NDS

World Vision
ISSUE 46 November 2008

[Commentary] Mandatory Data Breach Notices: Get Ready for the Latest from Brussels

By Gerry Oberst

Gerry Oberst is a partner in the Brussels office of leading law firm Hogan & Hartson. During his 17 years in Brussels he has participated in numerous CEPT and European Commission activities related to radio spectrum and regulation of electronic communications. The views in this article are his own and not based on client or law firm positions.

With the proliferation of massive databases and e-commerce comes the growing possibility of data theft. The regulatory requirement to report data breaches is already mandated in most states in the US. Similar obligations are now under consideration in Europe as well, and the scope is set to embrace private as well as public networks. The organisations subject to these new requirements can include ISPs and other communications service providers.

If the European Parliament gets its way and the European Union adopts changes to the electronic communications regulatory framework, European telecom network operators and service providers could face new, more serious obligations regarding data security. New requirements may be imposed as early as the end of this year since the proposed changes are currently making their way through the legislative process in Brussels. In particular, both public and private service providers may have to notify either their national regulators, or consumers, of any breach of security that threatens the protection of personal data. This can include addresses, credit card details and other information relating to, for example, pay-TV subscribers. In short, the new rules apply to any information that can be deemed to be “personally identifiable.”

While this type of data breach notice would be new to Europe, it is already a requirement across the United States. California enacted a data breach law as early as 2002. By the second half of 2008, 44 states plus Washington, DC, and Puerto Rico had laws on the books to require such notices.

Actual data security breach notices in the US have increased dramatically over the last few years. Between 2007 and the first half of 2008 they were up by 70 percent. By June 2008, some 336 incidents had already been reported for the year.

With the increase in e-commerce and the growth in large databases, European industries can expect similar numbers of reported breaches if the new rules are adopted by Brussels. Up until now, European regulations required service providers to take appropriate measures to safeguard security. But providers only had to notify customers of security breaches if there were actual security risks.

Consider the following examples:

- Subscriber information is stolen from an Internet Service Provider. This could result in unauthorised access to email, online transactions, even illicit

use of credit card details.
- A medical centre's database is compromised, possibly resulting in breaches in confidentiality pertaining to thousands of patients.

The fact is virtually any information on any electronic system – including search engines and banks – can be compromised.

As a result, dealing with mandatory data breach notices would require the creation of new procedures and lead to new costs for any company involved with communications services. Proposals are afoot to extend the data security notification both public and private networks which could, as a result, pull in hospitals, universities and other large systems, as well as any company providing services over the Internet.

1.1.1 European proposals for "ePrivacy"

The European proposals first came to light in mid-November last year when the European Commission proposed updates to the regulatory framework. Among the updates was an entirely new chapter to the Framework Directive* on communications security and integrity. This chapter would require providers of public networks or services to notify their national regulator of any breach of security with a significant impact on operations. National regulators, in turn, could issue binding orders to require operators to comply with security obligations.

A similar obligation was proposed for the Electronic Communications Privacy Directive, also known as the "ePrivacy Directive**." These changes would require both public and private service providers to notify both subscribers and national regulators of any breach of security that threatens personal data.

The new framework would give the European Commission the authority to establish formats and procedures for notification requirements. This could be a good development as long as some definite and harmonised approach is adopted, instead of a piecemeal assortment of national procedures.

The big debate now concerns how far the rules must go and how many companies will be swept into the new procedures. These Commission proposals must be adopted by the European Parliament and Council in order to become law.

In its first reading in late September, the Parliament agreed with the basic thrust of the Commission's proposals, but with some twists and changes. The Parliament developed mainly editorial changes to the Commission's proposals for the Framework Directive. However, for the ePrivacy Directive the Parliament proposed changes that could greatly expand its scope in several important respects.

1.1.2 Parliamentary proposals

First, the Parliament wants to extend mandatory data breach notices far beyond providers of public networks and services. Where the Commission would apply the rules to public networks and services, the Parliament would bluntly add the words "and private." It also would apply the rules on data breach notices to "any undertaking operating on the Internet and providing services to consumers, which is the data controller and the provider of information society services."

By way of explanation, a Parliament committee pointed to the increasing mix of public and private services. It also said the amendment followed recommendations from the European advisory body on data privacy known as the Article 29 Working Party, and from the European Data Protection Supervisor.

In April 2008 the Data Protection Supervisor justified such an approach by claiming that the overall rules should apply to all "private networks such as those of

employers providing employees with Internet access, hotels or apartment owners providing guests with telephone and e-mail as well as Internet cafes…"

Focusing on mandatory data breach notices, the Data Protection Supervisor wrote that they should apply to "online banks, online businesses, [and] online providers of health services, etc." Neither the supervisor nor the Parliament expressed any views on the cost or impact of this sweeping application.

A second Parliamentary change would draw back the notification requirement, at least a bit. The Parliament proposes that companies experiencing the data breach first must notify their national regulator. That regulator would in turn consider whether a company must give notice to its subscribers based on the seriousness of the problem and whether the company took appropriate security measures.

Nonetheless, under the amendments, companies would be required to notify their affected users of all breaches of security for public communications services once a year. It appears that the Parliament did not extend this annual requirement to Internet service providers.

A third change is subtle, but hugely important. The original Commission version would establish a new right for interested parties to take legal action against infringements of the ePrivacy Directive, but only under the provision on unsolicited communications, i.e., spam. The Parliament would extend this new cause of action to any infringement of the ePrivacy Directive.

If the Parliament's version goes through, consumers could conceivably sue for infringements of the network integrity requirement or mishandling of data breach notifications.

Under European Union procedures, the ball is now in the court of the Council of Ministers which will seek its own set of amendments in a meeting scheduled for November. Given the enormous scope of the overall electronic communications framework, there are likely to be very large differences, leading to much compromise and debate. Proposals already circulating in Brussels show that the Council is unlikely to agree to the broadest extension of the rules that the Parliament is pushing. However, with both Commission and Parliament supporting the basic outlines of data breach reporting, it is reasonable to expect that some version will be adopted – and European industry should be preparing for these new obligations.

____

* Directive 2002/21/EC on a common regulatory framework for electronic communications networks and services

** Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector