Deliverable 4.1:
Public assessments of the security/privacy trade-off:
A criminological conceptualization

Authors:	Kristof Verfaillie (VUB) and Evelien van den Herrewegen (VUB freelance) in collaboration with Jenneke Christiaens and Serge Gutwirth (VUB)
Reviewers:	Michael Friedewald (Fraunhofer ISI)
Dissemination level:	Restricted to a group specified by the consortium
Deliverable type:	Report
Version:	1.0
Due date:	30 January 2013
Submission date:	05 November 2013

About the PRISMS project

The PRISMS project analyses the traditional trade-off model between privacy and security and devise a more evidence-based perspective for reconciling privacy and security, trust and concern. It examines how technologies aimed at enhancing security are subjecting citizens to an increasing amount of surveillance and, in many cases, causing infringements of privacy and fundamental rights. It conducts both a multidisciplinary inquiry into the concepts of privacy and security and their relationships and an EU-wide survey to determine whether people evaluate the introduction of security technologies in terms of a trade-off. As a result, the project determines the factors that affect public assessment of the security and privacy implications of a given security technology. The project uses these results to devise a decision support system providing users (those who deploy and operate security systems) insight into the pros and cons, constraints and limits of specific security investments compared to alternatives taking into account a wider society context.

Terms of use

This document was developed within the PRISMS project (see http://prismsproject.eu), co-funded by the European Commission within the Seventh Framework Programme (FP7), by a consortium, consisting of the following partners:

- Fraunhofer Institute for Systems and Innovation Research (Fraunhofer ISI), co-ordinator,

- Trilateral Research & Consulting LLP,

- Dutch Organization for Applied Scientific Research (TNO),

- Vrije Universiteit Brussel (VUB),

- University of Edinburgh (UEdin),

- Eőtvős Károly Policy Institute (EKINT),

- Hogeschool Zuyd and

- Market & Opinion Research International Limited (Ipsos-MORI)

This document may be freely used, copied, and distributed provided that the document itself is not modified or shortened, that full authorship credit is given, and that these terms of use are not removed but included with every copy. The PRISMS partners shall take no liability for the completeness, correctness or fitness for use. This document is subject to updates, revisions, and extensions by the PRISMS consortium. Address questions and comments to: Michael.Friedewald@isi.fraunhofer.de

Document history

Version	Date	Changes
1.0	05 November 2013	

Contents

1 INTRODUCTION

In 2010 the Belgian newspaper *De Standaard* published a series of articles and interviews about the use of body scanners at international airports. One of the contributions, titled "*Rather naked than dead*" (De Standaard, 09/01/2010), focused on the investments made in the full body scanner *Pro Vision* at Schiphol International Airport. These investments were deemed necessary in the wake of a terrorist incident involving a Nigerian man aboard Northwest Airlines flight 253 from Amsterdam to Detroit on 25 December 2009. The journalist suggests there seems to be a growing public acceptance for body scanners at airports, hence the new creed 'rather naked than dead', and he wonders how far we can go to guarantee security for our individuals.

The debate and the questions raised in *De Standaard* revolve around a prominent and authoritative framing of crime control issues, one that is commonly known as the security-privacy trade-off. The security-privacy trade-off is a particular narrative about security and privacy which essentially suggests that providing security inevitably entails individuals giving up some of their privacy and vice versa: 'every gain in privacy must be a loss in security'.[1] It implies a particular connection between privacy and security and this connection is conceptualized in terms of a balancing metaphor.[2] Debates about crime control issues which are framed in terms of a security-privacy trade-off therefore always revolve around striking the *right* balance between safeguarding security on the one hand, and infringing upon privacy on the other. The trade-off itself, however, is never fundamentally questioned in such stories. The idea that security and privacy are two distinct concerns that need to be balanced in order for a democracy to retain its legitimacy is simply assumed, implicitly or explicitly accepted, and is often believed to be self-evident. Whenever particular, more or exceptional security measures are deemed necessary, more infringements of privacy seem justified ('rather naked than dead') and vice versa: whenever there is less or no more need for particular security measures, individuals can be granted more privacy or claims for a return to 'normalcy', establishing another equilibrium between privacy and security, seem more justified (though this rarely happens)

The story '*Rather naked than dead*' suggests that the act of balancing security and privacy is one in which the individual seems to be an important evaluative criterion: whenever individuals seem more approving or accepting of security measures, like body scanners, this legitimizes the mobilization of these measures. As one of the representatives of Schiphol Airport claims, the use of *Pro Vision* is not only more effective, it also increases passenger comfort: 'we conducted tests and the majority of passengers preferred the body scanner over a body search' (De Standaard, 09/01/2010).

---

[1] The trade off argument is described in those terms by Solove, Daniel J., *Nothing to Hide: The False Tradeoff between Privacy and Security*, Yale University Press, London, New Haven, 2011, [34]. See also in Wright D., R. Gellert, S. Gutwirth & M. Friedewald, 'Precaution and privacy impact assessments as modes towards risk management' in R. Von Schomberg (ed.), *Towards Responsible Research and Innovation in the Information and Communication Technologies and Security Technologies Fields*, 2011, Luxembourg: Publication Office of the European Union, 93 : 'According to this view, balancing consists in simply opposing two values; it assumes that supporting one interest ipso facto weakens the other, that it is only possible to uphold one at the expense of the other'. Others similar descriptions already in De Hert, Paul, "Balancing security and liberty within the European human rights framework. A critical reading of the Court's case law in the light of surveillance and criminal law enforcement strategies after 9/11", Utrecht Law Review, 2005, Vol. 1, No. 1, pp. 91-93.

[2] van Lieshout, Marc, Michael Friedewald, David Wright, et al., "Reconciling privacy and security ", *Innovation: The European Journal of Social Science Research*, Vol. 26, No. 1-2, 2013, pp. 119 - 132; Zedner, Lucia, *Security*, Routledge, London; New York, 2009.

The PRISMS project intends to explore whether people actually evaluate security practices in terms of a trade-off between privacy and security and to that end a large-scale public opinion survey will be conducted. In this conceptual paper (task 4.1), we contribute to the development of the survey by providing a framework to explore and understand opinion formation about security practices in both quantitative and qualitative terms. The intent of this paper is therefore not so much to focus on what privacy and security *should* be like from the perspective of legal, criminological or philosophical scholarship. What matters is that we come to understand *how individuals evaluate security practices*, how *their* evaluations of 'security' and 'privacy' should be understood in this process, and how these questions can be further explored empirically. In other words, we do not simply intend to assess *how* individuals *balance* security and privacy, assess to what extent individuals are willing to give up privacy to obtain more security, nor do we intend to evaluate whether individuals have properly understood what security and privacy *should* be like. We may find that individual attitudes to privacy and security conflict with particular normative frameworks and this may indeed pose a number of relevant and important policy implications and challenges but that is not our main concern here. What needs to be explored is whether individuals' attitudes to security practices can be thought of in terms of a trade-off and whether it is useful to think of their attitudes in terms of balancing metaphors. As such, this paper focuses on the development of a conceptual framework that allows us to understand individual evaluations of security practices and points to specific analytical clues that can be examined further empirically in a survey and on the basis of a research design build for qualitative purposes (D4.2).

2 THE SECURITY-PRIVACY TRADEOFF: A META-NARRATIVE ABOUT SECURITY PRACTICES

The story about the use of *Pro Vision* body scanners at Schiphol International Airport is only one of many stories that circulate throughout society and many more stories can be found and are produced every day in which the evaluation of security practices is framed in terms of a trade-off. Some of these stories may come to opposite conclusions than the one suggested in '*Rather naked than dead*'. Public support for particular practices may for instance be found to be low or declining, the public may not be willing to give up their privacy to gain more security, so that a mobilization of particular security practices does not seem legitimate or no longer seems justified. What matters, however, is not so much what each of these stories reflect in their own right but that they all seem to have a particular baseline in common. They are all framed on the basis of a meta-narrative, 'a paradigm', about how security and privacy are connected. There is thus a particular structure to the evaluations *individuals* are believed to make about security practices and this structure can be thought of as a narrative which consists of a range of specific assumptions. If we are to understand whether individuals actually evaluate security practices in terms of a trade-off, it is precisely this basic narrative structure and its composing assumptions that first needs to be made explicit so that they can be further explored.[3]

2.1 THE STRUCTURE OF THE SECURITY-PRIVACY TRADE-OFF

The security-privacy paradigm can be summarized along the following lines: when individuals want more security, they are willing to give up some of their privacy. They are especially willing to do so in exceptional times, in the wake of significant security incidents or when they are fearful that such events may occur in the future. Individuals are willing to give up their privacy because they trust the security provider and because they think they are not threatened because they assume they have, as the argument goes, 'nothing to hide'. [4]

Following this argument, and drawing from the plain and summarizing descriptions of Solove, the security-privacy trade-off narrative can then be broken down into three basic components: (i) the 'pendulum argument'; (ii) 'the all-or-nothing fallacy'; and (iii) 'the nothing-to-hide argument'.[5] Many stories circulate throughout society about each of these arguments or assumptions but together these 'micro-stories' make up the security-privacy trade-off paradigm. Each component implies a trade-off of some sort and reflects another dimension of the security-privacy trade-off paradigm.

---

[3] The identification and analysis of these narratives is also subject of PRISMS work package 6. See Schuhmacher, Jana, Simone Kimpeler and Michael Friedewald, "Privacy and Security in the Media — Quantitative Analysis", PRISMS Deliverable 6.1, 2013.
[4] Interestingly, on November 2, 2013 two journalists summed up 10 reasons to dismiss the 'nothing to hide' argument in an opinion published in the daily newspaper *De Morgen* under the title: "Nee je hebt wel iets te verbergen ! (No, you do have something to hide !) http://www.demorgen.be/dm/nl/2461/Opinie/article/detail/1733598/2013/11/02/Nee-je-hebt-wel-iets-te-verbergen.dhtml Very timely issue indeed, especially after the revelations about the spying habits of the NSA.
[5] Solove, 2011, [55, 33, 21].

2.1.1   The pendulum argument

The pendulum argument refers to the idea that 'in times of crisis, we must sacrifice fundamental rights and liberties to gain security'.[6] It suggests that the evaluations individuals make of security practices is a dynamic process. Whenever a significant security incident occurs or whenever individuals fear such an event might occur, they are more willing to give up some of their fundamental rights and liberties and vice versa: whenever individuals are not fearful, or when they do not believe such incidents might occur, they are much less likely to give up on their fundamental rights and liberties. The pendulum argument is in part reflected in another contribution in the above mentioned *De Standaard* (09/01/2010), titled "*The greater the control, the smaller your freedom*". In the interview, J. Dumortier suggests that social acceptance of more intrusive security policies grows with every incident. He refers to the post-9/11 climate and to a public opinion survey conducted right after the incident on flight 253 (*supra*). In that survey 92% of the passengers responded claiming they had no problem with a full body scan, whereas prior to the incident only 75% responded in this way.

The pendulum argument therefore suggests that individuals' willingness to give up their fundamental rights and liberties is a *temporal* and highly *responsive* process. In other words, individuals' evaluations of security practices are a response to specific security incidents and threats and this response is situated and limited in time. When individuals are no longer fearful they will no longer favour more security measures and they will legitimize a return to normalcy, that is, a restoration of the fundamental rights and liberties they enjoyed prior to the exceptional times in which particular infringements were deemed necessary or felt to be acceptable.[7]

2.1.2   The all-or-nothing argument

The all-or-nothing argument refers to the idea that evaluating security practices is a matter of all-or-nothing choices: we either choose privacy or we favour a particular security measure.[8] It is perhaps the best-known component of the security-privacy trade-off paradigm and it is reflected in such statements and stories like '*Rather naked than dead*' (*De Standaard* 09/01/2013, see above). Security and privacy are perceived as abstract, clear and unambiguous categories, and the connections and dynamics between them are perceived as a zero-sum game.[9] Whatever is gained or has to be gained on the security side inevitably results in an equal loss on the side of privacy.

2.1.3   The nothing-to-hide argument

With Solove stories which are based on the nothing-to-hide argument imply that individuals give up their privacy because they reduce privacy to 'the right to hide things' so that they only focus on specific privacy problems – 'the disclosure of personal information or surveillance –

---

[6] Ibid., 55

[7] Indeed, there is a broad literature about the current perpetuation of the "state of exception" stemming from the work from Foucault and Agamben (in particular by Didier Bigo), but this falls outside the scope of this deliverable

[8] Solove, 2011, [33].

[9] Dourish, Paul and Ken Anderson, "Collective Information Practice: Exploring Privacy and Security as Social and Cultural Phenomena", *Human-Computer Interaction*, Vol. 21, No. 3, 2006, pp. 319-342; Pavone, Vincenzo and Sara Degli Esposti, "Public assessment of new surveillance-oriented security technologies: Beyond the trade-off between privacy and security", *Public Undestanding of Science*, Vol. 21, No. 5, 2012, pp. 556-572, [557].

while ignoring others'.[10] The trade-off, which is implied here, is that individuals are willing to give up their privacy because this makes security providers more effective. Individuals do not experience giving up privacy as a problem precisely because they have nothing to hide ("I've done nothing wrong so I do not need to worry") and they feel they can enhance their security because decreased privacy standards makes security providers more effective in tracing and making visible those who do seem to have something to hide.

2.2 CONCLUSION

The three components of the security-privacy trade-off paradigm provide specific analytical clues that can be explored further to understand whether people assess security practices in terms of a trade-off. The point is not to refute these arguments on a theoretical basis but to think of them as focal issues for empirical analysis. Are people more willing to give up privacy when they are fearful? Are people responsive to particular security issues so that they are willing to temporarily give up privacy when these issues occur? Are people more willing to give up their privacy when they believe they experience exceptional times of insecurity? Do people choose to either enhance their privacy or enhance their security? Do people reduce privacy to the right to secrecy or the right to hide things? From these questions three more specific focal issues can be distilled.

- First, if we are to understand how people evaluate security practices it seems important to understand *whether they experience fear or not*. In the three components of the security-privacy paradigm the subjective feelings of fear and insecurity are a recurrent issue. The assumption is that when people are fearful they seem to focus more on security issues, they are more accepting of security practices and they express less privacy concerns.
- A second important focal issue that runs through the security-privacy paradigm is *trust in the security provider*. People are willing to give up privacy when they trust those who provide security.
- The third focal issue is the *reduction of the notion of privacy*. Individuals seem more willing to give up privacy because they reduce privacy to very specific problems, i.e. the right to secrecy, while ignoring or simply being unaware of the existence of many others.

We will advance our argument by examining the first focal issue, drawing from the extensive criminological knowledge base about fear of crime. Based on these findings we can contribute to the quantitative survey in terms of hypotheses and survey questions and we will be able to connect them to the two remaining focal issues.

---

[10] Solove, 2011, [29].

3 PUBLIC RESPONSES TO SECURITY INCIDENTS: MEASURING FEAR OF CRIME

Understanding how people evaluate security incidents is a first important focal issue in assessing how people evaluate security practices and how this connects to their evaluations of privacy. The security-privacy trade-off suggests that when people fear that a security incident might occur, or when they are fearful and worry about a security incident, this affects their evaluations of security practices: it increases their perceived need for more security and it affects their willingness to give up fundamental rights and liberties. From a criminological perspective, understanding how people evaluate security incidents is therefore deeply connected to the knowledge base about fear of crime. Measuring fear of crime, however, remains a risky business and many methodological pitfalls have been identified. As we will see, the history of fear of crime research suggests that fear of crime can never be captured in terms of a simple, linear or unmediated response to a security incident nor can (or should) the complexity of fear of crime be captured in terms of single-item questions in surveys. In what follows, we do not intend to simply provide a historical overview of the fear of crime research tradition. Our overview serves specific analytical purposes and is tailored to the development of the PRISMS survey and the forthcoming empirical work in WP 4.

3.1 HISTORY OF FEAR OF CRIME RESEARCH

In his book 'Inventing fear of crime' Murray Lee situates the origins of fear of crime research in North America in the 1960s.[11] In 1967, the *President's Commission on Law Enforcement and Administrations of Justice* published a report based on the first victim surveys that were then being developed.[12] Lee suggests that 'fear of crime' was not a phenomenon waiting out there to be discovered. Its emergence was prompted by a growing political responsiveness to the public (especially the growing interest in victims) and fuelled by developments in social scientific research (especially the victim crime survey). Both developments initiated a feedback loop that helped to sustain and intensify the interest in fear of crime. Because of its political orientation, research on 'fear of crime' initially focused mainly on mapping which individuals seemed more fearful than others and on simply describing levels of fear. This approach to fear of crime quickly amounted to a number of difficulties (e.g. the fear of crime paradox, see section 3.2.1) that prompted researchers to go beyond descriptive analyses and focus more on understanding fear of crime.[13]

Researchers thus began exploring new and more complex questions: what causes fear of crime and how can we control this fear of crime? Despite 50 years of research, and although a wide range of factors contributing to fear of crime have been identified, there still is no scientific consensus about the main features and causes of 'fear of crime' and 'surprisingly little can be said conclusively about the 'fear of crime''.[14] This has led some scholars to

---

[11] Lee, Murray, *Inventing fear of crime: Criminology and the politics of anxiety*, Willan Publishing, Cullompton and Portland, Ore., 2007.

[12] Katzenbach, Nicholas, Genevieve Blatt, Charles D. Breitel, et al., "The Challenge of Crime in a Free Society: A Report by the President's Commission on Law Enforcement and Administration of Justice", U.S. Government Printing Office, Washington, D.C., 1967.

[13] van den Herrewegen, Evelien and Kristof Verfaillie, "Over waarheidsaanspraken in het veiligheidsdomein. De kloof tussen objectieve en subjectieve onveiligheid anders bekeken", *Panopticon*, Vol. 3, 2011, pp. 4-20.

[14] Ditton, Jason and Stephen Farrall, *The fear of crime*, Ashgate, Aldershot, 2000, [xxi].

wonder if 'such research is still worth doing'[15], while others remain more optimistic about its potential. For instance, Pleysier suggests the fear of crime research tradition can be revitalized in two main respects.[16]

The first is to focus on the conceptualization and operationalization of 'fear of crime'. Many problems in measuring and understanding fear of crime can be contributed to a lack of theoretical clarification about the main concept and/or an ineffective design of the questionnaire. Second, the scholarship about fear of crime could be advanced significantly if models would be developed that could integrate the different factors that were found to influence 'fear of crime'.[17] For the purpose of the PRISMS survey, and given the importance of understanding people's perception of security to the assessment of the security-privacy trade-off, we connect to this revitalization of the fear of crime research tradition. To that end, we will review the challenges and new developments in measuring 'fear of crime'. Based on this overview, we intend to surface specific focal issues and methodological guidelines about how to measure people's perception of security.

3.2   CHALLENGES AND NEW DEVELOPMENTS IN MEASURING FEAR OF CRIME

Within the 'fear of crime' research tradition a predominantly quantitative research design is used.[18] The features and causes of people's perception of safety are explored through grand scale surveys (e.g. National Crime Survey in the US and the British Crime Survey in the UK). Quantitative research designs first conceptualize and operationalize the phenomenon that needs to be measured and explained. Conceptualization entails defining the main components of a phenomenon. Based on theory and previous studies, this definition specifies what is characteristic of the issue at hand and what isn't. To examine the phenomenon empirically, the theoretical concept needs to be operationalized, that is, the theoretical components have to be translated into notions that can be measured empirically.[19]

3.2.1   *Conceptualization of fear of crime*

In a quantitative design conceptualization usually is a process that precedes the operationalization phase. However, in 'fear of crime' research, particular in the early days, theoretically situating the main concept was not really a priority. We have seen that 'fear of crime' was a highly politicized concept and not particularly theory driven. The conceptualization of 'fear of crime' was often simply the outcome of questions available in the surveys that were used or it was based on the traditional question: "How safe do you feel walking in your neighbourhood at night?"[20] As a consequence, some state that 'the phrase

---

[15] Fattah, E. A. , "Research on fear of crime: Some common conceptual and measurement problems", in Bilsky, W., et al. (eds.), *Fear of crime and criminal victimisation*, Ferdinand Enke Verlag, Stuttgart, 1993, [61].

[16] Pleysier, Stefaan, *'Angst voor criminaliteit' onderzocht: De brede schemerzone tussen alledaagse realiteit en irrationeel fantoom*, Boom Juridische, Den Haag, 2010, [97-98].

[17] Farrall, Stephen, Jonathan Jackson and Emily Gray, *Social order and the fear of crime in contemporary times*, Oxford University Press, Oxford and New York, 2009.

[18] Pleysier, 2010; Hale, Chris, "Fear of Crime: A Review of the Literature", *International Review of Victimology*, Vol. 4, 1996, pp. 79-150.

[19] Waege, Hans, "Operationaliseren", in Billiet, Jaak and Hans Waege (eds.), *Een samenleving onderzocht. Methoden van sociaal-wetenschappelijk onderzoek*, De Boeck nv., Antwerpen, 2003.

[20] Hofman, H., "Onveiligheid als stedelijk probleem", *Panopticon*, Vol. 12, 1991, pp. 575-591.

'fear of crime' has acquired so many divergent meanings that its current utility is negligible'.[21]

The first attempt to conceptualize 'fear of crime' was the work of Frank Fürstenberg in 1971.[22] Fürstenberg was one of the first researchers who attempted to make sense of the problems and inconsistencies that sprang from the initial and poorly conceptualized measurements of fear of crime. He set out to make sense of a specific inconsistency that can be traced back to the 'discovery' of 'fear of crime':

> "One of the most curious findings of the surveys was that fear of crime is less closely associated with having been a victim of crime than might be supposed."[23]

So survey results showed that 'the people least in danger are most afraid'. [24] This finding, known as the 'fear of crime paradox', is widespread and is still an object of scientific and political debate.[25] The paradox states that people with the lowest risk of criminal victimization, exhibit the highest fear (e.g. women and elderly), whereas people with a higher risk of victimization seem to be less fearful (e.g. young men).[26] This discrepancy between the objectively measured risk of victimization (crime statistics) and the subjectively measured fear of crime (victims surveys) lead to a debate about the rationality of people's fear of crime and it instigated the question whether 'fear of crime' was in fact a legitimate focus for policy initiatives.

Fürstenberg suggested that the fear of crime paradox was in fact the outcome of a poor conceptualization of fear of crime, and in an attempt to settle this issue he developed a model in which he distinguished two different responses to crime. On the one hand, his model identifies 'fear of crime' as an emotional component, which refers to people's personal risk assessment of becoming a victim. On the other hand, the model puts forward a cognitive component, a 'concern for crime', that is expressed by people's perception of crime as a serious social problem. Both components are a response to crime, but they function – relatively – independently. According to Fürstenberg this two-dimensional conceptualization cancels out the 'fear of crime' paradox. Within the model an individual can express a great concern about crime in contemporary society, and therefore score a high fear level when asked how s/he would feel safe in their neighbourhood at night, but at the same time show no heightened risk awareness. In research, however, both components are not always clearly defined, mutually distinguishable or adequately operationalized.[27]

Ferraro and LaGrange built on the Fürstenberg model and attempted to clarify some of the conceptual issues that remained in assessing fear of crime. They introduced some refinements to better identify and situate the different possible reactions to crime. Their classification is presented in the figure below. The basic purpose is to distinguish between risk and fear. [28]

---

[21] Ferraro, K. F. and R. L. LaGrange, "The Measurement of Fear of Crime", *Sociological Inquiry*, Vol. 57, 1987, pp. 70-101, [71].

[22] Fürstenberg, Frank, "Public Reaction to Crime in the Streets", *American Scholar*, Vol. 40, 1971, pp. 601-610.

[23] Katzenbach, et al., 1967, [51].

[24] Fürstenberg, 1971, [602-603].

[25] van den Herrewegen and Verfaillie, 2011.

[26] Vanderveen, Gabry, *Interpreting fear, crime, risk, and unsafety: Conceptualisation and measurement*, Boom Juridische Uitgevers, Den Haag, 2006.

[27] Pleysier, 2010.

[28] Ferraro and LaGrange, 1987, [71].

Figure 1: Classification of responses to crime

Level of Reference	Type of Perception		
	Cognitive Judgements	*Normative* Values	*Affective* Emotions
General	**A**: risk to others; crime or safety assessments	**B**: concern about crime to others	**C**: fear of others' victimization
Personal	**D**: risk to self; safety of self	**E:** Concern about crime to self; personal intolerance	**F**: fear for self victimization

Source: Ferraro et al. (1987)

First, Ferraro and LaGrange added a vertical axis that refers to the level of reference of the perceptions ranging from the personal or self-oriented to the general or community-oriented. The horizontal axis differentiates the types of perceptions. In this dimension we can see the cognitive and emotional components introduced by Fürstenberg, but Ferraro and LaGrange added a third normative component that significantly amends Fürstenberg's model. In his model the emotional component is a result of a personal risk assessment. Conversely, in the model developed by Ferraro and LaGrange, the personal risk assessment is defined as a cognitive component.

As such the cognitive component refers to judgments that are explicit or implicit subjective estimates of the risk of victimization, either for oneself (cell D); or for a social group (cell A). The emotional component, on the other hand, entails negative emotions, that is, a personal fear of becoming a victim of crime (cell F) or being afraid that others might be victimized (cell C). In this sense, Ferraro and LaGrange agree with Fürstenberg that an individual can ascribe oneself or others a heightened risk to become a victim of crime, but it does not entail that this individual feels more afraid, or is more worried about the safety of others. Finally, the normative component refers to value statements that reflect a concern about crime, either as a personal level of tolerance for crime (cell E), or as the public opinion about the seriousness of the crime problem (cell B).

The model of Ferraro and LaGrange is known as the classical conceptualization of the different responses to crime. In their classification, 'fear of crime' is only one part of the model and 'refers to the negative emotional reaction generated by crime or symbols associated with crime' and is 'conceptually distinct from either judgments (risks) or concerns (values) about crime'.[29] The model Ferraro and LaGrange developed was an important step in the fear of crime research, one that allowed researchers to significantly refine their assessment of fear of crime and its basic assumptions remain important until today. Yet their conceptual efforts did not settle some of the problems in fear of crime research. Some 'fear of crime' researchers did not always respect the principles outlined by the classification system: one or more components (like risk perception) have been used to explain the emotional component (fear of crime). Moreover, even when the Ferraro and LaGrange conceptualization was consciously applied many difficulties and inconsistencies remained and many researchers felt fear of crime still could not be adequately explained.[30]

From the end of the 1980s onwards, the concept of 'fear of crime' has been further refined. This refinement is closely linked with new and further attempts to solve the 'fear of crime' paradox, and to find more conclusive answers to the question of the causes of people's

---

[29] Ibid., 73
[30] Pleysier, 2010.

reactions to crime. Synthesizing almost 50 years of etiological 'fear of crime' research, the factors identified as influencing 'fear of crime' can now be roughly organized into four broad models to explain 'fear of crime'[31].

1. The *'victimization model'*, which focuses on the influence of direct but also indirect experiences of crime (e.g. victimization of friends, relatives, media coverage);
2. The *'vulnerability model'*, which states that certain individuals are physically (e.g. gender, age) and/or socially (e.g. socio-economic status, ethnic origin) more vulnerable to crime and thus to fear of crime;
3. The *'environmental model'* examines the physical (e.g. disorder) and/or social organization (e.g. lack of informal social control) of one's neighbourhood and its effects on people's reaction to crime;
4. Recently, in what we will refer to as the *'uncertainty model'[32]*, 'fear of crime' is no longer exclusively thought of in terms of an emotional response to crime, or to other deviant behaviour, nor does it only reflect a lack of resources to cope with these experiences, but it has also come to be seen as a manifestation of a broader sense of ill-being inherent to late modern society.

What the recent state of affairs in fear of crime scholarship essentially suggests is that 'fear of crime' is not necessarily or exclusively related to specific security incidents, although it can be connected to such incidents. People's perception of security can be explained in terms of individual characteristics and biographies, environmental factors and an expression of people's attitudes and concerns about society. Especially the importance of these latter range of attitudes has moved to the fore of criminological inquiry. Rooted in sociological theories developed by Ulrich Beck[33], Anthony Giddens[34], and Zygmunt Bauman[35], fear of crime researchers now connect 'fear of crime' to a late modern anxiety which is triggered by a gap between people's heightened awareness of risks and their uncertainty about how to handle these risks. People's incapacity to control the future (uncertainty), and their lack of resources to deal with risks (insecurity) are channelled into concerns about safety, of one's body, family and property. Particularly, individuals as well as policymakers seem to focus their attention on sources of fear that are identifiable and assignable, that is, the categorization of the 'criminal other'.[36]

As such, crime 'serve[s] unconsciously as a relatively reassuring site for displaced anxieties which otherwise would be too threatening to cope with'.[37] People's preoccupation with crime, then, seems to be a way to cope with late modern anxieties. Unlike the late modern risks, crime and crime-related issues function as a relative familiar domain in which victims can be identified and specific culprits can be blamed and these identities can be managed and can potentially be controlled.

---

[31] We will briefly discuss these four models, but for a more elaborate review we refer to Hale, 1996. but also Ditton and Farrall, 2000; Pleysier, 2010; Vanderveen, 2006.

[32] van den Herrewegen, Evelien, ""Safety: everybody's concern, everybody's duty"? Questioning the significance of 'active citizenship' and 'social cohesion' for people's perception of safety", in Cools, M., et al. (eds.), *Safety, Societal Problems and Citizens' Perceptions. New Empirical Data, Theories and Analyses*, Maklu, Antwerpen, 2010.

[33] Beck, Ulrich, *Risikogesellschaft: Auf dem Weg in eine andere Moderne*, Suhrkamp, Frankfurt am Main, 1986.

[34] Giddens, Anthony, *The consequences of modernity*, Polity Press, Cambridge, 1990.

[35] Bauman, Zygmunt, *Liquid Modernity*, Polity Press, Cambridge, 2000.

[36] Ibid.

[37] Hollway, Wendy and Tony Jefferson, "The Risk Society in an Age of Anxiety: Situating Fear of Crime", *British Journal of Sociology*, Vol. 48, No. 2, 1997, pp. 255-266, [264].

What this amounts to is a conceptual model in which 'fear of crime' is no longer considered to be a direct and *exclusive* emotional response to crime or any other deviant behaviour ('security incident'). It becomes a manifestation of a broader sense of ill-being triggered by late modern processes. As such, 'fear of crime' now has a component that refers to everyday experiences with crime (victimization) and the lack of resources to cope with these experiences (vulnerability and social disorganization) *and* an 'expressive' component in which 'fear of crime' is the outcome of individual attitudes and opinions about society as a whole.[38]

What is furthermore added is a temporal dimension, which entails a distinction between a 'state anxiety' and a 'trait anxiety'. The first is a transitory experience that is a direct emotional response to a situated and temporary experience (e.g. criminal victimization). Whereas, the second, is a more stable and general predisposition that causes an individual to be inherently (more) fearful regardless the occurrence of any particular incident.[39] In several studies new measurement tools have been devised to operationalize this conceptual distinction. In the next section we will further discuss the challenges and guidelines to operationalize 'fear of crime' for the purpose of the PRISMS survey.

3.2.2   *Operationalization of fear of crime*

We have seen how conceptual vagueness in fear of crime research has often resulted in ad hoc operationalization and a posteriori conceptualizations: the questions used in surveys prescribed how fear of crime was measured and how it was defined.[40] In addition to profound conceptual issues, the operationalization process itself has therefore also come under scrutiny. Following the advances made at the conceptual level, important and recurring critiques have come to be aimed at the traditional standard question that a majority of studies have used (and continue to use) to measure 'fear of crime': 'How safe would/ do you feel being out alone in your neighbourhood after dark'.

Overall, there is a consensus that this 'global' measure is not effective because: (i) the crime or security incident is never specified or explicitly mentioned; (ii) the notion 'neighbourhood' is open to various interpretations by different people; and (iii) respondents are asked about an experience or activity many of them are unfamiliar with. Building on the more advanced models to examine fear of crime it has furthermore become clear that single item indicators are inadequate to capture and understand the complexities of 'fear of crime'.[41]

Although these problems are now generally acknowledged, the standard question is still used in many surveys. Its use is often legitimized by the argument that the using the same measures is crucial to make comparisons, both in time and between groups of respondents. However, Pleysier points out that that a single-item indicator, not only jeopardizes the validity of the concept, but it also makes the instrument sensitive to measurement errors (reliability).[42] As such, the potential benefits of 'comparison' – the main pro argument to use the standard question – are annulled.

---

[38] Farrall, et al., 2009.
[39] Gabriel, Ute and Werner Greve, "The Psychology of Fear of Crime", *British Journal of Criminology*, Vol. 43, 2003, pp. 600-614.
[40] Pleysier, 2010.
[41] Ferraro and LaGrange, 1987, [73]; Hale, 1996.
[42] Pleysier, 2010.

We have seen how the Ferraro and LaGrange classification (*supra*) significantly advanced the fear of crime argument at the conceptual level and their conceptual adjustments had profound implications for the measurement of fear of crime. Instead of a single item indicator their classification outlines for each cell an exemplary instrument (question) that has to be used to measure fear of crime (*infra*).

Figure 2: Examples of Crime perceptions

	Type of Perception		
Level of Reference	*Cognitive* *Judgements*	*Normative* *Values*	*Affective* *Emotions*
General	**A**: Do you think that people in this neighbourhood are safe inside their homes at night?	**B**: Choose the single most serious domestic problem (from a list of ten) that you would like to see the government do something about.	**C**: I worry a great deal about the safety of my loved ones from crime and criminals
Personal	**D**: How safe do you feel or would you feel being out alone in your neighbourhood at night?	**E:** Are you personally concerned about becoming a victim of crime.	**F**: How afraid are you of becoming the victim of (16 separate offences) in your everyday life?

Source: based on the model in Ferraro et al. (1987)

Overall, the measurement tool makes a distinction between the different components in reaction to crime: the emotional component (fear of crime), the normative component (concern about crime) and the cognitive component (risk of victimization). Additionally, Ferraro and LaGrange formulated some pertinent guidelines on how to effectively measure the emotional component ('fear of crime'). In his review, Hale summarizes these guidelines in three general points.[43]

1. *Measuring the level of fear:* First of all, the measure should include 'how afraid' or some similar phrase. As such the traditional question 'How safe do you feel walking alone at night in your neighbourhood?' is not a measurement of the fear level, but refers to a personal assessment one makes about his/her risk to be a victim of crime: 'a person who says he or she would not feel very safe may not be afraid at all, but simply aware of the relative risk'.[44] The other components are important in their own right and should not be used as surrogates for the emotional response, nor are they to be used to explain fear of crime.

2. *Making security incidents explicit:* Second, the measure should make explicit reference to crime. Ideally specific categories of victimization should be used. Consequently, there can be no discussion whatsoever about what the respondent fears exactly.[45] Questions that probe a person's general assessment about crime are ineffective to measure people's fear

---

[43] Hale, 1996.

[44] Ferraro and LaGrange, 1987, [76].

[45] Farrall, Stephen and Jason Ditton, "Improving the measurement of attitudinal responses: An example from a crime survey", *International Journal of Social Research Methodology*, Vol. 2, No. 1, 1999, pp. 55-68.

of crime. Hale suggests to make at least a distinction between personal crimes and crimes against property.[46]

3. *Avoid hypothetical questions:* The third guideline suggests hypothetical questions should be avoided. Survey questions often refer to situations that people rarely encounter in their daily lives. Most people do not wander the streets at night. Therefore respondents should not be placed in a position in which they need to reflect on how they 'would' feel in particular situations. Questions have to refer to normal practices and ordinary situations, and if this is not possible, the fictitious examples presented have to be realistic and come close to the practices people are accustomed to in their everyday lives.

Similar to developments at the conceptual level, researchers began to further refine the traditional operationalization of fear of crime and they focused on measurement errors, which could potentially distort the assessment of fear of crime. One of the important debates in this respect was that measurement errors were found to lead to significant overestimations of people's responses to crime:

> "The results of fear of crime surveys appear to be a function of the way the topic is researched, rather than the way it is. The traditional methods used are methods, which seem consistently to over-emphasize the levels and extent of the fear of crime. It seems that levels of fear of crime, and to a lesser extent, of victimization itself, have been hugely overestimated".[47]

Recently, new measurement tools have therefore been devised and tested to measure people's fear of crime more accurately and to avoid such overestimations. These new measurements are more sensitive to capture people's specific experiences with crime and they follow the recent conceptual developments that differentiate between a situated and transitory 'experienced' fear of crime, and a more general and stable 'expressive' fear of crime.[48]

To make this distinction, Gabriel and Grave argue not to measure the *intensity* of experienced fear ('how fearful are you to become a victim of…?'), but to measure the *frequency* or incidence of certain fearful experiences ('how often have you been afraid to be a victim of ….?').[49] Farrall and his colleagues[50] have made a similar argument. They argue that few people experience specific events of worry on a frequent basis. What the 'old'-style questions did was in fact magnify the everyday experience of fear because these questions tapped into a diffuse anxiety about risk (cf. 'the uncertainty model, *supra*). To avoid measuring fear of crime in ways which result in a gross overestimation of fear of crime, Farral and colleagues suggest that we should avoid tapping into people's diffuse anxiety about risk and to focus on

---

[46] Hale, 1996.

[47] Farrall, Stephen, Jon Bannister, Jason Ditton, et al., "Questioning the Measurement of the Fear of Crime: Findings From A Major Methodological Study", *British Journal of Criminology*, Vol. 37, No. 4, 1997, pp. 657-678, [676].

[48] Jackson, Jonathan, "Experience and Expression. Social and Cultural Significance in the Fear of Crime", *British Journal of Criminology*, Vol. 44, 2004, pp. 946.

[49] Gabriel and Greve, 2003.

[50] Farrall, Stephen and David Gadd, "The Frequency of the Fear of Crime", *Britisch Journal of Criminology*, Vol. Britisch Journal of Criminology, No. 44, 2004, pp. 127-132; Gray, Emily, Jonathan Jackson and Stephen Farrall, "Reassessing the Fear of Crime", *European Journal of Criminology*, Vol. 5, No. 3, 2008, pp. 363-380.

more accurate measurements of people's fear for criminal victimization[51] or their worries about becoming a victim of a specific criminal offence.[52]

To develop a more fine-tuned way to assess worries or fear, then, requires researchers to include a specific set of questions into survey tools, which intend to assess people's fear of crime.[53]

> Q1: 'In the past year, have you ever felt worried about … (car theft/burglary/robbery) or fearful about the possibility of becoming a victim of crime? [no, yes, cannot remember]
>
> Q2: [if YES at Q1] 'How frequently have you felt like this in the last year?' [n times recorded]
>
> Q3: [if YES at Q1] 'On the last occasion how fearful did you feel?' [not very worried, a little bit worried, quite worried, very worried or cannot remember]

The first two questions focus on the frequency of events that caused worry or fear in the last year. These are filter questions: they allow estimates of the regularity with which people worry about or fear crime and they allow researchers to classify respondents according to whether they worry about specific crimes, if they do, and how often. The third question asks the respondents to reflect on the last event, and indicate their intensity of worry or fear. Conversely to measuring individuals and the number of times each individual worries or felt fearful, this question samples events.

The results of the studies conducted in 2004 and 2008 on the basis of this measurement tool are remarkable. Both studies indicate that the incidence of worry or fear of crime is actually quite low in the population. The study in 2004 found that only a third of the respondents had experienced any fear provoking episode in the past year, and half of the sample who felt fearful in the past year only felt fearful between one and four occasions. In total around 15% of the sample had felt a moderate to high level of fear. When the researchers assessed the intensity and the frequency of fear, they found evidence that less than one in ten people (8%) frequently experienced (5 times or more per year) a moderate to high level of fear.[54]

In the 2008 study[55] the aim was to explore the utility of these new questions in direct comparison with the 'old' standard methods that have been used in surveys such as the authoritative British Crime Survey. Both instruments were presented to the same sample. For instance, based on the traditional measurements 47% of the respondents worried fairly (35%) or highly (12%) about burglary, 12% were 'not at all' worried, and 41% were 'a bit' worried. However, based on the new measurement focusing on the frequency of worry, 32% indicated that they had worried about being burgled over the past 12 months. Moreover, people worried relatively infrequently: 59% of those who confirmed some experience of worry in the past year, reported that they worried between 1 and 11 times, which is less than once a month. Only 12 per cent said they worried more than once a week. Meanwhile, taking into account the intensity of worry, the vast majority of the most recent events of worry were rather low:

---

[51] Farrall and Gadd, 2004.
[52] Gray, et al., 2008.
[53] Farrall and Gadd, 2004; Gray, et al., 2008.
[54] Farrall and Gadd, 2004.
[55] Gray, et al., 2008.

83% indicated to be either 'a little bit' or only 'quite' intensely worried. Overall, using the total sample, the researchers found that just 3% would describe their last fearful event as 'very' worrying.

3.3 CONCLUSION

Policymakers are convinced that fear of crime is a significant social problem and that fearfulness leads to increases in punitive attitudes among the population.[56] People's fear of crime is therefore often used as a legitimation for the mobilization of security practices and investments in security measures: many people seem to be fearful, and when they are fearful they are believed to be more punitive so that more security measures are believed to be needed to tackle fear of crime.[57] Gray, *et. al.* suggested that this basic assumption might be unwarranted: when research focuses on a more experientially based conception of fear, it seems to be a relatively infrequent experience and specific events of worry are relatively rare.(Gray et al. 2008)[58]

The findings thus far are important conceptually and methodologically and they go to the heart of the security-privacy trade-off. The way fear of crime is usually measured in surveys, and in particular those surveys adopting single-item indicators or old-style questions, is precisely what has prompted the policy assumption that the majority of the public wants more security. New and more accurate measurements of fear of crime directly challenge this idea. We furthermore explored the knowledge base of fear of crime research and found that, contrary to popular belief or intuition, fear of crime can never be thought of in terms of a straightforward, linear and exclusively emotional response to crime ('security incident') or any other deviant behaviour.

People's fear of crime is believed to reflect everyday experiences with crime (victimization) and the lack of resources to cope with these experiences (vulnerability and social disorganization) and it reflects their attitudes and opinions about society as a whole, which means that fear of crime can manifest itself as a broader sense of ill-being triggered by late modern processes. Fear of crime furthermore has a temporal dimension, which means that it can be seen as a response to a situated experience (e.g. victimization) and as a more stable and general predisposition that causes an individual to be inherently (more) fearful regardless the occurrence of any particular incident.[59]

One of the key assumptions of the security-privacy trade-off, the idea that when individuals want more security they are willing to sacrifice some of their rights and liberties, thus becomes a much more complex issue than the trade-off suggests. Precisely because fear of crime is no straightforward, linear and exclusively emotional response to crime ('security incident') or any other deviant behaviour it can never be thought of as a simple response to a security incident. For that same reason simply eliminating the security incident or mobilizing security practices to prevent such a specific event from occurring can never mitigate people's fear of crime. The connection between being fearful and wanting more security is much less clear than often assumed and the same holds true for the evaluations people make of rights

---

[56] Farrall, et al., 2009, [15].
[57] Garland, David, *The culture of control: Crime and social order in contemporary society*, University of Chicago Press, Chicago, 2001; Langworthy, R. H. and J. T. Whitehead, "Liberalism and fear as explanations of punitiveness", *Criminology*, Vol. 24, No. 3, 2006, pp. 575-591.
[58] Gray, et al., 2008, [378].
[59] Gabriel and Greve, 2003.

and liberties: it is not because people express fear of crime that they are willing to give up some of their rights and liberties to mitigate that fear. Because fear of crime never is a simple linear response to a security incident, the practices that need to be mobilized to mitigate that fear, including people's willingness to give up their rights and liberties, can never be known in advance but is precisely what needs to be examined in opinion studies.

What follows, then, is that the first focal issue to be examined in both the quantitative survey and the qualitative study is the connection between expressing fear of crime, a support for security practices, and the evaluations people make of their fundamental rights and liberties. Because no 'if-then' relationships can be assumed among any of these processes they need to be considered as distinct conceptual spaces and autonomous objects of research in which a connection, like the one suggested by the security-privacy trade-off, is not already assumed. Only when we treat each of these processes as autonomous focal issues empirically can we begin to understand the connections that exist between them and can we genuinely assess whether it is useful to think of them in terms of a trade-off.

What this means, then, is that we should avoid embedding a trade-off paradigm into survey questions, treat 'security' and 'privacy' as distinct focal issues instead, while developing research formats that allow for connections between these notions to be examined. For the purpose of the PRISMS survey this implies that we can formulate a first hypothesis: '*the more fearful people are, the less privacy concerns they have*'. Yet we examine this hypothesis without explicit referral to the security-privacy trade-off in the survey questions themselves, which is precisely what often leads to the creation of a security-privacy trade-off. For instance, the question: "*Should the government be allowed to read e-mails and listen to phone calls to fight terrorism?*"[60] is a question, which not only includes both the security and privacy issue. At the same time, it connects both issues for the respondent in highly specific ways, that is, a security-privacy trade-off is assumed and created. Some suggest that this issue might be overcome by simply rephrasing such issues, by restoring the balance between privacy and security in terms of making the privacy issue more explicit in the survey question. For instance: "*Should the government be allowed to read e-mails and listen to phone calls to fight terrorism without a search warrant or the appropriate court order required by law to fight terrorism?*"[61]

The point here is not that such questions may not be useful or that the latter question may not lead to more differentiated responses. The point is that such survey questions inevitably frame the issue at hand in terms of a trade-off. We therefore proceed by examining our first hypothesis by first focusing on the security issue and we do so following the work of Gray *et. al.*, who proposed an adjusted measurement strategy for fear of crime which 'focuses on events of worry; although it explores the intensity of the last fearful event, it does not elicit an overall intensity summary of worry', which is precisely what allows for more accurate measurements to be made[62].

---

[60] Solove, 2011.
[61] Ibid.
[62] Gray, et al., 2008, [368]. In their research the authors suggest that 'questions about the frequency of worry measure something more specific than questions about an overall intensity of worry; in many instances, standard indicators may be tapping into a more diffuse anxiety'. So what they did to obtain more accurate measurements is to eliminate more diffuse anxieties from the assessment of fear of crime. In doing so, Gray and colleagues do not suggest that these diffuse anxieties are unimportant. The authors have made a distinction for analytical purposes here, one that is highly relevant for our understanding of the security-privacy trade-off, which suggests that people are responsive to security incidents.

For comparative purposes, the methodological framework can simply be adopted (cf. *supra*) or it can be modified and given an explicit European focus, that is, the events that can be made explicit are those that European policymakers have come to focus on (which is not 'burglary' or 'robbery'). Based on the European threat assessments, three specific events can be identified that can be included in the survey: (i) terrorism; (ii) cybercrime; (iii) commodity counterfeiting with a focus on illicit trade in sub-standard goods and goods violating health and safety regulations (this includes foods and beverages, body care articles, medicines, electrical household items and toys.[63] The former phenomena are often explicitly connected to privacy concerns. The latter is a new trend in Europe, it can be seen as a specification of organized crime activity (another EU-priority), one that will be an important focus for policymakers in the definition of the EU's crime control strategy for the next four years.

As such, the questions to be included in the survey:

Q1: 'In the past year, have you ever felt worried about . . . ?' [terrorism / cybercrime / commodity counterfeiting]

Q2: [if YES at Q1] 'How frequently have you felt like this in the last year?' [n times recorded]

Q3: [if YES at Q1] 'On the last occasion how fearful did you feel?' [not very worried, a little bit worried, quite worried, very worried or cannot remember]

What needs to be further explored at this point is how the connection between expressing fear of crime, a support for security practices, and the evaluations people make of their fundamental rights and liberties can be understood, and how our focus on fear of crime connects to the second part of the first hypothesis '*the more fearful people are, the less privacy concerns they have*'.

For a further developed assessment of fear of crime including the measurement of more diffuse anxieties see Gray, Emily, Jonathan Jackson and Stephen Farrall, "Feelings and functions in the fear of crime: applying a new approach to victimisation insecurity", *British Journal of Criminology*, Vol. 51, No. 1, 2011, pp. 75-94.
[63] Europol, "SOCTA 2013. EU Serious and Organised Crime Threat Assessment", European Police Office, The Hague, 2013.

4   THE IMPORTANCE OF TRUST, KNOWLEDGE, AND FRAMING

In a study conducted in the European PRISE project researchers explored public assessments of new surveillance-oriented security technologies (SOSTs), and they examined whether individuals adopt a security-privacy trade-off in doing so and what factors individuals take into consideration when making such assessments.[64] What they found was that individuals can make different kinds of evaluations of SOSTs and only in specific cases do they evaluate these technologies in terms of a trade-off. Based on literature review, quantitative analysis and qualitative focus group interviews with individuals largely four potential evaluations can be discerned (Figure 3).

Figure 3: Interpretations of SOSTs as security enhancing and/or privacy infringing devices

SOSTs interpreted as…	…privacy infringing devices	
….security enhancing devices	Yes	No
Yes	Trade-off	Trusting attitude
No	Concerned attitude	Uninterested

Source: Pavone et al. (2012)

So what Pavone and Esposti suggest is that only those groups of individuals who think of SOSTs in terms of both security enhancing and privacy infringing evaluate these technologies in terms of a trade-off.[65] Individuals who believe that SOSTs are security enhancing and who do not believe these SOSTs infringe their privacy are individuals who trust the mobilization of SOSTs and they seem to think of 'security' as the most important issue at stake. Individuals who do not think of SOSTs as security enhancing and who believe these technologies infringe their privacy have a concerned attitude towards the mobilization of SOSTs and to them the main issue at stake is privacy. Finally there are those individuals who simply seem uninterested: they do not believe that SOSTs are security enhancing nor do they think of these technologies as privacy infringing. Pavone, *et. al.* suggest these individuals either find the debate uninteresting or they frame their evaluation of SOSTs in very different ways than the four potential responses suggest.[66]

In the qualitative section of their study, however, Pavone and Esposti found that individuals seldom evaluate SOSTs in abstract terms, that is, they hardly ever seemed to think of security and privacy as exchangeable goods.[67] The evaluations their respondents made were highly situated and connected to the contexts in which a particular SOST is mobilized. As such, the respondents could be divided in roughly two groups. The first group expressed concerns about the ability of SOSTs to enhance security and they perceived them as privacy infringing (cf. 'concerned attitude', table 3) and the second group believed SOSTs to be security enhancing without infringing their privacy. As such, Pavone and Esposti conclude that individual evaluations of SOSTs cannot primarily be thought of in terms of a trade-off: 'concerned

---

[64] Pavone and Esposti, 2012.

[65] Ibid., 558-559

[66] Pavone, Vincenzo, Sara Degli Esposti and E. Santiago, "Surveillance, Privacy and Security: A large scale participatory assessment of criteria and factors determining acceptability and acceptance of security technologies in Europe", SurPRISE Deliverable 2.2, 2013.

[67] Pavone and Esposti, 2012, [556, 568].

individuals saw their privacy being infringed without having their security enhanced, whilst trusting individuals saw their security being increased without their privacy being affected'.[68] The study of Pavone and Esposti surfaces new and important analytical clues that can help us make sense of the evaluations people make of security practices and whether it is useful to think of these evaluations in terms of a trade-off. As such, they allow us to advance our argument in three important ways: (i) trust in the security provider (ii) the issue of 'knowledge'; (iii) framing and authority.[69]

4.1 TRUST IN THE SECURITY PROVIDER

We have seen that Pavone and Esposti found two distinct and dominant attitudes or range of evaluations of SOSTs: a distinction could be made between 'concerned' individuals and 'trusting' individuals.[70] There is, however, one key issue that binds both attitudes together and that is the issue of *trust*: 'the extent to which an individual may engage with SOSTs will depend on the extent to which that individual perceives the security agency using the SOSTs as trustworthy'.[71] In other words, when people trust the security provider they believe their security will be enhanced and they do not believe their privacy to be (significantly) affected. When people do not trust the security provider, they do not believe their security will be enhanced and they believe their privacy will be infringed. The key issue to be understood, then, is trust in the security provider and as Pavone and Esposti suggest this issue is much more complex than might appear at first glance. What seems to matter is the mobilization of SOSTs, the way SOSTs are deployed as a security practice, or what Pavone and Esposti refer to as the contextual interplay between technologies and institutions:

> 'People displaying a low level of trust towards the scientific and political institutions implementing these technologies tended to join the first group, prioritizing privacy and expressing concern that these technologies could be manipulated and diverted to other purposes. In contrast, the people more trustful towards both technologies and institutions tended to join the second group, prioritizing security and showing a much lower level of concern for privacy'.[72]

What this means, at its most basic level, is that assessments of trust in the security provider and the most common SOSTs need to be included in the PRISMS survey. As is the case in fear of crime research, for pragmatic reasons surveys often adopt single-item indicators and questions to assess trust in public institutions. For instance, surveys might include the question: 'Can you say for each of the following institutions and measures whether you have much trust in them or little trust? (very little trust, little trust, little nor much trust, some trust, much trust). The security providers that would be assessed are the police, justice, private security, and so forth. The measures that could be assessed are CCTV, body scanners, profiling, and biometrics.

The problem with such survey questions is that they allow us to assess how much people trust institutions across Europe, and they might show that trust in security providers varies widely

---

[68] Ibid., 556
[69] Ibid.
[70] Ibid.
[71] Pavone, et al., 2013, [90].
[72] Pavone and Esposti, 2012, [561].

across Europe, as the current social surveys show.[73] They do not, however, allow us to assess and understand *why* and *how* trust in security providers matters to the evaluations people make about the mobilization of security practices. The research hypothesis that can be drawn from the study of Pavone and Esposti, which is that the higher the level of trust in specific security providers and measures, the less people believe their privacy is infringed, conceals a complexity that cannot simply be assessed in terms of single-item indicators and research questions. However, in the criminological knowledge base there are conceptualizations of trust that allow us to tackle precisely this issue.

4.1.1   *Procedural justice*

Recently, the issue of trust has been given much and renewed attention in European research programs and surveys (e.g. European Social Survey, round 5), as well as in criminological scholarship.[74] What this research interest focuses on is theories of procedural justice, which essentially suggests that 'how justice officials use their power is an important influence on public trust and institutional legitimacy'.[75] What researchers attempt to assess and understand is 'the ability of a criminal justice system to command legitimacy in the eyes of the public – whether the policed see the police as legitimate'.[76] The key proposition, then, is that if security providers, like the police, treat people fairly and respectfully, and if this treatment is aligned with public perceptions of morality, they will be regarded as having legitimate authority, and will be better able to command compliance and cooperation'.[77]

What this implies for the focal issue in this study is that when people evaluate security practices they are much more likely to perceive a security provider as legitimate and they are much more likely to comply and cooperate when they believe their rights are being respected and they are treated respectfully. In the following model (figure 4), Hough illustrates how these processes should be understood exactly.[78]

---

[73] Jackson, Jonathan, "Trust in European justice institutions is markedly lower in southern and eastern Europe, but legitimacy also requires that institutions meet substantive requirements to legitimise their power and structure",

[74] Hough, Mike, Jonathan Jackson, Ben Radford, et al., "Procedural justice, trust and institutional legitimacy", *Policing: a journal of policy and practice*, Vol. 4, No. 3, 2010, pp. 203-210; Hough, Mike, Jonathan Jackson and Brad Radford, "Legitimacy, trust and compliance: an empirical test of procedural justice theory using the European Social Survey", in Tankebe, Justice and Alsion Liebling (eds.), *Legitimacy and criminal justice: An international exploration*, Oxford University Press, Oxford, 2013; Tyler, Tom R. and Jonathan Jackson, "Future challenges in the study of legitimacy and criminal justice", in Tankebe, Justice and Alsion Liebling (eds.), *Legitimacy and criminal justice: An international exploration*, Oxford University Press, Oxford, 2013; Hough, Mike, B. Radford, Jonathan Jackson, et al., "Attitudes to sentencing and trust in justice: exploring trends from the crime survey for England and Wales", Ministry of Justice, London, 2013; Jackson, Jonathan , Tia Pooler, Katrin Hohl, et al., "Trust in justice: Topline results from round 5 of the European Social Survey", ESS topline results series 1, European Commission, 2011; Hough, Mike, "Researching trust in the police and trust in justice: A UK perspective", *Policing and Society*, Vol. 22, No. 3, 2012, pp. 332-345.
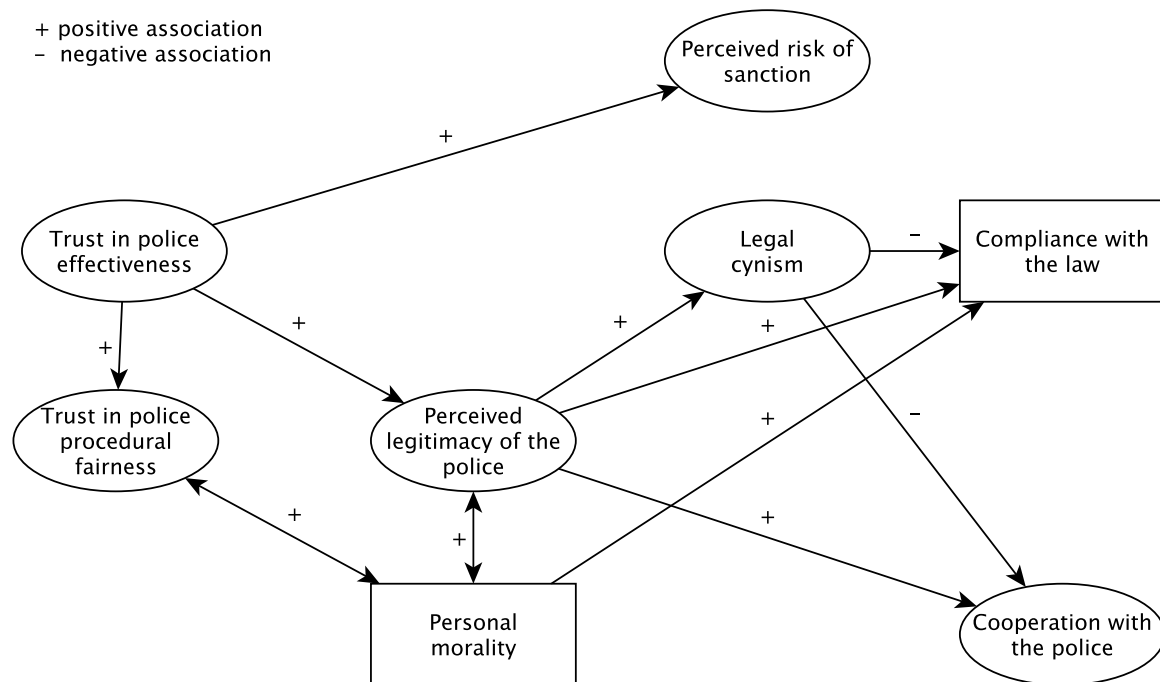
[75] Hough, et al., 2013, [55].

[76] Hough, 2012, [336].

[77] Ibid.

[78] Ibid., 341

Figure 4: Public trust and police legitimacy

+ positive association
− negative association

Source: Hough (2012), p. 341

This model visualizes the key findings about the relationships that exist between 'public trust', 'perceived legitimacy', and 'people's self-reported compliance with the law and cooperation with the police' and these findings can be summarized along the following lines: people seem to comply with the law not because they fear to be punished when they don't but because they feel they ought to. When they experience procedural fairness this prompts people to identify with the security provider, a motive-based trust emerges in the provider, so that people feel they are on the same side as the security provider. They begin 'to feel a sense of obligation to the police and more likely to feel aligned with the ethical and moral framework they believe the police to embody'. When this happens, when the security provider is perceived to be legitimate, this results in compliance.[79]

So when the security provider wields authority in ways, which are perceived to be unjust and unfair, Hough suggests this results in 'legal cynicism', that is people become cynical about human nature and legal systems of justice so that they no longer perceive of particular laws and norms as personally binding.[80] These same processes, legal cynicism, perceived legitimacy and personal morality are therefore also important drivers for cooperation with the security provider.

The key point to be retained from these studies is that 'trust in the effectiveness of the police and the justice system plays a smaller role than trust in fairness'.[81] What seems to matter to the legitimacy of the security provider, and to people's willingness to comply and cooperate is how they are treated by the security provider. Hough *et al.* point out that in perceptions of

---

[79] Ibid., 341-342
[80] Ibid., 342
[81] Hough, et al., 2013.

fairness both processes and outcomes are equally important: 'people pay particular attention to the presence or absence of fair procedures, and to the quality of treatment received from justice officials'. [82]

The connection between fair treatment, perceived legitimacy and people's willingness to cooperate and comply, then, is clear: 'fair and respectful handling of people, treating them with dignity, and listening to what they have to say, all emerge as significant predictors of legitimacy, and thus preparedness to cooperate with legal authorities and comply with the law'. [83]

4.2 THE SITUATED NATURE OF 'KNOWLEDGE'

Thus far we have seen how 'trust in the procedural fairness of the police and perceptions of the legitimacy of the police are the most important predictors of public willingness to cooperate with legal authorities'. [84] We believe these findings connect to and advance the argument made by Pavone and Esposti [85] in significant ways. They suggested that 'citizens' concerns about the introduction of SOSTs should first and foremost be attributed to their mistrust in the institutions that use and regulate these technologies. In other words, and following the recent findings about the importance of procedural justice, when people trust and experience procedural fairness in the contexts where security practices are mobilized, when they identify with the security provider, develop a feeling of motive-based trust ('the security provider and I are on the same side') and begin to feel a sense of obligation and alignment with the ethical and moral framework the security provider is believed to embody, this results in compliance and cooperation, i.e. the SOST is no longer perceived to be a problem. When this trust and experience of procedural fairness is absent and when the security provider is not felt to be legitimate, legal cynicism becomes important so that people become cynical about human nature and legal systems of justice and no longer perceive particular laws, regulations and the ensuing mobilization of security practices to be personally binding.

Pavone and Esposti furthermore suggest that the distinction between concerned individuals and trusting individuals should not be mistaken for a distinction between individuals who are knowledgeable about science and technology versus individuals who lack such knowledge. [86] In other words, there is no distinction between individuals who know what is really going on, they dispose of the proper information about the technical capabilities of SOSTs and they are fully informed about privacy regulations, versus those individuals who do not dispose of this information and only appear to know what is going on.

Individuals do not simply assess security practices in which technologies are mobilized on the basis of technical information about a particular technology. They seem to use, amend and refer to a variety of knowledges ('institutional, legal, social, moral') to evaluate security practices. [87] How this process works exactly, what kinds of information people use to evaluate security practices and what information sources they turn to, is precisely what needs to be

---

[82] Ibid., 56
[83] Ibid., 6
[84] Ibid., 55
[85] Pavone and Esposti, 2012.
[86] Ibid., 567
[87] Ibid.

further explored. At this point, the theory of procedural justice and the findings of Pavone and Esposti suggest that stories about procedural fairness and perceived legitimacy of the security provider will play a key role in individuals' evaluations of security practices but here too the challenge will be to better understand how such stories are constructed.

4.3 FRAMING

Finally, the study of Pavone and Esposti points to the importance of how people frame issues when they evaluate security practices. What they found was that

> 'the more citizens actually trusted public institutions, the more they saw security as a priority, which SOSTs effectively addressed. In contrast, the more they distrusted these institutions, the more they considered privacy as a priority, expressed doubts about the way in which security as an issue was constructed, and questioned whether technology could really be a solution to security threats'.[88]

Notice, then, how two groups of individuals frame the issue of 'a security strategy' in profoundly different ways and notice how they turn to conceptual spaces which are distinctly different to make these evaluations. In the first narrative trusting individuals perceive 'security' as *the most important issue* and they believe SOSTs effectively enhance security *and* they don't believe their privacy is infringed. Following our previous findings, these evaluations can be explained in terms of stories about SOSTs in which people experience procedural fairness in the mobilization of these technologies. They identify with the security provider. The security provider seems to share the focus and motives of the individual, or its motives and focus seem justified and are felt to embody the ethical and moral evaluative criteria the individual can identify with. In other words, this narrative reflects the experience of a procedural fairness and perceived legitimacy of the security provider so that no conflict exists between the objectives of the security provider and the way these objectives are attained on the one hand, and the definitions of security developed by the individual and his experiences and expectations with how this security is attained and should be attained on the other.

Notice then too how in the evaluations these individuals make the idea of a trade-off between privacy and security as a balancing act between two distinct conceptual spaces dissolves. As soon as an alignment emerges between what the security provider and the individual focus attention and action on, and as the individual begins to develop a sense of fairness in the way s/he is treated by the security provider there is no more perceived conflict between security and privacy. Yet, there is a second and closely related consideration that dissolves the idea of two separate considerations that can or need to be weighed off and this is connected to how issues are framed. When people attribute authority to a particular construction or framing of a security issue and when they identify with the framing of that same security issue by the security provider, the security issue becomes the main point of reference to evaluate security practices. In other words, the way people frame a particular problem points to potential settlements of that problem.[89] The framing of a security issue is therefore not only relevant for

---

[88] Ibid., 564
[89] van Swaaningen, René, *Critical criminology: Visions from Europe*, SAGE, London and Thousand Oaks, Calif., 1997; Hulsman, Louk, "Critical criminology and the concept of crime", *Contemporary Crisis*, Vol. 10, 1986, pp. 63-80; Verfaillie, Kristof, Kristel Beyens, Jan Blommaert, et al., "De overlastmythe: Het geïnstitutionaliseerd onvermogen om constructief om te gaan met samenlevingsproblemen?", *Panopticon*, Vol. 3, No. 28, 2007, pp. 6 - 20.

the security issue by itself, at the same time it frames the settlement of that issue. For instance, in its analysis of the 9/11 terrorist attacks, the National Commission on Terrorist Attacks upon the United States framed the security incident as a problem of foresight (imagination), policy, capabilities and management so that a solution to such future security incidents in terms of improvements of foresight, policy, capabilities and management becomes self-evident.[90]

What remains is not a balancing act between two distinct considerations but one particular narrative in which the problematisation of a particular security issue and its settlement is made and felt to be normal and self-evident and it becomes the reference point for the evaluation of security practices. As such, the privacy issue no longer is an issue in its own right, it simply becomes part of the security framing and it becomes subjected to the evaluative criteria of security issue.

In the second narrative we can discern the mirror image of the previous narrative. Concerned individuals distrusted the mobilization of particular security practices and the more they did the more they felt privacy was a priority, expressed doubts about the way in which security as an issue was constructed, and questioned whether technology could really be a solution to security threats. Based on the findings about procedural justice, these evaluations can then be seen to reflect a lack of perceived legitimacy of the security provider and a lack of trust in procedural fairness about the mobilization of SOSTs.

The observation that this group of respondents expresses doubts about the construction of security by the security provider and that they express concerns that 'these technologies might be manipulated and diverted to other purposes' implies that these individuals do not identify with the security provider the way the first group does.[91] They can be convinced or they experience that the security provider wields authority in ways which are perceived to be unjust and unfair and become cynical about human nature and legal systems of justice so that they no longer believe particular laws and norms apply to them. They might simply feel the security provider is not on their side in that its motives and focus do not embody the ethical and moral evaluative criteria the individual identifies with ('the security provider does not seem to take my fundamental rights and liberties seriously'). In other words, because trust in procedural fairness and perceived legitimacy is low there is no felt obligation to simply cooperate and comply, or to a much lesser extent.

The concerns emerge, then, from a conflict between the objectives of the security provider and the way these objectives are pursued on the one hand, and the definitions of security developed by the individual and his experiences and expectations with how this security is achieved and should be achieved on the other. The rights of these individuals have neither necessarily been violated nor do they necessarily feel the security provider does not comply with the law. These respondents may just as well feel the privacy standards upheld and embodied by the police is something they do not identify and align themselves with ('even though the police may act according to the law, I nevertheless find these standards insufficient').

In these evaluations too the idea of a trade-off between two distinct concerns dissolves. The fact that the security provider does not embody the moral and ethical framework these

---

[90] Kean, Thomas H., Lee H. Hamilton, Richard Ben-Veniste, et al., "The 9/11 Commission Report. Final Report of the National Commission on Terrorist Attacks upon the United States", Executive Summary, Washington, D.C., 2004.

[91] Pavone and Esposti, 2012, [561].

respondents can identify with, and because conflicts emerge over the construction of 'security', respondents frame the SOST in terms of a privacy issue. The evaluation of the SOSTs is thus no trade-off but one narrative in which privacy, a concern about privacy infringements, is what respondents focus action and attention on. In these cases, the SOST is framed as a privacy problem and it is this framing, which becomes the reference point for the evaluation of the SOST. They come to be seen as a privacy problem so that a mitigation or settlement of this problem can be found in measures, which first and foremost eliminate the privacy problem. This framing is felt to be normal and self-evident and because there is no alignment with the evaluative criteria of the security provider, its framing of the issue is felt to be abnormal or simply unjustified, that is, individuals do not believe the security provider is on their side and they feel their security is not enhanced and their privacy is infringed.

5 UNDERSTANDING INDIVIDUAL EVALUATIONS OF SECURITY PRACTICES: A QUALITATIVE STUDY

We outlined the structure of the security-privacy trade-off and the focal issues its key elements bring so that we could develop a basic framework to analyse and obtain a preliminary understanding of *how* individuals evaluate security practices. We did so on the basis of a literature review of the relevant key findings in public opinion research about fear of crime and trust in the police and justice. We argued that in order to make sense of people's evaluations of security practices, and to understand whether trade-off models or balancing metaphors are useful to that end, there are three distinct issues that need to be considered: fear of crime, a support for security practices and the evaluations people make of their fundamental rights and liberties.

We suggested that no if-then-relationships can be assumed among these processes but that the connections that exist between them is precisely what needs to be explored if we are to assess whether it is useful to think individual evaluations of security practices in terms of a trade-off. As such, we found that individuals' evaluations of security incidents can never be thought of as an unmediated response to such incidents, that is, the response is not 'dictated' or prescribed by the nature of the incident nor can analysis of the incident by itself provide any insight in how individuals respond to such issues. Yet this is precisely what is prescribed by the pendulum argument which suggests that in exceptional times individuals are temporarily willing to give up some of their Fundameltal rights and liberties to gain more security (an argument which is often legitimized by a particular field of surveys or opinion polls).[92]

Notice how the exceptional times are prescribed by the security incident and this is believed to result in a straightforward response in individuals toward the incident: they are believed to express fear or worry about the incident, demand more security measures to mitigate the event or prevent it from reoccurring, and they give up some of their fundamental rights and liberties to that end or they are willing to except a new equilibrium between security and privacy. We believe the knowledge base about fear of crime does not provide sufficient ground for such assumptions. Individuals are responsive to security incidents but their responses are always particular framings of such incidents and these framings are never simply prescribed by the security incident. How people frame security incidents and how this connects to expressions of fear of crime and demands for 'more security' is what therefore needs to be better understood empirically.

We also found that in the evaluations individuals make of security practices what seems to matter is (i) trust in the security provider, conceptualized in terms of the framework of procedural justice; (ii) the knowledges and information resources people mobilize to make sense of security practices, and; (iii) how individuals experience and frame security practices. The survey shall shed some descriptive light on individual evaluations of security practices. However, if we are to make sense of these evaluations, we will have to develop the above analytical clues. Therefore, in the last section of this paper we advance and refine our conceptual argument and we do so by developing a research design that will allow us to further clarify the analytical issues at hand and explore individual evaluations *qualitatively*. Because the focal issues under study have proven to be highly complex and situated processes, we need to further examine them from a qualitative perspective and more specifically we will do so on the basis of a critical discourse analysis.

---

[92] See also Watson, Hayley, David Wright, Rachel L. Finn, et al., "Report on Existing Surveys", PRISMS Deliverable 7.1, 2013.

5.1   CRITICAL DISCOURSE ANALYSIS

From a qualitative perspective, neither security nor privacy are static or uniform notions. They are situated *practices*, and their content has been subject to profound disputes over meaning, form and practice.[93] What thus needs to be examined is what 'security' and 'privacy' mean in practice and how these notions are shaped throughout individuals interactions. To that end we will conduct a critical discourse analysis.[94]

'Discourse analysis' is a generic term that refers to a wide variety of analytical perspectives that focus on the creation and emergence of meaning as a social practice.[95] As such, a discourse analysis differs significantly from traditional text – or conceptual studies in which concepts are either explored in philosophical terms or in terms of merely descriptive accounts of the content of a particular text. Discourse analysts essentially focus on how 'meaning' is made, and this process is believed to be a social practice. In other words, the analysis of concepts, in this case 'security' and 'privacy', is not something that should be done in an abstract sense and its outcome can never be the construction of generic definitions. If we are to make sense of any concept or notion, scholars in the field of critical discourse analysis suggest we should connect them to concrete and situated practices. What matters, then, is making sense of how 'security' and 'privacy' are used in people's daily lives so that what these notions mean exactly is the outcome of human interactions and these interactions are situated in time and place (or what discourse analysts refer to as context).

Critical discourse analysts suggest that we cannot understand how privacy and security are shaped, and how these concepts are used throughout people's daily interactions, by focusing on a particular conversation (a particular 'text') alone, but that we need to take the socio-cultural and historical context of a conversation into account as well. The creation and emergence of meaning, the way we use words and the conceptual spaces they trigger, are the outcome of a process that begins long before one particular conversation or interaction has taken place.

Context does not determine how individuals evaluate particular security practices, but as Pavone and Esposti suggested, within their evaluations of SOSTs individuals point to such elements, they mobilize 'security' and 'privacy' in specific ways and not others, they talk about some issues and not others, and they are asked to evaluate particular issues (in this case 'security practices') and not others.[96] To understand individual evaluations therefore requires a research design which acknowledges these contextual elements so that context is something that needs to be made explicit and accepted as an object of analysis. The first step, then, is to clarify and make explicit what we ask individuals to evaluate exactly and Blommaert[97] suggests such research designs unfold in three distinct steps: (i) analysis of the gradual key transformations of 'security practices'; (ii) analysis of the more rapid and visual

---

[93] See also Blommaert, Jan, *Discourse: A Critical Introduction*, Cambridge University Press, Cambridge, 2005.

[94] Ibid.; Blommaert, Jan and Kristof Verfaillie, "Discoursanalyse", in Decorte, Tom and Damián Zaitch (eds.), *Kwalitatieve methoden en technieken in de criminologie*, Acco, Leuven/Den Haag, 2009; Jaworski, Adam and Nik Coupland (eds.), *The Discourse Reader*, Routledge, London, 1999; Wodak, Ruth and Michael Meyer, *Methods of Critical Discourse Analysis*, Sage, London, 2001.

[95] Jaworski and Coupland (eds.), 1999.

[96] Pavone and Esposti, 2012.

[97] Blommaert, 2005. See also Blommaert, Jan, K. Beyens, H. Meert, et al., *Grenzen aan de solidariteit. Formele en informele patronen van solidariteit in het domein van migratie, huisvesting en veiligheid*, Academia Press, Gent, 2005.

transformations of the policy developments in the field under study; (iii) analysis of the micro-practices being developed in those sites selected on the basis of both previous steps. At this point we outline these three basic analytical steps and they will be further elaborated on and refined in the empirical analysis in PRISMS Deliverable 4.2.

5.1.1   Analysis of the gradual transformations of 'security practices'

A consensus has grown in criminological scholarship that in the past decades fundamental changes have occurred in the governance of crime and what it means to provide security.[98] According to Loader and Sparks[99] contemporary landscapes of crime, order, and control are characterized by 'a fragmentation and diffusion of power, the emergence of new sites of social authority, the deployment of new rationalities and technologies of rule, and the advent of new professional actors and expert knowledges'. In addition to this new governance of crime, with the reconfiguration of policing and prevention, the responsibilizing of individuals, and the rise of the private security industry, Loader and Sparks point to the centrality of a risk rationality in criminal justice matters and to the challenges a globalized crime control poses to our prevailing notions of democracy and individualship.

What these transformations amount to is that crime control is no longer to be localized within the well-defined boundaries of particular public institutions, but takes place in diverse sites and is dispersed over a wide variety of public and private actors.[100] In this fragmented field of crime control, the collection and sharing of personal data has come to play a pivotal role. The various actors involved in crime control have come to develop and use new surveillance technologies and rationalities to collect, process and analyse personal data about individuals or populations to regulate, control, govern, or enable their activities.[101]

Individual evaluations of security practices occur against the background of these gradual and basic transformations. Throughout their daily lives individuals experience and are subjected to such practices which therefore provide the context in which these evaluations are shaped and they provide the empirical clues as to what we ask individuals to evaluate exactly.

5.1.2   Analysis of policy developments

The next step is to understand how the broad transformations described in the first step have come to structure policy developments at the European level. The past 20 years, the EU has gradually begun to develop what is now referred to as an 'area of freedom, security and justice' (FSJ). What this means is that 'security' and privacy' became discursive themes, the object of particular political action at the European level. From the end of the 1990s onwards, the EU has developed three main strategic programmes, the *Tampere Programme* (1999-2004), the *Hague Programme* (2004-2009) and the *Stockholm Programme* (2010-2014). These multi-annual programmes have developed and shaped specific and fundamental notions of security and privacy, they entail the selection and categorization of specific 'security'

---

[98] See for instance Garland, 2001.

[99] Loader, Ian and Richard Sparks, "Contemporary landscapes of crime, order and control. Governance, risk, and globalization", in Maguire, Mike, et al. (eds.), *The Oxford Handbook of Criminology*, Clarendon Press, Oxford, 2002, [87].

[100] Rose, Nikolas, "Government and control", in Garland, David and Richard Sparks (eds.), *Criminology and social theory*, Oxford University Press, Oxford, 2000.

[101] Coleman, Roy and Mike McCahill, *Surveillance and Crime: Key Approaches to Criminology*, Sage, London, 2011.

problems and they point to specific settlements of those problems. As such, they have given rise to highly specific practices the individual is faced with and they entail a refinement of what the individual is asked to evaluate in empirical analysis.[102]

5.1.3 *Individual evaluations of security practices*

One of the sites where both the gradual transformations of security practices as well as its European framing have materialized, are international airports. Airports are contexts where the area of freedom, security and justice can perhaps best be felt and evaluated by individuals. As such, these are settings, which best allows us to explore how individuals evaluate contemporary security practices. The methodological choices that need to be made to study individual evaluations of security practices flow from the conceptualization developed thus far as well as the basic principles of a critical discourse analysis, and this results in three clear methodological pointers for further empirical study.

1. A focus on experiences

To understand individual evaluations is to focus on individual experiences. Following the literature review about fear of crime and following Blommaert[103], individuals have to be asked about practices, which seem part of their normal and ordinary routines and hypothetical questions should be avoided. Elliott[104], with Hollway and Jefferson[105], suggests that this requires interviews in which the respondent is enabled to tell stories and is asked 'to talk directly about his or her experiences' and is invited 'to talk about specific times and situations'.

Following our conceptualization, people have to be invited to tell stories about security incidents they worry about and why, about why they support particular security strategies and about the precise nature of their privacy concerns. We have seen that individuals evaluate each of these themes, and the connections that exist between them, in highly specific ways and it is precisely these categorizations we need to map and understand.

2. Focus on information resources

We have seen that when individuals evaluate security practices, they do not simply do so on the basis of technical information about SOSTs or by using 'factual' information about security practices. People evaluate security practices using various kinds of information and drawing from a variety of information resources. This focus on information resources is of great importance, not only because authors like Pavone and Esposti[106] found that individual evaluations of security practices are highly situated, but because one of the most robust findings in opinion research about security practices is that most people do not know that much about such practices.[107]

---

[102] For an overview and draft analysis see Bodea, Gabriela, Noor Huijboom, Sander van Oort, et al., "Draft analysis of privacy and security policy documents in the EU and US", PRISMS Deliverable 3.1, 2013.

[103] Blommaert, 2005.

[104] Elliott, Jane, *Using narrative in social research: Qualitative and quantitative approaches*, SAGE, London, 2005, [30].

[105] Hollway, Wendy and Tony Jefferson, *Doing qualitative research differently: Free association, narrative and the interview method*, SAGE, London and Thousand Oaks, 2000.

[106] Pavone and Esposti, 2012.

[107] See for instance Flanagan, Timothy J., "Public opinion on crime and justice: history, development, and trends", in Flanagan, Timothy J. and D.R. Longmire (eds.), *Americans view crime and justice. A national public opinion survey*, Sage, Thousand Oaks, Calif., 1996; Flanagan, Timothy J., "Public opinion, crime and justice. An

What matters, then, is not that we distinguish between groups of respondents who are knowledgeable about these practices and individuals who aren't and attempt to understand how such differences can be explained and to what extent factual information is important in these evaluations. Surely such distinctions can be useful for some purposes, policymakers might be interested to know how much individuals actually know about security practices and what the effects are of such knowledge. Yet the main focal issue our empirical work requires us to understand how individuals evaluate security practices and whether they do so on the basis of a trade-off. So what matters is that individuals in spite of their lack of factual knowledge do voice opinions about these issues. As such, it becomes important to understand the kinds of information resources do people turn to when they evaluate security practices. Which information sources seem important to them and which ones seem much less important?

3. Polycentrism

The final issue we will have to make sense of is that when exploring individual evaluations of security practices, scholars have found that people are ambivalent about such issues and that people's evaluations, when considered as a whole, seem to show many inconsistencies.[108] What this means is that we, contrary to what Pavone and Esposti suggest, cannot simply categorize individual evaluations of security practices into four different and clear cut responses.[109] Like people can seem to favour and support contradicting punishment ideologies at the same time[110], we can expect them to frame security practices both as a privacy issue and as a security issue. The different responses Pavone and Esposti found can therefore be expected to co-exist at the same time.

Following Blommaert[111], we therefore need to treat individual evaluations about security practices as a polycentric field: they contain multiple normative points of orientation, which can be contradictory when considered as a whole. In some of their evaluations about security practices people will thus orient toward particular kinds of information that prompts them to perceive security strategies as a privacy concern, while in other cases they will primarily be oriented towards particular categorizations of the security issue. As such, these evaluations cannot be thought of in terms of a trade-off or in terms of one general or abstract statement in the form of 'SOSTs enhance my security or infringe my privacy'.

American perspective", in Parmentier, S., et al. (eds.), *Public opinion and the administration of justice. Popular perceptions and their implications for policy-making in Western countries*, Politeia, Brussel, 2003; Roberts, Julian V. and J. M. Hough, *Understanding public attitudes to criminal justice*, Open University Press, Maidenhead and New York, 2005; Hough, et al., 2013.

[108] Flanagan, "Public opinion on crime and justice: history, development, and trends", 1996; Flanagan, "Public opinion, crime and justice. An American perspective", 2003; Stalans, L., "Measuring attitudes to sentencing", in Roberts, Julian V. and Mike Hough (eds.), *Changing attitudes to punishment. Public opinion, crime and justice*, Willan Publishing, Cullompton, 2002. See also Verfaillie, Kristof, "Punitive needs, society and public opinion: an explorative study of ambivalent attitudes to punishment and criminal justice", in Snacken, Sonja and Els Dumortier (eds.), *Resisting punitiveness in Europe?*, Routledge, London, 2012.

[109] Pavone and Esposti, 2012.

[110] Roberts and Hough, 2005.

[111] Blommaert, 2005, [254].

6. CONCLUSION

The security-privacy trade-off paradigm is a meta-narrative about how individuals are believed to evaluate security practices. It is story with a basic narrative structure, which suggests that when individuals want more security, they are willing to give up some of their privacy. They are especially willing to do so in exceptional times, in the wake of significant security incidents or when they are fearful that such events may occur in the future. Individuals are willing to give up their privacy because they trust the security provider and because they have nothing to hide.

Our conceptualization challenges many of the assumptions implied by the security-privacy trade-off and it suggests that we should think differently about how people evaluate security practices. When people express a fear of crime or when they worry about particular security incidents, this does not automatically imply support for particular security practices nor does it imply that people feel they have to give up their fundamental rights and liberties. When people evaluate security practices they do not simply balance or weigh off two distinct concerns. They frame a security practice in a particular way, and they do so on the basis of various information resources and by referring to or using specific points of reference, a process which cannot simply be reduced to their knowledge of the legal standards, efficiency and effectiveness of a security practice.

What seems to matter most in people's evaluations of security practices is trust in the security provider. As soon as individuals experience procedural fairness and begin to identify and align with the moral and ethical evaluative criteria of the security provider, they are much more willing to subject themselves to the security practices mobilized by the security provider, and they believe their security is enhanced without their privacy being infringed. When they do not trust the security provider, they can begin to challenge its categorizations of security and they can begin to voice privacy concerns, which becomes the most important issue to them.

The process of aligning and identifying with the security provider can, however, not be thought of in terms of one general attitude ('citizens either trust the provider or they don't'). Individuals evaluations of security practices are polycentric so that, depending on how a security practice is framed, individuals may or may not align or identify with the security provider and they may use distinctly different categorizations of privacy and security within this process. As such, making sense of individual evaluations no longer becomes a matter of assessing how and whether individuals strike the right balance between privacy and security. It becomes a matter of coming to grips with the complex and various ways in which people frame security practices, and the information resources and stories they turn to in that process. It becomes a matter of understanding how, within the stories they turn to, they identify and align themselves with the security provider and develop highly particular categorizations of 'security' and 'privacy'.

7. REFERENCES

Bauman, Zygmunt, *Liquid Modernity*, Polity Press, Cambridge, 2000.

Beck, Ulrich, *Risikogesellschaft: Auf dem Weg in eine andere Moderne*, Suhrkamp, Frankfurt am Main, 1986.

Blommaert, Jan, *Discourse: A Critical Introduction*, Cambridge University Press, Cambridge, 2005.

Blommaert, Jan, K. Beyens, H. Meert, S. Hillewaert, K. Stuyck, and Kristof Verfaillie, *Grenzen aan de solidariteit. Formele en informele patronen van solidariteit in het domein van migratie, huisvesting en veiligheid*, Academia Press, Gent, 2005.

Blommaert, Jan, and Kristof Verfaillie, "Discoursanalyse", in Tom Decorte, and Damián Zaitch (eds.), *Kwalitatieve methoden en technieken in de criminologie*, Acco, Leuven/Den Haag, 2009, pp. 311 – 338.

Bodea, Gabriela, Noor Huijboom, Sander van Oort, Merel Ooms, Bas van Schoonhoven, Tom Bakker, Livia Teernstra, Rachel L. Finn, David Barnard-Wills, David Wright, and Charles D. Raab, "Draft analysis of privacy and security policy documents in the EU and US", PRISMS Deliverable 3.1, 2013.

Coleman, Roy, and Mike McCahill, *Surveillance and Crime: Key Approaches to Criminology*, Sage, London, 2011.

van den Herrewegen, Evelien, ""Safety: everybody's concern, everybody's duty"? Questioning the significance of 'active citizenship' and 'social cohesion' for people's perception of safety", in M. Cools, B. De Ruyver, M. Easton, L. Pauwels, P. Ponsaers, G. Vande Walle, T. Vander Beken, F. Vander Laenen, G. Vermeulen, and G. Vynckier (eds.), *Safety, Societal Problems and Citizens' Perceptions. New Empirical Data, Theories and Analyses*, Maklu, Antwerpen, 2010, pp. 85-108.

van den Herrewegen, Evelien , and Kristof Verfaillie, "Over waarheidsaanspraken in het veiligheidsdomein. De kloof tussen objectieve en subjectieve onveiligheid anders bekeken", *Panopticon*, Vol. 3, 2011, pp. 4-20.

Ditton, Jason, and Stephen Farrall, *The fear of crime*, Ashgate, Aldershot, 2000.

Dourish, Paul, and Ken Anderson, "Collective Information Practice: Exploring Privacy and Security as Social and Cultural Phenomena", *Human-Computer Interaction*, Vol. 21, No. 3, 2006, pp. 319-342.

Elliott, Jane, *Using narrative in social research: Qualitative and quantitative approaches*, SAGE, London, 2005.

Europol, "SOCTA 2013. EU Serious and Organised Crime Threat Assessment", European Police Office, The Hague, 2013. https://http://www.europol.europa.eu/sites/default/files/publications/socta2013.pdf

Farrall, Stephen, Jon Bannister, Jason Ditton, and Elizabeth Gilchrist, "Questioning the Measurement of the Fear of Crime: Findings From A Major Methodological Study", *British Journal of Criminology*, Vol. 37, No. 4, 1997, pp. 657-678.

Farrall, Stephen, and Jason Ditton, "Improving the measurement of attitudinal responses: An example from a crime survey", *International Journal of Social Research Methodology*, Vol. 2, No. 1, 1999, pp. 55-68.

Farrall, Stephen, and David Gadd, "The Frequency of the Fear of Crime", *Britisch Journal of Criminology*, Vol. Britisch Journal of Criminology, No. 44, 2004, pp. 127-132.

Farrall, Stephen, Jonathan Jackson, and Emily Gray, *Social order and the fear of crime in contemporary times*, Oxford University Press, Oxford and New York, 2009.

Fattah, E. A. , "Research on fear of crime: Some common conceptual and measurement problems", in W. Bilsky, Christian Pfeiffer, and P. Wetzelf (eds.), *Fear of crime and criminal victimisation*, Ferdinand Enke Verlag, Stuttgart, 1993.

Ferraro, K. F., and R. L. LaGrange, "The Measurement of Fear of Crime", *Sociological Inquiry*, Vol. 57, 1987, pp. 70-101.

Flanagan, Timothy J., "Public opinion on crime and justice: history, development, and trends", in Timothy J. Flanagan, and D.R. Longmire (eds.), *Americans view crime and justice. A national public opinion survey*, Sage, Thousand Oaks, Calif., 1996, pp. 1-15.

Flanagan, Timothy J., "Public opinion, crime and justice. An American perspective", in S. Parmentier, G. Vervaeke, R. Doutrelepont, and G. Kellens (eds.), *Public opinion and the administration of justice. Popular perceptions and their implications for policy-making in Western countries*, Politeia, Brussel, 2003, pp. 53-76.

Fürstenberg, Frank, "Public Reaction to Crime in the Streets", *American Scholar*, Vol. 40, 1971, pp. 601-610.

Gabriel, Ute, and Werner Greve, "The Psychology of Fear of Crime", *British Journal of Criminology*, Vol. 43, 2003, pp. 600-614.

Garland, David, *The culture of control: Crime and social order in contemporary society*, University of Chicago Press, Chicago, 2001.

Giddens, Anthony, *The consequences of modernity*, Polity Press, Cambridge, 1990.

Gray, Emily, Jonathan Jackson, and Stephen Farrall, "Reassessing the Fear of Crime", *European Journal of Criminology*, Vol. 5, No. 3, 2008, pp. 363-380.

Gray, Emily, Jonathan Jackson, and Stephen Farrall, "Feelings and functions in the fear of crime: applying a new approach to victimisation insecurity", *British Journal of Criminology*, Vol. 51, No. 1, 2011, pp. 75-94.

Hale, Chris, "Fear of Crime: A Review of the Literature", *International Review of Victimology*, Vol. 4, 1996, pp. 79-150.

Hofman, H., "Onveiligheid als stedelijk probleem", *Panopticon*, Vol. 12, 1991, pp. 575-591.

Hollway, Wendy, and Tony Jefferson, "The Risk Society in an Age of Anxiety: Situating Fear of Crime", *British Journal of Sociology*, Vol. 48, No. 2, 1997, pp. 255-266.

Hollway, Wendy, and Tony Jefferson, *Doing qualitative research differently: Free association, narrative and the interview method*, SAGE, London and Thousand Oaks, 2000.

Hough, Mike, Jonathan Jackson, Ben Radford, Andy Myhill, and Paul Quinton, "Procedural justice, trust and institutional legitimacy", *Policing: a journal of policy and practice*, Vol. 4, No. 3, 2010, pp. 203-210.

Hough, Mike, "Researching trust in the police and trust in justice: A UK perspective", *Policing and Society*, Vol. 22, No. 3, 2012, pp. 332-345.

Hough, Mike, Jonathan Jackson, and Brad Radford, "Legitimacy, trust and compliance: an empirical test of procedural justice theory using the European Social Survey", in Justice Tankebe, and Alsion Liebling (eds.), *Legitimacy and criminal justice: An international exploration*, Oxford University Press, Oxford, 2013.

Hough, Mike, B. Radford, Jonathan Jackson, and Joanne R. Roberts, "Attitudes to sentencing and trust in justice: exploring trends from the crime survey for England and Wales", Ministry of Justice, London, 2013.

Hulsman, Louk, "Critical criminology and the concept of crime", *Contemporary Crisis*, Vol. 10, 1986, pp. 63-80.

Jackson, Jonathan, "Experience and Expression. Social and Cultural Significance in the Fear of Crime", *British Journal of Criminology*, Vol. 44, 2004, pp. 946.

Jackson, Jonathan, "Trust in European justice institutions is markedly lower in southern and eastern Europe, but legitimacy also requires that institutions meet substantive requirements to legitimise their power and structure", http://blogs.lse.ac.uk/europpblog/category/authors/jonathan-jackson/.

Jackson, Jonathan , Tia Pooler, Katrin Hohl, Jouni Kuha, Ben Bradford, and Mike Hough, "Trust in justice: Topline results from round 5 of the European Social Survey", ESS topline results series 1, European Commission, 2011. http://www.europeansocialsurvey.org/docs/findings/ESS5_toplines_issue_1_trust_in_justice.pdf

Jaworski, Adam, and Nik Coupland (eds.), *The Discourse Reader*, Routledge, London, 1999.

Katzenbach, Nicholas, Genevieve Blatt, Charles D. Breitel, Kingman Brewster, Garrett H. Byrne, Thomas J. Cahill, Otis Chandler, Leon Jaworski, Thomas C. Lynch, Ross L. Malone, James B. Parsons, Jr. Lewis F. Powell, William P. Rogers, Robert G. Storey, Julia D. Stuart, Robert F. Wagner, Herbert Wechsler, Jr. Whitney M. Young, and Luther W. Youngdahl, "The Challenge of Crime in a Free Society: A Report by the President's Commission on Law Enforcement and Administration of Justice", U.S. Government Printing Office, Washington, D.C., 1967. draft d4.1final draft clean.docx

Kean, Thomas H., Lee H. Hamilton, Richard Ben-Veniste, Bob Kerrey, Fred F. Fielding, John F. Lehman, Jamie S. Gorelick, Timothy J. Roemer, Slade Gorton, and James R.Thompson, "The 9/11 Commission Report. Final Report of the National Commission on Terrorist Attacks upon the United States", Executive Summary, Washington, D.C., 2004. http://www.gpoaccess.gov/911/pdf/execsummary.pdf

Langworthy, R. H., and J. T. Whitehead, "Liberalism and fear as explanations of punitiveness", *Criminology*, Vol. 24, No. 3, 2006, pp. 575-591.

Lee, Murray, *Inventing fear of crime: Criminology and the politics of anxiety*, Willan Publishing, Cullompton and Portland, Ore., 2007.

van Lieshout, Marc, Michael Friedewald, David Wright, and Serge Gutwirth, "Reconciling privacy and security ", *Innovation: The European Journal of Social Science Research*, Vol. 26, No. 1-2, 2013, pp. 119 - 132.

Loader, Ian, and Richard Sparks, "Contemporary landscapes of crime, order and control. Governance, risk, and globalization", in Mike Maguire, Rod Morgan, and Robert Reiner (eds.), *The Oxford Handbook of Criminology*, Clarendon Press, Oxford, 2002, pp. 81-111.

Pavone, Vincenzo, and Sara Degli Esposti, "Public assessment of new surveillance-oriented security technologies: Beyond the trade-off between privacy and security", *Public Undestanding of Science*, Vol. 21, No. 5, 2012, pp. 556-572.

Pavone, Vincenzo, Sara Degli Esposti, and E. Santiago, "Surveillance, Privacy and Security: A large scale participatory assessment of criteria and factors determining acceptability and acceptance of security technologies in Europe", SurPRISE Deliverable 2.2, 2013. http://surprise-project.eu/wp-content/uploads/2013/10/SurPRISE-D2.2-Draft-Report-on-Key-Factors.pdf

Pleysier, Stefaan, *'Angst voor criminaliteit' onderzocht: De brede schemerzone tussen alledaagse realiteit en irrationeel fantoom*, Boom Juridische, Den Haag, 2010.

Roberts, Julian V., and J. M. Hough, *Understanding public attitudes to criminal justice*, Open University Press, Maidenhead and New York, 2005.

Rose, Nikolas, "Government and control", in David Garland, and Richard Sparks (eds.), *Criminology and social theory*, Oxford University Press, Oxford, 2000, pp. 183-208.

Schuhmacher, Jana, Simone Kimpeler, and Michael Friedewald, "Privacy and Security in the Media — Quantitative Analysis", PRISMS Deliverable 6.1, 2013.

Solove, Daniel J., *Nothing to Hide: The False Tradeoff between Privacy and Security*, Yale University Press, London, New Haven, 2011.

Stalans, L., "Measuring attitudes to sentencing", in Julian V. Roberts, and Mike Hough (eds.), *Changing attitudes to punishment. Public opinion, crime and justice*, Willan Publishing, Cullompton, 2002.

van Swaaningen, René, *Critical criminology: Visions from Europe*, SAGE, London and Thousand Oaks, Calif., 1997.

Tyler, Tom R., and Jonathan Jackson, "Future challenges in the study of legitimacy and criminal justice", in Justice Tankebe, and Alsion Liebling (eds.), *Legitimacy and criminal justice: An international exploration*, Oxford University Press, Oxford, 2013.

Vanderveen, Gabry, *Interpreting fear, crime, risk, and unsafety: Conceptualisation and measurement*, Boom Juridische Uitgevers, Den Haag, 2006.

Verfaillie, Kristof, Kristel Beyens, Jan Blommaert, Henk Meert, and Karen Stuyck, "De overlastmythe: Het geïnstitutionaliseerd onvermogen om constructief om te gaan met samenlevingsproblemen?", *Panopticon*, Vol. 3, No. 28, 2007, pp. 6 - 20.

Verfaillie, Kristof, "Punitive needs, society and public opinion: an explorative study of ambivalent attitudes to punishment and criminal justice", in Sonja Snacken, and Els Dumortier (eds.), *Resisting punitiveness in Europe?*, Routledge, London, 2012, pp. 225 - 246.

Waege, Hans, "Operationaliseren", in Jaak Billiet, and Hans Waege (eds.), *Een samenleving onderzocht. Methoden van sociaal-wetenschappelijk onderzoek*, De Boeck nv., Antwerpen, 2003, pp. 390.

Watson, Hayley, David Wright, Rachel L. Finn, Iván Székely, Charles D. Raab, Kerstin Goos, and Michael Friedewald, "Report on Existing Surveys", PRISMS Deliverable 7.1, 2013. http://prismsproject.eu/wp-content/uploads/2013/03/PRISMS-D7-1-Report-on-existing-surveys.pdf

Wodak, Ruth, and Michael Meyer, *Methods of Critical Discourse Analysis*, Sage, London, 2001.

Zedner, Lucia, *Security*, Routledge, London; New York, 2009.

ANNEX: RECOMMENDATIONS ON HYPOTHESES

Introduction

The output of WP4 (D.4.1) points to 4 hypotheses to be included in the quantitative survey. Each of these hypotheses will be further explored in the qualitative fieldwork that will be developed in D.4.2. so that the output of D4.2 may provide a useful contextualization of the results of the quantitative survey. Because this is a criminological work package, its hypotheses focus more on the 'security' issue in the survey and on the *connections* that are assumed or may be expected with the issue of privacy. These connections, however, will have to be tested by correlating the security issue, as further refined in the questions developed below, and the 'privacy issue', which will be made explicit in other parts of the survey. In other words: the 4 hypotheses are further refined here in terms of survey questions that enable the assessment of the security issue in the survey *and* they point to the assumed connection of those questions to the privacy issue, and this connection is captured in terms of the formulation of the hypothesis itself.

As such, no explicit referral to the security-privacy trade-off is made in the survey questions themselves, which is precisely what often leads to the creation of a security-privacy trade-off. For instance, the question: "should the government be allowed to read e-mails and listen to phone calls to fight terrorism?" Is a question which not only includes both the security and privacy issue. At the same time, it connects both issues for the respondent in highly specific ways, that is, a security-privacy trade-off is assumed and created. Some suggest (e.g. Solove, 2011) that this issue might be overcome by simply rephrasing such issues, by restoring the balance between privacy and security in terms of making the privacy issue more explicit in the survey question. For instance: "should the government be allowed to read e-mails and listen to phone calls to fight terrorism without a search warrant or the appropriate court order required by law to fight terrorism?"

The point here is not that such questions may not be useful or that the latter question may not lead to more differentiated responses. The point is that such survey questions inevitably frame the issue at hand in terms of a *trade-off*. To go beyond such constraints *in opinion research*, is to recognize that both security and privacy can also be thought of as distinct conceptual spaces in which both issues are not automatically connected or may be taken up in ways very different than the traditional security privacy trade-off paradigm suggests.

So to avoid embedding a trade-off paradigm into survey questions, the attempt here is to make explicit how 'security' can be explored in terms of survey questions and to point to the connections that can be made with the respondents assessments of privacy, and infringements of privacy, (privacy concerns).

In the **first hypothesis**, such a connection will have to be explored between 'fear of crime' and privacy concerns. 'Security' in this hypothesis is conceptualized in terms of what is commonly referred to as 'subjective feelings of insecurity', and the proposition is that the more people worry about specific forms of international crime, the less privacy concerns they will have.

The **second hypothesis** focuses on the issue of trust in the security provider and its connections with privacy concerns. What is proposed here is that the higher the level of trust in specific security providers and measures, the less people believe their privacy is infringed.

In the **third hypothesis**, knowledge of the main security provider, 'the criminal justice system', is connected to privacy concerns. People who are knowledgeable about criminal justice will show less privacy concerns.

In the **final hypothesis**, the sources of information about crime control are connected to privacy concerns. Respondents whose most influential source of information is their direct experience will show more privacy concerns.

Hypotheses 1: fear of crime – privacy concerns

Measuring 'fear of crime' has a longstanding tradition in the social sciences. Recently, scientists have begun focusing on the finding that particular ways of exploring fear of crime in quantitative surveys, that is, the use of single-item questions, may actually magnify the everyday experience of fear, which may lead policymakers to believe that more substantial proportions of the population experience fear of crime than is actually the case (Gray, *et. al.* 2008; see also Farrall, 1997). To mitigate this problem, scientists have come to develop more fine-tuned ways to assess fear of crime. These state of the art approaches require a specific *set* of questions to be included in survey tools (Gray, *et. al.* 2008: 368).

> Q1: 'In the past year, have you ever felt worried about . . . ?'
> Q2: [if YES at Q1] 'How frequently have you felt like this in the last year?' [n times recorded]
> Q3: [if YES at Q1] 'On the last occasion how fearful did you feel?' [not very worried, a little bit worried, quite worried, very worried or cannot remember]

Gray, *et. al.* (2008: 368), with Farrall and Gadd (2004), point out that this adjusted measurement strategy 'focuses on events of worry; although it explores the intensity of the last fearful event, it does not elicit an overall intensity summary of worry'. What this means is that the events being surveyed need to be made explicit in the survey. Contrary to the British Crime Survey or to the work of Gray and colleagues, and given the explicit European focus of the study, the events that can be made explicit are those that European policymakers have come to focus on (which is not 'burglary' or 'robbery'). Based on the European threat assessments, three specific events can be identified that can be included in the survey: (i) terrorism; (ii) cybercrime; (iii) commodity counterfeiting with a focus on illicit trade in sub-standard goods and goods violating health and safety regulations (this includes foods and beverages, body care articles, medicines, electrical household items and toys (SOCTA, 2013). The former phenomena are often explicitly connected to privacy concerns. The latter is a new trend in Europe, one that will be an important focus for policymakers in the definition of the EU's crime control strategy for the next four years.

As such, the questions to be included in the survey:
> Q1: 'In the past year, have you ever felt worried about . . . ?' [terrorism / cybercrime / commodity counterfeiting]
> Q2: [if YES at Q1] 'How frequently have you felt like this in the last year?' [n times recorded]
> Q3: [if YES at Q1] 'On the last occasion how fearful did you feel?' [not very worried, a little bit worried, quite worried, very worried or cannot remember]

Hypothesis 1: the more people worry about crime, the less privacy concerns they have

Hypothesis 2: trust in the security provider

The second hypothesis is more straightforward and is based on studies in which trust in government is a decisive factor in people's assessment of security and privacy issues (e.g. Pavone and Esposti, 2010). The questions to be included in the survey should therefore include assessments of trust in specific 'security providers', and their most common measures. Trust in institutions in crime control can be measured in much more complex ways, that is, in terms of three dimensions (Jackson, 2011): effectiveness, procedural fairness, and distributive fairness. Although these dimensions would be highly relevant for the purpose of the Prisms survey, such an assessment of trust would quickly amount to a survey in its own right. For pragmatic reasons, we need to limit assessments of trust to one question.

> Q1: Can you say for each of the following institutions whether you have much trust in them or little trust? (very little trust, little trust, little nor much trust, some trust, much trust).
> Providers: Police / Justice / Private security / Airport security
> Measures: CCTV / Body scanners / Profiling / Biometrics

Hypothesis 2: the higher the level of trust in specific security providers and measures, the less people believe their privacy is infringed.

Hypothesis 3: knowledge of 'the criminal justice system' and privacy concerns

Knowledge of the criminal justice system is important in people's assessment of government institutions and systems of crime control (see Hough and Roberts, 2005). 'Knowledge' can be assessed in terms of questions in which people are asked about specific facts about crime and crime control. The prerequisite for such questions is that respondents are not given a choice among different responses, but that they are prompted to make their own assessment of the issue at hand. For instance, an example drawn from Jones (2008) illustrates a measurement of knowledge:

> Q: "Of every 100 people charged with [assault/home burglary] and brought to court, roughly what number do you think end up convicted?"
> Q: "Of every 100 men aged 21 or over who are convicted of [assault/home burglary], how many do you think are sent to prison?"

Answers ranging within 10% are considered to be correct and can then be used to determine whether a respondent is 'knowledgeable'. As such, European data about prosecution, conviction and imprisonment rates can be used to draft questions that can measure knowledge of the main security provider in the prisms-survey. Such data are made available by the UNODC.

> Q: How many persons, roughly, do you think were brought into formal contact with the police for rape in the EU in 2011?
> Q: How many persons, roughly, do you think were prosecuted in the EU in 2011?
> Q: How many persons, roughly, do you think were convicted in the EU in 2011?
> Q: How many persons, roughly, do you think were detained in the EU in 2011?

Hypothesis 3: People who are more knowledgeable about criminal justice will show more privacy concerns.

Hypothesis 4: sources of information and privacy concerns

The final hypothesis focuses on the sources of information people use about the criminal justice system. With Jones (2008), what needs to be surfaced is which sources of information are the most influential for the respondent (personally). The response options are:

- Personal experience;
- Relatives' and/or friends' experiences;
- Word of mouth/information from other people;
- Broadsheet newspapers
- Tabloid newspapers
- Local newspaper;
- News programs on TV/radio
- Internet
- Government publications
- Books
- School / college / university courses

The respondents can select more than one source of information.

> **Hypothesis 4: people whose most influential source of information is their direct experience will show more privacy concerns**

Co-ordinator:
Dr. Michael Friedewald
Fraunhofer Institute for Systems and Innovation Research ISI
Breslauer Straße 48 | 76139 Karlsruhe | Germany
Phone: +49 721 6809-146 | Fax +49 721 6809-315
michael.friedewald@isi.fraunhofer.de

Fraunhofer

ISI