COMPUTER LAW & SECURITY REVIEW ■■ (2017) ■■–■■

Available online at www.sciencedirect.com

ScienceDirect

www.compseconline.com/publications/prodclaw.htm

Computer Law & Security Review

Law enforcement access to personal data originally collected by private parties: Missing data subjects' safeguards in directive 2016/680?

Catherine Jasserand *

STeP (Security, Technology & e-Privacy) Research Group, University of Groningen, The Netherlands

Keywords:
Data protection
Directive 2016/680
Law enforcement access
Safeguards
Duty of notification
Purpose limitation
Digital Rights Ireland case
Tele2 Sverige case

A B S T R A C T

Access by law enforcement authorities to personal data initially collected by private parties for commercial or operational purposes is very common, as shown by the transparency reports of new technology companies on law enforcement requests. From a data protection perspective, the scenario of law enforcement access is not necessarily well taken into account. The adoption of the new data protection framework offers the opportunity to assess whether the new 'police' Directive, which regulates the processing of personal data for law enforcement purposes, offers sufficient safeguards to individuals. To make this assessment, provisions contained in Directive 2016/680 are tested against the standards established by the ECJ in *Digital Rights Ireland* and Tele2 *Sverige* on the retention of data and their further access and use by police authorities. The analysis reveals that Directive 2016/680 does not contain the safeguards identified in the case law. The paper further assesses the role and efficiency of the principle of purpose limitation as a safeguard against repurposing in a law enforcement context. Last, solutions to overcome the shortcomings of Directive 2016/680 are examined in conclusion.

1. Introduction

Law enforcement authorities around the globe have a growing appetite for personal data held by private parties and initially collected for a purpose different from law enforcement. Many examples can illustrate this trend: the huge amount of law enforcement requests made to high-tech companies at global level,[1] the case of the transfer of passenger name record data (air traveller data) to police authorities [2] or the retention

* European and Economic Law Department, STeP (Security, Technology & e-Privacy) Research Group, University of Groningen, PO Box 72, 9700 AB Groningen, The Netherlands.
E-mail address: c.a.jasserand@step-rug.nl.

[1] For the second half-year 2016, Microsoft reported more than 25,000 law enforcement requests to disclose content, subscriber data or transactional data at global level, see https://www.microsoft.com/about/csr/transparencyhub/lerr; compare with Apple's and Google's reports for the same period, available at respectively https://images.apple.com/legal/privacy/transparency/requests-2016-H2-en.pdf and at https://transparencyreport.google.com/user-data/overview; see also Oleg Afonin, 'Government request reports : Google, Apple and Microsoft ' on ElcomSoft blog, 16 January 2017, available at https://blog.elcomsoft.com/2017/01/government-request-reports-google-apple-and-microsoft/ [all websites have been last accessed on 01 August 2017].

[2] On the Passenger Name Record, see International Civil Aviation Organization, 'Guidelines on Passenger Name Record (PNR) Data', first edition 2010, available at https://www.iata.org/iata/passenger-data-toolkit/assets/doc_library/04-pnr/New%20Doc%209944%201st%20Edition%20PNR.pdf, Section 2.1. ; See also Directive 2016/681 of 27 April 2016 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offence and serious crime, OJ 2016, L 119/132.

https://doi.org/10.1016/j.clsr.2017.08.002
0267-3649/

Please cite this article in press as: Catherine Jasserand, Law enforcement access to personal data originally collected by private parties: Missing data subjects' safeguards in directive 2016/680?, Computer Law & Security Review: The International Journal of Technology Law and Practice (2017), doi: 10.1016/j.clsr.2017.08.002

of telecommunications data by Internet Service Providers (personal data retention) for further use by law enforcement authorities.[3]

Other examples for which the number of requests for access might not be publicly known could follow. Given their characteristics, one could think of the value that some types of personal data have for law enforcement authorities. This is the case of biometric data (such as fingerprints), which has been used for many decades by police authorities to identify individuals.[4] Private parties rely more and more on biometric data to control access to buildings, IT systems or applications. Several social media companies, e.g. Facebook, have even constituted biometric databases based on the facial images of their users. In Europe, Facebook stopped facial recognition in 2012, whereas in the USA the company is still collecting such personal data.[5] Of course, Facebook has more personal data than its users' facial images: it might also hold names (real or alias), date of birth, addresses, phone numbers and any kind of personal information a user is willing to provide under their profile. All this personal data, including biometric data, constitutes valuable information for criminal intelligence and criminal investigation.[6] Criminal intelligence is a form of surveillance carried out by law enforcement authorities to gather information about crime or criminal activities before their occurrence or to establish their occurrence.[7] It differs from criminal investigation, which corresponds to a procedural stage in relation to concrete criminal activities. [8] These two activities are covered in this paper.

From a data protection perspective, the obvious questions that arise from this scenario are which legal framework applies to the case of law enforcement access to personal data held by private parties, and whether that framework provides sufficient safeguards to data subjects. The adoption of a new data protection framework at EU level constitutes an excellent opportunity to assess the rules applicable to the scenario at that level. Adopted in April 2016, the new data protection framework is composed of a General Data Protection Regulation (Regulation 2016/679 or GDPR)[9] - replacing the Data Protection Directive - [10] and of a Directive on the protection of personal data processed for law enforcement purposes (Directive 2016/680 or the 'police' Directive).[11] The 'police' Directive replaces the Council Framework Decision 2008/977/JHA adopted under the previous pillar structure.[12] Directive 2016/680 defines the rules applicable to the processing of personal data for law enforcement purposes and more specifically for the purposes of "prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties."[13] The phrase 'law enforcement purposes' should therefore be understood, in the context of this article, as referring to the purposes regulated in Directive 2016/680. The Directive does not explicitly define the different purposes but relies on national laws. Criminal investigation purposes as well as criminal intelligence purposes can therefore fall within the scope of Directive 2016/680.

Against this background, the next section, Section 2, addresses the applicability of both the GDPR and the 'police' Directive to the scenario described in this article: provisions contained in the GDPR govern the initial processing of personal data by private parties, whereas rules set out in the 'police' Directive cover the further processing of the data by law enforcement authorities. After having established that the further processing of personal data falls within the scope of Directive 2016/680, Section 3 analyses the rules of that Directive to determine whether they lay down sufficient safeguards to protect individuals whose personal data is accessed by law enforcement authorities. The rules are assessed against the standards established by the European Court of Justice (ECJ) in two related judgments on the retention of personal data. *Digital Rights Ireland*[14] and *Tele2 Sverige*[15] are particularly

[3] See Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC, OJ 2006, L 105/54.

[4] E.g. S.A. Cole, *Suspect Identities: a History of Fingerprinting and Criminal Investigation* (Harvard Press University, 2001).

[5] It should be noted that the collection, storage, retention and subsequent use of facial images by Facebook have been challenged in Illinois for the lack of informed consent from the individuals concerned, see recent developments http://www.breitbart.com/tech/2017/01/03/class-action-lawsuit-filed-facebook-holding-biometric-data-potentially-violating-illinois-law/.

[6] See for example, https://www.theguardian.com/technology/2014/apr/11/facebook-2000-data-requests-police.

[7] Council Framework Decision 2006/960/JHA of 18 December 2006 on simplifying the exchange of information and intelligence between law enforcement authorities of the Member States of the European Union, OJ 2006, L 386/89; See Article 2 (c) that reads as follows: "crime and criminal activities with a view to establish whether concrete criminal acts have been committed or may be committed in the future."

[8] Council Framework Decision 2006/960/JHA, see Article 2 (b) that reads as follows: "a procedural stage within which measures are taken by competent law enforcement authorities or judicial authorities, with a view to establishing and identifying facts, suspects and circumstances regarding one or several identified concrete criminal acts."

[9] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ 2016, L119/1.

[10] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ 1995, L 281/31.

[11] Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, OJ 2016, L.119/89.

[12] Before the entry into force of the Lisbon Treaty, the EU policy areas were divided into three pillars. The first pillar was composed of the economic communities, whereas the third one regrouped police and judicial matters in criminal matters, see e.g. Catherine Barnard & Steve Peers, *European Union Law* (Oxford University Press, 2014).

[13] Article 1 of Directive 2016/680.

[14] Joined cases C-293/12 and C-594/12, *Digital Rights Ireland* and *Seitlinger and others* [2014], ECLI:EU:C:2014:238.

Please cite this article in press as: Catherine Jasserand, Law enforcement access to personal data originally collected by private parties: Missing data subjects' safeguards in directive 2016/680?, Computer Law & Security Review: The International Journal of Technology Law and Practice (2017), doi: 10.1016/j.clsr.2017.08.002