COMPUTER LAW & SECURITY REVIEW ■■ (2018) ■■–■■

Available online at www.sciencedirect.com

ScienceDirect

www.compseconline.com/publications/prodclaw.htm

Computer Law & Security Review

Comment

Data retention

Ian Lloyd *

National Research University, Moscow, Russian Federation

Keywords:
Data retention
European Law
Human rights
National security

A B S T R A C T

Use of our mobile communication devices tells a good deal about us. It is often the case that what number calls what number, at what times and frequencies and, in the case of mobile phones from and to what geographical locations can be as revealing to law enforcement and national security agencies as the actual contents of messages. Inevitably, though, this may involve the processing of data concerning millions of people who have no inclination to engage in unlawful conduct. Establishment of a legal regime for data retention that balances the claims of law enforcement agencies to prevent and detect criminal and terrorist activities has proved to be a difficult task. A number of legal challenges have been brought before the British and European Courts and this note seeks to consider and place in context the recent litigation involving the legality of the United Kingdom's Data Retention and Investigatory Powers Act 2014 (*Watson and Others v. Secretary of State* [2018] EWCA Civ 70).

1. Introduction

The recent decision of the Court of Appeal in the case of *Secretary of State v. Watson and Others*[1] marks the latest stage in a long and doubtless ongoing battle fought before the domestic and European courts. The regulation of communications privacy raises difficult issues, with an individual's wishes and expectations of privacy requiring to be balanced against a range of other factors, largely concerned with the roles of law enforcement and national security agencies in seeking to prevent or detect unlawful acts. Technology has always played a role in this process being used by both the watchers and the watched. The advent of electronic communications in the 19th century made possible virtually instantaneous communication regardless of distance and, through the use of encryption, with a high level of anonymity. It is not for nothing that the electric telegraph has been referred to as the "Victorian Internet" (See Tom Standage's book of this name. Bloomsbury Publishing 1999).

We now live in an age of near continuous electronic communications. Individuals communicate incessantly using mobile phone whether for voice calls or for text or email messages, billions of which are sent every day. Many millions of people rely also on the Internet to receive and in many cases to impart information using social networking sites. All of these activities involve leaving electronic trails and one of the key legal issues concerns the extent to which these may be monitored by law enforcement agencies. A broad distinction can be drawn between the monitoring of the contents of individual communications, a practice that, media hype apart, may affect the everyday lives and activities of relatively small numbers of people, and the monitoring of communications data. The concern here is not so much with what is said between

* National Research University, Moscow, Russian Federation.
E-mail address: ianlloyd@me.com.

[1] [2018] EWCA Civ 70.

https://doi.org/10.1016/j.clsr.2018.02.004

Please cite this article in press as: Ian Lloyd, Data retention, Computer Law & Security Review: The International Journal of Technology Law and Practice (2018), doi: 10.1016/j.clsr.2018.02.004

individuals but with patterns of communication. Who contacts who, and at what frequency and times, may be as significant to an investigator as the content of communications and much of the present debate concerns what is generally referred to as "communications data". This encompasses virtually every aspect of a communication other that the actual content.

It is fair comment that every action we take gives out information about ourselves. This has always been the case. We cannot live in a vacuum and have always needed to acquire goods and services from other people. What is novel about modern data practices?

The analogy is sometimes made with the building of a spider's web of data trails. The difference, however, is that we are flies and the watchers are the spider. Unlike the arthropod example where the spider creates the web, human flies produce the materials for the trap into which they may fall prey.

Modern forms of communication pose opportunities and threats to users and watchers. Traditional forms of real time interception are rendered difficult because of the use of technologies such as packet switching, which divides up a message into separate packages for the purpose of transmission with each packet potentially being routed differently. The message will be re-assembled by an intermediary, however, and a large-scale operator such as Google will hold data relating to many millions of users. Co-operation on its part with law enforcement requests for access to the data will facilitate speedy access to the contents of messages as well as to communications data.

2. Legal background

As with any tool, data can be put to both desirable and undesirable uses. A key task for the law is to maximise the potential of the former and minimise the risks of the latter. In the present context, a helpful start point is to be found in data protection legislation, which in the Acts of 1984 and 1998 formulated the principle that data should not be retained for longer than is necessary for the purpose for which it was initially obtained. This is not in itself an easy matter to determine. Data may well be obtained and processed for multiple purposes. In some cases, the data may be anonymised after a certain period although there is debate how effective such techniques might be given the processing capability of modern computers. It is, however, a potentially significant limitation and the first legislative move towards supporting data retention came with the Anti-Crime and Terrorism Act of 2001 providing that data controllers might retain data for longer than was necessary in data protection terms in order to support the interests of law enforcement. A voluntary code of practice was introduced under the auspices of the Act laying form procedures for access to such communications data to be sought by law enforcement agencies.

Although it is easy to ignore the financial implications of data storage, it is not a cost-free activity and an issue that has featured prominently in the data retention debate concerns the question "who pays?". The ability to pay to retain data that might prove useful to law enforcement proved to have little appeal to companies. The approach of the 2001 Act was essentially followed at the EU level with the adoption of Directive 2002/20/EC of the European Parliament and of the Council of 7 March 2002 on the authorisation of electronic communications networks and services (the "Authorisation Directive").[2]

The next step was to move to compulsion and the impetus came largely from EU legislation in the form of the 2006 Directive on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks.[3] This approach was adopted in stages in the UK with the principal measure being the Data Retention (EC Directive) Regulations 2009.[4]

Until this stage, data retention had enjoyed something of a legal – of not a political – honeymoon. Things changed significantly with the 2014 decision of the European Court of Justice in the case of *Digital Rights Ireland v. Minister for Communications*.[5] The Court here held the 2006 data retention Directive to be invalid, essentially on the ground that it constituted a disproportionate response to the undoubted dangers that it was directed at.

The effect of the Digital Rights judgment was to cast severe doubt on the validity of the implementing UK legislation. The legislative response to this took the form of provisions in the Data Retention and Investigatory Powers Act of 2014 (DRIPA). This measure was itself the subject of legal challenge and was declared to be invalid by the European Court[6] following a request for a Preliminary Ruling from the Court of Appeal. The case was joined with a reference from the Swedish courts for a ruling concerning the legality of aspects of Swedish law in the field.

Once again, the court ruled against the legislation. Its reasons were broadly similar to those of its earlier ruling. Directive 2002/58, it was ruled, had to be interpreted,

> *as precluding national legislation governing the protection and security of traffic and location data and, in particular, access of the competent national authorities to the retained data, where the objective pursued by that access, in the context of fighting crime, is not restricted solely to fighting serious crime, where access is not subject to prior review by a court or an independent administrative authority . . .*[7]

Criticisms of the legislation, therefore, were both substantive and procedural. This is a combination that has bedevilled the UK's dealings with the European Court of Justice and the Court of Human Rights from the beginnings of interception of communications legislation. In the seminal case of Malone that led to the enactment of the Interception of Communications Act 2000, the European Court of Human Rights held that the UK was in breach of its obligations under Article 8 of the Convention by permitting the interception of communications

[2] OJ 2002 L 108, 22.
[3] Directive 2006/24/EC. OJ 2006 L105/54.
[4] SI 2009 No 859.
[5] Case C-293/12.
[6] Case C-695/15. *Secretary of State for the Home Department v. Watson and Others*.
[7] At para 125.

Please cite this article in press as: Ian Lloyd, Data retention, Computer Law & Security Review: The International Journal of Technology Law and Practice (2018), doi: 10.1016/j.clsr.2018.02.004