

# dataprotectionlaw&policy

**FEATURED ARTICLE**  
**02/07**



cecile park publishing

Head Office UK Cecile Park Publishing Limited, 17 The Timber Yard, Drysdale Street, London N1 6ND  
tel +44 (0)20 7012 1380 fax +44 (0)20 7729 6093 info@e-comlaw.com  
[www.e-comlaw.com](http://www.e-comlaw.com)

# Nationwide: movements towards a notification regime

The Financial Services Authority's decision to fine Nationwide for failing to implement proper security procedures following the theft of a laptop highlights the dangers of inadequately tackling data breaches. Bridget Treacy and Lisa Sotto, partners in the global privacy practice at Hunton & Williams, examine the movement towards a data breach notification law in Europe, and explain lessons to be learned from the US' experience.

In the US, there are countless data breaches weekly. Some are reported in the press; most are not. How do we know about these breaches? In more than 30 states, organisations that suffer a data breach are required to notify individuals whose data were reasonably likely to have been compromised. Consequently, US businesses that experience a data security breach face the prospect of dealing with it in the full glare of the media spotlight. In stark contrast, from a European perspective, there is no accurate picture of how many security breaches occur. This is primarily due to the fact that despite a comprehensive data protection framework (based on EU Directive 95/46), there is no data breach notification requirement in Europe. Businesses are generally able to manage a data breach as an internal matter, away from the public eye. This may be about to change.

## Nationwide's £980,000 fine

On 14 February 2007, the UK's data protection landscape dramatically altered. The UK's financial services regulator, the Financial Services Authority (FSA), fined the UK's largest building society, Nationwide, £980,000 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 that Nationwide's systems and controls for preventing and managing a security breach were inadequate.

By US standards, Nationwide's experience might have resulted in a well-rehearsed containment plan swinging into action, with damage minimisation a key focus. In Europe, where data protection laws do not require businesses to notify affected individuals, businesses have long felt comfortable in the knowledge that, if there is a breach, it is unlikely to become public. Nationwide's experience shows that the days of dealing with a security breach as an internal issue may well be over.

If the facts of the Nationwide case were examined in light of the UK's data protection legislation, the Data Protection Act 1998, Nationwide would probably have escaped censure or, at worst, received a limited amount of adverse publicity. This is because despite a comprehensive data protection framework, including an obligation to safeguard the security of personal data, the UK legislation (and EU data protection legislation more generally) does not require the notification of data security breaches to the regulator, the UK's Information Commissioner, or affected individuals.

Further, even if he had been notified of the security breach, the Information Commissioner does not have the power to impose a fine in these circumstances. Fines may be imposed following the commission of a criminal offence (up to a maximum level of £5,000 per offence), but the conduct of Nationwide here did not amount to an offence.

## Overlapping enforcement

What is most interesting about this

case is that it was another regulator, the FSA, with responsibility for ensuring that financial services businesses maintain proper systems and controls, that intervened. Unlike the Information Commissioner, the FSA does have the power to fine businesses for breaches of their systems and controls and here, the FSA determined that Nationwide's risk assessment and security procedures were inadequate. The FSA specifically pointed to the fact that staff did not know what steps to take in the event of such a breach. Policies were inaccessible and staff were not adequately trained. The fact that no action was taken in the first three weeks after the breach increased the opportunity for the information to be misused (although there is no evidence of actual misuse).

This 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 fined Vodafone €76 million over a security breach and wiretapping incident at the time of the 2004 Athens Olympics.

## EU security breach law

The absence of a notification requirement does not mean that businesses may disregard security; rather, appropriate technical and organisational security measures are required to be implemented to safeguard personal data. The difficulty has been in enforcing this requirement.

The possibility of introducing a US-style security breach notification requirement into Europe has been a hotly debated topic. The background to some of these discussions has been the wide-ranging review of the European

telecommunications regulatory framework. Under the recent proposal, providers of electronic communications networks and services would be required to notify their regulator of a breach of security leading to the loss of personal data or to interruptions in service supply, and notify their customers of any breach leading to the loss, modification or destruction of or unauthorised access to their personal data. More generally across Europe, attempts to link data breaches to an increase in identity theft are perhaps inevitable, and may act to galvanise public opinion in favour of a notification requirement.

### US data breach laws

The contrasting US requirement for companies to notify individuals of security breaches that compromise their data had its genesis in the California Computer Security Breach Notification Act (SB 1386), which became effective on 1 July 2003. The Californian law applies to personal information, maintained in computerised form, which has been, or is reasonably believed to have been, acquired by an unauthorised 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 their customers which, over time, has come to mean all customers, whether resident in California or not.

More than 30 states have enacted similar laws. Although there is a widespread security breach notification obligation in the US, the state by state nature of its implementation leads to other difficulties. US businesses in the

**It is clear from Nationwide and Vodafone that other regulators regard such breaches as serious and will not hesitate to exercise their existing enforcement powers**

unfortunate position of having to deal with a breach face the challenge of co-ordinating their response, taking into account the differing (and sometimes inconsistent) requirements of the individual state laws. In the US, the legislative focus is on enacting federal legislation so as to bring security breach notification requirements onto a consistent footing. In addition, the US Federal Trade Commission recently formed a new division, called the Division of Privacy and Identity Protection, to handle data security and privacy issues.

### Learning from the US experience

We may not yet have a security breach notification requirement in Europe, but the topic is currently under active discussion by regulators. Irrespective of whether the data protection regulators seek to impose such an obligation, it is clear from Nationwide and Vodafone that other regulators regard such breaches as serious and will not hesitate to exercise their existing enforcement powers. Drawing on the US experience of data breach notification and bearing in mind specific criticisms made by the FSA that Nationwide was unprepared to deal with a security breach, what steps should UK and other EU businesses take to prepare for such an incident?

The starting point is to undertake a risk assessment of the organisation's systems and security, and assess which systems present the most significant risks to the organisation, if breached. Security procedures with respect to key systems should be enhanced and regularly monitored and assessed. An Incident Response Plan should also be devised to serve as an action plan in the event of a breach.

The Incident Response Plan

should deal logically with each stage of a data breach incident, including:

- engaging the incident response team;
- determining whether and which data may have been compromised;
- dealing with the breach itself, which may include fixing the vulnerability or literally kicking the intruder out of the system;
- determining whether and, if so, when and how staff, customers and regulators should be told about the breach;
- testing the plan and ensuring that staff members are trained to follow it.

The existence of the plan and any other security breach guidance must be familiar to staff. The incident response team should be designated in advance and able to implement the plan, should a data breach occur.

### The future

As for Nationwide, they have now taken steps to deal with their breach, apologised to customers and reviewed their risk assessment procedures. Yet they have learned the hard way. Personal experience of managing more than 60 security breaches in the US suggests that advance preparation is key to dealing successfully with these incidents. Once the breach occurs, events move at lightning pace. Under the full glare of the media spotlight, one false step can destroy attempts to contain these incidents. Other European businesses should consider themselves fortunate that they still have an opportunity to get their own house in order. If the US experience is anything to go by, this issue is unlikely to go away.

**Bridget Treacy** Partner (London)  
**Lisa Sotto** Partner (New York)  
 Hunton & Williams  
 btreacy@hunton.com  
 lsotto@hunton.com



# cecile park publishing

Head Office UK Cecile Park Publishing Limited, 17 The Timber Yard, Drysdale Street, London N1 6ND  
tel +44 (0)20 7012 1380 fax +44 (0)20 7729 6093 info@e-comlaw.com  
[www.e-comlaw.com](http://www.e-comlaw.com)

Registered number 2676976 Registered address 141 Wardour Street, London W1F 0UT VAT registration 577806103

## e-commerce law & policy

Many leading companies, including Amazon, BT, eBay, FSA, Orange, Vodafone, Standard Life, and Microsoft have subscribed to ECLP to aid them in solving the business and legal issues they face online.

ECLP, was nominated in 2000 and again in 2004 for the British & Irish Association of Law Librarian's Legal Publication of the Year.

**A twelve month subscription is £390 (overseas £410) for twelve issues and includes single user access to our online database.**

## e-commerce law reports

You can now find in one place all the key cases, with analysis and comment, that affect online, mobile and interactive business. ECLR tracks cases and regulatory adjudications from around the world.

Leading organisations, including Clifford Chance, Herbert Smith, Baker & McKenzie, Hammonds, Coudert Brothers, Orange and Royal Mail are subscribers.

**A twelve month subscription is £380 (overseas £400) for six issues and includes single user access to our online database.**

## data protection law & policy

You can now find in one place the most practical analysis, and advice, on how to address the many problems - and some opportunities - thrown up by data protection and freedom of information legislation.

DPLP's monthly reports update an online archive, which is an invaluable research tool for all those who are involved in data protection. Data acquisition, SMS marketing, subject access, Freedom of Information, data retention, use of CCTV, data sharing and data transfer abroad are all subjects that have featured recently. Leading organisations, including the Office of the Information Commissioner, Allen & Overy, Hammonds, Lovells, BT, Orange, West Berkshire Council, McCann Fitzgerald, Devon County Council and Experian are subscribers.

**A twelve month subscription is £355 (public sector £255, overseas £375) for twelve issues and includes single user access to our online database.**

## world online gambling law report

You can now find in one place analysis of the key legal, financial and regulatory issues facing all those involved in online gambling and practical advice on how to address them. The monthly reports update an online archive, which is an invaluable research tool for all those involved in online gambling.

Poker, payment systems, white labelling, jurisdiction, betting exchanges, regulation, testing, interactive TV and mobile gaming are all subjects that have featured in WOGLR recently.

Leading organisations, including Ladbrokes, William Hill, Coral, Sportingbet, BskyB, DCMS, PMU, Orange and Clifford Chance are subscribers.

**A twelve month subscription is £485 (overseas £505) for twelve issues and includes single user access to our online database.**

## world sports law report

WSLR tracks the latest developments from insolvency rules in football, to EU Competition policy on the sale of media rights, to doping and probity. The monthly reports update an online archive, which is an invaluable research tool for all involved in sport.

Database rights, sponsorship, guerilla marketing, the Court of Arbitration in Sport, sports agents, image rights, jurisdiction, domain names, ticketing and privacy are subjects that have featured in WSLR recently.

Leading organisations, including the England & Wales Cricket Board, the British Horse Board, Hammonds, Fladgate Fielder, Clarke Willmott and Skadden Arps Meagre & Flom are subscribers.

**A twelve month subscription is £485 (overseas £505) for twelve issues and includes single user access to our online database.**

- Please enrol me as a subscriber to **e-commerce law & policy** at £390 (overseas £410)
- Please enrol me as a subscriber to **e-commerce law reports** at £380 (overseas £400)
- Please enrol me as a subscriber to **data protection law & policy** at £355 (public sector £255, overseas £375)
- Please enrol me as a subscriber to **world online gambling law report** at £485 (overseas £505)
- Please enrol me as a subscriber to **world sports law report** at £485 (overseas £505)

**All subscriptions last for one year. You will be contacted at the end of that period to renew your subscription.**

Name

Job Title

Department  Company

Address

Address

City  State

Country  Postcode

Telephone  Fax

Email

**1** Please **invoice me**  Purchase order number

Signature  Date

**2** I enclose a **cheque** for the amount of

made payable to 'Cecile Park Publishing Limited'

**3** Please debit my **credit card**  VISA  MASTERCARD

Card No.  Expiry Date

Signature  Date

VAT No. (if ordering from an EC country)

Periodically we may allow companies, whose products or services might be of interest, to send you information. Please tick here if you would like to hear from other companies about products or services that may add value to your subscription.

priority order form

FAX +44 (0)20 7729 6093

CALL +44 (0)20 7012 1380

EMAIL [dan.towse@e-comlaw.com](mailto:dan.towse@e-comlaw.com)

ONLINE [www.e-comlaw.com](http://www.e-comlaw.com)

POST Cecile Park Publishing 17 The Timber Yard, Drysdale Street, London N1 6ND