MORRISON | FOERSTER

Legal Updates & News

Bulletins

Data Breach Notification: Debate in the EU

May 2008
by Ann Bevitt, Karin Retzer

Related Practices:

- Privacy and Data Security

Data Breach Notification: Debate in the EU

In the wake of a number of security incidents in the United Kingdom and elsewhere, the debate has reopened as to whether there should be a US-style security breach notification law, requiring those suffering a data breach to notify individuals, as well as national data protection authorities. The ICO ("ICO") recently published guidance on security breach management, including, amongst other things, "voluntary" notification. The European Commission also proposed that telecommunications operators and internet service providers should be required to notify affected persons about breaches. Below we outline the movement towards security breach notification in Europe and the lessons to be learned from the experiences in the United States and Japan, which both have security breach laws in place.

The UK data protection landscape has changed dramatically over the past 12 months as a result of several highly publicized security breaches in both the private and public sectors. For example, in February 2007, the Financial Services Authority ("FSA"), the financial services regulator, fined Nationwide Building Society, a major provider of mortgages and personal banking services, £980,000 (approximately €1,285,534 or US$1,939,879) for security failures resulting from a 2006 theft of an employee laptop computer containing sensitive customer data. The FSA found that Nationwide's security systems and its response to the breach, involving data relating to some of Nationwide's 11 million account holders, were inadequate. In November 2007, the government revealed that computer discs containing personal data on 25 million child benefit recipients were lost in the mail when tax officials sent the information to government auditors for review. Most recently, in January 2008, the ICO issued an Enforcement Notice against Marks & Spencer for its failure to encrypt customer data contained on a company laptop and to notify its customers following the theft of that laptop. The laptop, stolen from the managing director of a pension plan provider, contained data relating to 26,000 pension plan participants. These and other incidents have reopened the debate in the UK and elsewhere in Europe as to whether there should be increased security requirements and, in particular, whether those handling personal data should notify the affected individuals or the regulators about security breaches.

1. Prospects for Breach Law at EU Level

The need for security breach notification obligations has been debated for some time, particularly in the context of the review of the EU telecommunications regulatory framework. In fact, the European Commission proposed introducing mandatory breach notification requirements for any "*provider of publicly available electronic communications services*"[1] through amendments to the Electronic Communications Directive 2002/58.[2]

An "electronic communications service" is defined as a "service normally provided for remuneration which consists wholly or mainly in the conveyance of signals on electronic communications networks, including telecommunications services and transmission services in networks used for broadcasting, but excluding services providing, or exercising editorial control over, content transmitted using electronic communications networks and services." The Directive gives no further guidance on how to interpret the terms "publicly" or "normally provided for remuneration."

Therefore, while the Directive is aimed at telecommunications operators and internet service providers, the broad wording could be used by national regulators and law enforcement agencies to regulate employers providing employees with e-mail, internet cafes or hotels allowing guests to use communications devices, or even universities facilitating the use of the Internet. In France, for example, the term "electronic communications services" has been interpreted very broadly to include employers providing Internet access to

their employees,[3] and, in Denmark, housing societies and similar associations servicing more than 100 units are considered to be providing electronic communications services.

Under the European Commission's proposed amendments, providers would be required to notify users and regulators about any security breach "leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of or access to personal data." It is important to bear in mind that in the EU the term "personal data" is broadly defined to encompass any data relating to an identified or identifiable individual, which is any data that may be linked to individuals through other information even where that information is held by another person.[4] As a result, providers would be required to notify individuals about virtually all inadvertent disclosures of their data.

These notices would have to be provided "without undue delay" to enable the user to address the breach "in an adequate and timely manner." The notices must detail the nature of the breach, the economic loss and social harm that could result, and the recommended measures to mitigate possible negative effects. In addition, the regulator would have to be notified about the possible effects and measures taken by the company to remedy the breach.

Moreover, notification would not be limited to individuals who might suffer harm as a result of the breach, but rather would include all affected individuals and regulators. The Commission's declared aim is for national regulators to be able to inform the public at large if they consider it to be in the public interest. In order to ensure a high level of protection of personal data and privacy, regulators should also obtain "comprehensive and reliable data" about actual security incidents that have led to the personal data of individuals being compromised. In other words, notification should allow regulators to scrutinize data protection and security practices and, if these are considered insufficient, publish their findings and impose penalties.

The proposal would further allow the Commission to prescribe the "circumstances, format and procedures applicable to the information and notification requirement," after consultation with the regulator and the European Data Protection Supervisor."

In response to the Commission's proposal, the Article 29 Working Party, the group representing the EU data protection authorities, published comments applauding the Commission and arguing that it would like to see notification requirements extended to cover any "data brokers," banks or other online service providers.[5]

As the proposal was made in the context of the review of the EU telecommunications framework, and possible amendment to the Electronic Communications Directive 2002/58,[6] it is unlikely that the end result will impose obligations on organizations other than communication services providers. That said, the Working Party clearly wants to steer the debate towards a notification regimen. Peter Hustinx, the European Data Protection Supervisor, also said he would like to see data breach notification adopted more broadly in the EU. Consequently, debate on breach notification is likely to continue and may lead to proposals for enactment of a wider data breach law at the EU level.

2. The Debate in the United Kingdom

After a series of thefts and losses from government and private bodies, the House of Commons Justice Committee published a report on January 3, 2008,[7] calling for new reporting requirements under the Data Protection Act 1998 ("DPA"). In preparing for the Report, the Committee took evidence from Richard Thomas, the UK's Information Commissioner. Thomas told the Committee that a number of public and private sector organizations had approached his office, almost "on a confessional basis," to seek guidance on their own data security problems. The Committee recommended that a mandatory reporting system be introduced in the DPA that would incorporate workable definitions of data security breaches and clear rules on form and content of notification letters. Details have yet to be decided, but the Committee supports notification obligations that require organizations to inform all individuals affected, as well as the regulators, so that they can take "appropriate action."

In April 2008, the ICO released guidance on data security breach management.[8] The paper suggests that the adoption of a security beach response plan could be viewed as one of the appropriate security measures organizations are obligated to adopt under the Directive and national implementation legislation.

According to the guidance paper, a response plan should include four distinct elements:

(i) *Containment and recovery:* Following a data breach, in addition to the initial response to investigate and contain the breach, a more thorough recovery plan is necessary in order to limit damages. In particular, the plan should consider who should take the lead in the investigation, who should be notified, whether there is

anything the organization could do to recover the losses and limit damages, and whether to inform the police if appropriate.

(ii) *Assessing the risk:* The risk assessment for determining the necessary steps should focus on the analysis of the types of data involved and their sensitivity; whether data have been lost or stolen; whether the data were protected, including by encryption; how many individuals' data are affected by the breach; who the individuals whose data have been breached are; what harm can come to those individuals; and whether there are wider consequences to consider.

(iii) *Notification of breach:* The ICO stresses that notification is not an end in itself. The preferred approach seems to be to "encourage" organizations to notify the ICO, and, according to the Notification of Data Security Breaches paper,[9] there is a "presumption" that all "serious breaches" will be reported to the ICO, providing details on

- the types of data and number of records;
- the circumstances of the loss, release, or corruption;
- action taken to mitigate effect on individuals involved, including whether they have been informed, and details on how the breach is being investigated;
- whether any other regulatory body has been informed and its response;
- security measures in place such as encryption, and any remedial action taken to prevent future occurrence; and
- information on whether the media are aware of the breach.

The ICO would then decide, together with the organization, whether notification to affected individuals is required, depending on the nature and seriousness of the breach, *e.g.,* where a high volume of personal data is concerned, or where there is a high real risk of individuals suffering some harm, or where particularly sensitive data were lost, released, or unlawfully corrupted. The ICO may also decide that no further action is required, or decide on specific other actions to prevent, including formal enforcement action where the organization declines to take any recommended action, or where the ICO has other reasons to doubt future compliance or where there is a need to provide reassurance to the public. The ICO may also "recommend" that the organization make a breach public "where it is clearly in the interests of the individuals concerned or there is a strong public interest argument to do so."

(iv) *Evaluation of response*: In determining an effective response, an organization should consider whether sensitive data are involved and whether these data have been shared with or disclosed to others. The organization should establish a group of technical and non-technical staff to discuss "what if" scenarios.

In summary, while the ICO suggests that a response plan including notification may be legally required for an organization to meet its obligation to maintain appropriate security measures, the ultimate determination is for the organization to make. As a result, organizations are in a legal limbo as to how to react to breaches and whether to notify or not; and if they do, they may possibly face scrutiny from the Information Commissioner and the public.

3. And Elsewhere in Europe

Other regulators are less sanguine about the need for mandatory notification. While a law forcing organizations to disclose when personal data have been exposed would be welcomed by regulators, the general feeling that the law should "be a good one" precludes consumers becoming desensitized by overnotification. Within the context of the implementation of the amendments to the Electronic Communications Directive, Member States may introduce national statutes that apply to a much broader audience since there is nothing in EU law that would prevent them from doing so. In the meantime, given the investigative powers of the media, coupled with current data protection laws and industry-specific regulations in such areas as the health care and the financial services sectors, organizations should have processes already in place to manage data breaches or risk being exposed.

4. Learning from the Experience in the U.S. and Japan

As they begin drafting and implementing breach legislation, EU legislators and data protection authorities can draw lessons from the experience of those countries, such as the United States and Japan, which already have security breach notification laws in place. In particular, they should consider the following points:

a) Notification Trigger
A reasonable and balanced notification trigger should ensure that individuals receive notice when there is a

significant risk of substantial harm. The goal of a notification law should be to define a reasonable and balanced notification trigger, ensuring that individuals receive notice when and only when there is a significant risk of substantial harm as a result of a security breach. Notification of all incidents of data breach risks overwhelming individuals with notices that bear no relation to the actual risks. Overnotification would likely desensitize people and cause them to ignore the very notices that explain the action they need to take to protect themselves from harm when there is a significant risk.

This has been the experience in Japan and the US. In the case of Japan, notification of all incidents of data breach has been counterproductive. Some ministries, such as the Financial Services Agency, require notice to the relevant ministries, the public and affected individuals when there has been a security breach or leak of personal information, while other ministries state that such notice is "highly desirable." As a result, the general practice is for organizations to notify the public and the relevant ministry of every security breach, regardless of the size of the breach, the nature of the personal information involved, or risk of misuse. Notices bearing no relation to the actual risks posed by the breach have served to frighten and confuse people, as well as to desensitize them to future notices where they might need to take steps to protect themselves from harm. In response to this experience, Japan's Ministry of Economy, Trade and Industry ("METI") revised its guidelines and, among other things, established different notification triggers for notice to individuals and authorities.

The primary purpose of government reporting is to enable authorities to identify persistent or systemic problems and take action as needed to address those problems. Given these objectives, it does not make sense to establish requirements to notify government authorities about a security breach believed to affect only a few individuals. Moreover, frequent reporting about relatively minor security breaches will tax the already limited resources of data protection authorities. A reasonable and balanced approach is necessary.

The primary purpose of providing notices to individuals is to enable them to take steps to mitigate the risk of harm that might result from a breach. Thus, any individual notification requirement should be risk-based. Notification requirements should be limited to situations where there is a significant risk that information compromised in a breach will be used to commit identity theft or make fraudulent transactions, or where the breach could result in loss of business or employment opportunities.

Although serious, many, if not most, security breaches do not result in significant harm to the individuals to whom the breached information relates. For example, in many cases, media containing data about individuals is simply lost or misdirected. In addition, businesses increasingly store and transmit customer data in a variety of unique media forms that require highly specialized and often proprietary technology to read, including sophisticated encryption. Thus, even if customer data find their way into the wrong hands, they are often not in a readable or usable form. Any notification requirement should recognize that the risks associated with each breach will differ and, as a result, the appropriate response to each breach also will differ.

b) Definition of Personal Data

Legislation imposing notification obligations should specify the information that would be subject to these obligations.

The first US breach law, the California Computer Security Breach Notification Act,[10] which went into effect on July 1, 2003, defines "personal information" as an individual's first name (or initial) and surname in combination with one or more "data elements," if either the name or the data elements are not encrypted. These data elements are: Social security number (SSN); Driver's license or state identification card number; or Account, credit card or debit card number in combination with any required security code or password that would permit access to an individual's financial account. Many US state notification laws define "personal information" in similar terms; however, several laws provide that only the data elements that need to be encrypted, redacted or secured by another method rendering the element unreadable or unusable be considered "personal information." Several laws have expanded the scope of personal information to include different types of data elements such as medical information, biometric data and fingerprints. In addition, many of these state laws follow California law by providing an exception for certain types of information "available to the general public."

The European Commission proposal, by contrast, requires notification about any security breach "leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of or access to personal data." "Personal data" are broadly defined to encompass any data relating to an identified or identifiable individual, which are any data that may be linked to individuals through other information even where that information is held by another person. Any data which relate to a living individual who can be identified from those data, or from those data and other information which is in the possession of, or likely to come into the possession of the data controller, are captured.

Given the (perhaps) overly broad definition of personal data, it is important to limit notification obligations in order to avoid over-notification. Notification requirements should be limited to data that include an individual's

name together with one or more data elements such as a social insurance number, financial account information with passwords/PINs, or health information. Data that have been de-identified, encrypted, or otherwise adequately secured (using other technology), however, should not be covered because an incident affecting such data does not pose a high risk of significant harm to individuals. Moreover, if the breach involves data that are publicly available, such data elements should be excluded from the risk analysis.

c) Timing and Method of Notification

Notification of affected individuals should occur as soon as reasonably possible following proper evaluation of the scope and nature of the breach, remedying of any ongoing breach, and identification of the potentially affected individuals. The laws should, however, permit delays to notification at the request of law enforcement agencies in order for them to carry out their own investigations. Such delays to notification (and publication in the media) afford these agencies better opportunities to catch the culprits involved.

With regard to the method of notification, organizations should be able to select the most appropriate method of communication, taking into account the way in which the organization typically communicates with individuals and the circumstances surrounding a given breach. For example, some organizations, such as banks, regularly mail monthly statements to account holders. Consequently, postal mail notification may be the most logical choice for these organizations. Alternatively, other organizations may rely more on their websites as their means of communication with their customers and potential customers and, therefore, should be permitted to use electronic methods to notify individuals. In addition, website notification or other methods of mass communication may be more appropriate when a breach involves larger numbers of individuals.

d) Uniformity

Finally, when introducing breach notification requirements, uniformity is critical. EU Member State laws that impose a myriad of actual or potentially conflicting notification requirements would result in both higher costs and confusing and conflicting obligations.

Again, lessons can be learned from the US experience where the growing number of state laws has complicated the compliance obligations of organizations that operate in more than one state or industry. For example, although a security breach may involve the same types of information about individuals in different states, the individuals may be entitled to receive different types of notices (or no notice at all). The increasing array of obligations imposed on organizations makes it difficult for organizations to comply in one jurisdiction without running afoul of the obligations imposed on them in another.

In light of the blurred boundaries of today's increasingly technological world, security breaches do not recognize state boundaries. With respect to a security breach, the individual to whom the breached data relate may reside in one country, the criminal who caused the breach may reside in another country, the business victim of the breach may be located in a third country, and the information may have been obtained in a fourth state. In this context, the security of information will be promoted most efficiently and effectively by a uniform standard.

5. Outlook

So far, most organizations in the EU hit by a breach have been unprepared and, thereby, learned the hard way. Seldom were organizations prepared to deal appropriately with the breach and balance the different risks at stake in order to avoid public embarrassment and enforcement, and at the same time provide prompt notice to affected individuals. Once a breach occurs, events move quickly, and one false step can destroy years of diligent efforts towards attaining appropriate security protection and an untainted reputation.

Organizations should ensure, therefore, that they are prepared to deal with security breaches and get their houses in order now. An incident response plan, including reporting and handling by the appropriate level of management, is key. There may not yet be mandatory security breach notification requirements in Europe, but events in the last few months suggest that this state of affairs may be about to change, at least in some Member States. Regulators are proposing voluntary or obligatory breach notification plans or are exercising existing powers that require notification to be handled with care. More is to come.

Footnotes:

[1] Proposal for a Directive of the European Parliament and of the Council amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications

sector and Regulation (EC) No. 2006/2004 on consumer protection cooperation (COM(2007) 698 final).

[2] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (O.J. L 201/37).

[3] Article on French employers who provide staff with Internet access in relation to data retention: http://www.mondaq.com/article.asp?article_id=31701.

[4]Article of Directive 1995/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and the free movement of such data (O.J. L 281/31).

[5] Opinion 8/2006 on the review of the regulatory Framework for Electronic Communications and Services, with focus on the ePrivacy Directive.

[6] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (O.J. L 201/37).

[7] The report is available at: http://www.publications.parliament.uk/pa/cm200708/cmselect/cmjust/154/15402.htm.

[8] Guidance on data security breach management, available here (pdf).

[9] See Notification of Data Security Breaches to the ICO, available at: http://www.ico.gov.uk/upload/documents/library/data_protection/practical_application/breach_reporting.pdf

[10]Cal. Civ. Code § 1798.82.