Privacy Versus Collective Security

Bas Van Schoonhoven, Arnold Roosendaal, Noor Huijboom

Privacy versus Collective Security
Drivers and Barriers behind a Trade-off

Bas van Schoonhoven, Arnold Roosendaal and Noor Huijboom
{bas.vanschoonhoven, arnold.roosendaal, noor.huijboom}@tno.nl*

TNO, The Netherlands

Abstract. Many decisions concerning technological development and related policies in the field of protecting the privacy of individuals and security at the societal level include a perceived trade-off between these two interests. Sometimes, this trade-off is made explicitly, but often it is an implicit choice, driven by external factors. This paper assesses a set of factors acting as drivers or barriers towards the development of technologies for privacy and/or societal security. While some of the individual drivers and barriers do not show a clear bias towards security or privacy technology development, the overview gives a clear indication that some powerful factors are biased towards developing and using security technologies, and some other factors are biased towards hindering the development and use of privacy technologies. This bias may threaten the privacy of individuals on the long run and may obscure potential solutions that enhance both security and privacy.

Keywords: Privacy, security, trade-off, drivers, barriers.

1 Introduction

Many decisions concerning technological development and related policies in the field of protecting the privacy of individuals and security at the societal level include a perceived trade-off between these two interests. Security technologies that are developed and deployed to secure society against crime, terrorism or other threats often violate the privacy of individuals. Similarly some privacy technologies hinder security surveillance practices. Sometimes, this trade-off is made explicitly, but often it is an implicit choice, driven by external factors. An important question concerns what these factors are. The phenomenon of the perceived privacy-security trade-off has been recognised in literature before [1]. This research adds to the knowledge concerning this phenomenon by identifying drivers and barriers for the development of privacy and security technologies in order to explain why the trade-off turns out in a certain way.

How exactly the drivers and barriers identified in this paper work out in practice, depends on the specific technology used, the situation in which it is

* The authors would like to thank the reviewers and participants of the IFIP Summerschool for their valuable comments

applied, and the perceptions of the actors involved. This is not part of this paper, but is developed further in a number of case studies[1] in the PRISMS[2] project. In this paper, first a brief description of security and privacy will be presented. Then, drivers and barriers for development of security and privacy technologies will be discussed. Finally, some conclusions with regard to the impact of these drivers and barriers on the perceived trade-off between security and privacy technology development will be drawn.

2 Security and Privacy

Privacy and security technologies aim at enhancing privacy and security. To understand what these technologies do, it is necessary to have an idea of what security and privacy are. The *European Committee on Standardisation*s working group 161 provides a mainstream definition of security:

> "security is the condition (perceived or confirmed) of an individual, a community, and organisation, a societal institution, a state, and their assets (such as goods, infrastructure), to be protected against danger or threats such as criminal activity, terrorism or other deliberate or hostile acts, disasters (natural and man-made)" [2]

Security as a concept is multidimensional, and generally defined in a very broad sense. It relates to many different scales: international security, national security, corporate security, societal security, and individual security [3].

The concept of privacy has a long history in European and American cultures and it has been defined in many ways. Back in 1890, Warren and Brandeis defined it as "the right to be let alone" [4]. In 1967, the influential privacy researcher Alan Westin described it as "an instrument for achieving individual goals of self-realisation" and "the claim of individuals, groups or institutions to determine for themselves when, how and to what extent information about them is communicated to others" [5].

More recently, researchers have recognised that privacy is a concept that is impossible to fully define in a single definition, and that there are multiple dimensions to privacy, for example as argued by Daniel Solove in his book "Understanding Privacy" [6]. Solove differentiates between different dimensions of privacy according to the type of privacy invasions, e.g. surveillance, aggregation, or intrusion. However, the outlining of privacy problems or intrusions does little

[1] These case studies concern biometrics, deep packet inspection (DPI) and internet monitoring, Automated Number Plate Recognition (ANPR), smart grids, and body scanners at airports.

[2] PRISMS stands for "The PRIvacy and Security MirrorS" - Towards a European framework for integrated decision making. The project is part of the EU Seventh Framework Programme and analyses the traditional trade-off model between privacy and security and devises a more evidence-based perspective for reconciling privacy and security, trust and concern.

to provide an overarching framework that would ensure that *individuals* rights are proactively protected.

Rights to privacy, such as those enshrined in the European Charter of Fundamental Rights, require a forward-looking privacy framework that positively outlines the parameters of privacy in order to prevent intrusions, infringements and problems. For our analysis, we use the recent conceptualisation of privacy as seven types of privacy, as identified by Finn, Wright, and Friedewald. These types of privacy are: Privacy of the body, Privacy of behaviour, Privacy of communication, Privacy of data and image, Privacy of thoughts and feelings, Privacy of location and space, and Privacy of association [7].

The concepts of privacy and security partially overlap at the individuals' scale. This is especially visible in the field of information security which is also concerned with data protection. There is no such overlap, however, when comparing security at the societal scale with privacy at the individuals' scale.[3]

3 Collective Security versus Individual Privacy

Decisions concerning technological development and related policies in the field of protecting privacy and security are made within a certain policy context. The actors involved in the policy arena highly determine the definition of the notions *privacy* and *security* and develop certain *story lines* of the relation between the two notions. To understand the meaning given to the notions and their interrelationship, an extensive discourse analysis has been carried out within the PRISMS project. The discourse analysis shows that actors often perceive the balance between privacy and security as a trade-off; the one issue being at the expense of the other and vice versa. One of the many examples can be found in the Communication of the European Commission on the Stockholm Programme (a five-year plan with guidelines for justice and home affairs) in which it states that "it must also foresee and regulate the circumstances in which public authorities might need to restrict the application of these rules [regarding privacy] in the exercise of their lawful duties [security]" [8]. In other words, it is contended that in some instances privacy has to be restricted in order to enhance security. This perceived trade-off may as well be fed by the rather polarised policy field in which there is a clear distinction between actors who advocate increased privacy and actors who promote more security. Only few actors point to (e.g. technological) possibilities to strengthen both privacy and security at the same time. In addition, privacy and security policies are being developed by distinct policy bodies with their own specific focus (e.g. separate bodies within DG Justice and DG Home Affairs). This rather dispersed policy

[3] We acknowledge that there is a collective value of privacy as well. The research and use cases on which this paper is based, however, concern situations where collective security (e.g. fighting terrorism) counters individual privacy. For instance, the use of body scanners at air-ports concerns public/collective security, but each individual is affected in his privacy.

field and polarised discourse may explain certain technological developments in which the trade-off is visible.

4 The Trade-off: Drivers and Barriers

In technological developments, a trade-off between security at the societal scale and privacy of individuals is visible. Security technologies are developed and deployed that violate privacy, and similarly some privacy technologies hinder security surveillance practices. For example, advanced surveillance technologies applied in digital and physical environments make it increasingly possible to track and profile individual behavioural patterns, reducing the privacy of these individuals. On the other hand, some privacy enhancing technologies such as communication encryption and onion routing networks hinder online security surveillance practices. To gain a better understanding of how decisions based on this perceived trade-off play out we performed a preliminary analysis of the drivers and barriers that respectively drive security and privacy technological developments, or act as barriers to these developments. The drivers and barriers outlined here are based on a literature study of policy documents, technology roadmaps, foresight studies and impact assessments performed in the PRISMS project. Most drivers and barriers that were identified apply to both security and privacy technology developments, although to a varying extent. We identified the following drivers and barriers.

4.1 Driver 1: Technology and Industry Push

The *military industrial complex* has become a reality by the farewell speech of Dwight Eisenhower in 1961, ending his presidential career. Eisenhower first stipulates the emergence of the military industrial complex, new in the American experience, and in his view the result of the changing approach to arms and armaments after the three large wars in which the United Stated have been involved (the first and second world war, the Korean war). Eisenhower states:

> "Now this conjunction of an immense military establishment and a large arms industry is new in the American experience. The total influence – economic, political, even spiritual – is felt in every city, every Statehouse, every office of the Federal government [...] Only an alert and knowledgeable citizenry can compel the proper meshing of the huge industrial and military machinery of defence with our peaceful methods and goals, so that security and liberty may prosper together."

Eisenhower both addresses the emergence of a complex consisting of industries at arms length of military decision makers and the role and responsibilities of *alert and knowledgeable citizenry* in order that *security and liberty may prosper together*. Several authors indicate that this military-industrial complex meanwhile has experienced a transition into the direction of a security-industrial complex,

since the revenues for military undertakings are under pressure. The security-industrial complex is a significant phenomenon in Europe, and is developing at a rapid pace. The pace of these developments is to a large extent based on increasing demand [9]. However, a vested industry also has a significant interest in maintaining and increasing demand for its products and services. Industry, and to some extent research institutions, that are involved in researching and developing technologies for security and privacy provide a *technology push*, or solutions in search of a problem. Since the potential market for societal or national security is much larger than that of individual privacy, there is a strong financial incentive for companies in the security-industrial complex to invest in research and development of surveillance and other security technologies, even if this results in a negative outcome for the privacy of individuals. Companies dedicated to developing privacy protection solutions currently operate mostly in niche markets, and provide a *technology push* to a much lesser extent. In relation to the above, the level of organisation is much higher in the security industry field than in the privacy field. The establishment at the European level, supported by the EU government, of a Group of Personalities and the European Security Research Advisory Board (ESRAB), with a huge influence in the lobbying process, provided these bodies with a steady position. Moreover, these bodies have a strong relationship with industrial companies and are very well supported. On the privacy side, however, it often concerns *voluntary associations* [10] without a clear overarching structure or a social movement with an identifiable base [10].

4.2 Driver 2: Events with High Societal Impact

An analysis performed in the PRISMS project based on the use of keywords related to terrorism and organised crime in CORDIS project objective descriptions shows remarkable increase of projects in these fields from 2004 onwards. A possible explanation for this is that this is a delayed response to a number of high-profile attacks on the EU and its allies, resulting in an increased attention in fighting terrorism and organised crime. These attacks include the September 11 airplane hijack and subsequent attack in 2001 in New York and Washington, the July 7 2005 suicide bombings of the public transport system in London, and the March 11 2004 Madrid train bombings. All these events have had a high impact on the perception of societal security (or the lack thereof) of citizens in the EU, and as a consequence an increased call for security and protection against such terrorist attacks, even at the cost of losing privacy. The interplay between security and privacy as a consequence of high-profile societal events is seen as a possible driver of primarily development of security technologies. Historically, privacy-related incidents (e.g. leaks of large amounts of personal data) have had significantly less impact than the discussed security incidents, and as a consequence the drive for the development of privacy protection technologies because of incidents is much lower [11]. The recent NSA revelations and increased government surveillance can be a driver for privacy technologies. However, any individual privacy enhancing technology that is too difficult for a State to decipher will face difficulties, as was seen with the US government fight

against PGP in the 1990's. This can act as a barrier to new privacy technologies. One can also argue that legislation can act as a barrier to privacy technologies. Privacy is secondary to national security in all types of legislation (including Data protection and Human Rights). Generally States do not allow for the total privacy of an individual and this is manifested in legislative policy. Some States have specific legislation to combat certain privacy technologies in the interest of national security. For example the UK Regulation of Investigatory Powers Act 2000, allows authorities to compel a suspect in a criminal or terrorism related investigation to reveal his/her encryption key to enable the access to encrypted data.

4.3 Driver 3: National and EU-level Policy and regulation

Although national and EU-level regulation tend to be reactive and sometimes fragmented, legislation does act as a driver for organisations to implement certain privacy and security protections, to be compliant with the law [12] [11]. The strength of this driver depends amongst other things on the presence and actions of a supervising authority (e.g. data protection supervisor), and how well organisations understand what they have to do to be compliant, which is an issue especially with regards to privacy. A special case of this driver is the Charter of Fundamental Rights of individuals as argued in the 2010 EU Internal Security Strategy:

> "People in Europe expect to live in security and to enjoy their freedoms: security is in itself a basic right. The values and principles established in the Treaties of the Union and set out in the Charter of Fundamental Rights have inspired the EU's Internal Security Strategy: justice, freedom and security policies which are mutually reinforcing whilst respecting fundamental rights, international protection, the rule of law and privacy [...], transparency and accountability in security policies, so that they can be easily understood by citizens, and take account of their concerns and opinions [13]."

4.4 Driver 4: Citizen Demand for Security and Privacy

Another driver is related to some of the drivers we already mentioned: citizens demand a certain level of security and privacy, and as a consequence a market for products may arise, or governments may setup regulations. Citizen demand plays a role in the application of some surveillance technologies, such as CCTV cameras. A perception of public settings being insecure, e.g. being threatened by crime or violence in city centres, may increase the demand for technologies that are perceived to enhance security, such as surveillance systems. This does not necessarily mean that these solutions are effective in enhancing security [9]. With regard to privacy the same driver applies: citizens demand a certain level of privacy, for example while using internet services, and as a consequence new technologies get developed that fill in this demand. An example is the Do Not Track technology used in web browsers.

4.5 Barrier 1: Privacy and Security not Perceived as Unique Selling Points

Although citizen needs for security and privacy may increase demand for certain technologies that aim to enhance security or privacy, for many services and products security and privacy is not the primary focus, but rather a side issue. For example, for most of the transport sector, transporting goods and passengers is the primary activity, and security and privacy, while important, both do not act as positive selling features that companies advertise [14]. The same is true with regard to privacy: few companies see privacy as a unique selling point that allows them to sell products better or to compete better. Customers do currently not seem to find privacy a distinguishing feature of services, and are not overly willing to pay for enhanced privacy protection [11]. Increasing awareness of the importance of privacy and security with customers may possibly change this barrier into a driver, however. In the EU Security Industrial Policy, aspects such as privacy are mentioned as having a

> "[...]very tangible effect for a company that wants to invest in security technologies. The security industry has to be sure that its products will be compatible with the general opinion of the public. The commercialisation of their new technologies would otherwise be impossible. The financial and human efforts that go into the development and production of a security product can therefore be easily wasted [12]"

4.6 Barrier 2: Lack of Standardisation

Another important barrier to development and use of both security-enhancing and privacy-enhancing technologies is a lack of standardisation [11]. There are several related issues that act as barriers in this: the lack of a clear or commonly held definition of what *security* and *privacy* entails in practice; uncertainty about legal obligations and a fragmented regulatory landscape in the EU with regards to privacy and security; and incompatibility of different kinds of technological solutions with existing systems or other solutions. Some examples of where lack of standardisation hinders technology development and use are a lack of common technical and interoperability standards for automated border control systems, as well as standards for biometric identifiers, or a lack of standards for communication interoperability [12]. For privacy this issue is more pronounced than for security: as privacy is a relatively new issue many companies do not have extensive experience with best practices and reliable knowledge of what precisely to do to enhance privacy is hard to come by.

4.7 Barrier 3: Reactive, not Proactive Approach

Organisations tend to behave reactively and not proactively with regard to privacy protection and security. Similarly, governments tend to formulate regulations and mandatory requirements in response to issues that occur, and not in

a proactive manner. Technologies may not be applied because little attention to security or privacy issues was given during the design stage of products and services. The alternatives to such reactive approaches are usually described as *security by design* and *privacy by design*, for example by Ann Cavoukian, the Information Commissioner of Ontario, Canada [15]. A reactive approach may still create a demand for technologies in order to *patch up* security or privacy vulnerabilities in systems and services, but overall we expect that a proactive approach would increase demand for privacy enhancing and security enhancing technologies [12].

5 Conclusion

In the previous sections we discussed a number of key drivers and barriers in the development and application of technologies for privacy and security. Some drivers and barriers have a more pronounced effect on the development of security technologies, for others the effect is stronger on privacy technologies. We argue that there is a clear bias towards developing technologies for societal security, even at the cost of individual privacy, in both the factors driving and hindering technology development. This argument is based on the preliminary assessment performed, which is summarised in the tables below:

Table 1. Bias in factors driving technology development and use

Driver	Biased towards driving ...
Technology and industry push	Security
Events with high societal impact	Security
Government policy and regulation	-
Consumer demand	-

Table 2. Bias in factors hindering technology development and use

Barrier	Biased towards hindering ...
Lack of standardisation	-
Not a unique selling point	Privacy
Reactive approach	Privacy

While some of the individual drivers and barriers do show a clear bias towards security or privacy technology development, the overview gives a clear indication that some powerful factors are biased towards developing and using security technologies, and some other factors are biased towards hindering the development and use of privacy technologies. The drivers and barriers identified here are subject to ongoing developments. For example, with rising privacy

awareness in customers, privacy as a unique selling point may become a significant factor driving the development and use of these technologies. The Snowden revelations on the USA PRISM[4] scandal may boost awareness. At this point in time, however, this analysis indicates that there is no level playing field for the development and use of security and privacy technologies: current technological developments tend towards security at the cost of privacy. This bias does not only pose a risk for the privacy of individuals on the long run, but the bias against the development and use of privacy protecting technologies compared to technologies for security at the societal scale and the perceived trade-off between the two may obscure potential solutions that may enhance both security and privacy.

References

1. Solove, D.: Nothing to Hide: The False Tradeoff between Privacy and Security. Yale University Press (2011)
2. Sempere, C.M.: The European Security Industry: A Research Agenda. Technical report (2010)
3. Friedewald, M., Wright, D., Wadhwa, K., Gutwirth, S., Lieshout, M., Bodea, G., Raab, C., Szekely, I., Ploeg, I., Skinner, G., Kimpeler, S., Schuhmacher, J., Goos, K., Finn, R., Lagazio, M., Verfaillie, K., Gonzalez Fuster, G., Veenstra, A., Uszkiewicz, E., Pridmore, J., Valkenburg, G.: Central Concepts and Implementation Plan. PRISMS Deliverable 1.1. Technical report (2012)
4. Warren, S.D., Brandeis, L.D.: Right to Privacy. Harvard Law Review **4**(1) (1890) 72
5. Westin, A.F.: Privacy and Freedom. Volume 97. Atheneum (1967)
6. Solove, D.J.: Understanding Privacy. Harvard University Press, Harvard (2010)
7. Finn, R., Wright, D., Friedewald, M.: Seven Types of Privacy. In Gutwirth, S., ed.: European Data Protection: Coming of Age. Number January. Springer Science & Business Media, Dordrecht (2013)
8. European Commission: Action Plan Implementing the Stockholm Programme. COM/2010/0171. (2010)
9. Wright, D., Székely, I., Friedewald, M., Rodrigues, R., Kreissl, R., Johan, C., Raab, C., Wright, D., Beatrix, V., Goos, K., Hallinan, D., Charles, L., Webster, W., Galdon, G.: Surveillance, Fighting Crime and Violence. IRISS Deliverable 1.1. Technical report (2012)
10. Bennett, C.J.: The Privacy Advocates; resisting the spread of surveillance. MIT Press, Cambridge Massachusetts (2008)
11. van Lieshout, M., Kool, L., van Schoonhoven, B., Bodea, G., Schlechter, J.: Stimulerende en remmende factoren van Privacy by Design in Nederland. Technical report, TNO, Delft (2012)
12. European Commission: Security Industrial Policy: Action Plan for an innovative and competitive Security Industry. (2012)
13. European Commission: The EU Internal Security Strategy in Action: Five steps towards a more secure Europe (2010)

[4] The USA PRISM program should not be confused with the EU FP7 PRISMS research project.

14. European Commission: Commission Staff Working Document on Transport Security. (2012)
15. Cavoukian, A.: Privacy by Design The 7 Foundational Principles. Security (2011) 7–8