showed an overall acceptance of security measures at the airport by flight passengers. In more detail, the interview material revealed that acceptance mostly appeared in the shapes of forced compliance or ignorance. This finding lead to

the observation that both the dependency on the plane and modes of habituation on surveillance technologies overlay an active form of informed consent in the context of an airport. In this case an adequate balance between security and freedom has to be questioned from an ethical and a social standpoint to inspect, for example, if flight passengers tend to adapt to a culture of suspicion where everybody is treated as potentially dangerous.

Moreover, acceptance was found to be a multi-factorial construct that in the context of airports consists of various dimensions: privacy, transparency, trust, health, time and effort, intimacy, discrimination, adequacy, reasonability and costs of the measures, appearance of the security personnel and emotional factors. Overall the individual preferences for the single factors alternated significantly so that no general pattern of overall acceptance could be observed. It seemed, for example, that for women intimacy played a superior role compared to men when the body scanner was mentioned. Besides, time and effort was quite important for business travellers whereas for some passengers discrimination was the major aspect due to the ethics of equal treatment.

In preparation to the statistical testing with a representative sample, a preliminary theoretical model of acceptance could be derived from the interview material ( ). Although the model is an abstraction of the results from the problem-centered passenger interviews, it aims at putting single factors of acceptance in a broader context. The arrows should not be interpreted in a deterministic causal manner but rather as possible causalities that are in line with other theoretical models in the social sciences. The close linking of values, perceptions and acceptance relates, for example, to the model of value-attitude-social action (Van Deth/Scarbrough 1995). The abstract quality of the model permits to apply it to the diverse occurrences of security measures at the airport that can be divided in socio-technical systems (e.g. CCTV, metal detector, personal data analysis) and security staff (e.g. police, private security agencies). In addition to that the model can adopt the various dimensions of acceptance (e.g. privacy, discrimination, transparency). So, the dynamics in the emergence of certain types of acceptance can be structured and illustrated theoretically, for example with regard to the question why there is a gap between the overall social acceptance of video surveillance on the one hand and the stable level of subjective security perception when video surveillance is extended (Apelt/Möllers 2011: 485). For this case it could be asked how variables like the security culture or trust are connected with the perception and what kind of acceptance of video surveillance was observed. The analysis of the interview material revealed that there are connections between values and the type of acceptance on the personal level. Passengers who were assigned to the acceptance type „forced compliance" tended to be against the establishment of more security measures. As the model is the basis for the development of a survey questionnaire the single components of the model are covered and can be related to each other in the quantitative study where possible correlations will be tested statistically with a representative sample of flight passengers.

***Figure 1*: Preliminary theoretical model of acceptance in the context of security measures at airports**



CONCLUSION & OUTLOOK

SAFEST targets a holistic perspective concerning the relation between technical and social aspects in the field of technical safety and security systems. In this paper, we presented first steps towards a detailed and systematic explanation of acceptance in the context of security measures at airports. Moreover it was stated that non-intended social effects provoked by technical systems are a challenge that acceptable safety and security measures have to meet. Crisis management for critical infrastructures increasingly seems to follow a security logic that brings along new techniques for social control and social sorting what blurs the original intended purpose. For SAFEST this diagnosis means that the privacy by design approach should be combined with a

privacy in context approach in order to adhere to the fact that questions on privacy invasion always depend on the context. Tackling this challenge is part of our ongoing research jointly with the technical partners of SAFEST. Beyond that, methods for more participatory and deliberative socio-technical innovation (McPhail et al. 2009) seem promising for a more direct integration of stakeholders in the process of technical development.

REFERENCES

1. acatech (2001) Akzeptanz von Technik und Infrastrukturen. Anmerkungen zu einem aktuellen gesellschaftlichen Problem, acatech bezieht Position, 9, Springer Verlag, Heidelberg.
2. Adey, P. (2004) Secured and Sorted Mobilities: Examples from the Airport. , 1, 4, 500-519.
3. Ammicht Quinn, R. (2012) Fahrradbremse oder Navigationssystem: Was ist, will und kann eine Ethik der Sicherheit? Gerhold, L. & Schiller, J. (Ed.) . Beiträge aus dem Forschungsforum Öffentliche Sicherheit, Peter Lang Verlag, Frankfurt am Main.
4. Apelt, M., Möllers, N. (2011) Wie ‚intelligente„ Videoüberwachung erforschen? Ein Resümee aus zehn Jahren Forschung zu Videoüberwachung, , 4, 585–593.
5. Brunton, F., Nissenbaum, H. (2013) Political and Ethical Perspectives on Data Obfuscation, Hildebrandt, M., de Vries, K. (Ed.) , New York, Routledge, 164-188.
6. Cavoukian, A. (2012) Privacy by Design: Origins, Meaning, and Prospects for Assuring Privacy and Trust in the Information Era. In: Yee, George O.M. (Ed.): , IGI Global, 170-208.
7. Felt, U., Wynne, B. (2008) Taking European Knowledge Society Seriously: Report of the Expert Group on Science and Governance to the Science, Economy and Society Directorate, Directorate-General for Research, European Commission, IPOC Italian Paths of Culture.
8. Giddens, A. (1996) Risiko, Vertrauen und Reflexivität. Beck. U., Giddens, A., Lash, S. (Ed.): , Suhrkamp, Frankfurt am Main, 316-337.
9. Luhmann, N. (2000) – Vertrauen. Ein Mechanismus der Reduktion sozialer Komplexität, UTB, Stuttgart.
10. Lucke, D. (1995) , Leske + Budrich, Opladen.
11. Lyon, D. (2006) Airport Screening, Surveillance, and Social Sorting. Canadian Responses to 9/11 in Context, , 48, 3, 397-411.
12. Mayring, P. (2000) Qualitative Inhaltsanalyse. Grundlagen und Techniken, Beltz, Weinheim.
13. McPhail, B., Boa, K., Ferenbok, J., Smith, K. L., Clement, A. (2009) Identity, Privacy and Security Challenges with Ontario‟s Enhanced Driver‟s Licence. 2009 IEEE Toronto International Conference Science and Technology for Humanity (TIC-STH), 742–747.
14. Meuser, M., Nagel, U. (2002) ExpertInneninterviews – vielfach erprobt, wenig bedacht. Ein Beitrag zur qualitativen Methodendiskussion. Bogner, A., Littig, B., Menz, W. (Ed.) . Leske + Budrich, Opladen, 71-93.
15. Möllers, M., Hälterlein, J. (2013) Privacy issues in public discourse: the case of ‚smart„ CCTV in Germany. , 26, 1-2, 57-70.
16. Sanquist, T., Mahy, H., Morris, F. (2008) An Exploratory Risk Perception Study of Attitudes Toward Homeland Security Systems, , 28, 4, 1125-1133.
17. Schaar, Peter (2010) Privacy by Design, , 3(2), 267-274.
18. Siegrist, M., Cvetkovich, G. (2000) Perception of Hazards. The Role of Social Trust and Knowledge, , 20, 5, 713-719.
19. Sjöberg, L. (2001) Limits of Knowledge and the Limited Importance of Trust, , 21, 1, 189-198.
20. Töpfer, E. (2008) Videoüberwachung in Europa: Entwicklung, Perspektiven und Probleme. Kreowski, H.-J. (Ed.) , LIT Verlag, Berlin/Münster, 61-82.
21. Van Deth, J., Scarbrough (1995) The Concept of Values. Van Deth, J. W., Scarbrough, E. (Ed.): , 4, Oxford University Press, 21-47.
22. Viklund, M. (2003) Trust and Risk Perception in Western Europe: A Cross-National Study. , 23, 4, 727-738.
23. Witzel, A., Reiter, H. (2012) The problem-centred interview, Sage Publications, London.