Available online at www.sciencedirect.com
ScienceDirect
journal homepage: www.elsevier.com/locate/CLSR
Computer Law & Security Review

Balancing data protection and privacy – The case of information security sensor systems

Markus Naarttijärvi[*]

Department of Law, Umeå University, Umeå, Sweden

ARTICLE INFO

Article history:
Available online xxx

Keywords:
Data protection
Privacy
Information security
Sensor systems
Communications monitoring
Metadata

ABSTRACT

This article analyses government deployment of information security sensor systems from primarily a European human rights perspective. Sensor systems are designed to detect attacks against information networks by analysing network traffic and comparing this traffic to known attack-vectors, suspicious traffic profiles or content, while also recording attacks and providing information for the prevention of future attacks. The article examines how these sensor systems may be one way of ensuring the necessary protection of personal data stored in government IT-systems, helping governments fulfil positive obligations with regards to data protection under the European Convention on Human Rights (ECHR), the EU Charter of Fundamental Rights (The Charter), as well as data protection and IT-security requirements established in EU-secondary law. It concludes that the implementation of sensor systems illustrates the need to balance data protection against the negative privacy obligations of the state under the ECHR and the Charter and the accompanying need to ensure that surveillance of communications and associated metadata reach established principles of legality and proportionality. The article highlights the difficulty in balancing these positive and negative obligations, makes recommendations on the scope of such sensor systems and the legal safeguards surrounding them to ensure compliance with European human rights law and concludes that there is a risk of privatised policymaking in this field barring further guidance in EU-secondary law or case law.

1. Introduction

Maintaining information security in the face of antagonistic security threats is no easy task. While it is difficult to estimate the number and scope of attacks against information systems and associated data breaches – as all breaches might not be detected and those that are may not necessarily be reported – numbers from security companies seem to suggest an increase in the frequency of data breaches with a slight reduction in the number of records exposed over the last three years.[1] In any case, countering the threat to information systems from antagonistic actors is increasingly highlighted as a priority for the European Union,[2] as well as governments in many states around Europe.[3] A recent industry survey by PwC

[*] Correspondence to: Department of Law, Umeå Universitet, 901 87 Umeå, Sweden.
E-mail address: markus.naarttijarvi@umu.se

[1] Internet Society, ’Global Internet Report 2016′ (Internet Society, 2016) <https://www.internetsociety.org/globalinternetreport/2016/⟩ accessed 19 January 2018; Gemalto, ’Breach Level Index - First Half 2016′ (Gemalto, 2016) <http://breachlevelindex.com/assets/Breach-Level-Index-Report-H12016.pdf⟩ accessed 19 January 2018.

[2] European Commission, ’Cybersecurity Strategy of The European Union’ (European Union, 2013).

[3] E.g. Swedish Government Official Reports, ’Informations- och cybersäkerhet i Sverige: Strategi och åtgärder för säker information i staten (SOU 2015:23)’ (Swedish Government, 2015); Premier Ministre, ’French National Digital Security Strategy’

https://doi.org/10.1016/j.clsr.2018.04.006
0267-3649/© 2018 Dr Markus Naarttiji. Published by Elsevier Ltd. All rights reserved.

further suggest that a top information security priority for the public sector is adopting continuous monitoring of technical controls and further use of monitoring systems and security intelligence.[4]

One such type of monitoring system will be analysed in this article; the implementation of information security sensor systems in government information architecture.

The term 'information security sensor systems' is used here to describe network monitoring tools which detect attacks (including attempted breaches) against network servers by analysing traffic and comparing this traffic to known attack-vectors, traffic profiles or content, while also recording attacks and thus providing information to sensor databases for the prevention of future attacks. It is not a term that necessarily connotes a specific type of equipment or configurations of such measures as this may depend on the context where it is deployed or the manufacturer of the technology. Instead it refers to technologies, processes and other measures that may include or be described as '*Security Information and Event Management tools (SIEM)*',[5] 'New-Generation Cybersecurity Monitoring and Management Systems',[6] 'Network filters',[7] or 'proactive cooperative defense'.[8] Generally speaking though, the type of sensor system discussed here operates by monitoring the attributes of connections to information systems. This includes, for example, the originating IP-address or e-mail address, the requested resources, and may include the content of e-mails and other communications to and from information systems to enable the real-time or retrospective identification of potential malicious code, phishing attempts or DDoS attacks. A more detailed explanation and concrete examples of their function and use is given in Section 2 below.

There are several reasons why government implementation of such systems is different from that of private enterprises. Signatory states to the European Convention on Human Rights ('ECHR', 'the Convention') as well as member states of the European Union subject to the EU Charter of Fundamental Rights ('the Charter') are required to uphold the fundamental rights enshrined in those legal instruments. As such, they are legally precluded from monitoring private communications if doing so would violate their obligation to protect privacy under art. 8 of the Convention or art. 7 or 8 of the Charter. On the other hand, a growing doctrine of positive obligations in relation to those same human rights instruments illustrate how states also have a responsibility to take effective measures to protect the privacy of individuals under their jurisdiction, if feasible.[9] Consequently, states are obliged by human rights instruments to both act and to refrain from acting, in ways that private actors are not. Meanwhile, the EU General Data Protection Regulation ('GDPR') further highlights the responsibilities of data processors, including government agencies, to implement suitable security measures to prevent unauthorised access to – or disclosure of – personal data.[10]

Also of note is that government agencies in EU member states may also be operators of essential services as defined under the EU NIS-directive.[11] In such cases, they are under a further obligation to report information security incidents to national Computer Emergency Response Teams (CERT:s).[12] The aim of this reporting obligation is to allow national CERT:s to estimate the cross border effects of a security incident within the essential services.[13] Here, monitoring of traffic data may assist both the operators of essential services and the national CERT to estimate the effects of a security incident, while also providing actionable information to prevent such incidents in other systems. However, the role played by monitoring of traffic data by sensor systems has not been without controversy in the run-up to the implementation of notification requirements, as illustrated by a 2011 survey among regulatory agencies conducted by the *European Union Agency for Network and Information Security* (ENISA):

> *"Monitoring of traffic data proved to be a contentious issue among regulatory authorities. Out of the regulatory authorities surveyed by ENISA, 41% responded positively when asked if they thought data traffic should be monitored in order to discover data breaches. Those who responded positively, however, indicated that such monitoring should be conducted under strict legal conditions. In other words, the purpose of the monitoring should be clearly defined and relevant authorities should oversee the process. One regulator further suggested that the proportion of data monitored should be restricted only to the data required for the discovery of the data breach."*[14]

The difficulties involved in balancing security and privacy interests in this context can be illustrated by a recent initiative to implement sensor systems among Swedish government agencies information systems. There, an initial

(French Government, 2015); .BE, 'Cyber Security Strategy of Belgium' (Belgian Government, 2012); Department of Communications, Energy and Natural Resources, 'Irish National Cyber Security Strategy 2015–2017' (Irish Government, 2015).

[4] 'Industry Findings: Public Sector' (PwC, 2017) <https://web.archive.org/web/20170405225152/http://www.pwc.com/gx/en/issues/cyber-security/information-security-survey/public-sector-industry.html > accessed 19 January 2018.

[5] Kavanagh, Kelly M., Oliver Rochford, and Toby Bussa. 'Magic quadrant for security information and event management' *Gartner, Tech. Rep.* (2015).

[6] Igor Vitalévich Kotenko and Igor Borisovich Saenko, 'Creating New-Generation Cybersecurity Monitoring and Management Systems' (2014) 84 *Herald of the Russian Academy of Sciences*.

[7] Lech J Janczewski, Douglas Reamer and Juergen Brendel, 'Handling Distributed Denial-Of-Service Attacks' (2001) 6 *Information Security Technical Report*.

[8] Hakem Beitollahi and Geert Deconinck, 'Analyzing Well-Known Countermeasures Against Distributed Denial of Service Attacks' (2012) 35 *Computer Communications*.

[9] See Section 3 below.

[10] 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).

[11] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union.

[12] Ibid. article 1.

[13] Ibid. article 14.

[14] European Network and Information Security Agency, 'Data Breach Notification in The European Union' (ENISA, 2011) <https://www.enisa.europa.eu/publications/dbn⟩ accessed 19 January 2018.