dataprotectionlaw&policy

THE NEWSLETTER FOR DATA PROTECTION PROFESSIONALS
JULY 2006 VOLUME 03 ISSUE 07 **WWW.E-COMLAW.COM**

B4USearch to appeal ICO enforcement

B4U Business Media Limited lodged notice of an appeal on 28 July of the Information Commissioner's Office's (ICO) enforcement notice against it's website, over the use of personal information from electoral registers, published before 2002.

'B4USearch.com' offered a free 'people search' facility, which attracted almost 1,600 complaints to the ICO.

Prior to 2002, individuals had no choice over whether their personal details from the electoral register were sold on to other organisations.

People who complained to the ICO included a police officer whose family's names and addresses, along with a map to their house, appeared on the website.

Following an investigation, the ICO found that the personal information used by the website contravened the first principle of the Data Protection Act, and that the damage or distress to individuals was likely to have been caused by information being processed in this way.

An ICO spokesman confirmed that the latter could open the door to a civil action for damages against the website, but at this time, they were not aware of any case being brought.

IN THIS ISSUE

Enforcement The IC's B4U decision **04**
Data transfers The ICO guidance **05**
US Trade secrets v freedom of speech **08**
ENISA Promoting European networks **10**
Jurisdiction US over European nationals **12**
Data retention EU consistency **14**

UK Government consults on prison sentencing for illegal data traders

The UK government will seek the views of the public on whether prison sentences of up to two years should be introduced for those who profit from the illegal trade in personal data.

'The consultation document, 'Increasing penalties for deliberate and wilful misuse of personal data', launched on 21 July by the Department for Constitutional Affairs, explains that the government has been 'increasingly concerned' about the increase in trade in personal data, recently highlighted and presented to Parliament in the Information Commissioner's Report, 'What Price Privacy?'.

The government's proposals are to amend section 60 of the Data Protection Act to allow, on conviction under section 55, for up to six months imprisonment on summary conviction and/or a fine of up to £5,000; and up to two years imprisonment on indictment and/or an unlimited fine.

The consultation says 'Government wishes to facilitate greater data sharing within the public sector,' and believes it is necessary to increase the penalties available to the courts for three reasons; in order to provide a larger deterrence to those who engage in the illegal trade of personal data, to provide greater public reassurance that those who are successfully prosecuted may be jailed, and to achieve 'parity of approach' across a number of pieces of legislation which deal with similar types of offences.

However, a DCA press release, quoting the Secretary of State for Constitutional Affairs and Lord Chancellor, Lord Falconer, said "this does not mean that front-line public sector staff who, while sharing data for legitimate reasons, make an error of judgement in what are often complex cases, will be penalised as a result of this proposal."

The consultation closes on 30 October 2006, and the government will produce a report on the results shortly afterwards, according to a DCA spokesperson.

The spokesperson said that the DCA do not expect any significant problems in the proposals becoming law, but the timeframe depends on the findings of the consultation.

Meanwhile, new powers to allow banks and building societies to remove the credit cards of customers cautioned for, or convicted of, buying indecent images of children online, were agreed in Parliament on 18 July.

The Data Protection (Processing of sensitive personal data) Order 2006 amends the Data Protection Act, and allows card issuers to process sensitive personal data provided to them by law enforcement authorities so that they can withdraw the card used to commit the specified offences.

Brian Davidson

New York workers' negligence claims 'difficult' following data compromise

Up to 540,000 injured workers in New York state, whose personal data was compromised after computer hardware went missing, could find negligence action difficult unless they can prove that they have been 'harmed' by the incident.

The missing hardware has since been recovered. In a media statement, the Federal Bureau of Investigation said it had told independent insurance brokerage, CS Stars, that it is 'reasonably certain that the data was not compromised'.

"Workers could take legal action based on negligence," said Anita Boomstein, Counsel with Hughes Hubbard & Reed LLP.

"They would need to prove that parties had a duty to protect that data, and that they failed in that duty. However, for a negligence action to succeed, they would need to prove that they have been harmed by the incident."

CS Stars had stored New York state Workers' Compensation Board data, that it was moving to its computerised claims system, onto the computer that went missing.

Boomstein said that there have been a few negligence actions following data compromises, however all have been dismissed.

To date, 25 states have introduced data breach notification laws, which require companies and government organisations to notify customers when personal data may have been exposed to ID thieves.

Andy Brown

Data Retention Directive: ensuring consistency in the EU

The ITAA remains opposed to mandatory data retention as a concept, however in this article, it suggests practical guidelines for ensuring consistent standards across European Member States, following the passage of the Data Retention Directive. This article represents a consensus opinion from the members of the ITAA Global Public Policy Committee, as submitted by Committee raporteur, Chris Boam, director for international public policy & regulatory affairs, Verizon Communications.

The Information Technology Association of America (ITAA) provides global public policy, business networking, and national leadership to promote the continued rapid growth of the IT industry. The ITAA consists of over 400 corporate members throughout the U.S., and a global network of 60 countries' IT associations. Accordingly, the issue of data retention in Europe has, and continues to be, of critical importance to our growing global membership.

In past statements, the ITAA has urged governments to consider data preservation rather than the mandatory rules imposed by communications data retention. Data preservation allows for specific data to be 'frozen' until law enforcement can access it using a legal warrant. This preserved material can then often be augmented by traffic data that a provider had retained according to its business case. Data preservation is in fact the measure advocated in the Council of Europe Convention on Cybercrime, and we stand by advocacy of preservation as the most appropriate technical measure to meet the investigative needs of global law enforcement.

However, with passage of the Data Retention Directive (2006/24/EC), ITAA members recognize that it must suggest a way forward, irrespective of its objection to mandatory retention as a concept. National retention requirements that develop in the course of the Directive's transposition into national law will be collectively unworkable without consistency among European Member States. Further, this consistency must be based upon minimums – putting a ceiling on both types of data to retain, and the duration to retain them – applying the 'lowest common denominator' under the Directive's requirements. Without consistent requirements, setting minimized ceilings for the types of data to be retained and duration to retain it:

- Providers will be required to retain data according to varying national standards, with networks that are regional, not national;
- They will be tasked to retain data types and duration never contemplated for IP networks, storage media and search engines;
- Each will be required to do all of this without the promise of reimbursement for technical and manpower costs.

The result would increase both the cost of services in the EU and the likelihood that the goals of the Lisbon agenda will be affected. Thus, the ITAA advocates a consistent approach to national retention requirements that develop in Europe, recommending that authorities transpose the Directive according to the following five principles.

What data should be retained and who should retain it?

First, the obligation to retain "fixed telephony", "mobile telephony" and "Internet Access, Internet email and Internet telephony" data should only apply to the extent that such data is generated or processed by the given provider of the service.

Second, network providers – including providers of wholesale or transit (often referred to as "backbone") services - should not bear the obligation to retain data generated by the end-users served by Internet service providers (ISPs - the customers of those network access services). The obligation should rest with the owners of service networks and providers of service applications, not with network providers.

Under the above restrictions, Member States should harmonise data types and duration for retention according to the specific minimized ceilings provided under the Directive and detailed below.

Fixed Telephony and Mobile Telephony:

- The calling telephone number;
- The number(s) dialled (the called telephone number or numbers), and in cases involving supplementary services such as call forwarding or transfer, the number or numbers to which the call is routed;
- Name and address of the subscriber or registered user;
- The date and time of the start and end of the communication; and
- Mobile location data (Cell ID and geographic location by reference to their Cell ID).

Internet Access, Internet email and Internet telephony (VoIP) – Connection data: this data of dial-up and DSL IP service customers consists of:

- the source of a communication (IP address);
- duration of a communication;
- CLI (for the dial-up connection) or DSL user ID info.

Additional email and VoIP data: if provider of the service:

- The User ID or telephone number of the caller and intended recipient(s) of an Internet

telephony call;
- Name(s) and address(es) of the subscriber(s) or registered user(s) (of sender, recipient, or both if both are customers of the provider).

Providers of wholesale internet access or transit to ISPs should not be required to retain the data of users with whom they have no direct relationship. For instance, an ISP would be the party in direct relationship with an end-user of the internet services, their customer. The backbone provider would not be in a position to identify the specific users of internet services provided by its ISP customers.

Every IP-based communication is broken into packets, which are separately delivered over the network before being recombined at a designated end-point for the receipt of a communication. No one packet contains all of what the Directive might consider the "traffic" or "content" data of a given communication, and no single communication is complete without re-assemblage of all packets upon receipt. In turn, no single packet can be identified as "relevant" to an individual communication without trapping (retaining) and opening it.

Thus, unless a backbone provider is engaged in directly providing an email or other application service to the users of its customer's services, it would have no view of packetized email traffic data, as such, would be considered "content" at the network level. The same principle would be applicable in the context of VoIP, where the wholesale internet or transit provider is not the provider of the VoIP service itself. These distinctions make necessary the above two restrictions. Absent these restrictions, harmonisation of data types and duration, the cost for some providers of wholesale internet or transit services to store and search retained data has been estimated at greater than €2.1billion, whereas implementation of the above requirements could have an estimated cost for that same provider of between €450,000 and €750,000.

The ITAA has urged governments to consider data preservation rather than the mandatory rules

Further, the Directive calls for storage of the serial number of a mobile device (IMEI). It is doubtful that the collection of IMEIs will serve any investigative end. Manufacturers can assign such numbers multiple times, and they can easily be manipulated by users. Mobile terminals cannot be unambiguously identified by them. For this reason, the service provider does not use the IMEI to identify the mobile customer at log-in, but instead uses the international mobile subscriber identity (IMSI) number assigned by the mobile provider and stored on the customer's chip (SIM) card.

For what duration should data be retained?

"Fixed and Mobile Telephony" data: six months is likely sustainable by most providers in Europe, with one year likely pushing the limit of provider business cases.

"Internet Access, Internet email, and Internet Telephony (VoIP)" data (IP connection and the 'traffic' data of email and VoIP services provided): six months.

The restrictions on data retained, discussed above, must be addressed first in order to then set proportionate duration. The duration applicable to both sets of data would apply only to communications originating on the network of the provider of the service. For instance, in the case of email or VoIP traffic, such data could only be collected if a network access provider also directly provides the email or VoIP service, and thus (in the case of email service) controls the proxy server. The systems of network access providers cannot collect and store this sort of information for any duration, as the cost implications demonstrate. And further, for service providers, duration beyond the above would neither be sustainable nor proportionate to investigative ends.

What should service provider liability be for data retained?

National legislation should specify that providers acting in conformance with a valid request for access shall be granted a waiver from liability to a data subject for granting that access. Further, providers should not be liable for the costs attributable to securing data retained for purposes other than industry business cases.

Without such safeguards, a service provider burdened with a retention requirement beyond its business case would be held liable for the security for, and potential misuse of, data they have not decided themselves to retain. At issue under data protection law is the fundamental precept that data retained according to law enforcement requirements would deviate from the "purpose for which [the data] is collected" by the services provider. And further, when retention deviates from purposes for data collection due to an external (national) requirement, there is no precedent obligating service providers to bear cost, liability and human resource burdens applicable to securing data, used or misused by authorities for State purposes. Although the issue of potential liability is distinct, the costs from potential liability and data protection compliance obligations are directly related to the reasons for full reimbursement, addressed in point five below.

Access to retained data

Access to retained data must be restricted to law enforcement, under a clear process to achieve the requisite judicial authority for access, and for the sole purpose of investigating such 'serious crimes' as those which drove the development of retention legislation in the course of the past year.

The category of "serious crimes" for which retained data could be accessed by law enforcement should be a limited list, in order to ensure a proportionate impact on the privacy rights of individuals and the costs and liability to industry. The number of crimes for which retained data can be accessed will exponentially affect the burden on a service provider in servicing requests for access. A narrower focus of applicable "serious crimes", for which access is provided, will result in a decreased burden to providers, and in turn, decreased needs for reimbursement of costs.

Several existing national laws in Europe for mandatory retention have significant restrictions on the number of applicable "serious crimes" for access. For instance, the current UK voluntary retention program limits access to purposes of anti-terrorism investigation alone. National precedent exists for a narrow scope of applicable "serious crimes," which would also be consistent with the reasons for which the retention objective was launched.

Reimbursement and implementation period

Service providers must be fully reimbursed for the technical investment and human resource costs of both storing and facilitating the search and handover of data.

Cost reimbursement is a necessary component to any national retention legislation, to cover investment and operational (retention and search) costs beyond industry business cases, and to safeguard the privacy rights of individuals. Without full reimbursement, the costs of retention to industry will – without a doubt – drive up the cost of services. Ensuring internal security is a core State function, which must be financed with public budget funds. Therefore, government must also bear the costs of data protection requirements applicable to retention. Inadequate and non-uniform compensation within the EU would otherwise distort competition, endanger long-term competition structures and prevent the furtherance of a uniform internal market.

Further, Article 15 recognizes that a phased-in approach for purposes of IP-related retention – the most technically and economically difficult of retention requirements - will be critical to the success of any measure.

Finally, Articles 10 and 14 include a provision for national discussion and review of technical abilities, the collection of statistics on implementation and costs, and a review of the need for, and impact of, the retention legislation itself. Such analyses will be necessary:

- to gauge the need for continued retention, by analyzing the numbers of, duration for, and investigative utility of retention requests;
- to affirm that reimbursement measures are truly tracking actual costs;
- to ensure that data definitions reflect the global state of communications networks and services, and are flexible enough to assimilate next generation services; and
- to assess whether the need for mandatory retention obligations is indeed proportionate to its impacts on privacy and the economics of the industry sector.

However, industry should not be tasked to provide statistics on the data required by law enforcement. Tasks like this should be performed by the competent authorities themselves, or perhaps by a third party. For instance, only law enforcement can demonstrate in which cases the information gathered from retention or preservation actually leads to successful investigation, an insight that is necessary to assess the true effectiveness of any new investigative measure and the evidence retrieved. This will be critical to assessing whether the need for mandatory retention obligations is indeed proportionate to its impacts on privacy and the economics of the industry sector.

Chris Boam Global Public Policy Committee Raporteur
Director for International Public Policy & Regulatory Affairs
Verizon Communications
chris.boam@verizon.com