



# World Data Protection Report

International Information for International Businesses

Monthly news and analysis of data protection and privacy issues from around the world

Volume 9, Number 1

January 2009

## Privacy 2009: New Year, new US President, same old privacy problems

*Nicola McKilligan looks back on 2008 and predicts the trends for the coming year.*

Privacy professionals and their advisors planning for the year ahead could do worse than take some time to look back on 2008 and evaluate just what went wrong and what went right in terms of privacy compliance and regulation. However just in case you haven't got the time here are World Data Protection Report's Editor's favourite privacy ups and downs of 2008 which we predict will continue to be trends for the new year.

### Security breach notification law

Back in January 2008 we were still in the grip of security breach fever and reeling from the impact of the practical consequences of responding to, and indeed meeting the costs of, security breaches. This was particularly the case in the U.S. where every week seemed to bring a new breach and a new State data security law. According to the Identity Theft Resource Centre<sup>1</sup> data breaches were dramatically on the rise in 2008: "with 656 reported breaches at the end of 2008, reflecting an increase of 47% over last year's total of 446".

Most worryingly, the ITRC reported that, "only 2.4% of all breaches had encryption or other strong protection methods in use. Only 8.5% of reported breaches had password protection. It is obvious that the bulk of breached data was unprotected by either encryption or even passwords."

This was despite the fact that by the end of December 2008 the National Conference of State Legislatures re-

corded that 44 U.S. States, plus the District of Columbia, Puerto Rico and the Virgin Islands had all, "enacted legislation requiring notification of security breaches involving personal information".<sup>2</sup>

Many U.S. laws require credit reporting to be provided for victims of security breaches involving unencrypted data. The administrative costs for responding to U.S. security breaches can therefore be high and it wasn't always clear in 2008 exactly who would bear the burden of the cost. Companies who subcontracted out services to contractors who caused a breach often found they were unable to recoup all their losses under the terms of existing contracts. A recent report has also demonstrated that the infamous data breaches by the U.S. retailers TJX and Hanaford in the U.S. also cost third parties such as State banks and credit unions over \$2.1 million in expenses as they had to reissue cards and carry out their own investigations into possible frauds.

Security breach notification was far from being just a U.S. issue with many other jurisdictions calling for similar laws or self-regulated reporting of breaches. The U.K. continued to suffer breaches although a U.S. style law was ruled out at the end of 2008. But many countries such as Ireland and Australia are expected to follow a U.S.-style route. The European Network and Information Security Agency (Enisa) also called in May 2008 for a Europe-wide security breach notification law.

By the end of 2008, companies had, for the most part, gained a calmer perspective on the security breach threat. Panic gave way to a more considered approach

to incident reporting, management and response procedures. Insurance even became available to cover security breach costs. For most large corporations in 2009 compliance with security breach notification law will now be just another part of business as usual compliance.

## Encryption

Many businesses embarked on the roll out of large scale encryption programmes in 2008. Encryption of hard drives and removable media such as USB sticks and back-up tapes became the *de facto* standard in security conscious organisations. Encryption was also recognised by many legislatures as an effective prophylactic. Organisations using encryption to protect PII could avoid reporting requirements under most U.S. laws. A boom time followed for software providers who could offer robust encryption solutions.

In October, the U.S. State of Nevada broke new ground and brought in a law which made failure to encrypt PII an automatic offence even if no security breach occurs. According to privacy lawyers, Morrison and Foerster, “the Nevada encryption statute generally prohibits a business in Nevada from transferring ‘any personal information of a customer through an electronic transmission’, except via facsimile, ‘unless the business uses encryption to ensure the security of electronic transmission’ ”.<sup>3</sup>

This move towards encouraging encryption was not just a U.S. phenomenon either.

In the U.K., blighted by the HMRC data loss of 2007, a series of Government reports recommended the use of more robust technical solutions, and Government departments contacted all their sub-contractors with new requirements obliging them to encrypt or cease using removable devices such as laptops, USB sticks and even Blackberry-style mobile phones. The U.K. Government’s model contracts for suppliers were updated to include new information management requirements including a requirement to certify security plans with the information security standard ISO 177799. All of this, unfortunately, did not follow the high profile loss by Government sub-contractor PA Consulting of a USB stick containing the personal details of the U.K. Prison population. This painfully demonstrated that however good your contract is, it is still only as good as the staff on the ground who implement it.

## Accountability

This issue of accountability for data security at ground level would also be an important feature of compliance in 2008. Lack of accountability was seen as a major reason for the failings at HMRC in the U.K. and a number of key U.K. Government reports called for increased staff training and a clear line of accountability for data protection within Government departments. In the end if it is clear who will lose their job if things go wrong, the person accountable will no doubt make every effort to ensure that nothing does.

## Privacy, human rights and yet more giant databases

For the citizen, consumer and for human rights groups much of the focus in 2008 was on more sinister ‘Orwellian’ developments. Both the private and public sector came under scrutiny in the press for initiatives aimed at increasing their knowledge of the habits of the general population. Media sources frequently pointed out the irony that citizens were now expected to give up more of their most sensitive data to the State and big business, despite the growing evidence that neither Government nor commerce seemed to have overcome the problem of keeping such data secure.

This was the year of the ‘Big Brother Database’ as Governments in the U.K. and France announced plans in the summer to create giant communications logs to record Internet traffic. In the U.K. in May, The Times newspaper reported that the Government would keep stored details of emails and Internet visits on all U.K. Internet users with ISPs, and telecoms companies would be forced to share records with the Home Office. The data would be retained on a database for up to 12 months and would be accessible to the police and security services. The database has the go-ahead from the U.K. Government who argues that it will help fight terrorism.

In France, campaigners lobbied International Data Protection Commissioners attending an evening gala at their conference in Strasbourg to protest against a similar French database the ‘Edvidge’ system which would have held personal data on those as young as 13 in France. In light of these protests the French Government capitulated and withdrew its plans.

There was a ray of hope in December when two U.K. citizens, Mr Marper and a young person known only as ‘S’ appealed the inclusion of their details on the U.K.’s controversial DNA database to the European Court of Human Rights (ECHR). Neither of the appellants had been convicted of a crime but their DNA remained stored on the police system (apparently along with the DNA of millions of other people in exactly the same position). The Strasbourg court found the British Police had violated Article 8 of the European Convention on Human Rights – the right to respect for private and family life, when they failed to remove the data. Explaining their ruling, the judges warned that keeping their DNA had left the men, “under a cloud of suspicion because they were ‘entitled to the presumption of innocence, yet were treated in the same way as convicted persons’ ”.

The victory of the two men set a precedent which will prevent other European Member States taking the same position should they further develop their approach to DNA collection for crime prevention and detection along British lines.

## Google inside and out

Google’s Street View was launched in Europe in 2008 after attracting a fair degree of controversy in the U.S.. Many thought that it would not be possible to imple-

ment Street View in Europe because of strong data privacy laws. Initially Peter Hustinx, the European Data Protection Supervisor, suggested that the Street View feature of the Google Maps could be in breach of the E.U. Data Privacy Directive.

Hustinx took the opportunity to warn Google, that, “Complying with European data protection law is going to be part of their business success or failure. If they would ignore it, it is likely to lead to (court) cases, and I think they would be hit hard”.

However later in the year, the U.K. Information Commissioner, Richard Thomas, gave the go ahead to Street View in the U.K. and said he was ‘satisfied’ that Google had put in place safeguards to avoid risking anyone’s privacy or safety.

Overall, however, 2008 was not a good year for Google. In November, Hustinx’s warning to Google was fulfilled when the Italian prosecutor confirmed that four Google executives would stand trial in Italy on data protection and defamation related charges. The charges arose after a video clip of the bullying of a Downs syndrome boy appeared on a website allegedly under Google’s control. The defendants are due to appear in court in Milan on February 3, 2009. The results of the case could have serious implications about the jurisdictional reach of European Courts attempting to implement data privacy law in relation to Internet content.

## Standards: towards a Global understanding of Data Privacy

Finally another important trend of 2008 was the move towards greater standardisation the field of privacy regulation. In early October, the Security techniques Committee of the International Standards Organization (ISO) met in Cyprus and more progress was made towards the development of a new series of technical privacy standards which are the focus of Working Group 5 of the Committee. Kai Rannenberg, the convenor of Working Group 5, also presented the ISO vision to the International Commissioner’s Conference held in Strasbourg at the end of that month. At both meetings there was much discussion about the difficulties of combining different cultural approaches into a single paradigm for privacy protection. Some competition between the APEC approach, favoured by the U.S. and much of the Asia Pacific region, and the E.U. Directive approach is still apparent but in general the direction of standardisation in 2009 would seem to be moving towards closer cooperation and finding a pragmatic way to overcome differences.

### NOTES

<sup>1</sup> [http://www.idtheftcenter.org/artman2/publish/lib\\_survey/ITRC\\_2008\\_Breach\\_List.shtml](http://www.idtheftcenter.org/artman2/publish/lib_survey/ITRC_2008_Breach_List.shtml)

<sup>2</sup> <http://www.ncsl.org/programs/lis/cip/priv/breachlaws.htm>

<sup>3</sup> <http://www.mofo.com/news/updates/bulletins/12866.html>