



PRIVACY & SECURITY LAW



REPORT

Reproduced with permission from Privacy & Security Law Report, Vol. 6, No. 10, 03/05/2007, pp. 384-386. Copyright © 2007 by The Bureau of National Affairs, Inc. (800-372-1033) <http://www.bna.com>

EU Data Protection

Data Protection Regulation

In recent weeks, hefty fines for data breaches have been issued in the United Kingdom and Greece. Surprisingly, these fines have not been levied by data protection authorities, but by other regulators with overlapping jurisdiction over data security. The authors, from Hunton & Williams, write that data protection enforcement in Europe appears to be entering a new phase.

Nationwide Building Society Is Fined £980,000 (\$1.9 Million): Has The European Data Protection Enforcement Framework Suddenly Changed?

By BRIDGET TREACY AND LISA SOTTO

European privacy officers often bemoan the perception that data protection regulators in the European Union lack any real enforcement power. Consequently, many businesses adopt a patchy approach to data protection compliance, gambling on the relatively low risk of being caught. Many privacy officers believe the prospect of a hefty fine to punish breaches, or the requirement to notify regulators and affected individu-

als, would act as a significant deterrent for companies, forcing them to take data security seriously. In recent weeks, the European compliance landscape has changed dramatically: notification of data breaches is being discussed widely and businesses have been punished for data breaches, receiving hefty fines. Surprisingly, these fines have not been levied by data protection authorities, but by other regulators with overlapping jurisdiction over data security. Data protection enforcement in Europe appears to be entering a new phase.

Bridget Treacy (London) and Lisa Sotto (New York) are Partners in the Privacy and Information Management Practice at Hunton & Williams. They may be contacted at btreacy@hunton.com and lsotto@hunton.com

European Data Protection Enforcement

In November 2004, the Article 29 Working Party published its Declaration on Enforcement (WP101). In this paper, the Working Party committed itself to the development of proactive enforcement strategies and to an

increase in enforcement actions. Specifically, it sought to promote awareness-raising activities, the development of codes of conduct and the provision of guidance and advice as an important part of the data protection compliance agenda. In addition, the Working Party acknowledged the importance of sanctions as a necessary means of ensuring compliance, and made reference to the possibility of EU-wide, synchronized, national enforcement initiatives.

The reality is that the majority of European data protection authorities have only limited power to impose sanctions for breaches of domestic data protection legislation.

Despite the sentiments expressed in the Declaration, the reality is that the majority of European data protection authorities have only limited power to impose sanctions for breaches of domestic data protection legislation. Article 28(3) of the Data Protection Directive (95/46/EU) states that data protection supervisory authorities shall have investigative powers, effective powers of intervention and the power to engage in legal proceedings. In most member states, the exercise of those powers is severely curtailed, if not by the detail of domestic data protection legislation then, in practical terms, by a lack of funding for enforcement proceedings.

The reality of data protection enforcement across Europe to date is that there are notably few instances of fines and negative publicity. Outside the circle of businesses that take data protection seriously, many organizations are not compliant with data protection requirements. Privacy officers frequently express frustration that data protection compliance has little visibility at the executive level. Regulators may talk about encouraging organizations to be compliant, but within the corporate regulatory environment, it is the prospect of sanctions, particularly fines and adverse publicity, that in fact encourages compliance.

Against this background, there is an increasing level of discussion across Europe of the merits of introducing a U.S.-style data breach notification requirement. In part, these discussions have arisen from the current review of the European telecommunications regulatory framework. A recent legislative proposal in the context of the telecommunications framework would require providers of electronic communications networks and services to notify their regulator of a breach of security leading to the loss of personal data or to interruptions in service supply. Further, there would be a requirement to notify customers of any breach leading to the loss, modification or destruction of or unauthorized access to individuals' personal data. As a general matter, there is increasing concern over the rise in identity theft. In the mind of the general public, data breaches are linked to identity theft, irrespective of whether the research supports a causal connection.

In addition to the growing movement toward a European data breach notification requirement, there have been two recent examples of enforcement in this area

that have garnered the attention of the media and privacy officers alike. Both cases concern a breach of data security obligations, but the key feature of each is that it was a regulator other than a data protection authority that imposed substantial fines to punish the relevant companies. Overlapping jurisdiction over data security requirements and a determination by other regulators to take enforcement action for breaches suggests that regulated businesses (at the very least) have been warned that complacency in this area will not be tolerated.

Nationwide's £980,000 Fine

On 14 February 2007, the U.K.'s financial services regulator, the Financial Services Authority (FSA), fined a large U.K. financial services business, Nationwide Building Society, £980,000 (\$1.9 million) following the theft of an employee's laptop from their home. The laptop contained customer data relating to some of Nationwide's 11 million account holders. The FSA deemed Nationwide's systems and controls for preventing and managing a security breach to be inadequate.

Nationwide informed the police, the Information Commissioner and the FSA of the theft. It was the FSA, exercising its broad supervisory jurisdiction to protect consumers and reduce financial crime, that fined Nationwide. Under the Financial Services and Markets Act 2000 (FSMA) and the Principles for Business developed under FSMA, a regulated business must take reasonable care to establish and maintain such systems and controls as are appropriate to its business. In Nationwide's case, the FSA was highly critical of the fact that Nationwide's systems did not monitor or manage large downloads of information to portable storage devices. Further, its information security procedures for staff were dispersed across multiple documents covering a broad range of issues with no search facility. Staff training was generic. Consequently, when the theft occurred, the employee reported the fact of the theft but made no mention of what was on the laptop. The employee then went on holiday for three weeks, during which time there was no further investigation.

The FSA found that:

- Nationwide had failed adequately to assess its information security risks;
- Nationwide's information security procedures failed to manage the risks the business faced;
- staff was inadequately trained;
- there were inadequate controls in place to mitigate information security risks; and
- there were inadequate procedures in place to manage an incident involving the loss of customer information.

Significantly, the U.K.'s Information Commissioner would not have imposed a fine against Nationwide; a fine requires the commission of a criminal offense.

Although Nationwide settled the case at an early stage, receiving a 30 percent discount on the total fine

of £1.4 million, the discounted fine of £980,000 remains substantial, particularly for a security breach. The FSA's jurisdiction to impose a fine for a breach of FSMA is broad and the FSA had no hesitation making clear in its Notice to Nationwide that its objective in imposing the fine was not only to punish Nationwide but also to provide a deterrent to others.

Vodafone Fined €76 Million

Nationwide is not the only recent example of a regulator other than a data protection authority exercising jurisdiction over security breach issues in Europe. Recently, in Greece, the Hellenic Authority for Information and Communication Security and Privacy (the Authority) fined Vodafone €76 million (\$99.8 million) in response to a security breach and wiretapping incident at the 2004 Athens Olympics. The mobile phone calls of government officials had been illegally monitored. Vodafone was criticized for not having prevented hackers from circumventing a legitimate surveillance system, supplied by Ericsson, a Swedish telecommunications company, to spy on Greek officials. Unauthorized manipulation of the Ericsson-supplied surveillance software used by Vodafone enabled calls made to and from targeted phones to be relayed to certain mobile numbers. The Authority (which is different from the Greek data protection authority, called the Hellenic Data Protection Authority) found that Vodafone had failed to take adequate measures to protect its network and had not informed subscribers that their phones were being tapped. It further criticized Vodafone for obstructing its investigation by failing to admit the existence of the surveillance system itself.

Wider Regulatory Implications

If the facts of the Nationwide case were examined in light of the U.K.'s data protection legislation, the Data Protection Act 1998, it seems beyond doubt that Nationwide was in breach of the Seventh Principle (which implements Article 17 of the European Data Privacy Directive (EU95/46)). That principle requires data controllers to ensure an appropriate level of technical and organizational security to protect personal data. The Notice issued by the FSA in the Nationwide case states that the U.K.'s Information Commissioner was informed of the security breach. It is not known what steps the Information Commissioner required Nationwide to take. Typically this might have included improving information security and informing customers of the breach. Significantly, the Information Commissioner would not have imposed a fine; this requires the commission of a criminal offense, and the conduct of Nationwide here did not amount to an offense.

Similarly, in the case of Vodafone, it was a regulator with overlapping jurisdiction and a more proactive enforcement agenda that took action against conduct that might otherwise have fit squarely within the jurisdiction of the data protection regulator. Like in the case of Nationwide, the amount of the fine was intended not only as a punishment but also as a serious warning to others.

A U.S.-Style Security Breach Notification Law?

Attention is also focused in Europe on whether laws in the EU should require the mandatory notification of security breaches, along the lines of U.S. regulation. In the United States, individuals whose data was compromised must be notified of the breach. In a number of

states, state agencies also must be notified. The U.S. requirement had its genesis in the California Computer Security Breach Notification Act (S.B. 1386), which became effective on 1 July 2003. The California law applies to personal information, maintained in computerized form, which has been, or is reasonably believed to have been, acquired by an unauthorized person. "Personal information" means the name of the individual together with a Social Security number, driver's licence or state identification card, or bank account, credit or debit card number together with any required security code. Where these data are compromised, businesses must provide written notification to the affected individuals which, over time, has come to mean all affected persons, whether resident in California or not.

More than 30 states have enacted similar laws. They differ, however, in several key respects: some include other media (e.g., paper); the definition of "personal information" sometimes differs from state to state; in some states a harm threshold triggers the notification obligation; and, in a number of states, regulators and credit reporting agencies must be notified of the breach (in addition to affected individuals).

Although there is a widespread security breach notification obligation in the United States, the state-by-state nature of its implementation leads to other difficulties. U.S. businesses in the unfortunate position of having to deal with a breach face the challenge of coordinating their response, taking into account the differing (and sometimes inconsistent) requirements of the individual state laws. In the United States, the legislative focus is on enacting federal legislation so as to preempt inconsistent state laws.

In Europe, the Nationwide and Vodafone cases are likely to focus attention on the apparent inability of data protection authorities to enforce data protection legislation proactively.

It is significant that the U.S. Federal Trade Commission recently formed a new division, called the Division of Privacy and Identity Protection, to handle data security and privacy issues. This signals a new focus on data security and information breaches in the United States, and a likely increase in regulatory enforcement activities.

Next Steps in Europe

In Europe, the Nationwide and Vodafone cases are likely to focus attention on the apparent inability of data protection authorities to enforce data protection legislation proactively. Many privacy officers have long believed that a high profile enforcement action would assist them in raising the profile of data protection within their organizations, helping them to obtain an adequate compliance budget and a higher level of visibility for data protection and information security. It is ironic that we now have two such cases but that neither involved, in any public way, the relevant data protection regulator. Perhaps these cases will have the effect of re-energizing the data protection authorities in Europe.

There is no question that the heated discussion over the possibility of a U.S.-style data breach notification law has fueled the wider debate concerning effective data protection enforcement.

This article does not provide a complete statement of the law. It is intended merely to highlight issues that may be of general interest and does not constitute legal advice.