PATS

Privacy Awareness Through Security Organisation Branding

D7.2 Policy recommendations for privacy branding in the Security Industry

Authors:

Yoel Raban, Yair Sharan, ICTAF

Contents

1. Introduction

PATS (Privacy Awareness through Security Organizations Branding), is an FP7 project focused on CCTV and biometrics conducted across 6 partner countries (Germany, UK, USA, Finland, Poland and Israel). The final goals of PATS are to:

> Increase awareness and self-obligation to privacy among security organization. Increase awareness of governmental authorities in the EU as whole and individual member countries to privacy as an important ethical value to be kept even though security penetrates deep into day to day life. Develop regulation processes to realize standards of privacy as a brand label for security organizations.

The early phases of the project concentrated on issues of: security regimes, privacy awareness, and the symbolic representations of security agencies. We also developed a model of privacy accountability and branding for security organizations. Although there are a variety of security and privacy perceptions globally, concepts of safety and security have become more comprehensive, holistic, networked and global. Surveillance is enabled though more advanced technologies and is becoming less visible to citizens. Privacy awareness is generally very low, especially amongst security technology producers who sell their systems directly to service providers (and are therefore quite detached from citizens). Additionally, regulation with regard to CCTV in the countries studied lacks clarity and is implemented to varying degrees. Our analysis of sources of communication from the security organisations studied, and the study of symbolic representations therein, revealed that privacy is extremely weakly represented in advertising, public signage and in brand symbols. Our analysis of the symbolic representation of privacy by security organisations revealed that the concepts of privacy and data protection are, at best, a minor point in advertising, public signage and in branding.

The PATS project is one of several EU projects researching issues of privacy, such as HIDE, ETICAL, FIDIS, RISE, and Urbaneye. PATS differ from these projects in that it focuses on a privacy branding model, through which issues of privacy can be communicated by the security industry, to the public at large.

In the process of preparing this deliverable we were assisted by a group of EU policy experts. Their comments and feedback have been incorporated particularly in the final section of this report (5.3). We would like to thank Prof. Dr. Simone Fischer-Hübner from Karlstad University, Ms. Michelle Chibba from the IPC of Ontario, Prof. Lucas D. Introna from Lancaster University, Prof. Dr. IUR. Elmer M. Giemulla from the Berlin Institute of Technology, and Nils Leopold, scientific referent of Dr. Konstantin von Notz (Member of the German Parliament).

2. Privacy accountability and branding

The privacy accountability model that was developed in PATS is a set of activities (dimensions) that should be undertaken by security organizations in order to become a privacy-accountable entity. It provides the basis for privacy branding through which security organizations may communicate privacy accountability and responsibility to citizens. The model includes the following dimensions and indicators[1]:

a) Planning, awareness building, conceiving and strategizing related to privacy (reflexivity). Such activities may be fulfilled by appointing a privacy officer, by conducting regular consulting cycles regarding privacy and by the execution of privacy impact assessments.
b) Making privacy-related information available to the public (information availability). Indicators for information availability may include privacy statements, codes of ethics, the use of Transparency Enhancing Technologies (TETs), and compliance reports.
c) Exercising two-sided communication with stakeholders, including citizens, on issues of privacy (communicability). Indicators of communicability may include hotlines, discussions in forums and social media such as Facebook where issues discussed may include ethics and privacy.
d) Changing the behavior of security organizations with respect to privacy (action-ability). This may be indicated by the enabling of citizen's requirements to be implemented through focus groups or citizen's juries. Other indicators may simply be changes in products due to Privacy by Design (PbD), or the introduction of privacy enhancing technologies.
e) Evidencing and verification of privacy accountability (testability). Indicators may include compliance with standards and regulations, including compliance with self-regulation mechanisms.

[1] Indicators are concrete activities that are executed by organizations in specific dimensions and provide evidence of privacy branding

Accountability is one of the pillars of ethical branding; as Fan points out:

> "Ethical branding, as a subset of ethical marketing, relates to certain moral principles that define right and wrong behaviour in branding decisions. A brand needs to be evaluated not just by the economic or financial criteria but also by the moral ones. An ethical brand should not harm public good; instead it should contribute to or help promote public good… Ethical branding includes attributes such as honesty, integrity, diversity, quality, respect, responsibility and accountability[2]."

Perhaps the most well-known ethical brand is fair-trade coffee, which has been the subject of various academic studies since 2001. Another branding trend is related to Corporate Social Responsibility (CSR). CSR can be used to build a corporate image and create stronger relationships between firms and stakeholders[3].

In 2009, the Centre for Information Policy Leadership discussed the essential elements of data protection accountability, which include similar dimensions, such as: organizational commitment to accountability, mechanisms for privacy policy, internal oversight and assurance reviews and external verification, transparency and mechanisms of individual participations, and means for remediation.[4]

As in other cases of ethical branding, privacy branding may be practiced and communicated by security organizations based on the model presented here, its dimensions and indicators.

---

[2] Fan, Y. (2005). Ethical Branding and Corporate Reputation, Corporate Communications: An International Journal, 10(4) 341-350.

[3] Peloza, J., and Shang, J. (2010). How Can Corporate Social Responsibility Activities Create Value for Stakeholders? A Systematic Review, Journal of the Academy of Marketing Science, 39(1) 117-135.

[4] Data Protection Accountability: The Essential Elements, A Document for Discussion, The Centre for Information Policy Leadership LLP 2009.
http://www.huntonfiles.com/files/webupload/CIPL_Galway_Accountability_Paper.pdf

3. Policy alternatives

3.1 Incentives

One major barrier to privacy accountability and privacy branding practices among security organizations is the lack of incentives. The efforts involved in branding in general are perceived to be quite costly relative to the expected benefits, which seem low or even non-existent to most key stakeholders in the industry. Incentives can take many forms – tangibles, intangibles, monetary, non-monetary, positive and negative. Incentives may be formed in a top down or bottom up manner. Examples of top down incentives are standards and regulations developed by government bodies. Bottom up incentives may be created by NGOs (privacy watchdogs) and other key stakeholders who manage to bring privacy into their daily discourse. Such activities increase awareness and sensitivities of citizens and organizations towards privacy issues, and generate the necessary conditions for self-regulation activities among sectors of the security industry.

In a recent analysis of PbD (Privacy by Design) and PETs (Privacy Enhancing Technologies) in privacy regulation efforts in the US and the EU[5], the author suggests means by which privacy regulators may develop appropriate incentives for organizations to adopt such schemes. There are several reasons why PbD and PETs have had a limited success so far. Only few consumers understand the risks to privacy and fewer are familiar with PETs (information asymmetry), and firms are not certain about the benefits of PbD and PETs whereas the costs are quite clear to them. Privacy breaches are not publicized due to lack of transparency and regulatory enforcement, and therefore do not present real risks to reputation. Finally, the author suggests that self-regulation and government regulation should not be viewed as mutually exclusive and recommends the consideration of co-regulation alternatives, such as safe harbour programs that will incentivise self-regulation.

In some cases the incentives for privacy protection could come from governmental procurement practices. The German state Schleswig Holstein, for example, requires

[5] Rubinstein, Ira, Regulating Privacy by Design (May 10, 2011). Berkeley Technology Law Journal, Forthcoming.

authority to purchase with first priority on products that have been awarded a privacy seal[6].

3.2 Regulation and self-regulation alternatives

Across all partner countries the relevant regulation mainly concerns data protection laws, but their applicability to CCTV and Biometrics seems rather weak and is often perceived as irrelevant by key security industry players.

The European Data Protection Directive (95/46/EC) needs to be revised (according to EU officials) and may include a more rigorous treatment of privacy in future. In the meantime Privacy Impact Assessments (PIA) are gradually making their way into the public discourse of privacy protection in Europe. A PIA is a systematic process of evaluating the consequences regarding privacy of a specific system or technology. Concepts of PIA have already been introduced by data protection and privacy officers in Canada, and in some other countries as well,[7] and some scholars argue that PIAs should become mandatory.[8] The European Commission issued a Recommendation dated 12 May 2009 on the implementation of privacy and data protection principles in Applications supported by Radio Frequency Identification (RFID)[9]. This PIA process is intended to help RFID application operators to pinpoint privacy risks associated with specific applications, assess their likelihood, and describe the steps taken to address them.

In the US, FTC staff recently prepared a report on consumer privacy, which applies both to online and offline commercial entities that collect consumer data[10]. The FTC recommends that companies should adopt a "privacy by design" approach and develop privacy protections in their business activities, including limitations on data

[6] https://www.datenschutzzentrum.de/guetesiegel/hinweise-produkte.htm
[7] Tancock, D., Pearson, S., and A. Charlesworth, The Emergence of Privacy Impact Assessments, HPL-2010-63 2010. http://www.hpl.hp.com/techreports/2010/HPL-2010-63.html
[8] Wright, D., Should Privacy Impact Assessment be Mandatory, Communication of the ACM, vol. 54, no. 8, 2011.
[9] http://ec.europa.eu/information_society/policy/rfid/documents/recommendationonrfid2009.pdf
[10] Protecting Consumer Privacy in an Era of Rapid Change, A Proposed Framework for Business and Policymakers, Preliminary FTC staff report, 2010.

collections, assigning personnel to oversee privacy issues, and conducting privacy reviews in new product development.

Privacy by Design (PbD) is a more holistic procedure than PIA. PbD is described by one of its major promoters, Ann Cavoukian, as a process of "building fair information practice principles ("FIPs"[11]) into information technology, business practices, and physical design and infrastructures[12]." She also maintains that PbD may be attained by the adoption of the seven foundational principles:

1. Proactive not Reactive; Preventative not Remedial
2. Privacy as the Default Setting
3. Privacy Embedded into Design
4. Full Functionality: Positive-Sum, not Zero-Sum
5. End-to-End Security — Full Lifecycle Protection
6. Visibility and Transparency — Keep it Open
7. Respect for User Privacy — Keep it User-Centric

The International Privacy Commissioners' conference adopted a resolution last year that emphasizes the importance of PbD. The resolution called for recognizing PbD as an essential component of fundamental privacy protection, encouraging the adoption of PbD to establish privacy as an organization's default mode of operation, and inviting Data Protection and Privacy Commissioners to promote PbD in their jurisdictions.[13]

Another issue related to PbD is the development of Privacy Enhancing Technologies (PETs). An interesting taxonomy of PETs classifies them as substitutes or complementary.[14] Substitute PETs ensure that little or no personal data is collected in the first place, whereas complementary PETs are mechanisms that either provides individuals with increased level of control over personal data or guarantees their privacy through cryptographic technologies. The author maintains that there is a

[11] See Appendix 1

[12] Cavoukian, A., Taylor, S., and M. E. Abrams, Privacy by Design: essential for organizational accountability and strong business practices, IDIS (2010) 3:405–413

[13] http://www.ipc.on.ca/site_documents/pbd-resolution.pdf

[14] Rubinstein, Ira, Regulating Privacy by Design (May 10, 2011). Berkeley Technology Law Journal, Forthcoming.

stronger business case for complementary PETs since they support compliance obligation and enhance the trustworthiness of their providers.

Self-regulation can be an important policy measure for encouraging security companies to adopt privacy accountability and branding practices. Several mechanisms of self-regulation have been described and classified.[15][16] Here are some examples of self-regulation mechanisms:

- Codes of conduct: A set of rules and practices that guide the behaviour of individuals or organizations. An example related to privacy is the "Charter for a democratic use of video surveillance", which is part of a European project called "Citizens, Cities and Video-Surveillance" that is engaged in the exchange of practices of video surveillance and respecting human rights[17]. Project members (10 cities) recently published the charter for a democratic use of video surveillance, which includes 7 principles: legality, necessity, proportionality, transparency, accountability, independent oversight and citizen participation.

- Standards: Technical specifications that are to be used as norms, methods or processes. An example of a privacy standard is the P3P (Platform for Privacy Preferences)[18]. The P3P enable websites to describe their privacy practices in a standard format that can be easily accessed and understood by users. It was developed by the W3C organization, and gained some moderate success among popular websites. ISO Standard 17799[19] is a set of best practices and guidelines that defines an integrated process-based approach for managing IT services for ensuring effective security measures that protect data and privacy of user information.

- Accreditation, certification or licensing: Mechanisms that consider the fitness of a certain person or organization to perform certain activities. Examples regarding privacy are the privacy certification given to individuals by the International Association of Privacy Professionals (IAPP)[20], and privacy certification given to organizations by TRUSTe[21]. TRUSTe provides organizations with a privacy seal after examining their privacy policy and their compliance with federal and state requirements.

[15] Bennett, C., & Raab, C. (2003). The Governance of Privacy: Policy Instruments in a Global Age. London: Ashgate.
[16] Bendrath, R., The Social and Technical Self-Governance of Privacy, in Responsible Business: Self-Governance and Law in Transnational Economic Transactions. By Olaf Dilling, Martin Herberg, and Gerd Winter, eds, Hart Publishing 2008.
[17] http://cctvcharter.eu/index.php?id=31556&L=jhzokrbwpm
[18] http://www.w3.org/P3P/
[19] http://www.iso.org/iso/catalogue_detail?csnumber=39612
[20] https://www.privacyassociation.org/certification/
[21] http://www.truste.com/

- Industry guidelines: Guidelines prepared by an industry organization provide key issues that need to be addressed and adhered to by industry members. An example for privacy guidelines comes recently from the RFID industry. The European Commission and the RFID industry signed a voluntary agreement to establish guidelines for RFID applications to make sure that new tags undergo strict privacy impact assessment (PIA) prior to their market launch[22]. Europe's online advertising industry recently released a Self-Regulation Framework concerning Online Behavioural Advertising (OBA)[23]. The framework specifies good practices for increasing transparency and consumer control relating to third party OBA.

- Consumer signposting: This includes branding activities that are intended to communicate certain issues (privacy in our case) to consumers or users. It can take a form of a logo, a membership display, or other forms. Some examples: OFT's CCAS[24] and TRUSTe's privacy seal, privacy "nutrition labels"[25].

- Public commitments are demonstrations made by organizations to issues that are important to their success in the market. Many organizations already have public commitments to privacy on their websites. In the heat of competition with Facebook, Myspace changed their privacy policy, and state as part of their public commitment to privacy that the feature "friends only" will become the default setting for updates[26].

- Approval: Recognition given to organizations by governmental institutions (or others) in order to guarantee their claims to consumers. Again, TRUSTe is an example of third party organisation that provides companies with seals of approval. Another example is the European Privacy Seal that certifies IT products and services privacy compliance with European data protection regulations[27]. Examples of seals that were already awarded can be accessed via the EUROPRISE website[28].

3.3 Influencing the adoption of privacy branding

There is a vast literature on diffusion of innovations which we can draw from, when looking for models and examples for speeding up the adoption of privacy branding. A famous study of innovations diffusion was conducted by Rogers[29] who came up with

[22] http://packetstormsecurity.org/news/view/18950/European-Commission-Launches-New-Industry-Guidelines-On-RFID-Privacy.html
[23] http://www.iabeurope.eu/news/self-regulation-framework.aspx
[24] http://www.oft.gov.uk/OFTwork/ccas/
[25] Kelly, P. G. et al, A "Nutrition Label" for privacy. http://cups.cs.cmu.edu/soups/2009/proceedings/a4-kelley.pdf
[26] http://seodesignblog.com/2011/05/17/myspace-positions-itself-as-facebook-alternative-with-new-privacy-settings/
[27] https://www.european-privacy-seal.eu/about-europrise
[28] https://www.european-privacy-seal.eu/awarded-seals/certified-privnote
[29] Rogers, E. M., Diffusion of Innovations, Free Press 2003.

5 adopters categories (see chart) that a new product or service usually go through. In many cases the diffusion process gets stuck between early adopters and early majority having difficulties in crossing the "chasm"[30].

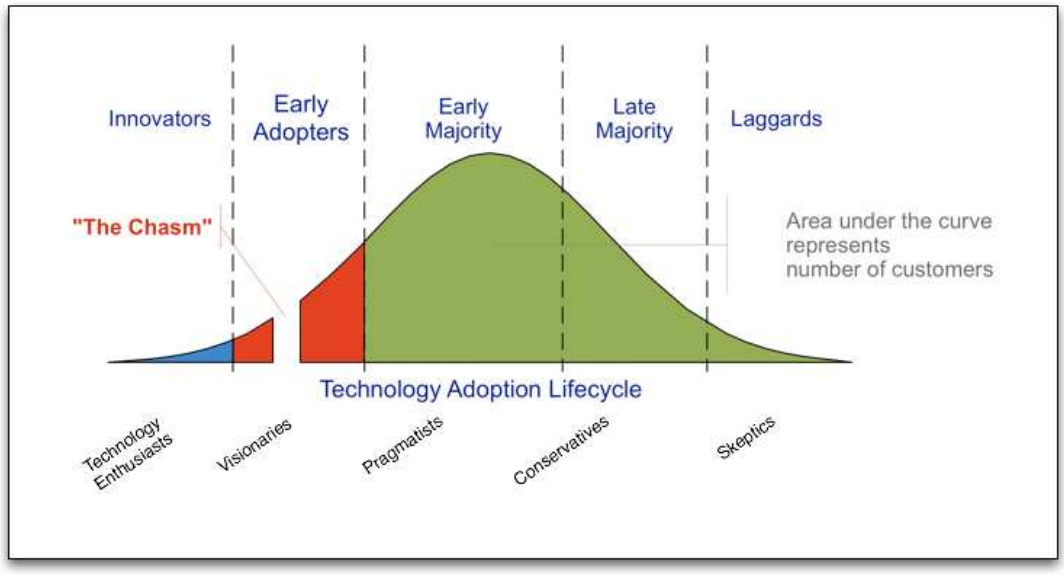

Chart 4.1: Diffusion of innovations

Rogers defined five stages in the innovation decision process (next chart), as well as the communications channels that can be used in order to favorably affect the process[31]. The stages are: 1) knowledge, 2) persuasion, 3) decision, 4) implementation, and 5) confirmation. At the first stage, individuals acquire knowledge and become aware of the existence of the idea or a product. At the first stage of awareness building, the mass media play a major role in disseminating knowledge. At the persuasion stage, individuals form an attitude towards a new idea or product, which guides them in the decision to adopt or reject. During this stage, interpersonal communications and discussions in peer-to-peer or near-peer networks are most important to persuasion and finally to adoption. As shown by the Bass model of product diffusion[32], the number of adopters due to interpersonal communications is far greater than the number of adopters due to mass media (next

[30] Moore, G. A., Crossing the Chasm, HarperCollins 1999.
[31] Rogers: 204
[32] Rogers: 210

chart). Mass media is more important for earlier adopters than for late adopters, but its importance decrease as the diffusion process moves forward to early and late majority.

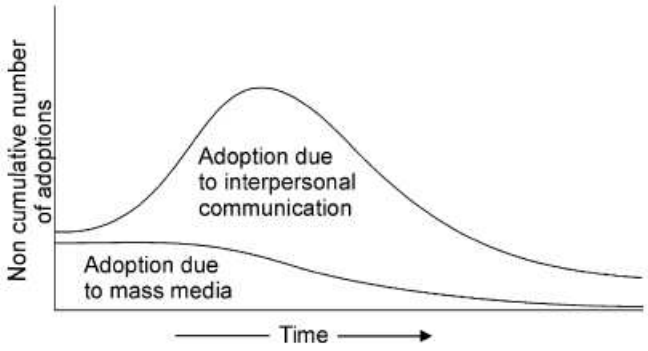

Chart 4.2: Adopters due to mass media and due to interpersonal communications

Rogers also discusses diffusion networks and the role of opinion leaders as enablers of diffusion of innovations[33] and cite many examples were proper use of opinion leaders led to faster and more successful diffusion.

A similar model of diffusion brings forward issues of tipping point, critical mass or threshold that must be reached before an innovation becomes a widespread success. The term "tipping point" was popularized by Malcolm Gladwell[34]. According to Gladwell "The notion of the tipping point comes from epidemiology, and refers to the moment a given social process becomes generalized rather than specific in a rapid rather than gradual manner. This is usually seen to occur as a result of this social process acquiring a certain critical mass and crossing a particular threshold, but ultimately it is "the possibility of sudden change [that] is at the center of the idea of the Tipping point""[35]. Gladwell identified three factors that have an impact on the popularity of trends:

- The law of the few: few key types of people play an important role in pushing an idea, or a product forward – connectors, mavens and salesmen. 20% of the people do 80% of the work (80/20 principle).

[33] Rogers: 300
[34] Gladwell, M., The Tipping Point: How Little Things Can Make a Big Difference, Little Brown 2000.
[35] Ibid: 12

- The stickiness factor: a quality that compels people to pay attention to an idea, or a product.
- The power of context: the conditions and circumstances of the times and place in which epidemics occur.

In order to enhance the adoption of privacy branding in the security industry we need to start by focusing efforts on possible innovators and early adopters. Gladwell suggests that in order to start an epidemic we need to concentrate efforts in groups of influencers (connectors, mavens and salesmen) that can help push innovations (privacy branding in our case) beyond the threshold into widespread public acceptance.

The proliferation of Internet and mobile phones and the popularity of social media and networks enable ever faster diffusion of new ideas as well as products and services. Studies of networks and diffusion are able to document contagion effects operating in social networks and highlight the important role of opinion leaders in such processes[36]. Social contagion happens when the behavior of person's peers affect the behavior of the person himself. I am more likely to buy a new product or to attend a public demonstration once some of my peers (e.g. Facebook friends) already bought the product or announced that they will participate in the demonstration. The process of social contagion may operate through "(i) spreading awareness and interest, (ii) social learning leading one to change one's beliefs about the product's risks and benefits, (iii) social-normative influence increasing the legitimacy of the new product, (iv) concerns that not adopting may result in a competitive or status disadvantage, or (v) direct and indirect "network" or installed base effects." [37] The customer lifetime value of opinion leaders is greater than other people because they tend to be early adopters and heavy users, and because they start influencing other people sooner and more effectively than others.

[36] Iyengar, R. et al, Opinion Leadership and Social Contagion in New Product Diffusion, Marketing Science, Vol. 30, No. 2, March–April 2011, pp. 195–212

[37] Iyengar, R. et al, Distinguishing among Mechanisms of Social Contagion in New Product Adoption, Research Paper 2011
http://marketing.wharton.upenn.edu/documents/research/MultipleMechanisms.pdf

The study of individuals with exceptional skills of generating word-of-mouth and catalyzing the diffusion of ideas and new products may be categorized under "influencer marketing". Influencers may be potential buyers or third party players in the supply chain or value-added influencers, such as journalists, academics, industry analysts and activists. Keller and Berry[38] propose five attributes of influencers:

- Activists: influencers get involved, with their communities, political movements, charities and so on.
- Connected: influencers have large social networks
- Impact: influencers are looked up to and are trusted by others
- Active minds: influencers have multiple and diverse interests
- Trendsetters: influencers tend to be early adopters (or leavers) in markets

4. Policy recommendations for PATS countries

Each PATS partner provided preliminary recommendations on how to promote privacy accountability and branding among security organizations in their own country.

4.1 Germany

State and private organisations as well as providers and clients of security services and products have only a low interest in citizens' privacy. The protection of civil rights is under-represented in terms of the State and furthermore is not a goal of private organisations. The blurring of the positions between the fields, especially the fact that the state is also a client of security systems with interest in surveillance, strengthens this constellation. Examples are the federal police (BPol), the federal office of criminal investigation (BKA) and the office for the protection of the constitution (BVerfS). This leads to an imbalance between state and security organisations, respectively providers and clients of security products and services, who have a common interest.

Citizens have a weak position and the only opportunity for the citizen side to engage in privacy issues is to exert pressure via civil liberty groups, who scandalize privacy

[38] Keller, Ed and Berry, Jon, The Influentials, Free Press, 2003

infringements and data breaches in order to challenge the reputation of Security Organisations. Trust is a necessary resource for security organisations, and this can be achieved mainly through a commitment to transparency and privacy. In order for this to be realized, security organisations' must engage with the dimension of reflexivity, eventually leading to a process of privacy branding.

Currently, the incentives to reconsider privacy practices are mainly the threat of scandals of data breaches from civil liberty groups and claims based on law breaches. Besides structures of reflexivity, a higher monetary redress for data breaches would change the cost-benefit balance of privacy enhancing instruments and strategies. As mentioned previously, we believe that a higher degree of reflexivity within security organisations would lead to stronger privacy awareness and better privacy practices. The emergence of reflexivity could be supported through specific mandatory monitoring measures which focus on privacy practices and data protection law compliance. Additionally it would be valuable to force organisations to make structures of data processing and handling more transparent. For example, it could be required that every data security breach gets published notwithstanding its consequences.

The large amount of different seals is more confusing than communicating a certain privacy practice. Additionally a seal without accountability of the certified company fails on generating trust and is worthless. So it is vital to establish a well-known privacy seal with clear requirements. These requirements have to be assessed by independent institutions. It should be considered to integrate different privacy levels for this seals.

A CPO (Chief Privacy Officer) can be an important institution of privacy reflexivity. The position of a CPO has to be defined more clearly. CPOs needs a strong mandate to take care of consumer data and have to be independent and well trained. It has to be considered if an external assessment can be made obligatory, or how the conformability of monitoring processes can be ensured.

Independent institutions for privacy impact assessments (PIAs) and privacy practice monitoring are vital. In Germany it is discussed whether to establish a Data Protection Foundation for this task (Stiftung Datenschutz). DPAs could get more resources and a stronger mandate to assess privacy practices, but they would still lack independence in regard to public authorities which are included in the Security Organisations.

External assessment and consultancy for privacy practice monitoring could be encouraged by subsidies. This would lower the cost and thus increase the benefit of enhanced privacy practice. This could also include resources for CPO personnel and privacy information and communication practices.

Campaigns to raise privacy awareness could be started, similar to anti-racism campaigns and campaigns against alcohol abuse and AIDS. This could include advertisements and TV spots. Besides campaigns, privacy conferences and panel discussions can be initiated and supported to stimulate the discourses about privacy issues.

Policy adoption plan:

Intuitively, we could expect that branding processes will most likely be started by actors who already are in a position of strength and could exploit their advantage in the marketplace. In our research, we have found that the pull is not strong enough, and that companies are still reluctant to stand out in the market in what we have called the "cat-and-mouse" atmosphere[39]. Ironically, it seems that in the field of security, the most elaborate branding and communication processes about privacy will come from the other direction: from scandal-ridden companies who have publicly failed. In our analysis, we termed one type of privacy awareness the "barking dog" - the company that had to take hard blows and reacts by coming out actively rather than retreating ("dog in the kennel").

[39] See German WP3 workshop report D3.3

The German team of the PATS project has successfully built a relationship with representatives of the Deutsche Bahn AG through workshops and cooperation in other research projects. The transport corporation is a major CCTV client who is motivated to go forward with privacy branding after extensive data protection scandals with regard to employees' data. The DB is in a very good position to introduce privacy branding when it comes to resources: it is the former state-owned railway company and is known by probably every German inhabitant. The majority of the population are customers, and the employee basis is large and generally rather loyal. In the case of a large multinational corporation such as the DB AG, it can be useful to act single-handedly and turn its scandal into an advantage. For other actors who have not yet entered the public sphere with respect to the topic of privacy and data protection, a feasible strategy that mitigates the fear of a confrontational atmosphere and being singled out is the creation of a common branding strategy.

Technology producers who offer privacy enhancing technologies can request that clients advertise this feature, presenting both themselves and the supplier as privacy aware. This can be done through dedicated web sites for products, services or programmes. The same applies to service providers. For example, think of a privacy respecting security concept developed for a production site or educational facility. Security providers and clients can set up a portal that offers information and contact details. On the part of the provider, this can be a welcome reference. Transparency also leads to identification on the part of the end-users who now know who is behind the products or uniforms.

A supportive policy measure that tackles the demand structure is public procurement. If public facilities would ask security providers for articulate privacy policies and the presentation of those to the end-users via media, products would probably change at the same time.

The cooperation between companies and clients also potentially remedies the problem of missing expertise or resources in either privacy protection or marketing. A policy measure to support privacy-related cooperation could reward consortia – the more participants, the more funding. Cooperation inducing measures are

essential in order to facilitate network building and niche development. When a number of actors start collaborating with regard to their privacy policies or specific product features, more knowledge is generated and possibly institutionalised. Standards can evolve and become part of association agendas. Cooperation is also a means of dragging pragmatists along.

External data protection professionals play a crucial role here. When part of a collaboration process, they bring in the necessary knowledge and prevent failure and reputation damage. As a policy tool, the subsidising of external help can trigger companies' involvement. Privacy experts can be complemented by marketing and PR experts who design awareness campaigns as well as branding strategies. This "privacy market" is a growing, but diffuse niche that overlaps with security and other consulting services. Data Protection Authorities could support this market by providing an interface between industries and consultancies or advocates. They already make information for companies available, so it would be little effort to build a platform where data protection and privacy experts can present themselves in a focused way. The envisioned "Data Protection Foundation" would of course be a suited actor to provide information directed towards companies.

4.2 UK

There are three key barriers that intersect in complex ways to create barriers to the adoption of privacy branding. First, there is the extent to which any security organisation from the public or private sector recognises privacy protection as having an ethical or social value. This kind of recognition in the absence of any financial or legal motivation seems rare. Second, there is the extent to which security organisations recognised a market value in privacy protection and in privacy branding. Many participants in the UK PATS research felt that designers, developers and manufacturers were not responsible for privacy protection and hence recognised little market value for these organisations in adopting a privacy brand. However, there were a few organisations pushing PETs and attempting to establish themselves as privacy-protecting market leaders. For users of surveillance technologies there was some recognition of reputational loss through privacy

infringements among private sector organisations. However, much stronger concerns were expressed on this issue among public sector users of surveillance systems. Third, legislation filled much of the UK PATS research. Legislation was often seen as too complex, out of date or problems were identified with compliance. Private and public sector organisations suggested that more effective legislation would lead to a higher value being placed on a privacy protection brand with public naming and shaming more likely through effective legislation and a higher value placed on the need to find efficient means (such as PETs) to comply with legislation at a lower cost.

The UK research undertaken for the PATS project points to stricter enforcement being required, prior to the possibility of organisations following voluntary codes of conduct, or self-regulation being an option. This is also linked to the issue of privacy having a social and a market value. In order to try and change organisations' views of the worth of privacy as gaining a competitive advantage, the first step in the UK is to enforce the existing legislation. This is an option for policy changes in the short term. However, in the UK PATS research some concerns have been expressed regarding the legislation [not up to date, too confusing – etc.]. Hence reconsidering enforcement of legislation might need to go hand in hand with a thorough overhaul of the suitability and clarity of existing legislation and its attendant infrastructure.

Following on from this, the question for policy is one of how to incentivise organisations to take up self-regulation and to abide by legislation and the enforcement of this legislation. One possibility would be to allow regulators such as the Information Commissioner's Office to enforce stronger penalties; to give the ICO 'some teeth', as many participants in the PATS project have stated. This has recently started to happen in the UK (the first instance of a monetary fine being imposed by the ICO was 24 November 2010), however press coverage and information about the changes has been minimal. With little information available and little press coverage, the question then becomes one of: will widespread change occur in security organisations in terms of privacy protection and data protection if the changes to enforcement are not known about (i.e. will improvements be made if no one knows

about the changes to the ICO, and will the fines act as a deterrent)? Furthermore, the maximum fine penalty has been increased to £500,000, however currently the fine imposed is based on the size of the breach of data protection, rather than the type organisation which is at fault. This is potentially a problem, both in terms of larger organisations taking smaller size fines seriously, but also in terms of public organisations being fined and paying with public money.

Since 2007, the Information Commissioner's Office (ICO) has advised organisations to use Privacy Impact Assessments (PIAs) as standard. Rather than a negative incentive (in terms of fining people for breaching data protection principles) this seems to have been a push towards prompting organisations to view privacy protection in a positive light, rather than imposing draconian penalties. In 2008, the ICO produced a handbook on PIA procedures, which included the following:

> "It requires any major initiative, which is going to collect and use personal information, to go through a checklist … showing how they have identified the risks, they have minimised the intrusion and they have put safeguards in place."

The ICO also recommended that the Government review their procurement processes so as to incorporate design solutions that include privacy-enhancing technologies in new or planned data gathering and processing systems. This advice was taken up by the UK Government and included in a report from the Cabinet Office (published in 2008) promoting the use of PIAs by organisations.[40] However, it is not clear that organisations in the UK have acted on this promotion to date. This advice could potentially be made mandatory (i.e. all organisations would need to carry out a PIA before continuing with the development or use of CCTV systems or data gathering). If it were to be made mandatory, this might also lead to a privacy market in the UK; if company profits were based on the ability to push ahead with the development of, or use of, surveillance technology products.

[40] http://www.cabinetoffice.gov.uk/resource-library/data-handling-procedures-government

There is also potential in offering more positive incentives to both private and public sector. This recommendation is potentially possible in the short to medium term. This might take the form of increased media coverage, depicting those with high standards of privacy and data protection in a positive light. This could potentially incentivise both the public and private sectors. Another possibility for incentivising the private sector to offer higher standards of privacy protection might be the inclusion of an industry award, which could be offered at events such as IFSEC.[41] In terms of the public sector, and in particular local authorities, one possibility for incentivising organisations to offer higher standards of data protection and privacy protection could be a new CCTV Challenge Competition with a focus on Privacy by Design (PbD) or Privacy Enhancing Technologies (PETs).[42] Local authorities would therefore compete on the basis of the uptake and installation of privacy enhancing features into visual surveillance systems. Although the emphasis of this Challenge Competition would be on the uptake of PETs by local authorities, this could potentially also have impacts on the design, development and manufacturing of CCTV systems incorporating PbD features (with higher demand resulting in higher production of these systems).

As mentioned earlier, it is unclear what the motivating factor for the public sector is in maintaining higher standards of data protection than other end users of the technology, such as small businesses and shopping centres (for example), i.e. whether this is due to recognising a social or ethical value to privacy or an interest in maintaining or cultivating a positive and trustworthy reputation with the public. In either case, greater public participation and consultation will be beneficial to the

[41] IFSEC is the largest annual security event in the UK. Currently, IFSEC does offer the annual Security Industry Awards. However, there is no category for 'best privacy protection' or 'most privacy aware company'. This could potentially be offered to incentivise private sector organisations.

[42] In 1994, the Home Office announced £2 million worth of funding for CCTV by way of a Challenge Competition. This allowed local councils to bid for funding to install CCTV into town centres and public spaces. By the end of the year, the number of towns and cities with CCTV systems had risen to 79. By March 1995, this number had increased to 90. A further £15 million CCTV scheme competition was announced in November 1995 to 'encourage the expansion of CCTV', with 800 bids received. There had also already been a £5 million project six months earlier. During 2000-2001, the Home Office continued to make large amounts of funding available through another Challenge Competition for the installation of cameras into town and city centres

public sector as end users of visual surveillance systems, and an emphasis on this engagement from a policy perspective may be a way forward. If the public sector leads the way, the private sector may follow. This recommendation is potentially achievable in the medium to long term. In terms of public sector reputation, the past few years have seen an increased public interest in privacy-related issues, with greater media coverage of debates surrounding ID cards[43], and increasing public debate around potentially privacy infringing developments such as the DNA database. In terms of public sector reputation, taking these debates into account and ensuring a certain standard of privacy protection is important. Following on from this, even if the private sector does not recognise the ethical or social value of privacy, greater public participation could potentially lead to a greater importance being placed on the value and importance of privacy by the public (at the moment, empirical research suggests that the British public are willing to trade their civil liberties in return for safety and security). This in turn may develop a market value for privacy, with the public demanding a higher level of privacy protection and awareness from security organisations and surveillance technology developers. A greater reputational risk may arise from a more aware public, demanding more privacy protection from both public and private sector organisations. Furthermore, the public sector may become a model for other end users, such as large inner city shopping centres (e.g. Westfield), who may in turn market themselves as a 'privacy protecting shopping experience'.

4.3 US

The primary barrier to the adoption of an ethical brand amongst the security industry as a manner of encouraging privacy awareness in a self-regulating way is the lack of direct financial incentive or prospect of legal directive. Self-regulation is most likely to occur in highly integrated industry sectors dominated by a small number of key players who share an incentive to coordinate their activities, either in order to prevent direct state regulation or because there is a financial incentive in doing so

[43] For more on this see Kroener, I. (2010) 'CCTV: A Technology under the Radar' UCL, unpublished thesis.

that is best achieved collectively[44]. Neither of these factors is present in the US security market at this time. The industry is simply too large and interests diverse, and the sudden growth of the multibillion dollar homeland security market after 9/11 combined with the lack of direct regulation in the future work against the idea of the industry as a whole being proactive about privacy.

An alternative scenario is the development of an ethical brand by individual firms. The motivation here is the judgement that doing it is a way to gain competitive advantage over market rivals. Classic examples of this include cosmetic firms that include 'not tested on animals' as part of their corporate communications or coffee companies that promote ethically sourced beans. While we have encountered isolated instances of comparable thinking in our research, there does not appear to be any significant interest in this course of action amongst industry either. As has been identified in multiple project reports, the main problem in this is the lack of direct relationship between the security industry and the wider public. The potential appeal of an ethically-sourced consumer item is that it may entice a greater number of consumers to buy their products, the evidence of which will register with the corporate bottom line. But unlike firms that directly responsible for the protection of personally identifiable information of citizens (banks or insurance companies, for example), the vast majority of the security industry caters directly to businesses and government authorities, and therefore does not have a direct relationship with the wider public.

Policy Recommendations:

1) *Create an independent Privacy Commissioner at the federal level*.

The United States does not have an independent office to uniformly enforce existing privacy law or act as a unified champion for privacy rights comparable to what exists in Canada, the UK, Australia, Japan, or many European countries. This makes the USA unique amongst western nations. Oversight of privacy related issues remains

[44] Bennett, C., & Raab, C. 2003. The Governance of Privacy: Policy Instruments in a Global Age. London: Ashgate.

fragmented amongst various industry and sector-specific authorities, many of which do have privacy issues as part of their core mandate. This is a significant weakness to the US privacy regime. Our first recommendation is that the United States creates an independent Privacy Commissioner. Regardless of its institutional configuration, the crucial attributes of this office are that it would be independent, to have lawful access to information that falls within the scope of its mandate, the power to order compliance under law, a broad mandate to conduct investigations and research, and the resources to pursue these aims.

2) *Elevate the threshold for the evaluation of public surveillance beyond the minimum standards of the Fourth Amendment*.

Many observers have expressed concern with the growth of surveillance networks in major urban centers. Surveillance cameras are one part of these networks but considerable efforts are being made to augment cameras with various analytics capabilities and integrate these and other sensor detection technologies into high-capacity, city-wide networks. Of particular concern is that this growth is practically unregulated at the federal level. This is directly attributable to the Supreme Court's position in *Katz* that there is no reasonable expectation of privacy while in public space, which means that such networks are not subject to the Privacy Impact Assessment process that other government initiatives are. This doctrine has not been revisited in over three decades despite the step-change in the depth and breadth of surveillance in public space. We therefore recommend that policies be adopted to elevate the regulation of public surveillance systems beyond the minimum requirement of existing federal legislation and case law.

3) *Require all public surveillance systems receiving federal money to adhere to the DHS Privacy Office's 'Best Privacy Practices for Public Video Surveillance.'*

The previous recommendation states that greater privacy protections ought to be required by law for public surveillance systems without specifying what those protections might look like. This recommendation provides that specificity. In particular, we recommend that the Department of Homeland Security's *Best Privacy*

Practices for Public Video Surveillance[45], hereafter the DHS Privacy Practices, be made mandatory for all public surveillance initiatives. They are modelled on the Fair Information Practice Principles, and as such they set out guidelines such as the purpose specification principle, data minimization principle, and the data quality and integrity principle. However, observance of these principles is voluntary at present because of the previously-cited doctrine that there is no expectation of privacy in public space, and our research suggests that adoption of these principles is highly uneven at best. We recommend that adoption of the DHS Privacy Principles be mandatory for all public agencies engaged any form of open-street surveillance program.

4) *Require authorities to publish codes of conduct explaining the privacy protections incorporated into the public surveillance system.*

Publishing codes of conduct is already an element of the DHS Privacy Principles but it is of sufficient importance to be treated separately than the rest. This is because the adoption of the DHS Privacy Practices is necessary but itself sufficient to foster trust and accountability with the public about surveillance and privacy. In order to achieve this goal, some manner of communicating the aims, purposes, and procedural and/or technological privacy safeguards of a security initiative to the public is necessary. The publication of codes of conduct by public agencies is a key means of doing so. Currently, however, there is no such requirement for public agencies to do so, so they not uniformly found amongst public agencies. New York City's 'Public Security Privacy Guidelines' is an exemplary instance, while Chicago has none. At a minimum, these commitments should identify the system administrator responsible for all operational and administrative elements, explain the system's capabilities; how it will be used, image retention, and release; and access to video center and image storage locations, and provide mechanisms for facilitating and responding to enquiries from the public[46].

5) *Require all public surveillance initiatives to undergo Privacy Impact Assessments on a 5-year basis.*

[45] DHS. 2007. Best Practices for Government Use of CCTV: Implementing the Fair Information Practice Principles. Washington, D.C.: Department of Homeland Security Privacy Office.
[46] DHS 2007: 24

Government programs are required to undergo Privacy Impact Assessments if they are deemed to collect and hold any form of personally identifiable information. The aim of these reviews is to ensure that an initiative meets all applicable legal requirements for handling personally identifiable information. However, open-street surveillance initiatives are exempt from these reviews at present because of the legal doctrine articulated in *Katz* that there is no presumed expectation of privacy in public space, and therefore these initiatives are not deemed to be privacy-sensitive. In light of the intensification in depth and breadth of surveillance in public today, we recommend that the existing Privacy Impact Assessment procedures be mandatory for all public surveillance initiatives. The aim of this review would be to establish compliance of an initiative to the DHS Privacy Practices. They would be conducted internally by the responsible agency but it would be mandatory to file these reviews with the federal privacy commissioner, the role of which is to oversee the process and step in if compliance is deemed to be lacking. Successful initiatives would be granted approval from the privacy commissioner, which would be necessary for an initiative to continue.

6) *When possible, only security firms with the appropriate privacy certification may be contracted to work on DHS-funded projects.*

Given that government agencies are a major source of funding for the industry (in 2009, the DHS grants program amounted to over $6 billion), controlling how government money is spent on security can have a significant impact on the industry. Specifically, this recommendation aims to add stipulations to how the DHS Homeland Security Grants program distributes funds to other government agencies and eventually the security industry by requiring, to the greatest extent possible, that only 'privacy certified' contractors be approved to work on DHS-funded security initiatives. The rationale here is that if such a certification appeared profitable, more firms would voluntarily adopt it.

7) *The development of an industry-based and government approved privacy certification scheme.*

The previous recommendation raises the obvious question of what a 'privacy certification' entails in practice. The most promising arrangement is an industry-

based education and assessment program leading to a certification awarded by an industry association and endorsed at the federal level, possibly by the new privacy commissioner. There are no such certification programs in the US at present but there are some indications of where to begin. The Security Industry Association, for example, already provides a wide range of training seminars and educational activities for the industry. Most of these are professional designations for individuals, such as the Certified Security Project Manager (CSPM) designation. Highly relevant here is that the SIA has also developed the 'Privacy Framework', a 12-point set of guidelines for how security firms can work with their clients to build privacy into the design and policy of their system. Accompanying the Framework is the 'SIA Privacy Framework' logo that firms can adopt for their promotional work. However, this initiative has its drawbacks; the Privacy Framework, while promising, is not accompanied by any sort of education or training, and use of the logo is not guarded and can be promoted without any observance of the Framework itself. We recommend that the SIA build upon these starting points by developing a 'Chief Privacy Protections Officer' certification. On the whole this certification would entail training individuals in contemporary legal, social, and cultural issues pertaining to security, surveillance, and civil rights today. The delivery of this training and award of the certification is the direct responsibility of the SIA but the program as a whole will be developed in conjunction with, and endorsed by, the federal privacy commissioner. On-going professional development requirements for this designation must include a track record of activities that reflect the elements of our brand model – raising privacy protection concerns internally, engaging with community stakeholders, facilitating feedback, and keeping abreast of emerging issues. Only by employing a person with this certification (on a proportional basis, depending on the size of the firm) can a firm advertise themselves as 'privacy aware', including promotion of the Privacy Framework commitment and associated seal of approval, and be eligible to work on DHS-funded projects.

4.4 Israel

The main barriers to privacy branding in the security industry is the low (or no) awareness of key players in the industry to the privacy needs of citizens. This is aggravated by the detachments of technology producers from citizens. Technology producers don't feel any need to address privacy issues, and assign this responsibility to their direct customers (security service providers) who are in daily contact with citizens.

Another barrier is a result of the global nature of this industry. In many cases CCTV systems are sold by relatively small companies that import these systems from larger manufacturers abroad. These small importers don't realize their own responsibility to privacy since they have no influence on the large multinationals who sell their products worldwide. They are too small to demand product changes from their sources and they are not in a position to make such changes themselves. We have to mention that there are some Israeli companies that are themselves large players globally, but they will start considering privacy branding when their major global clients demand it. Currently there are no pressures on them to engage in privacy branding activities.

The strong narrative of the great importance of security systems in Israel is also a barrier to privacy branding. Citizens are still influenced by past terrorist activities and this has mitigating effects on their demands for privacy rights. On the other hand, privacy watch dogs are not so active, and do not have a strong influence on the Government.

Public as well as private service providers seem to have low awareness to privacy issues and also have no clear guidance from regulators on this issue. There is no privacy guidance principles issued by the Government concerning the City without Violence national project, the major project in the area of public surveillance at present.

There is a question whether privacy branding practices should be introduced by government regulation or by industry self-regulation. It is quite clear from the work

carried out in earlier phases that self-regulation should be preceded by strengthening the regulatory regime concerning privacy, including issues of Privacy by Design (PbD). Indeed, PbD and PIA has already been offered last year by the Israeli Law, Information and Technology Authority (ILITA) in guidelines for CCTV service providers[47]. These guidelines include, among others, the following stipulations:

- Prior to a decision on using CCTV, providers have to conduct a PIA about the consequences of deploying surveillance cameras on human rights and privacy rights in particular.
- The deployments of surveillance cameras in public spaces must be preceded by a public hearing involving citizens.
- When a preliminary decision on placing surveillance cameras in public is taken, protecting the privacy of citizens must be a major concern. It is advised to conduct a PbD process to ensure that the infringement of the privacy of citizens is minimal.
- Signs about the use of surveillance cameras must be placed near cameras locations and at the entrance to the surveillance area. The sign has to be visible and include information about the service provider, the reasons for placing the cameras, and a link to the provider's web site where the list of the locations of the cameras must be placed.
- The duration of keeping the camera footage must be limited (one week is recommended), and citizens must have the right of accessing their personal data.

The policy recommendations for Israel include the following topics. The addition of more privacy-related regulation to the data protection law will encourage all industry players to practice a varying range privacy branding elements. The

[47] Surveillance Cameras: Law and Usage Guidelines, Ministry of Justice Opinion, November 2010 (Hebrew)

guidelines issued by ILITA may serve as a good starting point in this area. The second topic is the adoption of self-regulation mechanisms by local government (municipalities, police), that will force major technology producers to follow suit. The larger municipalities are in the process of installing CCTV infrastructure as part of the City without Violence national project. If they will take upon themselves to comply with self-regulation, based on government's guidelines, technology providers will have to provide suitable solutions and engage in privacy branding. Thirdly, the development of more strict privacy-related standards and regulation by The Standards Institute of Israel (SII) will enable the imports of security technology systems that are more oriented towards privacy. SII already issued the Green Seal that also provides branding advantages and is recognized by 49% of Israelis, according to a recent survey. They also are among the first to develop a Social seal Standard – IS 10000 for social responsibility, including issues such as employees' rights, human rights, sustainability, ethical management and transparency.

The process of diffusion and adoption of the privacy branding policy can take the following steps:

a) Awareness raising campaign initiated and orchestrated by the Government

b) Participation of citizens in the process

c) Government regulation formation

d) Municipalities take the lead

e) City without Violence project develops and practice privacy branding

f) Large integrators comply with regulation

g) The rest of the security industry follows large integrators

h) Evaluation of progress by the Government

4.5 Cross cutting issues

Several cross-cutting issues emerge from the country-specific privacy branding policy recommendations:

a) The main barrier to privacy branding is the lack of incentives (legal or monetary). Security industry organizations will not engage in privacy branding unless they can put a clear ethical or monetary value on privacy. Branding is a costly activity that is being practiced to varying extent by smaller and larger organizations. In the competitive environment that characterizes the security industry privacy branding at present is a luxury most organizations cannot afford.

b) Another barrier is the lack of direct relationships between technology producers and the public. Technology producers and suppliers sell their offerings to security service providers that operate surveillance (or biometric) infrastructures in public spaces. As a result, they don't seem to feel responsible for issues of privacy that may arise as a result of the public's interactions with their systems.

c) A clear policy recommendation that is recommended by all PATS partners is the need for stronger regulatory regime with more effective enforcement. A stronger regulatory regime that is in tune with current technologies and ethical norms will provide the needed value for privacy that is so lacking at present. If properly enforced, such regime may also provide strong incentives for innovators in the security industry to start practising privacy branding and influencing others to adopt such practices.

d) Privacy standard and certification scheme seem to be important for starting self-regulation procedures in the security industry, once the regulatory regime is crystalized. A national standard is needed to prevent a situation of multiple competing standards that may not be viewed by the public as important enough. A common certification scheme will distinguish organisations that have good privacy practices and comply with the national standard from the rest and foster privacy branding.

e) Another recommendation from PATS partners relates to public procurement of privacy-respecting technologies. The government is a very large player in the security industry, and a significant share of video surveillance (and biometrics) infrastructures are purchased by government. Once government will condition procurement on complying with privacy standards, the security industry will have to take notice and eventually also engage in privacy branding practices.

f) PATS partners recommend using Privacy Impact Assessment (PIA) and Privacy by Design (PbD) procedures in situations where new video surveillance and biometrics infrastructures are planned to be deployed. These procedures already appear in Israel's ILITA recommendations for public video surveillance and in the DHS Privacy Practices in the US.

g) In order to increase the awareness of the public and the security industry, privacy campaigns and awards schemes are recommended in most countries. In such campaigns it is also recommended to involve opinion leaders and influencers in order to speed the adoption process of privacy branding.

5. Policy recommendations for Europe

5.1 The General Data Protection Regulation

The European commission has issued its proposal for a regulation on the protection of individuals with regard to the processing and free movement of personal data (General Data Protection Regulation – GDPR) on 25 January 2012[48]. The proposal will change (once approved) the existing regulation by widening the geographical scope to data controllers outside the EU, reinforcing the rights of data subjects, defining new accountability obligations for data controllers, and by giving new powers to the national supervisory authorities (see appendix 1). As for the rights of data subjects, the proposal include issues such as the right to be forgotten (including erasure of personal data), the right for portability, a more restrictive definition of consent, and a specific protection for children under 13 years of age. The new obligations for data

[48] Proposal for a Regulation of the European Parliament and of the Council: on the protection of individuals with regards to the processing of personal data and on the free movement of such data, COM(2012) 11 final

controllers and processors include (among others) principles of transparency and data minimisation, the obligation to perform privacy impact assessments when rights of data subjects are at risk, the obligation to report data breaches within 24 hours, the obligation to appoint data protection officer in companies with over 350 employees, and accountability, the ability to demonstrate compliance with the regulatory regime.

The proposed legislation may provide the needed incentive for the CCTV and biometrics industries to start considering privacy accountability and branding practices seriously.

5.2 Hard law vs. soft law

Another approach to introducing privacy accountability is through "soft law" (or "soft governance"), such as guidelines, declarations, green books, codes of conduct; rather than rules and regulations that are considered "hard law". According to Anne Peters, "soft forms of international and European governance are proliferating dramatically... new forms of governance increasingly involve non-state actors." EU soft law may be classified into three groups: 1) Preparatory and informative instruments (action programmes, green and white papers), 2) Interpretative and decisional instruments (communications linked to primary or secondary EU norms), and 3) steering instruments (Council conclusions, resolutions, declarations, and codes of conduct).[49] According to Peters, private self-regulations and co-regulations are increasing in the EU. European-based transnational companies and industry associations are among the major self-regulators. Some of the more important examples for self-regulation are the Advertising self-regulation Charter and the EU Unfair Commercial Practise Directive of 2005. Another variant of private self-regulation is mixed public-private acts (co-regulation) – voluntary agreements that are subsequently enacted as directives by the council. The most important voluntary agreements at present are exercised in environmental policies.

[49] Peters, A. (2011). Soft Law as a New Mode of Governance. In The Dynamics of Change in EU Governance, Diedrichs. U., Reiners, W. and Wessels, W. Edward Elgar Publishing. pp. 21-51.

The question of hard law vs. soft law (and self-regulation) in the case of the CCTV and biometrics industries is somewhat complicated. Private companies may tend to practice self-regulation and branding when they can realize the benefits in the form of an improved competitiveness in the eyes of consumers. However, in the area of video surveillance in public places, some may argue that there is no real competition. Citizens have limited choices when it comes to using airports or other mass transportation infrastructures. Limited competition may curb the tendency to practice privacy self-regulation and branding among security service providers. This is not the situation in the security technology providers sector, which is a very competitive sector.

Such arguments tend to favour hard law over soft law when considering efforts to incentivise the use of privacy accountability and branding in the security industry. Since the competitive situation in the two sectors (service providers and technology providers) differs, the best policy would be to combine hard and soft law. Chronologically, hard law should precede soft law, enabling the assimilation of the need to comply in the entire security industry, especially in the service providers sector. The value of privacy branding lies in strengthening product responsibility and use privacy as part of CSR efforts in competitive situations.

5.3 Recommended policy for privacy accountability and branding

Now that the new approach to data protection in the EU is becoming clear, this may serve as a guideline for the security industry for co-regulation and privacy branding. The newly proposed legislation even calls for further self-regulatory activities to be practised in relevant industries (codes of conduct and certification, see appendix 2). We used PATS privacy branding model to associate the proposed General Data Protection Regulation (GDPR) articles with the privacy branding dimensions and with additional self-regulation activities (see next table).

By reflexivity we mean planning, awareness building, conceiving and strategizing related to privacy. We can see that articles 22 and 35 mention data protection obligations of controllers including the designation of a Data Protection Officer in

companies with more than 250 employees and in firms which are involved in processing operations. This regulatory activity can be now supported by privacy self-regulation and branding, such as the preparation of codes of conduct and privacy policies. A relevant example of codes of conduct is the charter for a democratic use of video surveillance (mentioned earlier), which is part of a European project called "Citizens, Cities and Video-Surveillance" [50]. Project members (10 cities) recently published the charter for a democratic use of video surveillance, which includes 7 principles: legality, necessity, proportionality, transparency, accountability, independent oversight and citizen participation.

As for information availability, the proposed GDPR includes specific demands for making privacy information available to data subjects including the right to access private data and to receive data breach notifications. Security organizations may comply with the law by making available information on privacy notices, charter and seals, and by using Transparency Enhancing Technologies (TETs). The use of privacy "nutrition labels" as part of privacy branding can be an effective means of communicating privacy values to citizens. The idea is to package privacy information so that privacy policy may be easily understood by users[51].

[50] http://cctvcharter.eu/index.php?id=31556&L=jhzokrbwpm
[51] http://cups.cs.cmu.edu/privacyLabel/

Table 5.3.1: Privacy regulation and branding dimensions

Privacy branding dimension	Regulation	Co-regulation, self-regulation, branding
Reflexivity	Controller to adopt policies and measures to ensure compliance, mandatory DPO[52],	Preparing codes of conduct[53] and privacy policies,
Information availability	Transparency, information to data subject & right of access, data breach notification [54]	privacy "nutrition labels", privacy notices, charters and seals, Transparency Enhancing Technologies (TETs)
Communicability	Right to be forgotten and to object to processing, right to compensation[55],	privacy hotlines,
Action-ability	Data protection by design, data protection impact assessment, Consultation[56],	PETs development, privacy by default products and services, citizen participation
Testability	Mechanisms to ensure verification of compliance[57],	Certification[58], standards, public procurement, industry guidelines, external audits (e.g. PIAs)

The new legislation (GDPR) will demand security organizations to open a bidirectional line of communication with their customers. Security organizations will need to comply with data subject's rights to be forgotten and to object to processing. The need to comply will create solutions, such as privacy hotlines, that will enable data subjects to demand the fulfilment of these rights from security organizations.

[52] Articles 22, 35, GDPR
[53] Article 38, GDPR
[54] Articles 11, 12, 14, 15, 32, GDPR
[55] Articles 17, 18, 77, GDPR
[56] Articles 23, 33, 34, GDPR
[57] Article 22 paragraph 3, GDPR
[58] Article 39, GDPR

The proposed GDPR includes general guidelines for companies on the need to carry out data protection impact assessments and data protection by design, which are part of the privacy branding dimension we call action-ability. Security organizations will have to comply by designing and executing these mechanisms and by developing and offering PETs to their customers. Some examples of PETs in the area of CCTV and biometric are the Privacy Protected Surveillance Using Secure Visual Object Coding technology developed at the University of Toronto[59], and Biometric Encryption (BE)[60]. Industry's initiative to design and tailor these mechanisms to the specific needs of security organizations (video surveillance service providers in particular), such as the PIA initiative of the RFID industry, is most welcomed. This initiative is in fact a co-regulation effort designed by the commission and RFID industry representatives.

According to the GDPR companies will have to adopt mechanisms that ensure verification of compliance, a provision that fits into the privacy branding dimension we call testability. In this area it is recommended to develop standards and certification mechanisms, as well as public procurement guidelines that will take privacy into consideration. Several examples were already mentioned in paragraph 3.2. As for industry guidelines, it is highly recommended to develop GDPR guidelines for the security industry, so that European security organizations will be able to implement the law to the best of their ability. An example of privacy guidelines for video surveillance is Ontario's guidelines for the use of video surveillance cameras in public places[61]. Another relevant issue could be the inclusion of privacy requirements as prerequisite for the provision of research grants in Europe. Since the EU framework program has become very popular this could affect a very large variety of industry sectors, including the security industry.

[59] Martin, K. and Plataniotis, K. N., Privacy Protected Surveillance Using Secure Visual Object Coding, IEEE TRANSACTIONS ON CIRCUITS AND SYSTEMS FOR VIDEO TECHNOLOGY, VOL. 18, NO. 8, AUGUST 2008

[60] Cavoukian, A. et al, Advances in Biometric Encryption: Taking Privacy by Design from Academic Research to Deployment, Review of Policy Research, Volume 29, Number 1 (2012)

[61] http://www.ipc.on.ca/images/Resources/video-e.pdf

Another dimension of EU policy includes measures that promote the uptake of privacy branding practices among security organizations. The principles of promoting the uptake of privacy branding could be based on the research summarised in paragraph 3.3. Firstly, there needs to be a plan with time frames and goals to be met. Secondly, EU-level influencers should be selected and motivated to participate. The platforms for communicating the messages should include social media as well as the more traditional media (TV, newspapers).

Implementation strategy should take into account the specific structure of the security industry, including mainly technology providers and service providers as well as their customers and different sizes of actors. The new GDPR rightfully distinguishes between two tiers of compliance obligations and sanctions - SMEs and large multinationals. But there should also be a distinction between technology providers and service providers. Technology providers operate in highly competitive markets and therefore privacy branding can be a competitive option once they can realize the benefits of engaging in privacy accountability efforts or suffer the consequences of not doing so. Service providers usually operate in markets with limited competition and therefore have low or no incentives to engage in privacy accountability activities. Security service providers should be the main target of the data protection and privacy new regulatory process, including mandatory DPO and other regulatory demands. Public service providers should also be subject to public procurement policies that favor privacy-responsible suppliers. As for technology providers, co-regulation seems to be the right approach regarding data protection and privacy. Since they offer security infrastructure to service providers, they will be affected by the stringent regulation faced by service providers and will also need to adapt by engaging in PbD, developing PETs and complying with national (or EU) privacy standard.

Awareness-raising events are highly recommended since the impact of privacy branding is very wide. The awareness level of citizens and organizations to privacy issues is quite low at present and awareness-raising activities are needed. Some activities, such as the European privacy day already exist. They should be supported

by new dissemination activities, such as the best PET award, the best privacy brand award, etc. In such campaigns it is recommended to use opinion leaders and influencers with a pronounced social media involvement.

Appendix 1: 10 Fair Information Principles

These principles are part of Canada's *Personal Information Protection and Electronic Documents Act*. They include[62]:

1. Accountability: An organization is responsible for personal information under its control and shall designate an individual or individuals who are accountable for the organization's compliance with the following principles.

2. Identifying Purposes: The purposes for which personal information is collected shall be identified by the organization at or before the time the information is collected.

3. Consent: The knowledge and consent of the individual are required for the collection, use, or disclosure of personal information, except where inappropriate.

4. Limiting Collection: The collection of personal information shall be limited to that which is necessary for the purposes identified by the organization. Information shall be collected by fair and lawful means.

5. Limiting Use, Disclosure, and Retention: Personal information shall not be used or disclosed for purposes other than those for which it was collected, except with the consent of the individual or as required by law. Personal information shall be retained only as long as necessary for the fulfillment of those purposes.

6. Accuracy: Personal information shall be as accurate, complete, and up-to-date as is necessary for the purposes for which it is to be used.

7. Safeguards: Personal information shall be protected by security safeguards appropriate to the sensitivity of the information.

8. Openness: An organization shall make readily available to individuals specific information about its policies and practices relating to the management of personal information.

9. Individual Access: Upon request, an individual shall be informed of the existence, use, and disclosure of his or her personal information and shall be given access to that information. An individual shall be able to challenge the accuracy and completeness of the information and have it amended as appropriate.

10. Challenging Compliance: An individual shall be able to address a challenge concerning compliance with the above principles to the designated individual or individuals accountable for the organization's compliance.

[62] http://www.priv.gc.ca/leg_c/p_principle_e.cfm

Appendix 2: General Data Protection Regulation

In 25.1.2015 the proposed new legal framework for the protection of personal data in the EU was revealed to the public. One of the major pillars of the new legislation is "putting individuals in control of their personal data", as stated in COM(2012) 9 final[63].

The new legislation recommends the following ground breaking principles concerning citizen's rights to privacy:

"Improve individuals' ability to control their data, by:

- ensuring that, when their consent is required, it is given explicitly, meaning that it is based either on a statement or on a clear affirmative action by the person concerned and is freely given;
- equipping internet users with an effective right to be forgotten in the online environment: the right to have their data deleted if they withdraw their consent and if there are no other legitimate grounds for retaining the data;
- guaranteeing easy access to one's own data and a right to data portability: a right to obtain a copy of the stored data from the controller and the freedom to move it from one service provider to another, without hindrance;
- reinforcing the right to information so that individuals fully understand how their personal data is handled, particularly when the processing activities concern children.

Improve the means for individuals to exercise their rights, by:

- strengthening national data protection authorities' independence and powers, so that they are properly equipped to deal effectively with complaints, with powers to carry out effective investigations, take binding decisions and impose effective and dissuasive sanctions;
- enhancing administrative and judicial remedies when data protection rights are violated. In particular, qualified associations will be able to bring actions to court on behalf of the individual.

Reinforce data security, by:

- encouraging the use of privacy-enhancing technologies (technologies which protect the privacy of information by minimizing the storage of personal data), privacy-friendly default settings and privacy certification schemes;
- introducing a general obligation for data controllers to notify data breaches without undue delay to both data protection authorities (which, where feasible, should be within 24 hours) and the individuals concerned.

Enhance the accountability of those processing data, in particular by:

- requiring data controllers to designate a Data Protection Officer in companies with more than 250 employees and in firms which are involved in processing

[63] Safeguarding Privacy in a Connected World: A European Data Protection Framework for the 21st Century, COM(2012) 9 final.

operations which, by virtue of their nature, their scope or their purposes, present specific risks to the rights and freedoms of individuals ("risky processing");

- introducing the "Privacy by Design" principle to make sure that data protection safeguards are taken into account at the planning stage of procedures and systems;
- introducing the obligation to carry out Data Protection Impact Assessments for organisations involved in risky processing."[64]

The proposal for regulation includes other aspects that are relevant to privacy branding, namely codes of conduct (article 38) and certification (article 39).

"**Codes of conduct**:
1. The Member States, the supervisory authorities and the Commission shall encourage the drawing up of codes of conduct intended to contribute to the proper application of this Regulation, taking account of the specific features of the various data processing sectors, in particular in relation to:

(a) fair and transparent data processing;
(b) the collection of data;
(c) the information of the public and of data subjects;
(d) requests of data subjects in exercise of their rights;
(e) information and protection of children;
(f) transfer of data to third countries or international organisations;
(g) mechanisms for monitoring and ensuring compliance with the code by the controllers adherent to it;
(h) out-of-court proceedings and other dispute resolution procedures for resolving disputes between controllers and data subjects with respect to the processing of personal data, without prejudice to the rights of the data subjects pursuant to Articles 73 and 75.

2. Associations and other bodies representing categories of controllers or processors in one Member State which intend to draw up codes of conduct or to amend or extend existing codes of conduct may submit them to an opinion of the supervisory authority in that Member State. The supervisory authority may give an opinion whether the draft code of conduct or the amendment is in compliance with this Regulation. The supervisory authority shall seek the views of data subjects or their representatives on these drafts.
3. Associations and other bodies representing categories of controllers in several Member States may submit draft codes of conduct and amendments or extensions to existing codes of conduct to the Commission.
4. The Commission may adopt implementing acts for deciding that the codes of conduct and amendments or extensions to existing codes of conduct submitted to it pursuant to paragraph 3 have general validity within the Union. Those implementing acts shall be adopted in accordance with the examination procedure set out in Article 87(2).

[64] Ibid, page 6

5. The Commission shall ensure appropriate publicity for the codes which have been decided as having general validity in accordance with paragraph 4.

Certification:

1. The Member States and the Commission shall encourage, in particular at European level, the establishment of data protection certification mechanisms and of data protection seals and marks, allowing data subjects to quickly assess the level of data protection provided by controllers and processors. The data protection certifications mechanisms shall contribute to the proper application of this Regulation, taking account of the specific features of the various sectors and different processing operations.
2. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements for the data protection certification mechanisms referred to in paragraph 1, including conditions for granting and withdrawal, and requirements for recognition within the Union and in third countries.
3. The Commission may lay down technical standards for certification mechanisms and data protection seals and marks and mechanisms to promote and recognize certification mechanisms and data protection seals and marks. Those implementing acts shall be adopted in accordance with the examination procedure set out in Article 87(2)." [65]

[65] Proposal for a Regulation of the European Parliament and of the Council: on the protection of individuals with regards to the processing of personal data and on the free movement of such data, COM(2012) 11 final, pages 67, 68.