MORRISON | FOERSTER

Legal Updates & News

Bulletins

Data Breach Notification: The Changing Landscape in the EU

April 2008
by Karin Retzer

Related Practices:

- Privacy and Data Security

Data Breach Notification: The Changing Landscape in the EU

PDF Version

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 U.S.-style security breach notification law to require those suffering a data breach to notify individuals as well as national data protection authorities. The European Commission proposed obligations for telecommunication operators and internet service providers to notify affected persons of breaches. In consultations on the draft, it was proposed to expand the regime to other organizations handling personal data. This article outlines the movement towards security breach notification in Europe and the lessons to be learned from experiences in the United States and Japan where security breach laws are in place already for some time.

I. Introduction

Over the past twelvemonths, the United Kingdom's data protection landscape changed dramatically. 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) following the theft of an employee's laptop. The laptop contained customer data relating to some of Nationwide's 11 million account holders. The FSA found that Nationwide's security systems and its response to the breach were inadequate. The government revealed that departments lost personal data, including the personal details and banking information from 25 million child benefits recipients. The Information Commissioner's office started 2008 by issuing BE48 8508 6795an Enforcement Notice against Marks &Spencer. Marks & Spencer had not formally notified its customers following the theft of a laptop. The laptop was stolen from the managing director of a pension plan provider during a burglary. The laptop contained data relating to 26,000 participants in the plan. The data were not encrypted.

These and other incidents have reopened the debate in the United Kingdom and elsewhere in Europe as to whether there should be increased security requirements and, in particular, whether those handling personal data should notify the individuals concerned or regulators of any security breach. Prior to the incidents in the United Kingdom, the European Commission proposed obligations for telecommunication operators and internet service providers to notify affected persons of breaches. There now are proposals to expand the regime to other entities handling personal data, and some EU members, namely the United Kingdom, are considering voluntary codes of practice.

The following summary outlines the movement towards security breach notification in Europe.

II. Prospects for Breach Law at EU Level

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

1. "Electronic Communications Services"

"Electronic communications services" is defined as "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 exclude 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 bring 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 under its regimen.

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 covered.

2. Proposed Notification

Under the proposed amendments, providers would be required to notify users, as well as 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 of virtually all inadvertent disclosures of their data. These notices would have to be provided "without undue delay" and detail the following:

- the nature of the security breach;
- recommended measures to mitigate its possible negative effects, including economic loss and social harm that could result from the security breach; and
- if to the regulator, possible effects and measures taken by the company to remedy the breach.

Recital 29 suggests that notification must allow the user to address the breach "in an adequate and timely manner."

Also, notification would not be limited to individuals who might suffer harm as a result of the breach, but rather would include all affected individuals as well as 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 European Commission to adopt technical implementing measures, prescribing "circumstances, format and procedures applicable to the information and notification requirement," after consultation with the regulator and the European Data Protection Supervisor."

3. Echo to the Commission's Proposal

Following that proposal, the Working Party 29, 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 to impose obligations on organizations other than communication services providers. That said, the Working Party clearly wants to steer the debate towards a notification regime. *Peter Hustinx*, the European Data Protection Supervisor, also said he would like to see data breach notification adopted more broadly in the EU. It is therefore likely that the debate may well loom for some time until the prospect of a wider data breach law at the EU level materializes (or vanishes).

III. The Debate at National Level

1. 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 3 January 2008.[7] The report calls for new reporting requirements under the Data Protection Act 1998 (DPA). In preparing for the report, the Committee took evidence from *Richard Thomas*, who is the United Kingdom's Information Commissioner. *Thomas* told the Committee that a number of organizations, both public and private sector, had approached his office, almost "on a confessional basis," to seek guidance for their own data security problems.

a) Mandatory Reporting System The Committee recommended that a mandatory reporting system be introduced in the DPA that would incorporate workable definitions of data security breaches, covering both a threshold for the sensitivity of the data lost and the criteria for the accessibility of that data, as well as clear rules on form and content of notification letters, which must clearly state the nature of the breach and provide advice on the steps that affected individuals should take to deal with the problem. Details have yet to be decided, but notification obligations should require organizations to inform all individuals affected, as well as the regulators, so that they can take "appropriate action."

Lord *Erroll*, one of the contributors to the Report, said the Committee recommended data breach notification laws not with a view to naming and shaming large corporations but in order to get a clear idea of the scale of the problem. "If things are encrypted properly then they are unusable [by criminals]," he added. "Technology helps us to do things properly, but when companies say they can't encrypt their databases because there are too many legacy systems it worries me."

b) Guidelines In the aftermath of the incidents, it is widely expected that the Information Commissioner's office will release guidelines recommending voluntary notification of security incidents to the Information Commissioner's office rather than directly to individuals. The Information Commissioner's office will then determine whether a notification of affected individuals is in order. The Commissioner's office may also decide that the security measures taken by the organization were insufficient and then impose penalties or publicize its findings widely. In light of these grave consequences, it is not entirely clear what the incentives for most organizations would be to notify the Commissioner's office of breaches if there was no legislative mandate to do so.

In light of the Marks & Spencer enforcement experience, it is questionable what the benefits are for those organizations that decide to report data breaches on a voluntary basis. While the Information Commissioner's office could potentially play an important role in being the first port of call after a security breach, advising on the right course of action to take, enforcement following voluntary notification may have a deterrent effect. Rather, there should be a safe harbor for organizations contacting authorities, shielding them from overly harsh penalties so that they are encouraged to come forward. Here it will be interesting to see whether the enforcement against Marks & Spencer constitutes a distinct change from the Information Commissioner's previous approach of encouraging informal notification and consultation.

2. Elsewhere in Europe

Other European regulators are more skeptical. There seems to be skepticism as to whether mandatory notification should be introduced or whether existing enforcement powers are sufficient. While a law forcing organizations to disclose if personal data have been exposed would be welcomed by regulators, the general feeling is that the law better "be a good one" in order to avoid consumers becoming desensitized if notified of every security breach. Within the context of the implementation of the amendments to the Electronic Communications Directive, Member States may introduce national statutes applying to a much broader audience than the proposed Directive – there is nothing in EU law that would prevent them from doing so. In the meantime, the investigative powers of the media, coupled with current data protection laws and industry-specific regulations, for example in the health care and the financial services sector, should result in organizations having processes already in place to manage data breaches or risk being exposed.

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

EU legislators and data protection authorities, when considering data protection laws or codes, should learn from the experience in the 38 states in the U.S., as well as in Japan, that have security breach notification laws in place.

In particular, the following elements should be considered when drafting and implementing breach legislation:

1. 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 that ensures that individuals receive notice when and only when there is a

significant risk of substantial harm as a result of a security breach. Notification in the wake of each incident of data breach promises to have the counterproductive effect of overwhelming individuals with notices that bear no relation to the actual risks. Over-notification is likely to 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.

In the case of Japan, notification in the wake of each incident 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 and 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 that bore no relation to the actual risks posed by the breach served to frighten and confuse people as well as 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 the 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 requirement should be limited to situations where there is a significant risk that information compromised in a breach will be used to commit identity theft, make fraudulent transactions, or where the breach could result in the 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 finds its way into the wrong hands, the data often are 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.

2. Definition of Personal Data

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

The first U.S. breach law, the California Computer Security Breach Notification Act,[8] which went into effect on 1 July 2003, defines "personal information" as an individual's first name or initial and last name 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 U.S. 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 the California law by providing an exception for certain types of information "available to the general public."

The European Commission's 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" 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. Data which relates 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.

Given the (perhaps) overly broad definition of personal data, it is indispensable 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 password/pin numbers 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.

3. 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 any ongoing breach and identifying the potentially affected individuals). The laws should, however, permit notification to be delayed at the request of a law enforcement agency in order for it to carry out its own investigation. For example, before notification is provided and before a breach is publicized in the media, law enforcement will have a better opportunity to catch the culprits involved.

As 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 to communicate 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.

4. Uniformity

Last, 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 U.S. experience where the growing number of state laws has complicated the compliance obligations of organizations that operate in more than one state or more than one 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 relates 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 party 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.

V. Outlook

So far, in the Europe, most organizations hit by a breach were unprepared and had to learn the hard way. Seldom were organizations prepared to deal appropriately with the breach and balance of 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 working towards appropriate security protection and an untainted reputation. Organizations should therefore ensure that they are prepared to deal with security breaches and get their house 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] 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).

[2] 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).

[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 24October 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] Cal. Civ. Code § 1798.82.

This article first appeared in CRi - Computer Law Review International', Issue 2 and is reproduced with permission. For more information on CRi please see www.cr-international.com.