Personal Data

Security breach notification in the European Union: First step taken, more to come

By Kristof Van Quathem, Data Protection Advisor, Covington & Burling LLP.

On 18 December 2009, the *Official Journal of the European Union* published Directive 2009/136/EC with amendments to the *ePrivacy Directive* (2002/58/EC).[1] Among other things, the amendments introduce a security breach notification obligation, the subject of this contribution. EU member states must "transpose" the obligation into their national laws by 25 May 2011.

As explained in previous contributions, the new breach notification obligation has been the subject of much controversy.[2] For the purpose of this contribution, however, we will only describe the final rules and take a look at what we can expect in the months and years ahead.

Who is subject to the current breach notification obligation?

The current rules only apply to providers of "public electronic communications services." This term is defined in Directive 2002/21/EC and essentially covers core communications services (consisting entirely or mainly in the conveyance of signals) such as terrestrial and mobile telephony and internet access services. The rules explicitly do not cover content services and "information society services," which are governed by other rules, such as the *Electronic Commerce Directive*.

The line between electronic communications services (ECSs) and information society services is not always easy to draw, and member states sometimes adopt diverging positions for particular applications. In particular for applications with a clear communication purpose, such as Voice over IP (VoIP) and "internet email" (eg Hotmail and Gmail), it may be difficult to determine the correct legal regime. As a general principle, however, services that rely on the existence of an ECS and do not convey signals themselves should not be considered an ECS. For example, the Hotmail and Gmail services can only be used if users have access to the internet. The respective internet service providers (ISPs) convey the signals between the users and Microsoft or Google and are ECSs. Microsoft and Google, however, who only provide software and server space where users can store their emails, are not ESCs.[3]

Kristof Van Quathem *is a Data Protection Advisor at Covington & Burling LLP. He can be contacted at: kvanquathem@cov.com*

For VoIP, matters are more complicated because of the obvious similarity with traditional telephony. Yet here as well, certain VoIP applications are often not considered ECSs. For example, certain VoIP services are not very different from internet email. The VoIP providers may only offer software, allowing users to communicate by computer without conveying any signals, unlike the users' ISPs. Other VoIP applications, however, allow for connection with traditional telephone lines (the PSTN) and are more likely to be considered ECSs.[4]

Irrespective of these nuances, it is clear that the current breach notification regime only applies to one particular sector of electronic communications and that all other sectors of the economy (eg banks, insurances and hospitals) escape, even though they process much more sensitive data.

What is a breach?

The new rules contain a definition of a "personal data breach" (Article 2h):

> "a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure, of or access to, personal data transmitted, stored, or otherwise processed in connection with the provision of a publicly available electronic communications service in the Community."

This definition is very broad as it covers breaches of any "personal data." The concept of personal data is defined in the *Framework Data Protection Directive* (95/46/EC) and is often interpreted broadly.[5] A simple IP address associated with relevant traffic data is sufficient to be covered by the breach notification obligation.[6] The definition of "personal data breach" would be less problematic if the notification obligation was limited by a standard of harm. However, as we will demonstrate below, this is not the case. Any breach of any personal data processed in connection with the provision of a publicly available electronic communications service will need to be notified to the competent authority.

Who should be notified?

All "personal data breaches" must be notified to the competent national authority. In some member states this will be the data protection authority, while in others it will be the telecommunications regulator. In case a breach is "likely to adversely affect the personal data or privacy of a subscriber or individual," the service provider must also, without undue delay, notify the subscriber or individual. In this case, the service provider must inform the affected individuals under its own ini-

tiative and should not wait for an instruction to do so from the competent authority (Article 4, 3).

This notification regime is probably one of the most problematic areas of the breach notification obligation. It demonstrates an inherent lack of trust in the private sector and its ability to analyse breaches and apply a harm-based standard by itself. Instead, all breaches, irrespective of their possible harm, will have to be reported to the competent authority. The competent authority will then analyse the case and tell the operator whether a user notice is required, if such notice has not already been given.[7]

The standard of harm

The standard of harm (breaches that are "likely to adversely affect the personal data or privacy of a subscriber or individual") is quite broad and vague. Recital 61 of the Directive offers some guidance as to the types of breaches that are expected to adversely affect individuals, namely breaches resulting in identity theft or fraud, physical harm, significant humiliation, or damage to reputation. It goes without saying that a consistent application of this standard by 27 different authorities across the EU is very unlikely. Inevitably, assessments will have to be made on a case-by-case basis, and it will take time before the competent authorities across the EU will have gained sufficient experience to reach consensus on what types of breaches are or are not likely to adversely affect individuals. Unfortunately, the Directive does not seem to foresee a mechanism by which competent authorities can share experiences and practices in view of a harmonised application of the harm standard.[8]

Appropriate technical protection measures

Notice to subscribers and individuals is not required if the service provider can demonstrate that the affected personal data was protected by "appropriate technological protection measures" that render the data unintelligible to any person without authorisation to access it (Article 4, 3). This provision is intended to encourage service providers to invest in technological protection measures to protect the data they convey in the provision of their services.[9]

Notifying other affected individuals

One area that raises concern is that notice may have to be provided not only to subscribers but also to other affected individuals. It is difficult to see how this would work in practice. Service providers generally only have contact (information) with their subscribers, not with other individuals that may be involved in a communication. For example, if a service provider conveys hospital records and erroneously discloses the records to an unauthorised recipient, surely one would not expect the service provider to inform the affected patients, who may not have any relationship with the service provider whatsoever. This is probably not how the Directive should be read. The intention is apparently to cover users of ECSs that are not "subscribers" but with whom the service provider does have contact, and thus can easily be contacted in case of a breach.[10]

What must be notified?

Notifications to subscribers must:

- describe the nature of the breach;
- offer contact points for more information; and
- recommend measures to mitigate possible adverse effects of the breach.

The notification to competent authorities must, in addition, describe the consequences of the breach and the measures taken by the service provider (Article 4, 3). In addition, the Directive provides that the authorities may issue their own guidance and instructions on the different aspects of breach notifications, such as their circumstances, format and manner (Article 4, 4).

Other obligations

Service providers must keep an inventory of all breaches (Article 4, 4). The inventory must list:

- the facts surrounding the breach;
- the effect of the breach;
- the remedial action taken; and
- any other relevant information demonstrating compliance with the breach notification obligation.

The inventory must be held available for the competent authorities so they can verify compliance, must be specifically made for this purpose and must not contain other data that is unrelated to breaches.

Expected developments

As explained above, member states are expected to transpose the Directive into national law by 25 May 2011. In the meantime, however, a number of additional initiatives are in the pipeline.

Implementing measures

First, the Directive provides that the European Commission may adopt technical implementing measures concerning the circumstances, format and procedures applicable to the breach notification requirements (Article 4, 5). In doing so, however, the Commission must consult with the European Network and Information Security Agency (ENISA), the European Data Protection Supervisor (EDPS) and the Article 29 Working Party. In addition, the Commission must consult all stakeholders to be "informed about the best available technical and economic means of implementation." Interestingly, the Commission does not have to consult telecommunications authorities, even though in some countries these authorities (instead of the data protection authority) may be responsible for enforcing the notification obligations.

The measures adopted by the Commission will be binding on the member states and will supersede any guidance developed by national competent authorities. In this respect, the Commission's measures will be a very important, and indeed essential, tool to guarantee an ef-

  WDPR ISSN 1473-3579

fective level of harmonisation across the EU. Failing that, the Directive is bound to be implemented in very divergent (if not conflicting) ways, which would have a significant impact on compliance, in particular for companies active on a pan-European scale.

The development of these technical measures should be the first priority of the Commission as these measures should be available before the member states start implementing their breach notification law.[11] First, the implementing measures may be essential for an efficient transposition of the breach rules in national law, particularly for harmonisation purposes. Second, once member states adopted their laws, they will be less inclined to approve Commission measures *a posteriori* that depart from their new national rules, which will result in less harmonisation.

Horizontal breach notification obligation

As indicated above, the current breach notification rules only apply to one sector. This is quite controversial as it indeed makes little sense to only subject the telecommunications sector to such a requirement. However, during the legislative process the European Parliament agreed to the limited scope of the obligation in exchange for a commitment of the Commission to investigate the implementation of a horizontal breach notification requirement covering all sectors of the economy. Recital 59 of the Directive clearly reflects this and calls for the introduction of a mandatory notification requirement applicable to all sectors as a matter of priority.

The most obvious way for introducing such a horizontal requirement would be through an amendment to the *Framework Data Protection Directive*. The Commission recently launched a consultation on the Directive and is widely expected to propose amendments in the coming years (probably 2011). However, it remains to be seen what a horizontal breach notification obligation would look like. A mere copy of the existing rules for electronic communications services does not seem very appropriate. In particular, the mandatory notification of all breaches to competent authorities, irrespective of possible harm, would turn into an absolute nightmare both for the authorities and the data controllers (private and public). But then again, if banks and hospitals are not required to notify all breaches, why should providers of electronic communications services be required to do so?

Moreover, recent evidence shows that the utility of breach notification may actually be quite low, or even not non-existent. A recent economic study conducted by Carnegie Mellon University demonstrates that (horizontal) breach notification in the US would only have a marginal effect on the reduction of cybercrime (1.8%).[12] That is in a country where cybercrime, and identity theft in particular, is much more prevalent than in the EU, so presumably the figures for the EU would be even lower. However, breach notification is about more than just fighting cybercrime. It is also a reflection of an individual's right to know what is happening with his personal data. And it can serve a policy tool to boost investments in security technology. Then again, whether breach notification is the most efficient way to boost investment is also subject to debate.[13]

National initiatives

While these EU initiatives are unfolding, some member states have jumped the gun and have either implemented their own breach notification rules or plan to do so. One notable example is Germany. In Summer 2009, the German Parliament adopted an amendment to the *Federal Data Protection Law* and to the *Telecommunications Law*, inserting a breach notification requirement applicable to all sectors of the economy (*Bundesdatenschutzgesetz*, section 42a; *Telemediengesetz*, section 15a). The obligation only applies for specific types of personal data (including traffic data held by electronic communications providers). Notification to the responsible authority and affected individuals is only required if the breach can have an important impact on the rights and legitimate interests of the affected individual. These new German rules, as applied to ECSs, are clearly not in line with the new Directive (which require notification of all breaches irrespective of harm) and will thus have to be amended.

In France, two Senators proposed a revision of the data protection law including the introduction of a breach notification obligation.[14] The obligation would apply to all data controllers and would thus be much broader than the one contained in the current Directive. In case of a breach, irrespective of any harm, data controllers would have to inform the data protection authority which, depending on the nature of the breach, could order the data controller to notify affected data subjects.

It goes without saying that, while well intended, such initiatives are not necessarily conducive to an efficient and harmonised regulatory regime across the EU. They preempt European initiatives and tend to complicate the work of the EU because the relevant member states are often reluctant to accept EU rules that would force them to change recent national rules. One can only hope that national legislators will show some restraint and give the EU the necessary time to develop a complete framework of rules on breach notification. The goal should be a framework that allows member states to implement a harmonised and efficient regime across the EU that does not raise unnecessary obstacles for businesses and offers individuals an equal, recognisable and equitable level of protection wherever they reside in the EU.

NOTES

[1] *Official Journal of the European Union*, L 337, 18.12.2009, pp. 11-36.

[2] See: BNA International, *World Data Protection Report*, October 2006, Vol. 6, Nr. 6 & April 2008, Vol. 8, Nr. 4 & 11.

[3] A recent paper on data retention confirmed that these services are not ECSs. See: Experts group "The platform for electronic data retention for the investigation, detection and prosecution of serious crime" established by Commission Decision 2008/324/EC – Series A (technical guidance papers) paper #2: the obligation to retain e-mail logs – when must records of spam e-mails be retained? Final version 8 June 2009.

[4] See study for the European Commission by Dieter Elixmann, J. Scott Marcus, and Dr. Christian Wernick, *The Regulation of Voice over IP* (VoIP) in Europe, March 19, 2008, available at: http://ec.europa.eu/information_society/policy/ecomm/doc/library/ext_studies/voip_f_f_master_19mar08_fin_vers.pdf.

[5] See, for example, the opinion of the Article 29 Working Party on the interpretation of the concept of personal data (Opinion 4/2007 of 20 June 2007, http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2007/wp136_en.pdf).

[6] See, for example, Article 29 Working Party opinion 1/2009 of 10 February 2009 (http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2009/wp159_en.pdf).

[7] The European Data Protection Supervisor also highlighted this concern and the risk that competent authorities are ill equipped to deal with all notifications, irrespective of any harm (see: EDPS, Second opinion of 9 January 2009 on the review of Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector, OJ C 128, 06.06.2009, sections 47-48). Similarly, the Article 29 Working Party called for a system in which breaches are notified only after a harm analysis by the service provider (see: Article 29 Working Party opinion 1/2009 of 10 February 2009).

[8] The Article 29 Working Party may not be the appropriate vehicle, because not all member states will appoint the data protection authority as the competent authority for security breaches. In some member states, the telecommunications authority may be the competent authority, and they are not represented in the Article 29 Working Party.

[9] Encryption is often referred to as an example of such a technological measure. However, in a context of electronic communications this may not always be the most appropriate solution as encryption is often applied at the source by the user, not by the entity that conveys the signals. This entity may have to turn to other technologies to make the data unintelligible.

[10] EDPS opinion of 9 January 2009, section 58.

[11] See EDPS event "Responding to Data Breaches" of 23 October 2009 in this respect: http://www.edps.europa.eu/EDPSWEB/edps/site/mySite/Events.

[12] See presentation by Alessandro Acquisti and Sasha Romanoski at EDPS event "Responding to Data Breaches" (http://www.edps.europa.eu/EDPSWEB/edps/site/mySite/Events).

[13] The Ponemon Institute estimates that an average breach in the US costs about $6.6 million; 69% of which would be attributable to loss in business (Ponemon Institute, 2008 Annual Study: Cost of a Data Breach, February 2009).

[14] See: Proposition de Loi visant à mieux garantir le droit à la vie privée à l'heure du numérique, présentée par M. Yves Détraigne et Mme Anne-Marie Escoffier (http://www.senat.fr/leg/ppl09-093.html).

The Information Commissioner's Office consults on online personal data

Oliver Bray, Partner, IP & Technology Group and Ben Hubbard, Trainee Solicitor, Reynolds Porter Chamberlain LLP.

On 9 December 2009, the Information Commissioner's Office launched a consultation process with the aim of finalising a new Personal Information Online Code of Practice. The purpose of the Code will be to set out clear and comprehensive recommendations for the proper handling of personal data and for giving individuals the correct degree of choice and control over that data. The Consultation seeks to capture best practice for all organisations involved in collecting and using personal data online.

Background

The consultation was announced at the ICO's *Personal information online conference 2009* in Manchester. The consultation was felt necessary due to the relative lack of specific ICO guidance in the face of the rapid pace of change in the use of personal information online and the requests for advice and legal uncertainty that this has generated. The consultation and new Code form part of the ICO Data Protection Strategy for 2009/10 which is set to tackle the problems caused by the black market in confidential personal information and promote the inclusion of issues of privacy into operational systems as an integrated feature through the *Privacy by Design* initiative (in essence, the idea that it is better to integrate data protection into new systems and technologies from their outset than bolt on a work-around at a later date). The Code will be the first attempt to address online privacy issues directly.

Oliver Bray *is Partner, IP & Technology Group at Reynolds Porter Chamberlain LLP. He is head of the branding and advertising team and has extensive commercial experience, coupled with expertise in advertising and marketing law, intellectual property and technology matters. He can be contacted at: Oliver.Bray@rpc.co.uk.* **Ben Hubbard** *is a Trainee Solicitor at Reynolds Porter Chamberlain LLP and can be contacted at: Ben.Hubbard@rpc.co.uk.*

Personal data

The new draft Code will apply to all "personal data". Part 6 of the draft Code highlights the concept that identification of behavioural characteristics can constitute personal data without the need for an obvious identifier such as a name or address to be attached. This includes browsing history tracked through cookies.

The draft Code attempts to cover the position where data gathered is linked to the device used as opposed to the person using it. Obviously, where a home computer is being used to access the internet, there may well be more than one person using it, causing problems in determining who is accessing which site at any one time and thus to whom the information relates and whether such information is personal data. The guidance in the draft Code is that all such information gathered should be treated as personal data, kept secure and protected from inappropriate disclosure. This also has implications in respect of the right of subject access which is covered at Part 11 of the draft Code. Here, the guidance is that, where an organisation cannot establish a reliable link between the applicant and the information (via a registered account for example), the Information Commissioner would not seek to enforce the right of subject access.

Whilst the concept of identification is key, the section of Part 6 on information gathered through cookies is rather vague. The phrasing used is:

  WDPR ISSN 1473-3579