

Chapter 7.9

What about the Balance between Law Enforcement and Data Protection?

Irene Portela

Polytechnic Institute of Cávado and Ave, Portugal

Maria Manuela Cruz-Cunha

Polytechnic Institute of Cávado and Ave, Portugal & University of Minho, Portugal

ABSTRACT

The Data Retention Directive (2006/24/EC) provides the obligation for providers of publicly available electronic communications services or of public communications networks to retain traffic and location data for six months up to two years for the purpose of the investigation, detection and prosecution of serious crime. In the regulatory framework imposed by this Directive, the Portuguese Law no. 32/2008, of 17 July, requires that providers of publicly available electronic communication services or of public communications networks retain specific communication data, so that such data can be accessed by competent authorities, exclusively for the purpose of investigation, detection and prosecution of serious crime. Retained (via digital storage) metadata of telecommunications acts change and transform into the content of something else: a surveillance program. The concept of a data space that provides movement within and between data described here illustrates the powers of data retention in an imaginable way. Considering potential uses and misuses of retained data such as traffic analysis, social network analysis and data mining, this chapter examines the degree of interference with the right to privacy posed by the data retention laws.

INTRODUCTION

The EU adopted the Data Retention Directive in March 2006. The purpose of the Directive is to achieve an EU-wide harmonisation of national requirements for the mandatory retention of com-

munications data. Seen from a broader scope, data retention fits well into the post-9/11 war on terror measurements. The shift toward an omniscient surveillance-state has generally often been compared to scenarios familiar from the prophetic novel 1984 by George Orwell (1949).

DOI: 10.4018/978-1-61350-323-2.ch7.9

What about the Balance between Law Enforcement and Data Protection?

After the terrorist attacks in Europe in 2004 and 2005, the EU passed the Directive because of the legal and technical differences between national provisions for data retention¹. The European Union Directive on data retention², though less than 10 pages long, is invested with considerable authority³. The Data Retention Directive requires EU governments to retain data for assistance in the investigation, detection and prosecution of serious crime³ and covers both telephones and the internet. It directs the member states to pass a law compelling each provider of telecommunications services to retain traffic and location data for at least the past six, and at most, the last 24 months.

Two key privacy protections were removed. The first of which said that data could only be held for the purposes of billing (ie: for the customer to check the details), usually only for a few weeks. The second allows member states to adopt national laws to require communications providers to retain data for a specified period so that law enforcement agencies can get access to it.

As stated in the first sentence of Article 1: This Directive aims to harmonise Member States' provisions concerning the obligations of the providers of publicly available electronic communications services or of public communications networks with respect to the retention of certain data which are generated or processed by them, in order to ensure that the data are available for the purpose of the investigation, detection, and prosecution of serious crime, as defined by each Member State in its national law (2006/24/EC: 56).

- And what are the data object of the EU Directive⁴?

The "Data" as is defined in this text is "data generated by or during an act of telecommunication with a mobile phone, a landline, or via the Internet", minus the content, means traffic data and location data.

These inquiries around data ask who, when, where, with whom, how long, and so forth — but

do not ask about the nature of the communication. The data generated during unsuccessful acts of telecommunication is also similarly analysed. (Davies & Trigg, 2006).

This differentiation between data that contains the structural components of communication and data that relates to content is that traffic data consists only of the information needed to technically initiate, sustain, and terminate an act of communication.

However, as the Directive aims at "the investigation, detection, and prosecution of serious crime," the relevant data is divided into the following categories⁵ as we can see at the article 5⁶ of the 2006/24/EC:

- (1) data necessary to trace and identify the source of a communication. For example:
 - The telephone number and subscriber name and address (telecoms);
 - The user ID and name and address of the subscriber or registered user (Internet);
- (2) data necessary to identify the destination of a communication. For example
 - the number called, any number to which a call is rerouted, name and address of subscriber/user (telecoms); user ID or telephone number of the intended recipient(s) of an Internet telephony call, name and address of subscriber/user (Internet);
- (3) data necessary to identify the date, time, and duration of a communication;
- (4) data necessary to identify the type of communication: the telephone or Internet service used;
- (5) data necessary to identify users' communication equipment or what purports to be their equipment: the calling and called telephone numbers, identifiers of mobile telephone and SIM card; the date, time and place of initial activation of prepaid card;

16 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage:
www.igi-global.com/chapter/balance-between-law-enforcement-data/61025

Related Content

Forensic Watermarking for Secure Multimedia Distribution

Farook Sattar and Dan Yu (2009). *Socioeconomic and Legal Implications of Electronic Intrusion* (pp. 261-280).

www.irma-international.org/chapter/forensic-watermarking-secure-multimedia-distribution/29369/

Machine Learning for Clinical Data Processing

Guo-Zheng Li (2011). *Digital Forensics for the Health Sciences: Applications in Practice and Research* (pp. 193-215).

www.irma-international.org/chapter/machine-learning-clinical-data-processing/52289/

Computer Hacking and the Techniques of Neutralization: An Empirical Assessment

Robert G. Morris (2011). *Corporate Hacking and Technology-Driven Crime: Social Dynamics and Implications* (pp. 1-17).

www.irma-international.org/chapter/computer-hacking-techniques-neutralization/46417/

Digital Image Splicing Using Edges

Jonathan Weir, Raymond Lau and WeiQi Yan (2010). *International Journal of Digital Crime and Forensics* (pp. 63-75).

www.irma-international.org/article/digital-image-splicing-using-edges/47072/

Image Watermarking

Nikos Tsirakis (2012). *Cyber Crime: Concepts, Methodologies, Tools and Applications* (pp. 587-599).

www.irma-international.org/chapter/image-watermarking/60970/