Chapter 15
The EC Data Retention Directive: Legal Implications for Privacy and Data Protection

Nóra Ní Loideain
Office of the Director of Public Prosecutions, Ireland*

ABSTRACT

The focus of this paper is the new European legislation designed to harmonize domestic laws on the retention of telecommunications data for the purpose of assisting law enforcement efforts. The European Union introduced the EC Data Retention Directive in 2006. This Directive requires the retention of every European citizen’s communications data for up to two years for the purpose of police investigation. There is, however, a major problem with the Directive in that it regularizes, and thereby entrenches, the practice of data retention across Europe. No systematic empirical evidence supports the introduction of such broad surveillance. The existence of data retention in principle raises concerns for data protection and the right to respect of privacy as protected under the European Convention of Human Rights (ECHR). This paper questions the proportionality of the Directive in line with data protection principles and Europe’s obligations under Article 8 of the ECHR.

I. INTRODUCTION

States have always been faced with the difficult task of striking a balance between the constitutional rights of the citizen to privacy and security. Debate continues as to whether the surveillance of innocent citizens can be justified as ‘a necessary evil’ (Sewell & Barker, 2001; Marx, 1988) in the pursuit of public safety and security. Continuing developments in modern technology in the area of telecommunications have had an impact upon how serious criminals now approach their operations. An example of terrorists incorporating modern communications technology in the undertaking and planning of their attacks was demonstrated in the terrorist attacks on Madrid in 2006 where mobile phone cards were used to detonate bombs on the trains in the Madrid terrorist attacks (BBC News, 2006). The need, therefore, for balance between the competing interests of security

DOI: 10.4018/978-1-60960-083-9.ch015
The EC Data Retention Directive and privacy has become all the more urgent. It is understandable that the State, via the police, would seek to utilize the power of technological advances in telecommunications and cyberspace for the purpose of safeguarding its citizens. To what extent, however, should the police be allowed to invade the privacy of citizens’ communications in the interests of State security?

The EC Data Retention Directive came into force from 3 May 2006 (Directive 2006/24/EC, Article 16). This Directive requires the retention of every European citizen’s communications data, including traffic data of communications and location data of the communication devices used, for up to two years for the purpose of police investigation. The Directive effectively gives investigative authorities across the European Union unprecedented access to the private lives of its citizens. This paper will set out the origins (Parts II and III) and main provisions of the Directive (Part IV). Its legislative development demonstrates the considerable unease among legislators and non-governmental organizations surrounding the Directive. The implications of the Directive for data protection and the right to respect of privacy as guaranteed under the European Convention of Human Rights (ECHR) will be then be addressed (Part V).

It is submitted that there is a major problem with the Directive in that it regularizes, and thereby entrenches, the practice of data retention in Europe. No empirical evidence has been put forward demonstrating that data retention will be effective in the fight against serious crime that would establish the necessity for such unprecedented invasions of privacy. Further, even if the retention of data can sometimes be justified, the measures under the Directive have blanket application to the communications of all citizens and not just those suspected of the commission of, or involvement with, serious crime. Hence, the proportionality of the Directive must be considered suspect. It will be recommended that the evaluation of the Directive’s impact and the future development of law reform and policy governing State surveillance of telecommunications and cyberspace should be evidence-based in order to ensure the development of proportionate and effective legislation (Part VI).

II. BACKGROUND OF THE DATA RETENTION DIRECTIVE

The blanket retention of communications data for the purpose of law enforcement was a measure first proposed by the EU Telecommunications Council shortly before the 9/11 terrorist attacks upon New York and Washington D.C. in 2001. Under this early proposal, Internet Service Providers (ISPs) would be required to retain all citizens’ communications data from telephones, mobile phones, faxes, emails and other internet use for up to 7 years (Lillington, 2001a). After the 9/11 attacks, the President of the United States of America sent a communiqué urging the EU to adopt provisions for the blanket retention of communications data “in the international effort against terrorism” (United States Mission to the European Union, 2001). More than thirty international civil rights organizations expressed concern to the EU Council of Ministers and U.S. President George Bush regarding the threat to civil liberties and the right to privacy posed by this unprecedented measure (Global Liberty Internet Campaign, 2001). These civil liberties organizations also highlighted the absence of such a data retention obligation for ISPs in the U.S. and pointed out that “there is a significant risk, if this proposal goes forward, that US law enforcement agencies will seek data held in Europe that it could not obtain at home, either because it was not retained or because US law would not permit law enforcement access.” The opposition of the Article 29 Working Party, Data Protection Commissioners across the European Union, was more direct:

*It is not acceptable that the scope of initial data processing is widened in order to increase the*
Related Content

Privacy-Preserving Transactions Protocol Using Mobile Agents with Mutual Authentication
[www.igi-global.com/article/privacy-preserving-transactions-protocol-using/2455?camid=4v1a](www.igi-global.com/article/privacy-preserving-transactions-protocol-using/2455?camid=4v1a)

Identity Theft and E-Fraud as Critical CRM Concerns
[www.igi-global.com/chapter/identity-theft-fraud-critical-crm/23277?camid=4v1a](www.igi-global.com/chapter/identity-theft-fraud-critical-crm/23277?camid=4v1a)

Port Scans
[www.igi-global.com/chapter/port-scans/13521?camid=4v1a](www.igi-global.com/chapter/port-scans/13521?camid=4v1a)

Digital Certificates and Public-Key Infrastructures
[www.igi-global.com/chapter/digital-certificates-public-key-infrastructures/23155?camid=4v1a](www.igi-global.com/chapter/digital-certificates-public-key-infrastructures/23155?camid=4v1a)