

Data Retention Directive - JISC Legal Overview



The Data Retention Directive: Implications for FE and HE

Andrew Charlesworth

Please note: this guidance has been prepared by **JISC Legal** for information purposes only and is not, nor is intended to be, legal advice. This information is not intended to constitute, and receipt of it does not constitute, a contract for legal advice or the establishment of a solicitor-client relationship.

16 April 2007

Table of contents

1. Introduction	1
2. Data Retention – A Primer	2
The current UK data retention regime	2
The new EU data retention regime	5
3. Implications for FE and HE institutions	7

1. Introduction

This overview paper briefly explains the current situation with regard to retention of communications traffic data by certain UK organisations; examines impending moves to impose mandatory retention based on European Union (EU) Directive 2006/24/EC on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks - http://europa.eu.int/eur-lex/lex/LexUriServ/site/en/oj/2006/l_105/l_10520060413en00540063.pdf (the Data Retention Directive); and explores the possible implications of those moves for current and future FE and HE provision of telecommunications and network services.

The phrasing of the Data Retention Directive, and the fact that considerable discretion is left to the Member States in the implementation of any Directive, has raised concerns in certain quarters that some Member States may seek to impose data retention requirements on a wider range of organisations than has, until now, been the case, by adopting a broad definition of 'publicly available electronic communications services' and 'public communications networks'.

In the UK, established forms of FE and HE communications service seem unlikely, at present, to fall within the scope of any implementing legislation or administrative practices. However, changes to current communications service practice, including the supply of

publicly accessible campus wi-fi networks, or involvement in the provision of wireless local area network (WLAN) services to communities local to FE and HE institutions, might not be viewed in the same way. Equally, if concerns already expressed about FE and HE institutions becoming 'safe harbours' for radical groups (or copyright breachers) become more widespread, there may be pressure on the Government to reconsider their position as 'private communications service providers', or that of the Joint Academic Network (JANET) as a 'private communications network'.

2. Data Retention – A Primer

The EU adopted the Data Retention Directive in March 2006. The stated purpose of the Directive is to achieve an EU-wide harmonisation of national requirements for the mandatory retention of communications data. It was proposed in a package of measures following terrorist atrocities in Europe in 2004 and 2005 and was pushed through during the UK presidency of the EU at the end of 2005.

The EU passed the Directive in part due to concerns that legal and technical differences between national provisions for data retention designed to aid the prevention, investigation, detection and prosecution of criminal offences might mean that Member States, by accident or by design, placed barriers to the cross-border supply of electronic communications services. For example, a mobile phone service provider might find that in order to provide services to customers in multiple Member States they were legally required to retain different types of communications traffic data, under different conditions, and for different time periods, in each of those Member States - this would be a potential disincentive to their moving into other Member State markets. However, as will be seen below, the broad leeway afforded to Member States in the implementation of the Directive may still result in problems for cross-border service providers.

The UK already operates a voluntary system of data retention of communications traffic data. The effect of the Directive will be to require that this is replaced by a mandatory system of data retention.

Member States must implement the provisions of the Directive concerning fixed network and mobile telecommunications in their national laws by 15 September 2007. Member States have been given the option to delay the application of the Directive to retention of communications data relating to Internet access, Internet telephony and Internet e-mail until 15 March 2009, and the UK has made a Declaration to the Commission that it intends to utilise that option.

The current UK data retention regime

As noted above, the UK already has a system of data retention of communications traffic data. Although the Code is a voluntary system, there was considerable pressure on the telecommunications industry to introduce a scheme, following September 11th 2001, under the threat from the Government of a mandatory scheme being imposed. The Code was unpopular, largely because of industry concern that compliance with a voluntary code, – as opposed to a legal obligation – could breach human rights and data protection legislation. However, the Home Office indicated that if the voluntary code of practice was not effective then they would make the code compulsory through a statutory instrument.

This scheme is the Code of Practice for Voluntary Retention of Communications Data <http://security.homeoffice.gov.uk/news-publications/publication-search/general/5b1.pdf>

(the "Code") which was provided for in Part 11 of the Anti-Terrorism, Crime and Security Act 2001 - <http://www.opsi.gov.uk/ACTS/acts2001/10024--l.htm> - (ATCSA 2001), and came into force in January 2004.

In principle, the ATCSA 2001 applies to all communications networks. However, the Code only applies to communication service providers who provide a public telecommunications service in the United Kingdom, as defined in s.2 of the Regulation of Investigatory Powers Act 2000 - <http://www.opsi.gov.uk/Acts/acts2000/20000023.htm> - (RIPA 2000), and who retain communications data in line with the provisions of the ATCSA 2001.

The Code is thus not intended to apply to individuals and organisations that do not provide a public service (e.g. corporate telecommunications and computer networks). As FE and HE institutions are not seen to provide a public telecommunications service as defined under RIPA 2000, they are not currently covered by the Code.

Regulation of Investigatory Powers Act 2000 s.2

"public telecommunications service" means any telecommunications service which is offered or provided to, or to a substantial section of, the public in any one or more parts of the United Kingdom;

"public telecommunication system" means any such parts of a telecommunication system by means of which any public telecommunications service is provided as are located in the United Kingdom;

"telecommunications service" means any service that consists in the provision of access to, and of facilities for making use of, any telecommunication system (whether or not one provided by the person providing the service); and

"telecommunication system" means any system (including the apparatus comprised in it) which exists (whether wholly or partly in the United Kingdom or elsewhere) for the purpose of facilitating the transmission of communications by any means involving the use of electrical or electro-magnetic energy.

The Code does not require telecommunications service providers and Internet service providers to retain communications data, but it is designed to:

- suggest agreed time periods for retention of certain types of communications data, and
- where those time periods for retention are longer than the period for which a relevant organisation would normally retain data for business purposes, to provide a basis upon which they may legitimately continue to retain that data for national security purposes and the prevention or detection of crime or the prosecution of offenders relating to the national security.

The Code is not concerned with the powers of public authorities, such as the police, to obtain communications data that has been retained in line with its guidance. This issue is dealt with by Chapter II of Part I of RIPA 2000 and other statutory powers.

The Code is concerned solely with retention of communications data, not with the contents of communications: in other words it deals with data "about" communications, rather than the data "in" communications. The type of data involved is outlined in s.21(4) RIPA 2000, and comprises 3 main elements:

- traffic data - e.g. data about telephone numbers called, email addresses, and location data.
- use made of service - e.g. services subscribed to.
- other information relating to the subscriber - e.g. installation address.

The Code does not require that service providers collect any information that they would not otherwise collect in the course of their business activities. Retention periods for traffic data start at the point when a communications ends, e.g. when a telephone caller hangs up; for service usage data at the completion of a use, e.g. following a mobile phone service transaction; and for subscriber-related data, when the data changes or when the subscriber leaves the service.

The maximum retention period for communications data held under the Code is 12 months. If the communication service provider's business practices require a longer retention period, the Code does not prevent this.

Example

Midwich Telco, a telecommunications service provider, processes and retains communications data about telephone calls made via its system, for the purposes of subscriber billing. Its customers are told that its business practice is to hold data for each quarterly billing period until the end of the following quarterly billing period, providing, at most, a six month retention period.

As the data can be linked to an individual subscriber, it falls under the Data Protection Act 1998 (DPA 1998). The Fifth Data Protection Principle requires that once the purpose for which data has been collected has ended, the data controller, in this case Midwich Telco, should stop using it. As Midwich Telco's purpose for holding communications data is met at the end of the quarterly billing period after which it was collected, the data would normally be deleted/destroyed at that time.

However, the Code provides a further purpose for the communications data that Midwich Telco processes and retains. It provides the necessary conditions under both Schedule 2 DPA 1998 (processing of personal data) and Schedule 3 DPA 1998 (processing of sensitive personal data), namely that it is necessary for Midwich Telco to retain the data to enable the Secretary of State to fulfil his function for the protection of national security. Under the Code, the retention period for the type of communications data collected by Midwich Telco is twelve months.

Midwich Telco's communications data is thus held for dual purposes for the first 6 months of its retention (business purposes + national security purposes). It is then held for a further 6 months for the single purpose of national security. During the first six months, Midwich Telco can process and retain the data as it would normally have done for business purposes. After six months, however, the business purpose is complete, and the data is now being held for the national security purpose.

Midwich Telco thus needs to be able to identify when its retained communications data passes the business purpose time period. After that point, Midwich Telco may not use the data for its own business purposes, and may only hold it in case it is required for national security purposes. Any communications data collected by Midwich Telco for business purposes, and which is not covered by the Code, should be identified, removed from the retained data, and properly disposed of at that point.

If Midwich Telco has a legitimate business purpose for which it retains communications data for each quarterly billing period for up to 18 months, then the business purpose time period will extend past the national security purpose time period. The Code does not prevent this, and Midwich Telco may need to carry out less 'data cleaning' as a result, as holding more data than the Code requires is fine, where it falls within the business purpose.

The Code also provides that the Home Office may enter into more detailed service level agreements with individual communication service providers who receive requests for

communications data stored under its provisions. These agreements are designed so that communication service providers can inform the necessary public authorities, e.g. the police, of their retention practices where necessary. The Home Office recognises that meeting these requirements costs the individual communication service providers time and money and the government will make payments to communication service providers to cover these retention costs. However, payments will only be made where data retention periods are significantly longer for national security purposes than for business purposes, and may include capital investment into retention and retrieval equipment and/or running costs. Agreements are voluntary and can be terminated by either party subject to an agreed period of notice.

An example of such an agreement being reached by the Government was reported in *The Financial Times* (p.4, 11 November 2005). The Government reportedly paid £875,000 to cover mobile operator O₂'s data retention costs, and to provide a system capable of retrieving the type of specific information likely to be requested by law enforcement agencies.

The new EU data retention regime

Like the Code, the Directive is only concerned with the traffic and location data of legal entities and natural persons, and any related data necessary to identify a subscriber or registered user. It explicitly states that the retention of the content of electronic communications, including information consulted using an electronic communications network, is outside its scope - while it does not require such retention, it does not bar it.

Unlike the ATCSA 2001, the Directive does not apply to all communications networks. As with the UK Code of Practice, it instead refers to a limited sub-set of communications networks. It requires that certain data are to be retained where those data are generated or processed by providers of publicly available electronic communications services or by providers of a public communications network in the process of supplying the communications services concerned. Determining what activities will cause an organisation to be deemed to be a 'provider of publicly available electronic communications services' or 'a provider of a public communications network' is left to the Member States (Kosta & Valcke 2006). There is no requirement in the Directive for communications service providers to create new data for retention purposes, merely a requirement to retain existing data generated or produced in the course of their service provision.

Some concerns have been raised that the idea that all data "generated or processed" by a communications service provider will be caught by the Directive; whilst nominally technology-neutral, this seems more geared to telecommunications than to internet services. It appears unclear whether internet service providers are supposed to retain only data of their own subscribers, or whether they are supposed to retain the data of users whose communications simply pass over their network (Davies & Trigg 2006). It would seem, however, from a purely pragmatic point of view that the former interpretation must logically apply.

The Directive sets out several categories of data which must be retained. These are data necessary to:

- trace and identify the source of a communication, e.g. the telephone number and subscriber name and address (telecoms); user ID and name and address of the subscriber or registered user (Internet)
- identify the destination of a communication e.g. 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)
- identify the date, time and duration of a communication
- identify the type of communication e.g. the telephone or Internet service used
- identify users' communication equipment, or what purports to be their equipment
- identify the location of mobile communication equipment e.g. cell ID and geographic location of cell.

The Directive also requires the retention of data relating to unsuccessful call attempts where those data are generated or processed, and stored (e.g. telephony data) or logged (e.g. Internet data). This is not data that would normally be held, for example, by telecommunications companies for billing purposes (Davies & Trigg 2006).

As far as retention periods are concerned, the Directive states that Member States may set a retention period of not less than six months and not more than two years from the date of the communication. However, Member States can, if circumstances dictate, and for a limited period of time, extend the maximum period as long as they inform the other Member States and the Commission that they have done so, and their reason for doing so. The Commission will then check after 6 months to ensure that the extended retention period is not being used as a disguised trade restriction. It appears that where such an extension is approved by the Commission, it may be continued indefinitely. Previous experience, in arenas such as data privacy, suggests that the broad scope of the discretion over time periods may not bode well for uniformity of retention and the harmonisation process.

The Directive indicates that data retained must be kept subject to appropriate technical and organisational measures to ensure that they can be accessed by specially authorised personnel only and, except for data that has been accessed and preserved (presumably for the purposes specified under the Directive), retained data must be destroyed at the end of the period of retention. With regard to the former point, it has been noted that given that data generated or processed by communications service providers in the process of supplying communications services is likely to include items such as billing data, and that this might mean either designating billing clerks as 'specially authorised personnel', or requiring separate systems for business purpose data and data retained pursuant to the Directive. (Davies & Trigg 2006) Again, in practice, it seems likely that, at least while the data is still being used for business purposes communications, service providers in the UK are likely to be able to continue with their existing operational practices under the voluntary Code of Practice.

A final area of interest lies with the use of the retained data. The Directive provides that data retained under the Directive is to only be provided to "the competent national authorities in specific cases and in accordance with national law." It does not specify any criteria for 'competent authorities', which means that some Member States may choose to widen access beyond law enforcement agencies, nor does it provide guidance as to the reasons for which retained data may be accessed, again leaving this to the discretion of the Member States. (Davies & Trigg 2006, Kosta & Valcke 2006) Germany has already indicated that access to traffic data will be permitted not just for the investigation of

"substantial" offences, but also for the investigation of any offence committed using telecommunications networks - including the sharing of copyrighted content.

It is unclear at present whether the Directive will produce any major changes to the practical operation of data retention in the UK. There will certainly be pressure to increase at least some retention periods from their current maximum of 12 months to the permissible 24 months. However, this will inevitably face resistance from communications service providers, particularly internet service providers, many of whom already work on razor-thin margins, and who are going to be unwilling to engage in significant expenditure on data retention that does not have a clear direct benefit to them. The government has faced extensive criticism from trade groups regarding the resource and costs telecommunication companies will have to spend on the retention of data. Any resistance may be overcome if funding is forthcoming from the government to cover capital expenditure and running costs for data retention outside the scope of normal business purposes. While the Directive itself is silent on the issue of costs, informal indications have suggested that a similar approach to such costs to that adopted under the Code of Practice could be followed under a new UK regime.

There is no precise indication at present as to the scope of 'competent national authorities' envisaged by the Home Office. The furore caused in 2002-2003 by the then Home Secretary, David Blunkett proposing (unsuccessfully) to widen access to RIPA data from the police, the intelligence services, Customs & Excise and the Inland Revenue to a wide array of public bodies including Whitehall departments, local authorities and quangos, suggests that significant changes to the existing regime in this area would be unpopular and, at this time, probably politically undesirable.

3. Implications for FE and HE institutions

As was suggested in the introduction, it is unlikely that FE and HE institutions will face any immediate implications from national measures to implement the Data Retention Directive in the UK. FE and HE institutions provide communications services to a closed group of individuals - their staff, students and authorised visitors. This does not appear to constitute a service being 'offered or provided to, or to a substantial section of, the public in any one or more parts of the United Kingdom' as per s.2 RIPA 2000.

Whether FE and HE institutions fall within the definition of a 'provider of publicly available electronic communications services' is the key to establishing whether these institutions will have duties of retention under the Directive. It is probable that the current interpretation under the Code of the definitions of 'public telecommunications system' and 'public telecommunications service' will continue to apply under any new UK data retention framework. This would mean that, in the normal course of events, the types of communications service that FE and HE institutions currently supply should remain outside the scope of mandatory data retention.

UKERNA, which operates the JANET network, submitted a statement to the All Party Internet Group's public inquiry - <http://www.apig.org.uk> [Note now called The All Party Parliamentary Communications Group (apComms) - <http://www.apcomms.org.uk/>] - into the retention of, and access to, communications data for law enforcement purposes in 2002, prior to the adoption of the Code, outlining why neither UKERNA, nor its customer organisations, were appropriate targets for mandatory data retention. It noted that most FE and HE institutions would not collect the relevant communications data under the Code because they have no specific purpose for doing so under the DPA 1998, and there was

no requirement in UK law for private networks to routinely collect or retain data solely for the purpose of assisting investigating authorities.

This is not to say that this current exemption from the mandatory data retention regime will necessarily remain a given. Some commentators (usually affiliated with ISPs) have made the point that some universities and colleges may have more internet communications service users than the smaller commercial ISPs. It is not implausible that FE and HE institutions could find themselves in a position where, if they, or their spin-off companies, enter into ventures, such as community freenets, which offer internet communications services to a wider user base than their staff, students and authorised visitors, they are deemed to have passed the tipping point from being a private supplier of a communications service to being a public supplier of such a service. If this is deemed to be more than an insubstantial provision of service, this would then trigger the requirement to participate in the mandatory data retention process.

It is likely that should this occur there would be out-cry from the FE and HE institutions. The costs involved in retaining data would be prohibitive for FE and HE institutions. Unlike private companies who may have the budget to retain data, FE and HE institutions will not have extra funds to spend on retaining data. In addition, there would potentially be public dissatisfaction if FE and HE institutions have to divert funding from education to pay for data retention. Unless the Government is willing to provide funding for the retention of data the FE and HE institutions would be severely affected.

Example

The University of Wyndham decides to provide public wi-fi hotspots in all its open access areas, including parts of the Library, University cafes and student bars. The service is open access and not restricted to the University of Wyndham's staff, students and authorised visitors. The University will run this service, part-funded by advertising, through a wholly owned spin-off company, Chocky Comms, as it does not believe that the open access service will fulfil the criteria laid down in the University's agreement with UKERNA for the proper use of JANET. Chocky Comms will buy Internet access and bandwidth from a network operator, BT.

Chocky Comms will also supply a restricted (500kb/s) broadband service to a range of local community centres, as part of the University's outreach programme, which aims to widen local community access to information communication technologies (ICTs). Members of the public will be able to access the Internet through this service without charge, but as there is a cap on individual downloads of 100MB/day, users will be required to go through a registration process, including collection of the user's name and address, before access is granted via a username/password system.

In this example, Chocky Comms appears to be acting as an internet service provider. The internet access services it provides are not private and limited to a closed category of users: it is clearly offering or providing those services to the public. Whether this is deemed to be a 'substantial section' of the public in that part of the UK is likely determine whether Chocky Comms is subject to mandatory data retention requirements under UK legislation implementing the Directive. It is arguable that both services would fall beneath the threshold as defined, despite being accessible by the public.

If Chocky Comms does become subject to the data retention framework, it will need to consider whether the data generated or produced in the course of its service provision is required to be retained. It will also have to assess its ability to store and retrieve retained data effectively and securely, and to make provision for additional storage and running costs.

Finally, FE and HE institutions should not interpret current developments in the data retention sphere to mean that they should not, or cannot, continue to retain and process the communications data they need for their own purposes, including administration and

protection of their computers and networks, and compliance with other legal obligations e.g. contracts and connection agreements (such as the JANET Acceptable Use Policy - <http://www.ja.net/services/publications/policy/aup.pdf>). Where there is an identified institutional purpose that satisfies the necessary conditions under Schedule 2 DPA 1998 (processing of personal data) and, if necessary, Schedule 3 DPA 1998 (processing of sensitive personal data), and data subjects have been appropriately informed of that purpose, such retention and processing will be legitimate.

Background materials

Davies, G. & Trigg, G. (2006). Being Data Retentive: A Knee Jerk Reaction. *Communications Law*. 11(1): 18-21.

Kosta, E. & Peggy Valcke, P. (2006). Retaining the Data Retention Directive. *Computer Law and Security Report*. 22: 370-380.

Taylor, M. (2006). The EU Data Retention Directive. *Computer Law and Security Report*. 22: 309-312.

Whitley, E.A & Hosein, I. (2005). Policy discourse and data retention: The technology politics of surveillance in the United Kingdom. *Telecommunications Policy*. 29: 857-874.

Regulation of Investigatory Powers Act 2000 - <http://www.opsi.gov.uk/Acts/acts2000/20000023.htm>

Part 11 of the Anti-Terrorism, Crime and Security Act 2001 - <http://www.opsi.gov.uk/ACTS/acts2001/10024--l.htm>

UK Code of Practice for Voluntary Retention of Communications Data (2003) <http://security.homeoffice.gov.uk/news-publications/publication-search/general/5b1.pdf>

UKERNA statement to the All Party Internet Group's public inquiry into the retention of, and access to, communications data for law enforcement purposes (2002) - <http://www.apig.org.uk/archive/activities-2002/data-retention-inquiry/written-evidence-for-the-data-retention-inquiry/ukerna.pdf>

European Union (EU) Directive 2006/24/EC on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks - http://europa.eu.int/eur-lex/lex/LexUriServ/site/en/oj/2006/l_105/l_10520060413en00540063.pdf

Andrew Charlesworth

16 April 2007