Security breach notification in Europe

Kristof Van Quathem, Data Protection Advisor, Covington & Burling LLP (Brussels), examines the status of the European Parliament's position on security breach notification

Following months of debate, on 6th May 2009 the European Parliament ('the Parliament') adopted a new position on security breach notification. Although the complexities of the EU decision-making process delayed the final adoption of the breach notification provisions, hopes are high that the Parliament's text constitutes the final legislative text. This article discusses the status of the current text, and its expected short-term consequences. We also take a close look at the main features of the anticipated breach notification obligation, in particular its scope, the procedure for submitting notifications, and the level of harmonization that can be expected across EU Member States.

Status and expected future developments

The recent position taken by the Parliament constitutes the second phase of the process launched by the European Commission ('the Commission') in November 2007. As part of its comprehensive revision of the regulatory framework for telecommunications services ('the telco package'), the Commission also proposed to amend the ePrivacy Directive (2002/58/EC). One of the most important amendments under debate was the introduction of mandatory security breach notification for providers of public electronic communications services.

The Parliament and the EU Member States, assembled in the Council, substantially amended the Commission's breach proposal during the "first reading" round of negotiations. In formal terms, the most recent text is the result of the Parliament's "second reading" deliberations. However, the recent text is more significant in practical terms. In order to speed up the process and avoid a "third reading" of the legislative text, the Parliament, the Council, and the Commission held intensive informal negotiations during the second reading stage. Therefore, the Parliament's current text on security breach notification represents the consensus text of the three institutions, which would normally be adopted without further change.

For reasons unrelated to breach notification, a third reading between the Council and the Parliament will be inevitable. However, in principle this should not affect the current consensus on the breach notification provisions, unless these provisions enter into the mix of unrelated outstanding disagreements and fall victim to last-minute political horse trading. Otherwise, the breach notification provisions should be adopted in their current form by the end of 2009.

The informal discussions between the three institutions have led to one further important development that will significantly affect European businesses in the coming years. In order to reach consensus, the Commission was forced to commit to investigating the possibility of a horizontal security breach notification obligation; one that applies to all industry sectors, not only the telecommunications sector. At this point, it is unclear how the Commission proposes to achieve this. The most obvious avenue is via amendment of the Data Protection Directive (95/46/EC). However, in light of the general reluctance to review the Data Protection Directive, alternative mechanisms, such as a stand-alone Directive (or even Regulation) on breach notification, are apparently under consideration. The coming months will hopefully shed more light on the Commission's plans.

Security breach notification

The anticipated security breach notification obligation adopted by the Parliament will be inserted into Article 4 of the current ePrivacy Directive. A new paragraph 3 is expected to read as follows:

"In the case of a personal data breach, the provider of publicly available electronic communications services shall, without undue delay, notify the personal data

(Continued on page 4)

(Continued from page 3)
breach to the competent national authority."

"When a personal data breach is likely to adversely affect the personal data or privacy of a subscriber or individual, the provider shall also notify the subscriber or individual of the breach without undue delay."

Who should notify?

In terms of responsible entities, the security breach notification obligation applies only to providers of publicly available "electronic communications services." This term is defined by the Electronic Communications Directive (2002/21/EC) as:

"a service normally provided for remuneration which consists wholly or mainly in the conveyance of signals in electronic communications networks, including telecommunications services and transmission services in networks used for broadcasting, but exclude services providing, or exercising editorial control over, content transmitted using electronic communications networks and services..."

While the rapid development of new communications technologies makes the scope of this term difficult to determine, it is basically intended to cover telecommunications services (fixed and mobile) and internet access services.

The narrow application of the breach notification obligation to a specific type of service provider is fundamentally different from US security breach requirements, and has been the subject of much debate in the EU. In particular, the Parliament and the EU Data Protection Supervisor Peter Hustinx have challenged the narrow scope of the obligation, arguing that it simply does not make sense to exclude other services, such as "information society services" (defined in Directive 98/48/EC as mainly covering e-commerce activities, which would include online retail and other online activities such as e-banking). Such services are already covered by some provisions of the ePrivacy Directive, and often involve the processing of more sensitive customer information. However, the Commission and the Council appear to have successfully resisted the application of the security breach notification obligation to this type of service provider.

"The definition of personal data breach represents probably one of the biggest flaws of the anticipated breach notification obligation [and] as a result, providers of electronic communications services will be subject to a notification obligation as a result of any security breach that affects any type of personal data, however harmless the effects of the breach may be."

While the Parliament's arguments undoubtedly have merit, the Commission and Council's resistance probably has greater merit. The application of the security breach notification obligation to all "information society services" would have been a dramatic departure from the Commission's publicly-stated intentions. Moreover, the Parliament's suggestion is haphazard; it does not appear logical to subject information society services to a security breach notification requirement and exclude other sectors of the economy and society from such requirements (e.g. hospitals, insurance companies, and banks). It is likely that the Parliament has obtained a better deal by accepting the current narrow application and securing the Commission's commitment to investigate a horizontal breach notification obligation in the future.

What should be notified?

The anticipated breach notification obligation would apply to 'personal data breaches,' which are defined as:

"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 represents probably one of the biggest flaws of the anticipated breach notification obligation. Even though the term 'personal data' is interpreted broadly under EU law, the breach notification obligation is not restricted to breaches involving specific types of personal data (e.g. 'sensitive personal data' and financial data). As a result, providers of electronic communications services will be subject to a notification obligation as a result of any security breach that affects any type of personal data, however harmless the effects of the breach may be.

The value of such a measure is questionable. It appears to be motivated by an inherent distrust in the ability of service providers to independently assess the impact of personal data breaches. An alternative solution could have required service providers to only notify serious breaches to competent authorities, and keep an inventory of all data breaches, whatever their impact, for purposes of regulatory scrutiny. In fact, the new paragraph 4 of Article 4 provides that service providers should keep such records, which should describe personal data breaches and corresponding remedial steps. These records should be sufficient for relevant authorities to verify operators' compliance with the breach notification obligation. It is difficult to understand why less serious security breaches need to be notified to regulators if

they can be verified ex post by consulting such inventories.

The only limitation on the scope of the mandatory breach reporting requirement can be found in the third section of the new paragraph 3. If a personal data breach is likely to adversely affect an individual, the individual must not be notified if the data were sufficiently protected such that the data are unintelligible. However, security breaches affecting encrypted personal data must still be notified to the relevant competent authority.

Who should be notified?

According to the new paragraph 3, providers of electronic communications services who experience a personal data breach must inform the competent national authority, and without undue delay. Member States may individually designate the competent authority with responsibility for such cases. In some countries, this will be the Data Protection Authority ('DPAs'), while in others it may be the telecommunications regulator or a similar body.

According to the new paragraph 4, competent authorities must have the right to audit service providers' compliance with the breach notification obligation and have the power to impose sanctions in case of non-compliance.

Only where a personal data breach "is likely to adversely affect the personal data or privacy of a subscriber or individual" must the provider of the electronic communications service also inform the subscriber or individual concerned, and without undue delay (unless, as indicated above, the personal data is sufficiently protected).

The notification to the competent authority and subscriber/individual must describe the nature of the breach, offer a contact point for more information, and indicate what measures will be taken to mitigate any possible adverse effects. The notification to the competent authority must also describe the consequences of the breach and the measures taken, or to be taken, to address the breach. Following notification, the competent authority can order service providers to notify subscribers/individuals where the service provider would ordinarily not have done so (for example, because it assessed the breach to be low risk).

In practice, the procedure set out above will unfold in several stages. First, when faced with a personal data breach, a service provider should assess the circumstances of the breach, including whether the data were protected or not, and the possible adverse impact on subscribers/individuals. Second, the service provider will need to inform the competent authority and, if necessary, the subscriber/individual. However, the notification to the competent authority may still trigger a requirement to notify the subscriber/individual, regardless of the service provider's own risk assessment. This process must be implemented without undue delay.

The procedure raises a number of questions and concerns. It is unclear how DPAs, who already suffer from lack of administrative resources, will handle the notifications they receive, which are likely to be high in number given that the notification obligation applies to any type of breach. It is also unclear whether DPAs possess the necessary technical expertise to evaluate the notifications they receive, and apply appropriate redress measures. From the service provider's perspective, it is unclear when a breach creates adverse effects for individuals or what is meant by "undue delay." Furthermore, there is no guidance on the level of detail than needs to be provided in the notification. Some of these issues are likely to be covered in implementing rules and guidelines (discussed below).

Future harmonization

When the Commission first launched its proposal for a breach notification obligation, one of its principal objectives was to ensure a sufficiently harmonized regime across the EU. The US approach, which is characterized by a patchwork of state-level rules imposing different requirements for different types of breach, was not considered a good model. In order to achieve its objective, the Commission proposed a very general breach notification provision combined with a "comitology procedure" for the adoption of detailed secondary implementing measures, designed to guarantee a high level of harmonization.

Unfortunately, this approach was not to the taste of the Members of the European Parliament, presumably because the Parliament's competence in comitology procedures is limited. As a result, the Parliament poured extensive detail into the draft proposals and at one stage even considered removing secondary measures entirely. Fortunately, the Commission stood firm and managed to retain the ability to adopt secondary implementing measures.

The new paragraph 4 provides that the competent authority (being DPAs or other) may issue guidelines and instructions on the circumstances in which notification is required, the format of such notifications, and the manner in which they can be made.

The need for this provision is not entirely clear. Surely competent authorities do not need to be told that they may issue guidance or instructions? Service providers can only hope that authorities will see the need to cooperate with each other in developing these guidelines and instructions in order to achieve a high level of harmonization — something the draft Directive unfortunately does not guarantee or even suggest. Past approaches of DPAs have been very disappointing in this respect: the lack of harmonization, for example, surrounding the conditions for, and form of, notification imposed by the Data Protection Directive is indicative of the possible chaos ahead. Moreover, the fact that the authority designated to handle breach notifications may be different in each country, appears to work against a harmonized regulatory structure.

All is not lost however; the new paragraph 5 contains a comitology procedure allowing the Commission to adopt mandatory technical implementing measures "to ensure consistency in implementation of the measures referred to in paragraph 2, 3 and 4." These measures may cover the circumstances, format, and procedures applicable to the notification requirement. The Commission thus preserved the possibility of adopting more detailed rules to achieve harmonization.

(Continued on page 6)

(Continued from page 5)
This competence could be used by the Commission to resolve many of the issues raised above, such as the trigger for notification to subscribers/ individuals, the content of notification forms, the precise notification procedure and timeframes, and the identification of the competent authority where breaches involve more than one jurisdiction.

In implementing these secondary measures, the Commission will need to consult three bodies: the European Network and Information Security Agency, the Article 29 Working Party, and the European Data Protection Supervisor. In addition, the Commission will have to involve all relevant stakeholders "to be informed of the best available technical and economic means of implementation."

Conclusion and prospects

The current legislative text marks a significant improvement over previous versions. Nevertheless, if adopted in its current form, the breach notification obligation will have an important impact on providers of electronic communications services.

While it is clear that the obligation to notify any breach of any personal data to the relevant competent authority will present a heavy burden, the value of such a wide obligation is unclear. Moreover, this does not appear to be a model that can be applied to a breach notification requirement affecting all industries. While regulatory authorities might be able to develop the competence to handle breaches committed by electronic communications service providers, they simply are not equipped to deal with personal data breaches committed by data controllers from every sector of industry.

In July 2009, the German Parliament adopted its own horizontal breach notification rules. Unlike the rules for electronic communications service providers, this notification requirement is limited to breaches that:

1. concern sensitive personal data, judicial data, data subject to professional secrecy rules or banking and credit card data; and
2. carry the risk of "seriously harming" the rights and legitimate interests of the individual.

Such breaches generate a notification obligation to the affected individual and the competent authority.

The German approach seems a more effective and appropriate approach to mandatory breach notification. It also raises the question as to whether breaches of communications data are worthy of greater scrutiny than breaches that occur in other contexts. In other words, why must a competent authority be informed about the inadvertent disclosure of an IP address by a provider of an electronic communications service, but not of the inadvertent disclosure of name and address details by a retailer or an insurance company (assuming the context does not qualify the data as sensitive)?

The European Data Protection Supervisor was opposed to limiting the security breach notification requirement in the electronic communications services sector to sensitive personal data. He considered the limitation too narrow, and insufficient to cover all cases where an individual could be adversely affected (financial data, for example, is not covered by the Data Protection Directive's definition of sensitive data). It will be interesting to see if this broad notification trigger (i.e. breach of any personal data that is "likely to adversely affect") will be applied in the context of a horizontal breach notification rule, or if the German approach, which limits the breach notification obligation to particular sensitive types of data, will prevail.

It will be interesting to see if and how mandatory breach notification rules are extended to other sectors in the coming months and years.

For a link to the draft Directive, send an email to docs@pdpjournals.com

Kristof Van Quathem
Covington & Burling LLP
kvanquathem@cov.com