Available online at www.sciencedirect.com

SciVerse ScienceDirect

www.compseconline.com/publications/prodclaw.htm

Computer Law & Security Review

Privacy by design and anonymisation techniques in action: Case study of Ma^{3}tch technology☆

*Paolo Balboni**, *Milda Macenaite*

European Privacy Association, Belgium

Keywords:
Privacy by design
Anonymisation
Ma^{3}tch technology
Financial intelligence unit
Personal data protection
Personal data security
Distributed network

ABSTRACT

Privacy by Design is now enjoying widespread acceptance. The EU has recently expressly included it as one of the key principles in the revised data protection legal framework. But how does Privacy by design and data anonymisation work in practise? In this article the authors address this question from a practical point of view by analysing a case study on EU Financial Intelligence Units ("FIUs") using the Ma^{3}tch technology as additional feature to the existing exchange of information via FIU.NET decentralised computer network. They present, analyse, and evaluate Ma^{3}tch technology from the perspective of personal data protection. The authors conclude that Ma^{3}tch technology can be seen as a valuable example of Privacy by Design. It achieves data anonymisation and enhances data minimisation and data security, which are the fundamental elements of Privacy by Design. Therefore, it may not only improve the exchange of information among FIUs and allow for the data processing to be in line with applicable data protection requirements, but it may also substantially contribute to the protection of privacy of related data subjects. At the same time, the case study clearly shows that Privacy by Design needs to be supported and complemented by appropriate organisational and technical procedures to assure that the technology solutions devised to protect privacy would in fact do so.

1. Introduction

Privacy by Design is now enjoying widespread acceptance. This is the principle that data protection should be implemented in information and communication technologies and systems used for the processing of personal data from the planning stage to the deployment, use and ultimate disposal.[1] The word "Privacy by Design" was first used in the report "Privacy-enhancing technologies: the path to anonymity" published by the Dutch Data Protection Authority and the Ontario Information Commissioner in 1995. According to Ann Cavoukian, Information & Privacy Commissioner of Canada, who invented the concept, "to build in privacy from the outset" can help "avoid making costly mistakes later on, requiring expensive retrofits".[2]

The discussion on Privacy by Design in the academic circles and among policy makers started with Privacy-enhancing

☆ The Authors would like to thank Dr. Arnold Roosendaal LLM (Fennell Roosendaal Research and Advice, and TNO) for his inputs on this paper.

* *Corresponding author*.
E-mail address: pbalboni@europeanprivacy.eu (P. Balboni).

[1] European Commission, *A Digital Agenda for Europe*, EUC, 26/8/2010 [2010] OJ COM (2010) 245 final/2; Jan Philipp Albrecht, Committee on Civil Liberties, Justice and Home Affairs, Draft Report on the proposal for a regulation of the European Parliament and of the Council on the protection of individual with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), COM (2012)0011 – C7-0025/2012–2012/0011(COD).

[2] Ann Cavoukian, *Privacy by Design*, Information & Privacy Commissioner, 1, 2009, available at http://www.ipc.on.ca/images/Resources/privacybydesign.pdf.

0267-3649/$ – see front matter © 2013 Paolo Balboni & Milda Macenaite. Published by Elsevier Ltd. All rights reserved.
http://dx.doi.org/10.1016/j.clsr.2013.05.005

technologies, or PETS, applications or tools that enhance privacy.[3] Subsequently the debate developed into a more systematic –Privacy by Design- approach which now embraces much more than PETS and also takes into account fundamental data protection principles, such as data minimisation, privacy by default, data security, transparency.[4]

Moreover, it has become a hot political agenda on both sides of the Atlantic. The EU has recently expressly included the principle of "Privacy by Design" into the revised data protection legal framework. The General Data Protection Regulation proposed by the European Commission (the "*Draft Regulation*"[5]) requires data controllers, and technology designers and producers, to embed privacy and data protection principles into the design of the ICT from the planning stage to "implement mechanisms for ensuring that, by default, only those personal data are processed which are necessary for each specific purpose of the processing and are especially not collected or retained beyond the minimum necessary for those purposes, both in terms of the amount of the data and the time of their storage",[6] and other necessary tools to enable users to better protect the personal data, such as access controls and encryption. Furthermore, data controllers are obliged to adopt internal policies and to implement appropriate measures in order to demonstrate their compliance with this principle.

Similar developments took place in the US, where a recent report of the Federal Trade Commission ("*FTC*") proposed a framework consisting of three elements: Privacy by Design, simplified consumer and businesses choice and greater transparency of data collection.[7] The FTC calls for companies to use Privacy by Design by promoting substantive and procedural consumer privacy protection at all stages of the design and development of their products and services.[8] In order to do so, companies should, first, "build in" privacy protection systematically into their practices, such as data security, reasonable collection limits, sound retention and disposal practices, and data accuracy and, second, maintain comprehensive data management procedure.[9]

1.1. *Topic and aim*

This paper focuses on the Privacy by Design approach promoted by the EU. In other words, Privacy by Design not only means that ICT systems should maintain security but also includes the idea that ICT products and services should be designed and created in a manner which minimises the amount of personal data in use.[10] Known as data minimisation, this principle includes the separation of personal information and content data, the anonymisation of them, and the immediate deletion of personal data when they are no longer necessary for the initial purpose.[11]

The authors will look at Privacy by Design from a very practical point of view, by analysing a case study on FIUs[12] using the Ma^{3}tch technology[13] as additional feature to the existing exchange of information via FIU.NET decentralised computer network.[14] This paper will look at this case of data processing as a possible and practical way of implementing the Privacy by Design principle. Ma^{3}tch technology will be briefly presented, and then analysed, and evaluated from the perspective of personal data protection. In doing so, the authors aim to answer the following research questions: How have the data protection requirements been taken into account when designing the technology? Does it comply with the data protection legislation? Are there any specific points to consider in relation to the rights and obligations based on the European legislative framework?

For the sake of clarity, it is important to mention that the analysis of privacy and data protection aspects related to the existing exchange of information via the FIU.NET

[3] See, e.g., John J. Borking, Charles D. Raab, *Laws, PETs and Other Technologies for Privacy Protection*, Journal of Information, Law and Technology, vol. 2001, no. 1, 2001; John J. Borking, *Why adopting Privacy Enhancing Technologies (PETs) takes so much time*, in Serge Gutwirth, Yves Pullet, Paul de Hert, Ronald Leenes (eds.), Computers, Privacy and Data Protection: an Element of Choice, 309-341, Springer, Netherlands, 2011, Communication from the Commission to the European Parliament and the Council on Promoting Data Protection by Privacy Enhancing Technologies (PETs), 2.5.2007 [2007] OJ COM (2007) 228 final.

[4] See Le Métayer, D., Privacy by Design: A Matter of Choice. In: Gutwirth, S., Poullet, Y., De Hert, P. (eds.) Data Protection in a Profiled World, pp. 323–334. Springer, Netherlands, 2010; Peter Schaar, Privacy by Design. Privacy by Design Issue of Identity in the Information Society Volume 3, Number 2, August 2010; Shapiro, S.S., Privacy by design: moving from art to practice, Communications of the ACM 53(6), 2009; Rubinstein, Ira, Regulating Privacy by Design, Berkeley Technology Law Journal, Vol. 26, 2012. Available at SSRN: http://ssrn.com/abstract=1837862.

[5] Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) [2012]OJ COM (2012) 11 final, available at http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf.

[6] Article 23 of the Draft Regulation requires to implement "appropriate technical and organisation measures and procedures in such a way that the processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject'' (data protection by design), and that measures are implemented ''by default'' so that ''only those personal data are processed which are necessary for each specific purpose of the processing'' (data protection by default).

[7] FTC, Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policy Makers (March 2012), available at http://www.ftc.gov/os/2012/03/120326privacyreport.pdf.

[8] Ibid., pp. 22-32.

[9] Ibid.

[10] Cf. Draft Regulation, Article 23; Art. 29 Data Protection Working Party, 02356/09/EN, WP 168, the Future of Privacy (2009), Sections 44–58, *available at* http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp168_en.pdf.

[11] Peter Schaar, *Privacy by Design*, IDIS (2010) 3:267–274, p.267.

[12] "A Financial Intelligence Unit (FIU) is a central, national agency responsible for receiving (and, as permitted, requesting), analysing and disseminating to the competent authorities, disclosures of financial information: (i) concerning suspected proceeds of crime and potential financing of terrorism, or (ii) required by national legislation or regulation, in order to counter money laundering and terrorism financing." http://www.egmontgroup.org.

[13] For a description of Ma^{3}tch Technology see Section 2 and U. Kroon (forthcoming), *Privacy and Knowledge: Solving the Double Edged Information Sword. Ma^{3}tch Information Revolution*.

[14] "FIU.NET is a decentralised computer network supporting the FIUs in the European Union in their fight against Money Laundering and Terrorist Financing." http://www.fiu.net.