iBusiness, 2012, 4, 168-172
http://dx.doi.org/10.4236/ib.2012.42020 Published Online June 2012 (http://www.SciRP.org/journal/ib)

Privacy Accountability Model and Policy for Security Organizations

Yoel Raban

Interdisciplinary Center for Technological Analysis and Forecasting (ICTAF), Tel Aviv, Israel.
Email: raban@post.tau.ac.il

Received April 17th, 2012; revised April 24th, 2012; accepted May 20th, 2012

ABSTRACT

This paper describes a new model of privacy accountability and associates its dimensions with elements of the proposed European Commission regulation on the protection of individuals with regard to the processing and free movement of personal data. The model is applied to the security industry with special emphasis on the video surveillance and biometrics sectors. The use of the specific dimension and indicators described in the model enables security organizations to provide privacy accountability to customers such that the principles of data protection regulation and self-regulation are met.

Keywords: Privacy; Data Protection; Accountability; Regulation; Self-Regulation; Privacy by Design; PATS Project

1. Introduction

PATS (Privacy Awareness through Security Organizations Branding[1]), is an FP7 project focused on CCTV and biometrics conducted across 6 partner countries (Germany, UK, USA, Finland, Poland and Israel). The main goal of the project was to increase awareness and self-obligation to privacy among 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 organizations studied, and the study of symbolic representations therein, revealed that privacy is extremely weakly represented in advertising, public signage and in brand symbols.

2. Privacy Accountability Model

The essential components of accountability that relate to regulations and self-regulations and to privacy responsibilities exercised by organizations has already been studied in the past [1]. They include adoption of internal policies, mechanisms to implement privacy policies, internal oversight systems, transparency and remediation. Another approach to accountability describes it in 3 dimensions, namely who is accountable for what and for whom [2]. These aspects are important issues for regulatory processes concerning privacy.

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. The model includes dimensions and indicators (concrete activities) as follows:

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

[1]See project's website at http://www.pats-project.eu

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.

Privacy business practices that demonstrate reasonable level of accountability are described in [3] and [4]. Accountability is one of the pillars of ethical branding [5]. Ethical brands do not have a negative impact on public good, and include attributes such as honesty, integrity, responsibility and accountability. Some practical aspects of ethical branding are included in [6]. The privacy accountability model may serve as the basis for privacy branding, which is part of ethical branding. 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.

3. Policy Alternatives

3.1 Privacy by Design

Some of the main building blocks of privacy policy are Privacy Impact Assessments and Privacy by Design. 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]. Privacy by Design (PbD) is a more holistic procedure than PIA. PbD is described by one of its major promoters, Ann Cavoukian [1], as a process of "building fair information practice principles (FIPs[2]) into information technology, business practices, and physical design and infrastructures." Privacy Enhancing Technologies (PETs) are also related to PbD. There are several definitions of PETs and the EC communication on PETs[3] use the definition from the PISA project "PET stands for a coherent system of ICT measures that protects privacy by eliminating or reducing personal data or by preventing unnecessary and/or undesired processing of personal data, all without losing the functionality of the information system".

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.

In a recent analysis of PbD and PETs in privacy regulation efforts in the US and the EU [9], 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 harbor programs that will incentivize self-regulation.

3.2. Hard Law versus 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 [10], "soft forms of international and European governance are proliferating dramatically... new forms of governance increasingly involve non-state actors".

There are several self-regulation mechanisms that can be practiced by security organizations, including codes of conduct, standards, certification, industry guidelines, consumer signposting, approval and public commitments.

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 favor hard law over soft law when considering efforts to incentivize the use of privacy accountability and branding in the security industry. Since the competitive situation in the two sectors (service pro-

[2]See the Federal Trade Commission definition of FIPs in http://www.ftc.gov/reports/privacy3/fairinfo.shtm

[3]Promoting Data Protection by Privacy Enhancing Technologies (PETs) (COM 2007 228 final), 2007.

viders 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.

4. Policy Recommendation

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[4]. 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.

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 controllers and processors include (among others) principles of transparency and data minimization, 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. The PATS privacy accountability model was used to associate the proposed General Data Protection Regulation (GDPR) articles with the privacy branding dimensions and with additional self-regulation activities (see **Table 1**).

Reflexivity means 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"[5]. 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[6].

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 fulfillment of these rights from security organizations.

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 called actionability. 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 [11], and Biometric Encryption [12]. 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 accountability dimension that is called 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. As for industry guide-

[4]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.

[5]http://cctvcharter.eu/index.php?id=31556&L=jhzokrbwpm

[6]http://cups.cs.cmu.edu/privacyLabel/

Table 1. Privacy regulation and accountability dimensions.

Dimension	*Regulation*	*Co-regulation*
Reflexivity	Controller to adopt policies and measures to ensure compliance, mandatory DPO[7]	Preparing codes of conduct[8] and privacy policies
Information availability	Transparency, information to data subject & right of access, data breach notification[9]	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[10]	privacy hotlines
Action-ability	Data protection by design, data protection impact assessment, Consultation[11]	PETs development, privacy by default products and services, citizens participation
Testability	Mechanisms to ensure verification of compliance[12]	Certification[13], standards, public procurement, industry guidelines, external audits (e.g. PIAs)

lines, 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[14]. 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.

5. Conclusions

Privacy accountability in security organizations can be achieved and communicated to customers using the model described in paragraph 2. This is demonstrated by allocating the mandatory requirements of the proposed GDPR to the specific privacy accountability dimensions, and implementing the recommended self-regulatory activities described in **Table 1**.

The method used to develop the privacy accountability model is based on the characterization of distinct accountability components and their classification into 5 dimensions. For each dimension, indicators of privacy accountability may be chosen by security companies in order to differentiate their privacy brands from the competition.

The results of this research are significant since they lay the basic foundations for practicing privacy accountability and branding activities in the security industry. The results may also be generalized to other industries.

[7]Data Protection Officer (DPO), see Articles 22, 35, GDPR.
[8]Article 38, GDPR.
[9]Articles 11, 12, 14, 15, 32, GDPR.
[10]Articles 17, 18, 77, GDPR.
[11]Articles 23, 33, 34, GDPR.
[12]Article 22 paragraph 3, GDPR.
[13]Article 39, GDPR.
[14]http://www.ipc.on.ca/images/Resources/video-e.pdf

6. Acknowledgements

This research was assisted by a group of EU policy experts. We would like to thank Prof. Dr. Somone 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.

REFERENCES

[1] A. Cavoukian, S. Taylor and M. E. Abrams, "Privacy by Design: Essential for Organizational Accountability and Strong Business Practices," *Identity in the Information Society*, Vol. 3, No. 2, 2010, pp. 405-413. doi:10.1007/s12394-010-0053-z

[2] C. Bennett, "International Privacy Standards: Can Accountability Be Adequate?" *Privacy Laws and Business International*, Vol. 106, 2010, pp. 21-23.

[3] D. Guagnin, L. Hempel and C. Ilten, "Privacy Practices and the Claim for Accountability," In: R. Von Schomberg, Ed., *Towards Responsible Research and Innovation in the Information and Communication Technologies and Security Technologies Fields*, Publication Office of the European Union, Luxembourg, 2011, pp. 99-110.

[4] C. Ilten, D. Guagnin and L. Hempel, "How Can Privacy Accountability Become Part of Business Process?" *Privacy Laws and Business International*, No. 112, 2011, pp. 28-30.

[5] Y. Fan, "Ethical Branding and Corporate Reputation," *Corporate Communications*: *An International Journal*, Vol. 10, No. 4, 2005, pp. 341-350. doi:10.1108/13563280510630133

[6] A. Crane, "Unpacking the Ethical Product," *Journal of Business Ethics*, Vol. 30, No. 4, 2001, pp. 361-373. doi:10.1023/A:1010793013027

[7] D. Tancock, S. Pearson and A. Charlesworth, "The Emergence of Privacy Impact Assessments," Technical Reports, Hewlett-Packard Laboratories, 2010.

[8] D. Wright, "Should Privacy Impact Assessment Be Man-

datory," *Communication of the ACM*, Vol. 54, No. 8, 2011. pp. 121-131. doi:10.1145/1978542.1978568

[9] I. Rubinstein, "Regulating Privacy by Design," *Berkeley Technology Law Journal*, Vol. 26, 2012, pp. 1409.

[10] A. Peters, "Soft Law as a New Mode of Governance," In: U. Diedrichs. W. Reiners and W. Wessels, Eds., *The Dynamics of Change in EU Governance*, Edward Elgar Publishing, Cheltenham, 2011, pp. 21-51.

[11] K. Martin and K. N. Plataniotis, "Privacy Protected Surveillance Using Secure Visual Object Coding," *IEEE Transactions on Circuits and Systems for Video Technology*, Vol. 18, No. 8, 2008, pp. 1152-1162.

[12] A. Cavoukian, M Chibba and A. Stoianov, "Advances in Biometric Encryption: Taking Privacy by Design from Academic Research to Deployment," *Review of Policy Research*, Vol. 29, No. 1, 2012, pp. 37-61. doi:10.1111/j.1541-1338.2011.00537.x

