INTERNATIONAL NEWSLETTER

PRIVACY LAWS & BUSINESS
DATA PROTECTION & PRIVACY INFORMATION WORLDWIDE

Europe's emerging breach notification regime

Consensus over need for law, but differences over who is subject and when notice is required. By **David Fink** and **Henriette Tielemans**.

The European Council and the European Parliament appear to be moving towards agreement on legislation that would require all 27 EU Member States to introduce breach notice rules in accordance with EU-level provisions. Parliament is expected to vote on a revised proposal in early May, and observers currently predict a final agreement with the Council before the European Parliament elections in June.

Breach notice is a rare area in the data protection field where the EU has lagged significantly behind other parts of the world. In the US, for example, some 44 states have breach notice laws. By contrast, in Europe, there is no EU-level law and Member States have generally limited their activity in this area to non-binding guidance.

The European Commission believes that data security would be enhanced by a mandatory, EU-wide approach, and it proposed legislation to that effect in November 2007 (COM (2007) 698). The Commission adopted a revised proposal in November 2008 (COM(2008) 723) in response to amendments approved by Parliament on 24 September. The Council subsequently adopted its Common Position on 9 February of this year. At the time of this writing, the Council and the Parliament had

Continued on p.3

Finland: employers get right to snoop on employee email

Monitoring allowed by new law for trade secret leaks. **Laura Linkomies** looks at the DP implications.

Finland's controversial changes to its Electronic Communications Act will give employers right to monitor employees' email traffic if suspecting that they are leaking trade secrets.

The Finnish Parliament adopted on 4 March, with a majority of 96 over 56, changes to the existing Electronic Communication Act 516/2004. The amended law, which has been claimed to go against the Constitutional right to the privacy of communications, will come into force on 1 June this year.

The Act allows an employer to examine traffic data relating to employee emails if it suspects the leaking of trade secrets or any wrongdoing seen as particularly harmful to

Continued on p.20

Issue 98 **April 2009**

NEWS

2 - Comment
EU data breach notice law soon?

4 - News

Yahoo appeals Belgian fine • EU starts legal action against UK over Phorm • Swiss co-operate with OECD against tax evasion •

NEWS

6 - Deutsche Bahn scandal may spur changes to employee rights

7 - Strasbourg Court rules minor's privacy violated

8 - Japan's FSA considers data leak

ANALYSIS

9 - Privacy Trustmarks – don't be fooled

12 - Slow progress on APEC Privacy Initiative

14 - How influential will Ixquick be in the debate over search engines?

LEGISLATION & REGULATION

15 - Art 29 WP's new Opinion on clauses for 3rd-country transfers

18 - Queensland's Privacy Bill

- Canadian anti-spam bill

- US: new online advertising rules

19 - US two-year data retention bill

- UK: law on ISP data retention

21 - France: Bill to cut Web connection

- Germany: new restrictions on direct marketing

22 - Netherlands: DP Bill retains administrative burdens

26 - Will there be mandatory breach notification in the EU?

INTERNATIONAL newsletter
ISSUE NO 98 APRIL 2009

EDITORIAL DIRECTOR & PUBLISHER
Stewart H Dresner
stewart@privacylaws.com

EDITOR
James Michael
james.michael@privacylaws.com

DEPUTY EDITOR
Laura Linkomies
laura@privacylaws.com

ASIA-PACIFIC EDITOR
Professor Graham Greenleaf
graham@austlii.edu.au

NEWSLETTER SUBSCRIPTIONS
Glenn Daif-Burns
glenn@privacylaws.com

CONTRIBUTORS
David Fink and Henriette Tielemans
Covington & Burling
Lucy Fisher
PL&B Correspondent
Dugie Standeford
PL&B Correspondent
Chris Connolly
Galexia, Sydney, Australia
Yoshiyuki Omori and Eric Kosinski
White & Case, Tokyo
Nigel Waters
PL&B Correspondent
Hester de Vries
Kennedy van der Laan, Amsterdam

PUBLISHED BY
Privacy Laws & Business, 2nd Floor,
Monument House, 215 Marsh Road, Pinner,
Middlesex HA5 5NE, United Kingdom
Tel: +44 (0)20 8868 9200, Fax: +44 (0)20 8868 5215
Website: www.privacylaws.com

The *Privacy Laws & Business* International Newsletter is produced six times a year and is available on an annual subscription basis only. Subscription details are at the back of the newsletter. Whilst every care is taken to provide accurate information, the publishers cannot accept liability for errors or omissions or for any advice given. No part of this publication in whole or in part may be reproduced or transmitted in any form without the prior permission of the publishers.
Design by ProCreative +44 (0)20 8429 2400
Printed by Printflow Ltd +44 (0)20 7689 8697

ISSN 0953-6795

comment

EU data breach notice law soon?

Underlying at least some of the continuing transatlantic conflict over personal information is a European assumption that the United States simply does not care as much about privacy. After all, the first data protection laws were adopted by European countries in the 1970s, and the US still does not have even a realistic prospect of a comprehensive federal data protection statute. Data breach notification laws, forcing data controllers to tell people when their personal data have been lost, are a different matter, however: 44 US states now have them. There also is now a real prospect of an EU Data Breach Notification Directive, pending agreement over how bad the breach must be to require telling, who must tell, and who must be told (p.1) The discussion involves a new bit of data protection jargon: "notice fatigue" (when people tire so much of being told their data are lost that they no longer care).

Rules about what can and cannot be done with data about employees, customers and subscribers continue to attract attention. Finland adopts a new law for employers to monitor employees' email (p.1), while Deutsche Bahn faces criticism and possible prosecution for investigating 173,000 of its employees over several years (p.6). Switzerland and several other countries are beginning to relent on banking secrecy to disclose customer details in cases of suspected tax evasion (p.5). Yahoo is appealing against a Belgian fine for refusing to disclose users' identities to fraud investigators (p.4), while the European Court of Human Rights rules that Sweden violated the privacy of a minor when police were unable to force a service provider to identify for prosecution a subscriber who had posted a sexual advertisement about the child (p.7) The EU starts infringement action against the UK over Phorm advertising, which targets subscribers based on monitoring their online activities (p.4).

James Michael, Editor
PRIVACY LAWS & BUSINESS

Contribute to PL&B newsletters

Do you have a case study or opinion you wish us to publish? Contributions to this publication and books for review are always welcome. If you wish to offer reports or news items, please contact James Michael on Tel: +44 (0)20 8868 9200 or email james.michael@privacylaws.com.

Data breach, continued from p.1

just concluded a series of negotiations, facilitated by the Commission, intended to bring about a compromise solution (below we refer to the Commission, Council and Parliament collectively as the "Institutions").

We believe an EU breach notification regime would be positive for data protection in Europe. Such a requirement would help ensure that citizens are able to take steps to address potential harms arising from a breach concerning their personal data. A notice requirement might also incentivise service providers to enhance security. To be effective, however, breach notification rules must be designed to result in notices that are useful to recipients, that is, that contain information about risks of material harm. Service providers will incur costs from administering the breach notice system, and it would be unfortunate if these expenditures did not result in notices that are truly helpful for citizens. In this article, we provide an overview of the legislative proposals and recent developments, compare key aspects of the proposed measures with US practice, discuss potential interpretive issues, and consider whether additional legislation might be desirable.

The EU legislation

Breach notification would be introduced by amending the e-Privacy Directive (2002/58/EC), which regulates privacy in the electronic communications sector. Under Article 4 of the Directive, publicly available electronic communications services must take appropriate measures to ensure the security of their services. The Institutions would build on this obligation by requiring that service providers issue notice in the event of a "personal data breach". All the Institutions appear to be in agreement that a "personal data breach" means "a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of or access to personal data transmitted, stored or otherwise processed …".

Despite consensus on these basic points, the Institutions diverge in their approach to a number of important issues. While there is reportedly movement towards a compromise on some of these matters, they raise significant questions about the scope and purpose of breach notice.

First, European policy makers have been divided over which businesses should be subject to the requirement. The Council and the Commission would limit the measure to electronic communications services. While Member States differ in their interpretation of this term, it is generally understood to encompass ISPs and some web-based communications services.

However, influential voices in the data protection community, such as the European Data Protection Supervisor and the Article 29 Working Party, have called for a broader requirement. Parliament agreed, and it has supported extending the breach notification measure to "information society services", a category of service provider that includes most online businesses and search engines. The European Data Protection Supervisor has pointed out that covering information society services would bring important processors of personal data, such as online banks and online health providers, under the ambit of the requirement.

Others have countered, correctly we believe, that the e-Privacy Directive is not the appropriate instrument for a broad breach notice measure. The Directive's provisions are, in fact, predominantly geared to electronic communications services and network operators (telco companies). Breach notice requirements that are suitable for electronic communications services would not necessarily be appropriate for other businesses.

A second issue is the standard of harm that should trigger notice. In its original proposal, the Commission did not include such a standard, raising concerns that the issuance of immaterial notifications would confuse users and lead to "notice fatigue". All the Institutions now agree that notice should only be required if there is a risk of harm to an individual, but they differ on the precise formulation. The Council and the Parliament have supported language focusing on whether a breach presents a "serious" risk of harm, while the Commission's revised text calls for an analysis of whether "harm to the rights and interests of consumers is reasonably likely…".

Both privacy advocates and industry groups have weighed in on the debate, the former generally favouring a broader standard, while many in industry have pushed for a standard that is limited to material cases. A compromise may be emerging that would define the notification standard as "likely to adversely affect" an individual's privacy, while indicating that adverse effects should be understood to include serious harms such as theft or fraud, physical harm, significant humiliation or reputational damage. In our view, however, a "serious" risk standard would provide the best assurance that users will only receive notices concerning meaningful risks of harm. The alternatives, we fear, could lead to over-notification that would confuse users and possibly undermine confidence in the Internet.

A related issue is the question of which entity should determine if the standard has been met. The Council favours a self-assessment approach in which the service provider makes this determination. In contrast, Parliament is concerned that service providers might not correctly apply the law, and has instead called for Member State regulators to undertake the risk analysis. Critics have questioned, however, whether Member State authorities have the resources to carry out such assessments, which must also be done quickly to maximise their usefulness. The Czech Presidency of the Council is reportedly backing a compromise proposal in which service providers would have the initial responsibility for carrying out the analysis, but national regulatory authorities (NRAs) could also order service providers to issue notice. A key European Parliamentary committee has also recently voted in favour of such an approach. On balance, we believe service providers are best positioned to make the assessment as they have first hand information on the circumstances of the breach. We also share the concern that NRAs may not always be properly resourced to assess breaches,

Continued on p.24

Yahoo appeals Belgian fine

Yahoo! Inc. has appealed a 3 March Belgian court ruling fining the search engine for refusing to divulge users' identities in a fraud investigation, reports Dugie Standeford. While not centred on data protection issues, the case could prove tricky for Internet service providers seeking to shield user privacy in Belgium.

The litigation arose when Yahoo refused to provide the true identities of people using pseudonyms in Yahoo email addresses on the grounds that it is a US company and that such information should be requested through US authorities. The court in the northern town of Termonde fined the company €55,000 and an additional €10,000 per day until it complies with the order.

"We strongly disagree with the court's ruling," the company said. "Yahoo is a US corporation which has no business operations in Belgium and does not maintain the customer information at issue there. The US and Belgium have a Mutual Legal Assistance Treaty (MLAT) which the prosecutor should have followed to seek the personal data".

Yahoo "is not withholding information from the Belgian government," it said. "We have a legal and policy basis for not disclosing information in this type of case until the recognised international legal process is followed." Yahoo said it raised this issue with the US government.

The search engine claimed disclosure of users' personal information violates data protection principles, said Hogan & Hartson privacy attorney Wim Nauwelaerts. The court, however, held that privacy laws are not relevant because they protect individuals, not Internet service providers (ISPs), and that it is up to prosecutors to decide what information they need for investigations, he said. A central question is whether the prosecutor should have complied with the treaty, he added.

The court ruled that all ISPs physically or "virtually" present in Belgium that offer online services are subject to the criminal law obligation to supply information to prosecutors, Nauwelaerts said. Letting providers avoid those measures could encourage them simply to set up shop over the border to serve Belgian users, the court said.

A "crucial" issue in the appeal, therefore, will be whether or not Yahoo actually has a presence in Belgium, Nauwelaerts said. The court noted that Yahoo could have restricted access to its website, but cutting off an entire country could set a dangerous precedent.

"This decision could have negative implications for all foreign companies" by unduly expanding the reach of a law that should not apply to a company organised outside of, and without a presence in, Belgium, Yahoo said. Its appeal is expected to be heard in the autumn.

EU starts legal action against UK over Phorm

On 14 April the European Union took the first step in a legal action against the UK for failing to protect Internet users from Phorm, a behavioural advertising technology tested by BT without its customers knowledge in 2006 and 2007. The Commission said the U.K. had failed to enforce EU data protection rules because broadband Internet subscribers were not informed that their browsing was being tracked. The Commission opened an infringement proceeding against the United Kingdom after a series of complaints by UK internet users, and extensive communication by the Commission with UK authorities, about the use of Phorm by Internet service providers. The proceeding concerns the UK's implementation of EU ePrivacy and personal data protection rules, under which EU countries must ensure the confidentiality of communications by prohibiting interception and surveillance without the user's consent. These problems emerged during the Commission's inquiry into the UK authorities' action in response to complaints from internet users concerning Phorm.

"Technologies like internet behavioural advertising can be useful for businesses and consumers but they must be used in a way that complies with EU rules. These rules are there to protect the privacy of citizens and must be rigorously enforced by all Member States," said EU Telecoms Commissioner Viviane Reding. "We have been following the Phorm case for some time and have concluded that there are problems in the way the UK has implemented parts of EU rules on the confidentiality of communications. I call on the UK authorities to change their national laws and ensure that national authorities are duly empowered and have proper sanctions at their disposal to enforce EU legislation on the confidentiality of communications. This should allow the UK to respond more vigorously to new challenges to ePrivacy and personal data protection such as those that have arisen in the Phorm case. It should also help reassure UK consumers about their privacy and data protection while surfing the internet."

The Commission announced that since April 2008 it had received several questions from UK citizens and UK Members of the European Parliament concerned about the use of Phorm by Internet service providers in the UK. Phorm technology works by constantly analysing customers' web surfing to determine users' interests and then delivers targeted advertising to users when they visit certain websites. In April 2008 BT admitted that it had tested Phorm in 2006 and 2007 without informing customers involved in the trial. BT carried out a new, invitation-based, trial of the technology in October-December 2008. BT's trials resulted in a number of complaints to the UK Information Commissioner's Office (ICO) and to the UK police.

The European Commission wrote several letters to the UK authorities since July 2008, asking how they have implemented relevant EU laws in the context of the Phorm case. Following

an analysis of the answers received, the Commission expressed concerns that there are "structural problems" in the way the UK has implemented EU rules on the confidentiality of communications.

The UK has two months to reply to this first stage of an infringement proceeding, the letter of formal notice. If the Commission receives no reply, or if the observations presented by the UK are not satisfactory, the Commission may decide to issue a "Reasoned Opinion" (the second stage in an infringement proceeding). If the UK still fails to fulfil its obligations under EU law after that, the Commission will refer the case to the European Court of Justice.

Commissioner Reding said that EU rules are adequate to deal with new technologies, but that they are not always being properly enforced at national level. "European privacy rules are crystal clear: a person's information can only be used with their prior consent. We cannot give up this basic principle, and have all our exchanges monitored, surveyed and stored in exchange for a promise of 'more relevant' advertising. I will not shy away from taking action where an EU country falls short of this duty."

The head of Phorm insists that the technology does not store information to identify a user, that participants can opt out, and that it complies with the UK Data Protection Act and EU data protection rules.

On 4 April 2008 the Office of the Information Commissioner said that BT intended to run a trial of Phorm, and that "We will continue to maintain close contact with Phorm and BT throughout the trial. Clearly the trial should reveal whether this is a service that web users want, whether it is privacy friendly and that users are comfortable with the privacy safeguards put in place by Phorm."

On 20 April the ICO said "The ICO has been involved in discussions with Phorm regarding the technology's compliance with the DPA [Data Protection Act] and PECR [Privacy and Electronic Communications Regulations] only. A system such as Phorm can operate in a way which is in compliance with both these acts but must be sensitive to the concerns of users. Infor- mation must be provided to individuals that enables them to make a meaningful choice about whether or not to be involved in the use of the technology. The ICO will keep this technology under review as it develops."

Regarding the EU infringement action the ICO said "The ICO regulates and enforces the Data Protection Act, Freedom of Information Act and Privacy and Electronic Communications Regulations. These infringement proceedings from the EU appear to relate to the interception of communications, which is not part of the ICO's remit. Interception of communications is covered by the Regulation of Investigatory Powers Act, which is separate to the Data Protection Act and not regulated by the ICO."

Swiss co-operate with OECD against tax evasion

On 13 February Switzerland announced that it would assist other countries' tax authorities and re-define "tax evasion", after a similar announcement by Liechtenstein and Andorra the day before. Monaco followed the next week.

The governments agreed to cooperate with US authorities and those in other countries in investigating tax evasion, and in some circumstances to disclose data on accounts at banks within their jurisdictions. Along with Austria, Belgium, Luxembourg, Singapore and Hong Kong, the countries have told the OECD that they will abide by the standards outlined under Article 26 of the OECD's Model Tax Convention that requires the tax authorities to exchange information on request if there is probable cause to suspect tax evasion.

Switzerland, unlike the United States and many other countries, distinguishes between tax fraud and tax evasion, and does not consider tax evasion to be a crime. But by adopting the OECD definition, it will now cooperate with countries with which it has information-sharing treaties in pursuing tax evasion.

Other countries seeking Swiss co-operation must already possess names of clients suspected of tax evasion, and then ask Switzerland for assistance. "The privacy of foreign clients not under suspicion will continue to be protected by Swiss bank-client confidentiality," the Swiss Bankers Association said. "An automatic exchange of information is excluded." President Hans-Rudolf Merz told a news conference on 13 March: "We want assistance to be restricted to individual cases to prevent fishing expeditions."

Switzerland's largest bank, UBS, has already provided the US government with the details of 250-300 US taxpayers with UBS accounts, and paid $780 million to the US Internal Revenue Service and Securities and Exchange Commission to settle a pending criminal prosecution. The day after the payment was made the US Department of Justice asked the US District Court in Florida to order UBS to disclose the details of an additional 52,000 US taxpayers. That will be argued on 13 July. The Swiss government also announced on 13 March that it would participate in the US civil case against UBS to protect Switzerland's "sovereign interests".

The Swiss banking authority had authorised UBS to make the initial disclosure, but the Swiss administrative court has ordered UBS not to make any further disclosures. (*PL&B International*, February 2009, p.1) The bank and the government say that further cooperation would violate Swiss law.

In related developments, the Swiss Federal Criminal Tribunal on 30 March ordered bank account details to be given to the British Serious Fraud Office investigating bribery in Nigeria. The *Financial Times* reported on 27 March that Swiss banks were prohibiting international travel, including travel in Europe outside Switzerland, by executives, after the arrest of a UBS officer in the US last year. A Swiss Sunday newspaper reported on 12 April that Credit Suisse is giving US customers a choice between moving their accounts to a subsidiary that will disclose details to US authorities, and closing their accounts.

Deutsche Bahn scandal may spur changes to employee rights

German rail company Deutsche Bahn was caught spying on nearly all its employees for eight years. The resulting investigations could clarify employee privacy rights. **Dugie Standeford** reports.

Allegations of widespread monitoring of Deutsche Bahn (DB) employees surfaced in German newspaper *Der Stern* in January, according to various news reports. At the time, it was thought that around 1000 employees had been targeted, but the company soon admitted the spying involved some 173,000 of DB's 220,000 employees and 800 executives in the course of three major screenings in 1998, 2002-2003 and 2005-2006.

DB said the investigations were aimed at uncovering corrupt business deals between staff and suppliers. The company compared legally obtained employee bank data such as account names and numbers with those of suppliers to see if there were matches, a DB spokesman said. The search uncovered some instances where an employee and a supplier had the same accounts and the supplier was charging higher rates than competitors because of its connection with the employee, he said.

The company is also facing criticism for monitoring email traffic to and from its employees, not only to vendors but to journalists, said Axel Spies, a data protection and telecommunications lawyer with Bingham McCutcheon LLP. It is unclear whether the reportedly massive filtering of external and internal emails involved delving into content or simply using normal software filtering in accordance with a 2008 agreement between DB and the Works Council, said CMS Hasche Sigle partner Christian Runte. Former DB CEO Helmut Mehdorn, who stepped down on 31 March because of the scandals, said monitoring the sender, receiver and subject lines of emails, but not the content, is a common practice, the company spokesman said

The furore sparked three separate investigations. DB management and public prosecutors have already presented an interim report to the relevant parliamentary committee, the company spokesman said. DB's supervisory board commissioned a probe by KPMG and a two former government ministers, he said. A third investigation, by employee unions, is under way.

On 1 April, Berlin Data Protection Commissioner Alexander Dix sent a "preliminary final report" to DB which, however, does not address the alleged email filtering allegations, Runte said. The company has until 21 April to respond. On 7 April, CEO-designate Ruediger Grube promised a full review of the data protection issues and asked for a report by 1 June, the DB spokesman said.

Grey areas

DB's predicament raises several data protection questions, the company spokesman said. Chief among them are whether the sheer volume of banking data checked was not proportionate to the need to fight corruption, and whether, under German data protection rules, the company should have informed workers, unions and employee bodies of the probe, he said.

Another question is whether organisations can legally use such monitoring to fight corruption, the spokesman said. The state prosecutor has not yet issued any accusations, he said. Still another zone of uncertainty is what level of suspicion a business can reasonably have before it conducts mass surveillance, he added.

There are growing concerns and awareness in Germany about email and telephone surveillance by employers, Spies said. That is increasing pressure on the legislature to pass an employee data protection act that has been under discussion for years, he said. Employee privacy matters are now covered by the general Federal Data Protection Act, case law, inter-company agreements and individual employment contracts, he said: "There are a lot of grey areas."

DB not alone

The rail company surveillance has been compared to recent incidents at Deutsche Telekom and supermarket chain Lidl, but they are not the same because DB only accessed bank information lawfully in its possession, the company spokesman said. The Deutsche Telekom case involved allegations that telephone call records were monitored to stop damaging leaks by board members to journalists (see *PL&B International*, June 2008, p.1). Lidl came under fire for installing hidden cameras and hiring investigators to watch for possible employee thievery, Runte said.

It is not that data protection and security have worsened in Germany but that until recently, "no one cared" or took it seriously, he said. Germany has the reputation for being strict on privacy, but in fact it lacks a centralised data protection authority and some of its local bodies are "seriously understaffed" or not as effective as they could be.

German organisations seeking legal advice on data privacy issues used to say, "This is complicated. What could happen to me if I don't do it?" Runte said. That was before data protection authorities could impose hefty fines. Now, when clients think about introducing surveillance measures, Runte advises them not only to adhere to the law but to be "super-careful" about involving all relevant interests in the decision. Consulting data protection authorities is the safest way of ensuring a proposed scheme is legal, he added.

Strasbourg Court rules minor's privacy violated

Unidentified person posted sexual advertisement about a minor. Subscriber who posted abusive advertisement not identified for prosecution. By **James Michael**.

The European Court of Human Rights in Strasbourg ruled in December that Finland had violated the right to privacy of a twelve-year-old boy by not disclosing the identity of someone who had posted a sexual advertisement about him on an Internet dating website. Although Finland has since changed the law (in 2004), in 1999 the police and prosecuting authority had no power to order the identification of the person who had made the posting, as confirmed by the Finnish Court of Appeal, and the Supreme Court, which refused leave to appeal.

The Finnish District Court noted that under the Coercive Measures and the Protection of Privacy, and Data Security in Telecommunications Acts the police had the right to obtain telecommunications identification data in cases concerning certain offences, but the "calumny" charged in this case was not such an offence. The managing director of the Internet service provider might have been prosecuted under the Personal Data Act for publishing a defamatory statement on the website without verifying the identity of the sender, but the Act only went into effect in June 1999, and the posting was in March of that year.

The Strasbourg Court considered Recommendations of the Council of Europe Committee of Ministers, the Council of Europe Cybercrime Convention, UN General Assembly Resolutions, the EU Data Retention Directive and comparative national laws in several countries, all of which provide for disclosure of subscriber information in the investigation of serious crime.

Although the posting was done by a private individual, the Court said that a state had a positive obligation to provide a remedy against such an invasion of privacy. "[P]rivate life" covers the physical and moral integrity of the person, and although the sexual advertisement was seen in Finnish law as "calumny", the Court preferred to highlight the physical and moral integrity aspects of private life, "having regard to the potential threat to the applicant's physical and mental welfare brought about by the impugned situation and to his vulnerability in view of his young age." The Court said that Article 8 does not merely compel the State to abstain from interference: private life: "in addition to this primarily negative undertaking, there may be positive obligations inherent in an effective respect for private or family life… [E]effective deterrence against grave acts, where fundamental values and essential aspects of private life are at stake, requires efficient criminal-law provisions."

In this case "The act was criminal, involved a minor and made him a target for approaches by paedophiles." As to the mere existence of the criminal offence of calumny and the possibility of bringing criminal charges or an action for damages against the server operator, the Court noted that the existence of an offence has limited deterrent effects if there is no means to identify the actual offender and to bring him to justice. The Court considered that "practical and effective protection of the applicant required that effective steps be taken to identify and prosecute the perpetrator, that is, the person who placed the advertisement. In the instant case such protection was not afforded. An effective investigation could never be launched because of an overriding requirement of confidentiality. Although freedom of expression and confidentiality of communications are primary considerations and users of telecommunications and Internet services must have a guarantee that their own privacy and freedom of expression will be respected, such guarantee cannot be absolute and must yield on occasion to other legitimate imperatives, such as the prevention of disorder or crime or the protection of the rights and freedoms of others… Finland's positive obligation with respect to the applicant could not be discharged. This deficiency was later addressed. However, the mechanisms introduced by the Exercise of Freedom of Expression in Mass Media Act … came too late for the applicant."

The Court found that there had been a violation of Article 8 and awarded €3,000 for non-pecuniary damage. Nothing was awarded for legal costs because no documentation had been submitted. (*K.U. v. Finland*, application no. 2872/02, 2 December 2008)

Analysis

The case demonstrates an increased willingness by the Court to deal with privacy issues involving the state, as in the *Marper* ruling, holding that the UK violated Article 8 by its DNA database including people not convicted of any crime (*PL&B International,* December 2008, p.14), and regarding the state's positive obligation to provide remedies for privacy violations in the private sector in cases such as *Hannover. v. Germany*, involving invasions of privacy by press photographers, and, more recently, the case of *Reklos v. Greece*, in which the Court found a violation in the absence of a remedy for invasion of privacy by a photograph of a day-old baby that was never published (p.8).

The question of whether Internet service providers should be required to identify subscribers, or at least their IP addresses, is now before the courts in Belgium, where Yahoo is being fined for not making such a disclosure in a fraud investigation (see p.4). In the *Promusicae* case, the European Court of Justice said that it was up to indi-

vidual states to decide whether service providers should be required to disclose identities of file-sharers to copyright enforcers (*PL&B International,* February 2008, p.21). The distinction made by the Spanish authorities in that case was between criminal investigations, in which identification could be required, and civil cases, where it could not. The Council of Europe Cybercrime Convention similarly concentrates on a duty to co-operate in criminal investigations, and is silent on co-operation in civil matters.

The distinction is attractive, but flawed. Defamation in common law countries is usually civil (except for criminal libel), but in many civil law countries is criminal ("calumny" was a crime in Finland, as the case reports). Copyright enforcement can be both civil and criminal. If the distinction is made between requiring co-operation in protecting human rights, such as privacy in this case, and not to protect other rights, such as intellectual property, there remains one problem: Article 27 of the Universal Declaration of Human Rights says that intellectual property is also a human right.

STRASBOURG RULES UNPUBLISHED PHOTO BREACHES PRIVACY RIGHTS

The European Court of Human Rights has ruled that taking a photograph, which was never published, without permission, of a one-day-old child violated the baby's right to privacy. This has serious implications for journalism and security in the UK, and it cost the Greek government €8,000.

The case was decided on 15 January, and attracted very little attention in the UK, perhaps because the judgment was only in French (although there was an English press release). It involved a baby in a private Greek hospital who was placed after birth in a sterile room, to which only doctors and nurses were admitted – and a photographer, allowed by the hospital to take photos of newborn infants to sell to the parents. The hospital had informed parents of his services.

The parents of Anastasios Reklos (although the Strasbourg court normally does not name children in cases) emphatically did not want to buy the photos. They objected to the fact that their baby had been photographed, and demanded the negatives (this was in 1997, when digital cameras were rare). The hospital refused. The parents sued.

In the Greek courts the parents lost, largely because the courts thought that a one-day-old baby was not developed enough to have any privacy rights. The parents appealed to Strasbourg, arguing that if privacy rights depended on maturity it would mean that people with various forms of disability would have fewer privacy rights.

The Court said that the Human Rights Convention can be violated by individuals as well as by states, and that states can be held responsible for allowing such violations (as Germany was responsible for allowing publication of photos of Princess Caroline of Monaco). It went on to emphasise that the baby was in a place with very restricted access, and that the photograph was a deliberate act, photographing only the baby, face forward. It did not matter that the photos were never disseminated in any way – the violation was in taking the photographs.

The parents had not consented, and the baby was not a public figure of any kind, which might have justified photography. Refusing to hand over the negatives not only made the violation worse, it raised the possibility of future publication.

The parents asked for €36,000 in compensation for 'moral damage' (they had asked for 11,739 (in drachma equivalent) in the Greek courts in 1997. The Greek government said it should be no more than €5,000. The court awarded €8,000. The parents did not ask for costs of legal representation, perhaps because Dimitrios Reklos, of the Athens bar, the father, was representing the family (*Reklos v. Greece*, application no.1234/05, 15 January 2009).

Implications for other countries

What does this mean for countries other than Greece? The 56 other countries in the Council of Europe (quite separate from the European Union) are also bound by the Strasbourg court's interpretation of the European Convention on Human Rights. If the courts in those countries do not follow the interpretation in this case, the parents of a newborn baby photographed in a private place without their consent can go to Strasbourg and win if they lose in their country's courts. It means that photographers who photograph people in non-public places without their consent can be liable even if the photographs are never published. But photographing babies and other people in non-public places who are "public figures" may be ok.

For security surveillance, the case means that just capturing a person's image without consent in a non-public place will be wrong, even if it is never published in any way. The Court has yet to decide whether "consent" is obtained by posting the ubiquitous 'CCTV recordings' signs.

Japan's FSA considers data leak at Mitsubishi UFJ Securities

On April 8, 2009, Mitsubishi UFJ Securities Co., Ltd. ("MUFJ") announced that one of its systems engineer employees had taken personal data of 1,486,651 MUFJ customers off company premises and sold the personal data of 49,159 of the customers. At the time of the illicit copying from company computers, which is said to have been between 26 January and 4 February 2009, the system engineer was one of the limited number of employees at MUFJ who was given a password providing access to the data base. The misappropriated data contained names, addresses, telephone numbers, gender information, birthdays, occupations, yearly incomes, places of work, etc. According to a 9 April 2009 article in the *Yomiuri* newspaper, the employee emailed the data to three data merchants and the information eventually came to be possessed by 13 companies, including sellers of futures and real estate. MUFJ became aware of the leak after a series of customer complaints in March. As of 9 April 2009, MUFJ was trying to obtain promises from the 13 recipient companies to destroy the data.

MUFJ announced that it punitively fired and is preparing to file a criminal complaint against its former systems engineer. According to the *Yomiuri* newspaper, the former employee claims he needed the ¥328,000 (about $3,280) proceeds from the sale of the data to help pay off his consumer debt.

Continued on p.27

Privacy Trustmarks – don't be fooled

'Surprising and alarmingly high proportion of inaccurate and out-of-date information.' By **Chris Connolly**.

Privacy "whitelists" are published by trustmark schemes to help identify which organisations have been certified as compliant members of their scheme. If an organisation is on the list, consumers may have an increased level of confidence that they will be covered by the rules of the trustmark scheme, including privacy protection and dispute resolution. Consumers can also use the whitelists to check that the use of the trustmark is valid, as a significant proportion of trustmarks that appear on websites are often fake or expired.

There is a trend towards the global expansion of whitelists, and there is a proposal to develop an APEC whitelist of organisations that comply with the APEC Privacy Framework Cross Border Privacy Rules.

This article summarises a Galexia study of whitelists published by trustmark schemes (surprisingly, not all trustmark schemes publish whitelists). The study only examined whitelists where the trustmark operators claim that organisations on the lists have passed strict verification of privacy protection standards. Also, the study only examined whitelists that have some form of Government backing, oversight or approval. Only six published whitelists meet all of these criteria, and the Galexia study excluded one whitelist (ESRB) because it was limited to one very specific type of product (computer games).

This resulted in a study of five whitelists ranging from nine to 340 members. Where the published whitelist was larger than 300 entries Galexia studied 50% of the members on the list. For all other whitelists Galexia studied every entry on the list.

The study included the "Government oversight" criteria, as Galexia considers there are risks for consumers where Governments lend credibility to trustmark schemes and whitelists without adequate quality control and regulation in place.

Overall the study found that privacy whitelists contained an alarming proportion of inaccurate and out-of-date information. Depending on the trustmark scheme administering the white- list, between 22% and 73% of information is inaccurate or out of date.

WHITELISTS IN THE STUDY

Mexico – the AMIPCI Trust Mark. In Mexico a generic e-commerce trustmark is in operation that includes some privacy requirements. The trustmark is administered by AMIPCI (Mexican Internet Association) with some Government funding and support. There are approximately 278 members and information is available in Spanish and English.

The AMIPCI rules state that all certified members must: "Comply with the provisions of the guidelines or principles on privacy of APEC information, also known as Asia-Pacific Economic Cooperation (APEC)."

Table 1 shows the findings of Galexia study.

A cumulative total for each table has been included so that organisations are only counted as non-compliant once, even though they may be non-compliant across several categories.

The Galexia study of the AMIPCI trustmark also tested whether the claim that organisations comply with the APEC Privacy Framework is valid, as this is the privacy standard required by AMIPCI. The APEC Privacy Framework contains nine high-level Principles and it is quite complex to test a privacy policy against all of them. However, Principle 2: Notice, is relevant to website privacy policies and does contain an item that is easy to check – item (e) regarding notice of access and correction rights and processes:

"Personal information controllers should provide clear and easily accessible statements about their practices and policies with respect to personal information that should include: (e) the choices and mean the personal information controller offers individuals for limiting the use and disclosure of, and for accessing and correcting their personal information."

Some sites have a privacy policy, but 68 of the AMIPCI trustmark sites (30%) did not comply with the one APEC Privacy Principle that Galexia was able to check (Principle 2: Notice, regarding access rights). Many of the privacy policies are only one paragraph long and it is difficult to understand how they can have been certified by AMIPCI as compliant with the APEC Privacy Framework. While the APEC standard is weak, it cannot be complied with in a one paragraph privacy policy. A more thorough examination of AMIPCI members is likely reveal an

TABLE 1: MEXICO

Issue	Test	Non-Compliance
No working seal	A working seal does not appear on the organisation's website	5%
Membership has expired	The membership is not current	5%
Privacy policy not available	The organisation's privacy policy is not available	17%
Overall non-compliance	Cumulative total	23%

TABLE 2: SINGAPORE		
Issue	**Test**	**Non-Compliance**
No working seal	A working seal does not appear on the organisation's website	45%
Membership has expired	The membership is not current	14%
Privacy policy not available	The organisation's privacy policy is not available	26%
Overall non-compliance	Cumulative total	54%

even lower level of compliance.

AMIPCI strengths:

- The AMIPCI whitelist is available to the public;
- Data is relatively up-to-date (although a few seals had expired, no expiry was more than three months old);
- Information is available in multiple languages;
- A deep verification link is provided wherever the seal appears; and
- Privacy standards are published (although only in the form of a link to APEC).

AMIPCI weaknesses:

- Many of the privacy policies were very short (one paragraph only); and
- AMIPCI overstates compliance with the APEC Privacy Framework.

Singapore – CommerceNet

The Singapore Government promotes a generic e-commerce trustmark known as TrustSG. It is provided by multiple organisations, the largest of which is CommerceNet Singapore. It is a generic ecommerce seal with short privacy requirements. There are approximately 340 members.

TrustSG is an initiative of the National Trust Council (NTC). The council is industry led with support from the Government through the Infocomm Development Authority of Singapore (IDA).

When a consumer clicks on the trustmark a verification page appears with the following statement:

This member has been awarded the TrustSg seal as it adheres to the Code of Practice set by CommerceNet Singapore Ltd to promote good e-business practices.

To save time, the Galexia study examined the first 168 organisations on the CommerceNet whitelist (50% of the total). The Galexia study did not examine the remaining smaller provider of TrustSG seals in Singapore.

Table 2 shows the findings of the Galexia study.

It was difficult to study the CommerceNet whitelist as it is out-of-date. The list was visited on numerous occasions between February and April 2009 and it was clear that the expiry dates listed on the site were not being updated or maintained. At the time of completion of this article (14 April 2009) the CommerceNet whitelist describes ALL members as "expired".

This is a good example of the problems consumers may have when relying upon out of date whitelists. For the purposes of the study Galexia visited each site and clicked on the seal (where available). The expiry date was checked by analysing the verification page, rather than relying on the whitelist.

CommerceNet strengths:

- The CommerceNet whitelist is available to the public;
- The privacy seal is self-served (served from CommerceNet's domain) and is considered current best practice;
- A deep verification link is provided wherever the seal appears; and
- The privacy standards are published.

CommerceNet weaknesses:

- The entire whitelist is out of date (it shows that all seals have expired);
- A very high proportion of sites were not displaying the seal at all.

TABLE 3: THAILAND		
Issue	**Test**	**Non-Compliance**
No working seal	A working seal does not appear on the organisation's website	18%
Membership has expired	The membership is not current	36%
Privacy policy not available	The organisation's privacy policy is not available	18%
Overall non-compliance	Cumulative total	73%

Thailand

The Thailand Department of Business Development (part of the Ministry of Commerce) runs a generic ecommerce seal with one privacy provision (sites must have a privacy policy). It has around 22 members and information is available in English and Thai.

Table 3 shows the findings of the Galexia study:

Department of Business Development strengths:

- The Department of Business Development whitelist is available to the public;
- Information is available in multiple languages;
- A deep verification link is provided wherever the seal appears; and
- Privacy standards are published.

Department of Business Development weaknesses:

- The privacy standards are very low – only requiring publication of a privacy policy; and
- A high proportion of seals had expired.

USA – Privo

Privo's Privacy Assurance Program is a specific privacy seal with particular focus on children's privacy requirements. Privo has 9 members. A whitelist is not published, although there is a page of company logos for sites accompanied by the following text:

"Click on any of the logos below to check out our newest PrivoLock-enabled websites or Privo certified sites!"

Privo was approved as a trustmark scheme for compliance with the Children's Online Privacy Protection Rule (COPPR) in 2004. Privo highlights this FTC approval on their front page and numerous other pages of their website:

Privo is the first and only infome-

diary service to be recognised by the Federal Trade Commission (FTC). "As an FTC-designated Safe Harbor, it is our responsibility to ensure compliance with current federal and proposed state privacy laws. Privo is an FTC-approved, neutral third-party service provider."

Does the FTC approval mean that consumers can rely on sites that claim to be Privo members, or rely on the list of approved sites on the Privo website? Privo only has nine members and even with this small number there is minimal compliance and poor quality control.

Table 4 shows the findings of the Galexia study.

In addition, Privo does not publish any information at all regarding their standards for approving a website, and they provide no information (or even contact details) regarding reporting breaches and dispute resolution.

Privo strengths:

- A deep verification link is provided wherever the seal appears (although some links were broken or contained basic errors).

Privo weaknesses:

- No privacy standards are published;
- The whitelist is a series of company logos rather than organisation names or URLs; and
- Privo overstates the significance of their FTC approval considering the lack of information on concerning privacy standards and dispute resolution on their website.

USA – TRUSTe

Children's Privacy Seal

TRUSTe offers a Children's Privacy Seal – a specific privacy seal with special children's privacy requirements. It has approximately 41 members (although this includes multiple sites belonging to a single organisation such as Disney).

TRUSTe (like Privo) is approved as a trustmark scheme for compliance with the Children's Online Privacy Protection Rule (COPPR), and they highlight this Government approval on their website:

"The Federal Trade Commission has approved TRUSTe as a COPPA Safe Harbor programme. The TRUSTe Children's Seal certifies that your business is compliant with the COPPA Rule – letting parents know that their kids' information is safe."

TABLE 4: USA PRIVO

Issue	Test	Non-Compliance
No working seal	A working seal does not appear on the organisation's website	44%
Membership has expired	The membership is not current	44%
Privacy policy not available	The organisation's privacy policy is not available	0%
Overall non-compliance	Cumulative total	55%

However, this Government approval does not mean that privacy protection is assured – TRUSTe has the same issues with broken and missing seals and expired members as other trustmark schemes.

Table 5 shows the findings of the Galexia study.

The TRUSTe whitelist does not publish expiry dates, so the Galexia study assumes all working seals are current.

The Galexia study also examined whether member sites still describe TRUSTe as non-profit, as this is an ongoing concern with TRUSTe.

On 15 July 2008 TRUSTe changed its status from non-profit to for-profit and accepted investment from Accel – part-owners and Directors of Facebook. Nearly a year after the change the majority of TRUSTe members still retain the standard (old) TRUSTe wording in their privacy policies:

"XYZ is a licensee of the TRUSTe Web Privacy Seal Program. TRUSTe is an independent, non-profit organisation whose mission is to build user's trust and confidence…"

The Galexia study found that 29 out of the 51 sites still claim that TRUSTe is non-profit. This misleading information should be corrected.

TRUSTe strengths:

- The TRUSTe whitelist is available to the public;
- A deep verification link is provided wherever the seal appears;
- Privacy standards are published; and
- All sites had published privacy policies.

TRUSTe weaknesses:

- No expiry dates are published;
- A high proportion of links were broken (although sites could still be located through searches); and
- A large number of sites still incorrectly claim that TRUSTe is non-profit.

Summary of findings

Overall the study found that privacy whitelists contained a surprising and alarmingly high proportion of inaccurate and out-of-date information. Depending on the trustmark scheme administering the whitelist, between 22% and 73% of information is inaccurate or out of date. If a consumer relied on the whitelists they would face the risk that they would receive no privacy protection from the trustmark scheme as the organisation's membership had expired. Similarly the enormous number of missing or broken seals means that consumers are unable to verify membership for a large number of organisations.

This finding raises concerns about the use of whitelists as a privacy protection mechanism and adds to more general concerns regarding privacy trustmarks and self regulation.

TABLE 5: US TRUSTE CHILDREN'S PRIVACY SEAL

Issue	Test	Non-Compliance
No working seal	A working seal does not appear on the organisation's website	22%
Membership has expired	The membership is not current	n/a%
Privacy policy not available	The organisation's privacy policy is not available	0%
Overall non-compliance	Cumulative total	22%

SUMMARY OF FINDINGS					
Compliance issue	**Mexico – AMIPCI**	**Singapore – CommerceNet**	**Thailand – DBD**	**USA – Privo**	**USA – TRUSTe (Children)**
Number of organisations in the sample	278	168	22	9	41
No working seal	5%	45%	18%	44%	22%
Membership has expired	5%	14%	36%	44%	n/a
Privacy policy not available	17%	26%	18%	0%	2%
Overall non-compliance	23%	54%	73%	55%	22%

It is also alarming that all of the whitelists examined in this article received Government approval. The two US whitelists were both accredited by the Federal Trade Commission (FTC) and the other lists receive Government funding and high-level endorsement. There are risks for consumers in having Governments lend this type of credibility to trustmark schemes and whitelists without adequate quality control and regulation in place.

AUTHOR

Chris Connolly is a Director of Galexia, an independent consultancy specialising in privacy and electronic commerce. www.galexia.com.au

Slow progress on APEC Privacy Initiative

Cross-border Privacy Rules similar to EU Binding Corporate Rules. By **Nigel Waters**.

The work of the APEC Privacy Sub-group, last reported in *PL&B International* in February 2007 (p.14), has progressed with a further meeting, and an associated two-day seminar in Singapore in February 2009 (Singapore is this year's host for all APEC meetings). This followed the two Sub-group meetings in Lima, Peru, in 2008. The Sub-group is primarily focused on progressing a Cross Border Privacy Rules (CBPR) approach to implementing the APEC Privacy Framework for transfers of personal data by individual businesses, but is also supporting domestic implementation of the Framework by APEC member economies.

February 2009 APEC seminar

The February seminar comprised open sessions on current developments followed by a day of detailed discussion of the various Pathfinder projects which are designing and testing the CBPR approach.

The UK Information Commissioner, Richard Thomas gave a frank assessment of the merits and drawbacks of the contrasting EU and APEC approaches to privacy protection, emphasising the degree of common ground and calling for greater dialogue with a view to convergence and greater cooperation. He saw the APEC CBPR Pathfinder as covering very similar ground to the EU Binding Corporate Rules work, and raising very similar issues. The EU Data Protection Directive is currently under review and the opportunity exists for progress towards a best practice global model if the proponents of the EU and APEC approaches are prepared to acknowledge legitimate criticisms and concerns and cooperate on designing a new approach.

In a session on Trustmarks, Chris Connolly of Galexia Consulting summarised his research findings on the weaknesses of a sample of trustmark schemes. Representatives of TRUSTe and of the US Department of Commerce acknowledged that a number of the Galexia criticisms were fair in relation to other schemes, but not in relation to TRUSTe, which remains a key participant in the Pathfinder and an obvious candidate for Accountability Agent role in the US in any long term implementation of the CBPR approach. TRUSTe and AMIPCI (Mexico) dispute some of Galexia's findings and have challenged its methodology.

Sessions on governance saw a consensus on the importance of addressing a range of key issues such as independence, transparency, ongoing monitoring and the relationship to existing domestic legislation, and identified that progress had only just begun on the necessary work (Project 8). Guidelines and criteria for public sector accountability agents (part of Project 2) are closely related to the governance work.

Seminar sessions on the Pathfinder demonstrated continued confusion amongst participants as to the objectives and scope of self-certification and compliance review (Projects 1 & 3). It remains unclear whether an organisation will be tested on its compliance with all of the Principles in the APEC Framework or only those aspects of the Principles that relate directly to cross-border transfer. If the latter, how realistic is it to separate out cross border aspects, and to present this clearly to consumers? Will the answers to the questions be meaningful at a general organisational

policy level, and if not, how realistic is it to expect organisations to complete, and consumers to understand, multiple CBPRs for different products, services or types of personal data?

The work on cross-border enforcement co-operation (Projects 5-7) is showing signs of progress with a very useful draft Cooperation Agreement. Subject to resolution of concerns about re-use of information shared between Enforcement Agencies, this agreement could prove very valuable across the board of cooperation, independently of any CBPR system.

The test stage of the Pathfinder (Project 9) is expected to commence in April 2009, with trustmark schemes in Mexico, Chinese Taipei [Taiwan] and the USA, and several of their members, having agreed to participate in the Project 1&3 testing, and several Enforcement Authorities committed to testing other aspects.

The APEC Sub-group meeting

The closed APEC privacy Sub-group meeting on 24 February was mainly a "report-back", and no significant decisions were made for ratification by the parent Electronic Commerce Steering Group (ECSG). The meeting noted the progress on the various Pathfinder projects, and committed to further engagement with the OECD, EU and Council of Europe – including potentially a meeting in Madrid in November adjacent to the International Commissioners Conference.

The Philippines, Peru, Thailand, Mexico, Malaysia and Chinese Taipei [Taiwan] all reported privacy or data protection legislation at varying stages of consideration, with both EU and APEC based models still being considered in some jurisdictions.

Fourteen economies have now submitted an Individual Action Plan (IAP), as required by the APEC Privacy Framework, but these have still not been published (except for the USA Plan which is on the website for the February 2006 meeting) – renewed efforts will be made to get them all onto the APEC website.

The Chair of the Sub-group has now initiated email discussion on further domestic implementation work.

Work on development and testing of the components of the CBPR approach will continue before the next (late July 2009) Sub-group meeting, through an inter-sessional Study Group and various subordinate working groups, operating by email and telephone conferences.

Civil society concerns

Civil Society representatives have been participating in the APEC process since 2003 as "critical observers". At the International Data Protection and Privacy Commissioners Conference in Strasbourg in October 2008, the civil society position was allegedly misrepresented as "support" for the Cross Border Privacy Rules approach to implementation of the APEC Framework. A clarifying statement was circulated in October 2008 to those involved in the APEC processes, the main points of which were:

(a) Civil Society has not endorsed either the APEC Privacy Framework or the Pathfinder process.

(b) Civil Society has very limited expectations of the Pathfinder process and it remains unclear to us whether it can produce anything of value other than better cooperation between national authorities, which would be very valuable. We also remain concerned that the Pathfinder could lead to undesirable outcomes in terms of either lower standards of privacy protection and/or misleading compliance claims.

(c) However, Civil Society considers that it needs to be aware of what is happening in the APEC privacy processes, and therefore welcomes opportunities to participate in sub-group meetings when limited resources allow. While attending it is our policy to make constructive suggestions where appropriate, but these do not represent either support or expectations of successful outcomes.

The February 2009 meetings did little to satisfy Civil Society concerns about the CBPR approach. What Civil Society representatives see as insuperable problems in relation to governance and enforcement are recognised by the proponents but only as challenges to be overcome. Civil Society remains sceptical as to whether CBPRs will, overall, offer any net benefit to consumers.

Civil Society's strong preference remains comprehensive privacy legislation with higher standards; independent data protection or information privacy authorities; conditions on the transfer of personal information to third countries and effective enforcement mechanisms.

Accountability also a focus

Accountability is a key principle both in the new APEC Framework and the older OECD Guidelines, yet remains an elusive concept, clearly meaning different things to different stakeholders. The Galway Project initiative, organised by The Center for Information Policy Leadership (CIPL) at Hunton & Williams LLP and the Irish Data Protection Commissioner, is "a collaborative process to develop a white paper articulating essential, commonly-accepted elements required of a company to establish and demonstrate accountability for its information processes." Following an initial experts meeting in Dublin in January, a further meeting will be held on 28 April in Galway, sponsored by the OECD. The project aims to provide its white paper to the OECD Working Party on Information Security and Privacy, the APEC Data Privacy Sub-group and the EU Article 29 Working Party later in 2009. Anyone interested in the evolution of international privacy standards, including the APEC Framework, should also follow the progress of the Galway Project – CIPL were also consultants to APEC during the drafting of its Privacy Framework.

INFORMATION

For APEC source documents, see the APEC website at www.apec.org/apec/apec_groups/committee_on_trade/electronic_commerce.and find the detailed papers by browsing the meetings document database for specific meetings. Chris Connolly's paper *Trustmark Schemes Struggle to Protect Privacy* may be found at www.galexia.com/public/research/articles/research_articles-pa07. Details of the Galway Project are at www.huntonfiles.com/files/webupload/CIPL_Galway_Conference_Summary.pdf.

AUTHOR

Nigel Waters represents Privacy International (PI) at meetings of the Privacy Sub-Group. PI was granted independent guest status for the first time at the February meeting.

How influential will Ixquick be in the debate over search engines?

Awarded first Euro privacy seal, a little-known 'metasearch engine'. **Lucy Fisher** investigates.

Having spoken to a number of privacy lawyers, compliance professionals and IT experts, I discover there is a surprising lack of awareness about Ixquick, the Dutch metasearch engine which announced earlier this year that it would no longer store users' IP addresses. This is despite the confident words of the company's chief executive, Robert Beens. "Using a search engine is sharing your innermost secrets and habits ... Ixquick has the best privacy policy of the search industry," he claims.

Last July, the company was awarded the first EuroPriSe privacy seal, following an independent privacy review. Effectively, this promises users that its services present no threat to their right to privacy. Certainly it represents a positive move in terms of raising privacy awareness itself, however little known the search engine might be.

A lack of understanding

But the correct term "metasearch engine" is not widely understood. Google's Global Privacy Counsel, Peter Fleischer, points out that there is an important difference between search engines such as Yahoo! and Google, and metasearch engines like Ixquick, which enter search queries into other search engines and then aggregate the results.

Therefore, he says, Ixquick has far less of a need to operate the same types of retention and statistical analysis practices of real search engines. And, in turn, it has less of a need for individual users' IP addresses in order to function optimally. "Imagine if a travel agency that sells aeroplane tickets issued promotional material that says it generates less pollution than any major airline. Readers would laugh at that, because a travel agency doesn't actually fly a plane. It just sells or resells a ticket from the company that flies the plane," Fleischer explains.

And he is not the only privacy professional who could be excused for feeling frustrated by the lack of widespread understanding surrounding Ixquick's flaunted privacy credentials. "It is a pity that no-one is aware of the difference. People just don't know what a metasearch engine is," adds Véronique Grouard, EMEA Privacy Attorney, Microsoft EMEA. "Ixquick exists because of the search engines; it relies on information from the search engines. We are not really competitors."

Calls for greater clarity

So major search engines appear not to be threatened by Ixquick's arrival; rather they are eager to explain that they cannot be directly compared. However, as far as Europe's Article 29 Data Protection Working Party (WP) is concerned, the search engines themselves could also be far clearer when it comes to effectively communicating their working practices and business models to users. According to the WP's opinion on data protection issues related to search engines, published last year: "Search engines in their role as collectors of user data have so far insufficiently explained the nature and purpose of their operations to the users of their services."

Many agree that their complex privacy notices leave a lot to be desired. According to Chris Parkinson, Group Compliance Director at database and digital marketing company The Lateral Group: "A lot of people aren't aware of the amount of information search engines like Google store on you, nor that the ads around your search results are targeted."

Limited uptake

Parkinson, like many others, had never heard of Ixquick before we spoke. Despite the fact that he finds it an interesting initiative, he believes that consumers have become very used to targeted ads on search engines, accepting terms and conditions that they never have fully understood. "There's definitely a lack of awareness. People have got so used to targeted ads that they may actually complain if they don't get them," he warns.

Even the IT and privacy cognoscenti have been found lacking when it comes to an in-depth understanding or direct experience of this metasearch tool and how it compares to the major search engines. Martyn Thomas, visiting professor of software engineering at the Oxford University Computing Laboratory, and a fellow of the Royal Academy of Engineering, is one of the exceptions. "I use Ixquick as my main search engine and find it effective. Other search engines keep far too much data and serve up adverts that I don't want. I have asked around my privacy-aware colleagues and find that some haven't heard of it and others haven't got round to switching," he says.

The retention debate

This widespread lack of awareness may not be so surprising given that the debate around for how long search engines should reasonably store IP addresses has only in recent months reached a crescendo. Google announced in 2007 that it would stop keeping logs indefinitely and would delete them after 18 to 24 months. Privacy activists then asked why all search engines had been keeping them for so long anyway. In turn, last September Google reduced its retention period to nine months, and Yahoo! announced in December that it would retain addresses for 90 days only.

Microsoft, however, still keeps IP addresses for 18 months. According to Grouard, however, its mode of deletion after this period is more robust: "What Google and Yahoo! have done is really not enough. Their method of anonymisation is too weak. Their proposals do not constitute full deletion after the retention period."

"We acted on the Article 29 opinion and said we are ready for deletion after six months as they suggest," she continues, "But only if they others do it, too. It is a competition issue. We want full deletion to become a standard. But Google said no – at this stage, they'll change nothing."

Grouard adds that it would be impossible to provide good search information without keeping data for a certain amount of time – six months as a minimum. Thirteen months, she says, is better, since being aware of seasonal trends can improve services. Google and Yahoo! have made similar claims.

According to the WP's published opinion, search engine providers must delete or anonymise personal data once they are no longer necessary for the purposes for which they were collected. It has called for the development of appropriate anonymisation schemes by search engine providers.

Is anonymisation realistic?

How far this is actually happening is unclear. Renzo Marchini, a solicitor at Dechert, admits that he doesn't know "enough about the whys and hows" to know whether current retention practices are justified. "But," he adds, "they could anonymise data, take IP address out of it – to keep the Article 29 party happy."

Marchini believes that increased anonymisation could work well. Although he admits that it is always necessary to take the idea of anonymisation "with a pinch of salt" since, in theoretical terms, something is only anonymous if it is completely useless and has no distinguishing elements whatsoever. "You'll still have the problem of inference," he explains.

What's more, given that the WP and the search engines themselves cannot agree about whether the Data Protection Directive generally applies to the processing of personal data by search engines, even when their headquarters are outside of the EEA, some claim that it will not be the law, but the consumer that is most likely to force any change in terms of practice. Donald Hamilton, UK managing director of behavioural targeting specialist Wunderloop, the second company to be awarded the EuroPriSe seal, is one of these. "We need more consumer power," he says. "Google is risking losing consumer trust. If you actually read the terms and conditions, Google can do with your data what they wish. Consumers don't really know that, but there will be a backlash."

Consumer power

If indeed there is a sudden change in behaviour on the part of consumers, whether or not it is Ixquick that they turn to for their web searches ultimately depends on how easy it is to use, as well as the strength of its marketing efforts. "It may still remain the domain of a few serious people who are serious about privacy," comments Rosemary Jay, partner at Pinsent Masons.

Certainly, despite the fact that privacy advocates are up in arms about what they see as excessive online data-sharing, consumers give up information when they see services as of benefit to them. Sites like Facebook and LinkedIn, for example, remain popular. According to Marchini, "These things are here to stay. I don't think it's privacy seals that people are swayed by."

Ixquick is an interesting development, but it operates within a context of limited consumer awareness. Its profile – and the profile of privacy itself – will have to be raised yet further in order for its popularity to surge; and no-one knows what the trigger for that might be.

RELATED LINKS

Ixquick: www.ixquick.com
EuroPriSe: www.european-privacy-seal.eu
WP opinion on data protection and search engines: http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/tasks-art-29_en.pdf.

AUTHOR

Lucy Fisher is *a PL&B* Correspondent

Art 29 WP's new Opinion on clauses for 3rd-country transfers

The recommendations include subprocessors' handling of sensitive data, individuals' right, audits and inspections, governing law and transitional provisions for old contractual clauses.

On 5 March the Article 29 Working Party adopted an Opinion on the Commission's draft Decision on standard contractual clauses for the transfer of personal data to processors in third countries. Subject to several recommendations, the Working Party (the national Data Protection Authorities) gave a favourable opinion on the Commission's draft decision, and invited the Article 31 Committee (the Member States) to continue its work with a view to adopting the Commission's Draft Decision.

The recommendations included:

1. Recitals in the Decision providing for authorised international transfers outside the European Union/ European Economic Area
2. Allowing sub-processors to stipulate agreements when sensitive data such as biometric, genetic, judicial, or financial data are exported
3. Organisational solutions for data subjects' rights, such as a single corporate contact point

4. Auditing and inspections
5. Governing law to be the law of the exporting state
6. Transitional provisions for old contractual clauses.

The Working Party noted that for several years companies and Data Protection Authorities have been working with the standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46 (data controller to data processor 2002/16/EC). An update had become necessary because of the advent of "global outsourcing". As more and more companies not only transfer their data to a processor but to "sub processors" and sometimes transfers data to subsequent "sub-subprocessors", the standard contractual clauses 2002/16/EC no longer provide a means to deal with these complex onward transfers. The European Commission considers it necessary to modify the standard contractual clauses 2002/16/EC to make a contract better equipped for current business arrangements by adopting a new Decision based on Article 26(4) of Directive 95/46/EC.

Comments on the Draft Commission Decision.

Concerning subcontracting by processors established in the Community versus subcontracting by processors outside the Community, the Working Party said that international subprocessing outside the EEA by a processor established in the European Union/EEA was not foreseen in the Draft Commission Decision and was becoming more common. They said that the adoption of this Draft Commission Decision would introduce a remarkable flexibility in processing services, as far as the authorisation system provided for in Article 26.2 of the Directive is concerned. "However, this flexibility would not apply equally to the different players in an increasingly global market. Indeed the Draft Commission Decision would allow a processor established in a third country to carry out onward transfers for the purposes of subprocessing only with an authorisation granted by the controller, while those processors established in the EU/EEA and which would like to subcontract part of their processing activities to a sub processor in a third country should continue to use the current legal system." This could cause a competitive disadvantage for European companies that would be required to bear an administrative burden greater than that of their equivalents in third countries, in order to perform equivalent processing as service providers.

The Working Party said that because of the different legal nature of intra community and international transfers, it would be necessary to find a legal solution that would allow international subprocessing by processors established in the EU/EEA without generating unnecessary inequalities in the market. The Working Party urged the Commission to develop promptly a new separate and specific legal instrument to allow international subprocessing by processors established in the Union to sub processors in a third country. This could take the form of a new set of Standard Contractual Clauses, through which the controller and the processor established in the EU/EEA could provide for transborder subprocessing, in accordance with the necessary and adequate guarantees for such transfers.

In the absence of a specific Community legal instrument, the Working Party encouraged national supervisory authorities to consider, as an adequate guarantee for the international subprocessing contracts entered into by the controller and a processor in the EU/EEA, that they apply by analogy the same principles and guarantees of these Standard Contractual Clauses. That is to say, contracts made between an EU/EEA data controller and an EU/EEA data processor under which the controller authorises the transfer of data to a sub-processor outside the EU/EEA should be viewed by a national data protection authority as providing adequate protection for the rights of the data subjects whose data is being transferred if they apply by analogy the same principles and guarantees of these Standard Contractual Clauses 2002/16/EC. This would amount to a similar regime to that provided by the Draft Decision to processors outside the EU.

The Working Party invited the Commission to consider whether the Commission Decision adopting the standard contractual clauses could contain a statement explaining this question, for instance by including specific recitals in the Commission Decision which would expressly provide the possibility for Member States to authorise international transfers based on the Standard Contractual Clauses annexed to the Commission Decision to sub processors established outside the EU/EEA in the specific situation in which both the controller and the processor are established in the EU/EEA. These references should include the advisability of allowing this type of outsourcing through an authorisation system identical to that provided for processors established outside the EU/EEA.

Multi-layered sub-contracting

The Working Party acknowledged the need to adjust Standard Contractual Clauses to the new trans-national dimension of the processing of personal data – in particular taking account of the widespread practice of "subprocessing" certain processing operations. The Working Party noted the inclusion of a sub-contracting clause in the Standard Contractual Clauses (SCCs) "controller to processor", where such clause is designed in accordance with the scheme that is contained in the document mentioned in Clause no. 11 (that is, as a written agreement between data importer and subcontractor based on the data exporter's prior written consent and modeled after the controller-to-processor Standard Contractual Clauses). subprocessing of the processing operations mostly consists in appointing entities established in third countries as data processors; the third countries in question often do not ensure adequate safeguards and the processed data are also exposed to the application of local laws.

The Working Party urged the Commission to evaluate the advisability of also allowing a sub processor to stipulate subsequent subprocessing agreements with further third parties; in particular when sensitive data are processed or in case of processing operations carrying specific risks to data

subjects (that is, biometric data, genetic data, judicial data, financial data, data on children, profiling). This would actually give rise to major chains of sub processors that might act independently of the data controller's instructions; additionally, it would be difficult to keep track of the various sub processors especially in order to establish tasks and responsibilities vested in the individual entities.

In its Working Document on preliminary views on the use of contractual provisions in the context of transfers of personal data to third countries, the Working Party indicated that onward transfers to bodies or organisations not bound by the contract should be specifically excluded by the contract, unless it is possible to bind such third parties contractually to respect the same data protection principles.

The Working Party said that the current organisational pattern of worldwide markets involving long chains of sub-processors are an integral part of the international business structure. Given this context, a system of SCCs envisaging a single subprocessing layer (from the data importer to one sub processor) is unsuitable for coping with the existing business scenarios. The Working Party accordingly decided to accept the introduction of a "multi-layered" subprocessing clause, on condition that appropriate safeguards are laid down to protect data subjects in the light of the aforementioned risks.

Applying contractual clauses to all different layers of subprocessing operations will introduce greater uniformity in business, as all subcontracts of processing operations covered by the standard contractual clauses would be subject to the same clauses and stipulations. This would simplify the current situation by increasing legal certainty, whereby it is not evident that where data importers subcontract their processing activities to other sub processors they require prior written consent of the data controller and impose contractual obligations that will ensure the same level of protection as provided by the contractual clauses. "Following this line of thought, it would appear appropriate to consider that a 'multi-layered' subprocessing clause can be lawful if the decision to commit the processing to further sub processors goes hand in hand with the careful assessment of the specific requirements and features of the processing operations that justify such decision. The assessment in question will have to be especially accurate if the number of subprocessing layers is especially high and should also pay particular attention to the purpose limitation principle so as to ensure that the initial purpose for which the controller transferred the data to the data importer for processing services is not altered by the different subprocessing contracts that could be entered into."

Organisational solutions

The data exporter should also introduce organisational solutions to facilitate exercise of data subjects' rights (access, rectification, objection, erasure, etc.). This might entail, for instance, specifying a single corporate contact point for data subjects to exercise their access rights (at the data controller's headquarters), or else developing clear-cut procedures – to be made known to all processors and sub-processors – in order to provide data subjects with the personal data to which they may request access.

Subcontracting

The Article 29 Working Party considered that Clause 11 –Subcontracting- of the Commission's Draft Decision includes the elements necessary to adequately ensure that the whole chain of possible subprocessing operations will continue to ensure the level of protection set out by the standard contractual clauses. In addition the obligations imposed in Clause 4 (obligations of data exporter) and Clause 5 (obligations of data importer) will ensure that the controller and the processor are obliged to ensure this level of protection through all the layers of subcontracts.

The Working Party suggested that in parallel with the obligation imposed on the data importer (processor) of sending a copy of any subcontract he concludes to the data exporter, the data exporter should keep an updated list of the individual processors and sub-processors making up the "contractual chain". In the same vein, the competence of data protection authorities to conduct audits of the data importer as well as sub processors of the data importer will be essential to ensure compliance with contractual clauses and the level of protection required by all different sub processors involved in the processing activities of the personal data being transferred subject to the standard contractual clauses.

Other issues

Audits: The proposed standard contractual clauses should make it possible for data protection authorities to have powers allowing them to inspect the full chain of subprocessing: the data controller, the data processor(s), and the sub processor(s) and, where appropriate, to take binding decisions on them. The Working Party recommended adapting Clause 8 (Cooperation with supervisory authorities).

Governing law: To ensure legal certainty and consistency, it should be stated that the law governing contracts entered into for subprocessing services should also be the law of the Member State in which the data exporter is established.

Consequences for old clauses

The Working Party recommended that the Commission include transitional provisions in the Decision itself providing that the international transfers authorised pursuant to the repealed Decision 2002/16/EC shall remain in force as long as the transfers and data processing described in the initial signed contractual clauses have not changed. However, if the companies that have used the "old" clauses wish to amend the "old" clauses or wish to introduce subprocessing arrangements, they will be required to amend the "old" clauses to bring them into line to the new Standard Contractual Clauses and apply for a new authorisation in accordance with national legislation.

Conclusions

Subject to its recommendations, the Working Party had a favourable opinion on the draft Commission decision on standard contractual clauses for the transfer of personal data to data processors established in third countries. The WP invited the Article 31 Committee to continue its work with a view of adopting this Draft Commis-

Queensland's Information Privacy Bill

Queensland is one of the few Australian States not to have an information privacy law covering its private sector. The state government has invited comments on a draft Information Privacy Bill, following recommendations by an independent review of FOI and privacy in mid-2008. To some extent the Bill will codify existing administrative rules (embodied in Standards), but will add individual remedies and rights of appeal which are not currently provided. The government is also considering extending its ambit to cover local government bodies, as is common with state privacy laws in Australia.

The Information Privacy Principles in the Bill, while covering most aspects of OECD-influenced sets of principles, are somewhat different from those adopted by any other Australia law, and in particular have many differences from the UPPs proposed by the Australian Law Reform Commission in its review of the private sector and federal agency provisions.

The Bill will establish a Privacy Commissioner (as a deputy to the Information Commissioner) with broad powers including conducting reviews of systemic privacy issues, issuing compliance notices to agencies found in breach of privacy principles, and approving exemptions ("Public Interest Determinations") from the principles.

The Bill will giver persons who have a complaint about the handling of their personal information by an agency a right make a complaint first to the agency , and then if the agency is unable to satisfy the person's complaint, to the Privacy Commissioner who must take all reasonable steps to mediate the complaint. If mediation is unsuccessful, unresolved complaints are referred to the Queensland Civil and Administrative Tribunal (QCAT) for hearing. QCAT will be able to make orders for a range of remedies for breaches of the privacy principles. This approach is most similar to that in the Victorian legislation.

• *For information about this consultation, and the draft Bill, see web page www.qld.gov.au/righttoinformation.*

Canadian anti-spam bill

The Canadian Senate is considering an anti-spam bill that would impose penalties ranging from a fine of up to $500,000 or prison for two years, to $1.5 million or prison for five years in repeated spamming cases. The bill would also require companies to pay an additional fine based on the profits from spamming.

The senator who introduced the bill said that Canada is the only G8 nation which does not have anti-spam legislation. In absence of Canadian anti-spam legislation a Canadian resident, Adam Guerbuez, was ordered by a US federal court to pay $873 million to Facebook for flooding users with sexually-explicit spam emails (*PL&B International*, December 2008, p.5).

The anti-spam bill, S-220, titled as "An Act Respecting Commercial Electronic Messages (the Anti-Spam Act)" would allow Internet Service Providers (ISPs) to refuse, filter and block spam emails.

US: new online advertising rules

In December 2008 the US Network Advertising Initiative (NAI) published a new Code of Conduct on the collection, use, and sharing of information for behavioural advertising. The NAI is a self-regulatory organisation of online marketing and analytics companies. The binding principles are to regulate the use of targeted or customised advertising.

The Code was published one year after the Federal Trade Commission (FTC) released proposed principles for self-regulation of online behavioural advertising. The Code governs Online Behavioural Advertising (OBA), defined as including "any process whereby data are collected across multiple web domains owned or operated by multiple entities to categorise likely consumer interest segments for use in advertising online." OBA is distinct from "Ad Delivery and Reporting," defined as "the logging of page views or the collection of other information about a browser for the purpose of delivering ads or providing advertising related services," including the provision of specific advertisements based on the type of browser or time of day, statistical reporting, and tracking the number of ads served to a particular website.

The revised Code added a new category, "Multi-Site Advertising," which means "Ad Delivery and Reporting across multiple web domains owned or operated by different entities." This additional term was included because there is "cross-domain Ad Delivery and Reporting that does not necessarily involve use of passive tracking tools" (for example cookies and pixels) and that certain provisions of the code should extend to such activity. The Code does not address the issue of behavioural targeting by ISPs, but NAI stated in its commentary that the "spirit of the consumer protection goals" of the code might "inform future self-regulation" of ISP behavioural targeting.

The revised Code includes requirements relating to consumer notice of privacy practices, consumer choice about the use of their personally identifiable information (PII) and non-PII.

Interestingly, PII is defined in the code as including "data . . . intended to be used to identify, contact or precisely locate a person." The NAI commentary to the code states that this standard is designed in part to acknowledge that information that is not traditional PII may be PII based on its intended use and thus protections should be afforded to such information.

The notice and choice requirements that apply to OBA, Ad Delivery and Reporting, and Multi-Site Advertising depend on the type of data (non-PII, PII, sensitive information, etc.) used for those activities. The code now includes a requirement that NAI members that serve ads based on "sensitive consumer information" (defined as including social security numbers, financial account numbers, real-time geographic location, and health or medical information) obtain users' opt-in consent prior to using such sensitive information, regardless of whether that sensitive information contains traditionally defined PII. The code states that the provisions relating to sensitive consumer information, and particularly health information, will be further developed in implementation guidelines.

The code also says that member companies engaging in behavioural advertising of children known to be under age 13 (even if PII is not used in the targeting) must obtain opt-in verifiable parental consent. The new standards place increased emphasis on requirements relating to transparency and add a data retention principle that states that members may retain data collected for OBA, Multi-Site Advertising, and/or Ad Delivery and Reporting "only as long as necessary to fulfil a legitimate business need, or as required by law."

The FTC may still release its revised behavioural advertising principles, and are currently engaging in a series of non-public investigations relating to behavioural advertising.

US two-year data retention bill

A bill introduced in the US Congress on 19 February would require Internet service providers and Wi-Fi access points to keep records on users for two years. The bill has been introduced in both the Senate and the House of Representatives, both bills with the same title: "Internet Stopping Adults Facilitating the Exploitation of Today's Youth Act," or Internet SAFETY Act.

Each contains the same language: "A provider of an electronic communication service or remote computing service shall retain for a period of at least two years all records or other information pertaining to the identity of a user of a temporarily assigned network address the service assigns to that user." Critics say that the Internet Safety Act would apply not just to service providers such as AT&T, Comcast, Verizon, but also to all Internet providers and operators of millions of Wi-Fi access points, even hotels, local coffee shops, and home users. The 1996 Electronic Communication Transactional Records Act already requires Internet providers to retain any "record" in their possession for 90 days "upon the request of a governmental entity."

The two Texas Republicans, Representative Lamar Smith and Senator John Cornyn, sponsoring the bills, said that they are necessary to protect children online. The Internet's "limitless nature offers anonymity that has opened the door to criminals looking to harm innocent children," Cornyn said. In an article in the *Dallas Morning News*, Representative Smith defended the bills by saying: "How many times have we seen TV detectives seek call logs of a suspect in order to determine who he has been talking to? What if the telephone companies simply said to the detectives, 'Sorry, we get rid of that information after 24 hours?'"

Marc Rotenberg, director of the Electronic Privacy Information Center in Washington, D.C., said the Internet Safety Act would "create new risk" for Internet users and expose them to "possible liability in civil suits and subpoena fishing expeditions – it's a terrible idea."

Large copyright holders that are members of the Recording Industry Association of America (RIAA) and the Motion Picture Association of America have supported similar data retention regulations in Europe. In 2005 they wrote in a letter to the European Parliament that "it is essential that service providers retain the relevant data for a reasonable period and that the data can be disclosed for appropriate purposes". In filing lawsuits over suspected copyright breaches RIAA lawyers hope to link an Internet Protocol address with a person's identity, so the RIAA would benefit from longer data retention durations.

UK: new law on ISP data retention

On 11 February the UK government laid before Parliament Data Retention Regulations to require ISPs to keep records logs of subscribers' usage for one year. The IP addresses, destination of emails and recipients of VoIP calls information will be available to the police and other government authorities. This implements the 2006 EU Data Retention Directive, requiring all EU telephone companies and ISPs to keep records of communications traffic and location data on their networks: the "who", "when" and "where" information about telephone calls, Internet access and email. This includes: subscribers' names and addresses, IP addresses assigned to users, log-on and log-off times, email addresses to which emails are sent, and information about who is called using VoIP telephony.

The contents of email messages and VoIP calls are excluded from the retention requirement. ISPs in the UK will be required to retain the data from April 2009.

The British government has prom-

ised to reimburse service providers the costs of retaining data, estimated at £46 million.

Fixed-line and mobile telephony providers and ISPs are covered by the Regulations, but web-based email services and Internet VoIP applications are not, because they are outside the definition of public communications services in the Communications Act 2003, which does not cover purely Internet-based services and applications.

The Directive requires countries to retain data for a minimum of 6 months or a maximum of months. The UK period of 12 months is consistent with France, Ireland and the Netherlands, but Germany has adopted the minimum 6-month period. The Regulations will allow authorities to use the information to identify online copyright infringement. ISPs can be asked for IP addresses and subscriber names and addresses in order to take action against illegal file-sharers.

Finland employers, continued from p.1

the employer. While the definition of trade secret is in the criminal law, it will be much more difficult to define what is harmful activity.

Employers need to inform users in writing about their user policy regarding their communications network, and the possibility of applying the law's monitoring provisions, as well as make sure that they have taken steps to ensure adequate data security. Any monitoring requires prior notification to the Data Protection Ombudsman's Office.

Reijo Aarnio, Finland's Data Protection Ombudsman, has said that this change to the Electronic Communications Act, in fact, breaches the confidence of communications. He has also questioned the usefulness of the monitoring aspect relating to trade secrets; the law's provisions on monitoring will not help. If employees are inclined to leak confidential information this will have happened by the time any monitoring takes place.

There are restrictions as to when monitoring is allowed. For example, an employer cannot use the monitoring function to record hours worked, or to verify whether the employee in question has been communicating with a workers' representative, health and safety authorities or occupational heath providers.

After monitoring, the email messages and traffic data have to be destroyed or manipulated so that no connection can be made to the person monitored.

Ombudsman's role

In addition to prior notification, employers need to report annually their monitoring activity to the Data Protection Ombudsman. The Ombudsman can charge for its services in relation to supervising compliance with this Act. Companies may face a bill of thousands of euros for a monitoring request, as any documentation will have to be assessed by the office. If need be, the Ombudsman can also inspect the organisation's computer and data security systems – again a time consuming exercise.

The negotiations on just how much and how the Ombudsman can charge are now ongoing with the various stakeholders involved, and the Ministry of Justice will announce the charging structure by June. While the Government has already allocated the Ombudsman's office €260,000 for the extra expenditure that supervising the law will take, it is very likely that the office will have to charge to cover its costs fully.

Wider application

The Act also applies to organisations that have their own servers, that is, universities, housing associations, libraries, etc. Thus the monitoring power reaches many more citizens that first thought.

Much will now depend on interpretation. A narrow interpretation would make monitoring possible in a very limited number of cases, and might not be of much use to companies.

On the other hand, a wider interpretation would provide companies with much traffic data, including information about the senders and recipients of emails, duration of the communication, route used, time, and the amount of information transferred. The right to monitor will not apply to the actual content of the message.

Opposition

Following a wide-reaching public debate on the privacy implications of the monitoring power, the Parliament adopted two further statements. The Ministry for Transport and Communications has to follow closely whether the objectives of the law are met, and to file a report at the Parliament by the end of 2010. Also, any possible misunderstandings or faults in police investigations regarding cases of leaked company secrets need to be reported promptly.

There was strong opposition against adopting the law, dubbed "Lex Nokia", because of its snooping provisions. The nickname refers to a case in which Nokia got the police involved to investigate a suspected leak of classified information to a Chinese competitor. At the time, Nokia suspected its employees, and when the amendments to the Communications Act were being drafted, it was widely claimed that Nokia was heavily involved in lobbying for the monitoring powers.

Nokia CEO Olli-Pekka Kallasvuo has described in the Finnish media the law as "important to Nokia," but has denied having put any pressure on decision-makers. Following media claims that Nokia was planning to withdraw its headquarters from Finland if Lex Nokia was not adopted, Kallasvuo commented in a TV interview: "No, we have certainly not been guilty of threats, pressure or anything of that nature."

After the Act was adopted, Electronic Frontier Finland (Effi), suggested that the President should ask for a Supreme Court opinion before signing the law. However, she ignored this request and Effi now says that as a last resort it will appeal to the European Court of Human Rights.

"We think that this law goes against citizens' constitutional right to privacy. We trust that the European Court of Human Rights will have the same view," said Tapani Tarvainen, Effi's Chairman.

France: Bill to cut off Internet for file-sharers

This threatened cut-off of Internet services may have the consequence of prompting more intensive monitoring of employees.

In France a bill has been passed by the Senate that would introduce the "three strikes" or graduated response system against illegal downloading. Those suspected of breaching copyright would first be sent a warning email by a new government agency, followed by a second warning. If they continue illegally to download copyright material the internet service provider would be required to cut off access to the Internet for a year.

The bill faced stiffer resistance in the National Assembly than in the Senate, as "internautes", as web surfers are known in France, organise against the law. La Quadrature du Net (Squaring the Net), a French pressure group, organised a "Black-out" protest, in which web designers, bloggers and others darkened their webpages in protest at the bill.

Jeremie Zimmerman, a Quadrature representative said that "The law is based on the surveillance of Internet users by a public body but employing so-called proof of illegal activities supplied by private actors, such as collecting societies and the music companies, over which, unlike the police who would normally be the actors who monitor for illegal activities, we have no democratic control… It will also use harvested IP addresses as proof, which is so imprecise that it is certain that there will be innocents that will be caught up in its net… And finally, there is no recourse against this until after your Internet access is cut off… It's a Kafkaesque legal procedure."

As of 18 April the bill had been rejected by the National Assembly, but it is expected to be re-introduced soon. Carla Bruni-Sarkozy, the wife of the president who has made popular recordings, is reported to support the proposal.

Analysis

If the bill becomes law it is likely to put French law in conflict with the EU 's recently amended telecommunications directive, which prohibits such termination of service.. It also would make the position of employers precarious: a single file-sharing employee could put the whole company's Internet access at risk. Employers outside Finland would then press for their own Lex Nokia to monitor employees' activities, on the ground that to have Internet access cut off for a year would certainly amount to "wrongdoing seen as particularly harmful to the employer".

Germany: new restrictions on direct marketing

No 'soft opt-in' in Germany. **Lucy Fisher** reports.

This year, Germany has seen the introduction of a number of new restrictions with regards to direct marketing, following the country's new "Competition Law", which came into force on 30 December 2008.

At the Direct Marketing Association (DMA)'s recent annual data protection conference this March, Michael Siegert of Siegert Attorneys in Freiburg, Germany, spoke about the latest data protection scandals and the new restrictions for direct marketing.

The law imposes new limitations on email and fax marketing. With regards to advertising by fax, Siegert explained that there is now a "specified permission requirement" for both business- to-business (B2B) and business-to-consumer (B2C) marketing via this channel. Undue harassment is automatically assumed in cases of advertising by fax without the prior express consent of the recipient – and there is no exception to this rule.

Specific opt-in is also required for marketing by email or SMS text message – as enshrined in Article 7 of German competition law as well as within the EU Data Protection Directive. This applies to both B2B and B2C marketing. "There is no soft opt-in in Germany," added Siegert.

Email addresses can be used without consent only if a customer gives his or her address in the context of the purchase of a product or service and if the vendor uses it for the direct marketing of its own similar products and services. In addition, the customer must not have objected to such a use, having "clearly and distinctly" been given the opportunity to object, "free of charge and in an easy manner" when the address is collected and on the occasion of each message being sent. "We have the same problem as many other countries when it comes to defining 'similar'," added Siegert.

There are also changes to competition law with regards to telemarketing, but here the regulations vary depending on whether the communication is targeted at businesses or consumers. A new law which comes into force on 1 July this year states that telemarketing in the B2C space is illegal without prior express consent and there is no exception in the context of contractual relationships with clients. In the B2B space, however, presumed consent is deemed adequate and there is an exception for contractual relationships with clients.

There is also a new administrative offence for telemarketing without

prior consent, which will involve fines of up to €50,000. Bundesrat proposals of fines up to €250,000 were not accepted by Federal government. Consent can only be in text form, so by email, letter or fax. Oral consent, or consent over the telephone, is not sufficient.

The catalogue of sanctions, in the event of violations of competition law, said Siegert, involves "total profit skim-off": the destruction of advertising material; high court penalties of up to €250,000; contractual penalties; and legal costs. "Injunctions are very quick, usually within one day," he added.

Current events

Siegert said that public perceptions of direct marketing in Germany are "very bad" and that the list or address business is perceived as being close to the illegal drug trade in terms of respectability, despite being regulated by law. "Germany is now the country of the data protection catastrophe. Whereas in former times the media reported from time to time on data protection scandals, the term now used is catastrophe," he said. "You don't want to be named and shamed there."

"The media, consumer associations, data protection authorities and consumers demand detailed investigations and severe punishment – as well as further legal restrictions of the address trade," he continued. Privacy violations in Germany can lead to imprisonment of up to two years and fines are being introduced of €300,000. "However Spanish fines are still the largest in the world," added Siegert. "They can be over €600,000."

Siegert told delegates that direct marketing in Germany is also becoming increasingly restricted, due to the introduction of consent as a general principle in the context of the address trade, advertising and market research. This means that the processing or use of personal data is permissible if the person concerned has consented according to Article 28, para 3a of the Federal Data Protection Act (*Bundesdatenschutzgesetz, BDSG*).

This may be problematic for direct marketers since it means lists can only be disclosed to third parties with consent, and in the B2C space there can be no use of pubic data for customer acquisition without consent. In B2B marketing, data use without consent is limited to the list privilege.

Care also has to be taken with regards to the form that consent takes. "In the offline world it's not sufficient just to tick a box, although it is in the online space," said Siegert.

The lifespan of consent

The issue of the lifespan of an average consent has come to the forefront lately, and been picked up in the courts, added Siegert. "Consent has been found to apply only for a limited time, especially in the address trade," he said.

In the Appeal Court of Berlin, for example, it was found that consent to email marketing becomes ineffective two years after declaration if not used before, whereas a Stuttgart court found that consent to fax marketing becomes ineffective four weeks after declaration if not used before.

The data protection authority in the ministry of the interior Baden-Wuttermberg working report 2007 highlights the limited validity of consent declarations, stating: "consent declarations may only be used for a limited time; especially if the data have been derived from the address trade."

"The law is full of conflicts and unclear wording," added Siegert.

Netherlands: DP Bill retains administrative burdens

By **Hester de Vries**.

Already before the entry into force of the Dutch Personal Data Protection Act (*Wet bescherming persoonsgegevens*) ("PDPA") in 2001, the administrative financial burden for the corporate sector when complying with this law was the subject of fierce discussions (memorandum of reply – Upper House of Parliament 25892, 92c , pages 19-21 and pages 23-24. See also document in response to report 25892, no. 6, pages 12-13).

At that time, the government took the position that Dutch law follows the literal text of the European Personal Data Protection Directive as much as possible. Only in a limited number of situations would there be supplements. The government therefore took the position that the extra costs involved in the implementation of the PDPA compared with the predecessor of the PDPA, the Registration of Persons Act (*Wet persoonsregistraties*), were the result of the obligations pursuant to the Directive, and not the result of extra (superminimal) obligations that would be imposed pursuant to the PDPA but do not directly arise from the Directive (25892, no. 13, page 27). In the final stage of the parliamentary discussions the Minister promised that he would (once again) have an investigation carried out into the administrative burden pursuant to the PDPA.

In the following years various reports were published in which the administrative financial burden as a consequence of the PDPA was proven. In December 2004 the Dutch Data Protection Authority (DPA) made ten proposals for a reduction of the administrative burden pursuant to the PDPA. In the spring of 2006 the Minister of Justice promised that he would submit a bill to amend the PDPA. The intention of the bill that was announced at

that time was to make as many proposals as possible to reduce the administrative burden. It is remarkable that the promise had already been made before the official evaluation of the PDPA was completed. In 2007 the report of the first stage of the evaluation of the PDPA was published, and in 2008 the report of the second stage of the evaluation. The evaluation reports confirm that the PDPA leads to a (partly unnecessary and disproportionate) administrative burden.

The Bill

On 5 February 2009 the bill to amend the PDPA was finally submitted to the Lower House of Parliament. Given the long run-up and the extensive reports on the administrative financial burden, expectations were high. However, the harvest in the field of the administrative reduction of costs appears to be meagre. Many proposals for a reduction of costs that were launched before appear not to have been included in the bill. In the explanatory memorandum to the present bill this is explained as follows: after investigation and consultations with the parties involved (including the DPA and VNO-NCW, the Dutch Association of Entrepreneurs and Employers) a number of the proposals that were made appeared not to be feasible. A number of proposals appeared not to constitute an actual reduction of the financial burden, could not count on a sufficient level of support in the corporate sector, or appeared to be in conflict with the Data Protection Directive. According to the explanatory memorandum to the bill, the Directive stands in the way of the realisation of many proposals to reduce the administrative burden and compliance costs.

These are some of the proposed amendments that are relevant for the international corporate sector.

Cancelled Obligation to Have a Licence for Transfers

The Netherlands is one of the countries in which the use of standard contractual clauses for the transfer of personal data to third countries without adequate level of protection as approved by the European Commission requires a permit in advance from the Minister of Justice (Section 77 (2) of the PDPA). The application for a licence must be filed with the DPA, which, after testing the application, advises the Minister whether or not to grant the permit. This procedure for granting a permit is time-consuming and causes annoyance, especially in situations in which unaltered use is made of the standard contractual clauses. After all, in these situations the test by the DPA does not relate to the extent of protection offered to personal data, but only to the actual description of the proposed transfer, as reflected in the Annex to the standard contractual clauses.

Although the proposed statutory provision seems to suggest that the obligation to have a licence is cancelled in any case in which use is made of the standard contractual clauses, it clearly appears from the explanatory memorandum that the obligation to have a licence will only be cancelled when unaltered use is made of the standard contractual clauses. This means that no clauses in the model contract clauses may be altered. In practice it regularly occurs that parties integrate the model contractual clauses in a more comprehensive "Data Transfer Agreement" or add one or more single clauses to the standard contractual clauses. In these situations one could take the position that there is, strictly speaking, no question of "unaltered" use of the standard contract clauses, and therefore a licence for the transfer may still have to be applied for.

It has been repeatedly pointed out that the obligation to have a licence has a wider scope than the obligations that directly arise from the Data Protection Directive. It is therefore correct that the obligation to have a licence is now cancelled. This cancellation should not be accompanied and by a very strict interpretation of the term "unaltered use" of the model clauses.

Mitigation of the Obligation to Provide Information

In the Netherlands, in the event of use of personal data for direct marketing purposes the data controller has a relatively heavy obligation to provide information. For instance, the data controller who intends to provide data to third parties so that these parties can use these data for direct marketing purposes must inform the data subjects thereof and must give them the opportunity to raise an objection by means of an advertisement in one or more newspapers or free local papers, or in some other suitable way. In addition, the data controller who himself sends a message for commercial, non-commercial or charitable purposes to a data subject must point out to the data subject in each message that the data subject has a right to raise an objection against that.

The obligation to inform the data subject via the media and the obligation to inform the data subject in each message does not directly follow from the Data Protection Directive. For this reason it has been proposed to amend the text as follows: "The data controller who processes personal data in connection with the creation or maintenance of a direct relationship between the data controller or a third party and the data subject, will take appropriate measures to inform the data subject of the possibilities of raising an objection".

This (as such undisputed) administrative reduction of costs, however, seems to be particularly symbolic, now that the obligation to provide information continues to apply fully with regard to the popular forms of e-marketing. After all, on the basis of the implementation of Directive 2002/58, in each message that is addressed to him, the addressee must be informed that he has the right to oppose this. In addition, in the event of forms of telemarketing via the telephone which are also broadly applied and detested by many consumers, as of 1 July 2009 there will be an explicit obligation to inform the person who receives an unsolicited telephone call in each telephone call about the existence of a so-called "do not call me registry".

In other words: the intended administrative reduction of costs only seems to apply for the classic and meanwhile less popular forms of direct marketing by regular mail.

Prior investigation

In conformity with the bill the regulation of prior investigation has been amended with regard to some issues. A new provision is, for instance, that a prior investigation does not have to be requested if another data controller has already applied for a prior investigation and the DPA has issued a declaration of lawfulness. The fact is that experience

in practice shows that the DPA always attaches conditions to a declaration of lawfulness. Usually, a data controller must clearly substantiate by means of self-regulation (a protocol) which measures are taken to guarantee the lawfulness of the data processing. Only in that case the DPA will issue a declaration of lawfulness to the data controller. It is therefore obvious that the exception to the obligation to request for a prior investigation only applies in situations in which the data controller subscribes and complies with the protocol developed by the other data controller.

It should also be mentioned that the obligation to request for a prior investigation for the use of black lists or warning lists of, for instance, fraudulent personnel or fraudulent customers will be cancelled, if these lists are used within a "group of companies". When black lists or warning lists are shared with third parties, for instance within a particular sector, the obligation of the prior investigation continues to apply. As indicated above, in that case it is not necessary (anymore) that each third-party data controller applies for a prior investigation, provided that the protocol on which the assessment of lawfulness by the DPA is based is subscribed.

Conclusion

The long-awaited bill, which would have to contribute to an administrative reduction of costs for the corporate sector when complying with the PDPA, is disappointing. Only in a limited number of respects is an administrative burden or a compliance obligation actually mitigated. It is remarkable that in a number of respects new burdens or obligations are also created. For instance, previously, in the event of an objection against data processing for direct marketing purposes, the data controller only had the obligation to "immediately" terminate the data processing. The (additional) obligation has now been imposed on the data controller to inform the data subject, if so requested, within four weeks about the measures that have been taken. Mind you, this is an increase of the administrative burden.

For the time being, no mitigation is offered for a lot of obvious administrative burdens, for instance, not for the obligation to report a data processing to the DPA. However, it is announced that the Exemption Decree PDPA (*Vrijstellingsbesluit Wbp*), in which the exceptions to the duty to report are described, will be revised and extended.

For many other forms of reduction of costs wished for by the corporate sector all eyes will be looking at Brussels, now that the room for reduction of costs is apparently very small given the straitjacket of the European Data Protection Directive.

• *Hester de Vries is attorney with Kennedy Van der Laan, Amsterdam, The Netherlands. See web page www.kvdl.nl/KVdL/en-GB.*

Continued from p.3

increasing the likelihood that service providers will be directed to make unnecessary notifications.

There has also been controversy surrounding a proposal to exempt from the notification requirement data that has been rendered "unintelligible" to unauthorised persons due to "technological protection measures" (such as encryption). Such an exception would seem to make sense in light of the consensus that notice should only be issued if there is a risk of harm – unintelligible data does not pose a risk. All the Institutions now favour such a provision, though, curiously, the Council's version would include the exception in the Directive's recitals, meaning that it would not be binding on Member States.

The Article 29 Working Party, however, has come out against a blanket exception, emphasising the importance of an overall risk assessment in determining whether notice should be given. Some in industry, on the other hand, have expressed concern that the measure may not be broad enough, and have asked for language to be included clarifying that it covers methods in addition to encryption.

The Institutions have also disagreed on who should receive notice. The Council's text refers to "subscribers" of electronic communications services. The Parliament and the Commission, on the other hand, have proposed to broaden the requirement to embrace "users" (Parliament) and the "individual concerned" (Commission). It appears that a consensus may be emerging that notice recipients should include the "subscriber or individual concerned". This is not a minor semantic issue – subscribers should be much easier for a service provider to identify and locate. As we discuss below (under Issues for Europe), we believe a requirement that extends beyond subscribers could lead to significant complications for service providers.

Finally, the Institutions have sparred over whether the Commission should have the authority to harmonise Member State rules on the circumstances, format and procedures for breach notice through the adoption of "technical implementing measures". This would be done through the so-called comitology procedure, giving the Council and the Parliament the right to block rules adopted by the Commission. Nonetheless, there has been resistance to the harmonisation provision in both the Parliament and the Council, where it has been viewed as an unwarranted extension of Commission authority, particularly vis-à-vis the Member States. Many in industry, however, would support a mechanism for EU level harmonisation as there are concerns that Member State rules may diverge, complicating compliance efforts and increasing costs.

Comparison with the US

The emerging EU regime bears both similarities and contrasts with the patchwork of state laws that have developed in recent years. Indeed, many of the issues that EU policy makers are currently grappling with have been addressed in some form by US legislation.

First, state breach notice laws normally apply to any company deemed to "conduct business" in a particular state. In many cases, government agencies are also covered. Thus, the scope of most US laws – with respect to the covered entities – extends well beyond any of the current proposals under consideration by the

Institutions (it should be noted, however, that the scope of personal data in the EU is much broader than the "personal information" covered by US state breach laws).

Second, US state laws adopt a self-assessment approach in which the affected entity is responsible for evaluating if notice is warranted (law enforcement authorities may often delay the issuance of notice if it is determined that notice would impede an investigation). In many states, notice is not required in the absence of a reasonable risk of harm. On these issues, then, the emerging EU regime and the US approach appear to be broadly similar – Europe seems to be heading towards a model based on self-assessment of breaches in which a finding of a risk of harm triggers the notice requirement.

Third, encrypted data is generally exempted from notification in the US, including in states that do not have a "harm" requirement for notice. Most of these exemptions also apply to data that has been subjected to some other form of protection. As noted above, EU policy makers seem to agree that at least encrypted data should be exempted.

Finally, the individuals a business is required to notify in the US generally include any affected resident of the state. In the EU, the categories of persons that should receive notice are still unsettled, and it is unclear whether these categories will in practice be linked to residency in a specific Member State.

Issues for Europe

The law that emerges from the legislative process may raise interpretive and implementation-related issues that policy makers, service providers, and other stakeholders will eventually need to address. While much will depend on the text of the final approved provisions, we believe there are several potential issues that could have significant consequences for the effectiveness of the notice regime.

First, which Member State law should apply to a breach? The proposed measure is silent on this question, and the e-Privacy Directive lacks jurisdictional provisions. A number of difficulties could arise in the breach context. Would the applicable law be that of the Member State where the service provider is established, or where the subscriber is located? What happens if a service provider is established in several Member States, or if the subscribers affected by a breach are in several Member States? We suspect that EU-level guidance may need to be adopted on this, if not a binding measure.

Second, problems could arise if service providers are required to notify affected individuals other than their subscribers. Such a requirement would increase the scope of the investigation in the event of a breach. Service providers would likely have to devote significant resources to assessing whether personal data has been affected and, if so, whose data it is. Determining how to contact the individuals with whom the service provider has no relationship could also be unduly burdensome, in addition to raising privacy issues. In order for a service provider to contact a person who is not its subscriber, the provider would likely need to obtain personal data from another entity (such as an ISP). Setting aside any legal issues that might arise in this context, increasing the amount of personal data available to third parties would seem to run counter to the very purpose of breach notice.

Another potential problem is "notice fatigue". While the introduction of a standard of harm for triggering notice goes a long way towards addressing this issue, it does not eliminate the problem altogether. Service providers may be tempted to err on the side of over-notification to protect themselves from any potential liability. On the other hand, if NRAs are tasked with the analysis of breach incidents, we fear that they too may over-notify due to a lack of resources properly to assess such incidents.

A final significant issue is the potential for diverging regimes at the Member State level. The EU proposals would leave key details to the Member States to sort out. For example, the precise circumstances that necessitate a breach notice would be left to the Member States, as would the method and timing of notice. Under the Council's text, Member States would not even be obligated to exempt encrypted data from the notice requirement. Consequently, it is possible that the Commission will need to harmonise aspects of the Member State rules, and we believe it is important that the Commission have the authority to do so through the comitology procedure.

> 'Notice fatigue' from over-notification is a problem

A General European Breach Notification Requirement?

Ultimately, stakeholders will need to consider whether a breach notification requirement applicable to all businesses would be an appropriate privacy safeguard for Europeans. We believe such an extension would be consistent with the policy considerations underlying breach notice. If one assumes that there is value in informing individuals when their personal data has been compromised, it would not seem sensible to limit the scope of the measure to the telecoms sector, or even to online businesses generally.

A breach notification measure applicable to all business could be added to the Framework Privacy Directive (95/46/EC), in the event that the Directive is opened for review. Such a measure would require any data controller to provide notice in the event of a breach affecting personal data. The Framework Directive currently includes a security of processing provision that requires data controllers to implement appropriate measures to protect personal data from "accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access… " (Article 17(1)). The breach notice requirement would be a logical extension of this provision. Alternatively, a general breach notifica-

tion measure might also be introduced through specific legislation on breach. In either case, however, policy makers would need to carefully consider whether such a regime should merely track the requirements of the e-Privacy Directive, or whether different provisions might be needed for a measure applicable to "bricks and mortar" businesses.

AUTHORS

The authors are attorneys with Covington & Burling, Brussels.
www.cov.com

EU LIMITS BREACH NOTIFICATION RULES TO TELECOMS

On 16 February the Council of Ministers of the European Union published its rejection of proposals from the European Parliament to extend data breach notification requirements beyond telecommunications companies. The Parliament had proposed an extension of the breach notification rules in an amendment to the Privacy and Electronic Communications Directive.

The European Data Protection Supervisor (EDPS) and the Article 29 Working Party both supported extension of the breach notification requirement from telecommunications companies to information society service providers (ISSPs) generally. The Council of Ministers disagreed and proposed a changed wording in the Directive making it clear that the breach notification requirements apply only to publicly available electronic communications service providers. The amendment leaves the decision as to whether a breach is serious enough for notification to the companies.

The amendment says "In the case of a personal data breach, the provider of publicly available electronic communications services shall assess the scope of the personal data breach, evaluate its seriousness and consider whether it is necessary to notify the personal data breach to the competent national authority and subscribers concerned. When the personal data breach represents a serious risk for the subscribers' privacy, the provider of publicly available electronic communications services shall notify the competent national authority and the subscribers of the breach without undue delay."

The proposal from the Parliament and the Commission would have the regulator decide whether a breach is serious enough to require notification.

The Article 29 Working Party said in February that "An extension of personal data breach notifications to Information Society Services is necessary given the ever increasing role these services play in the daily lives of European citizens, and the increasing amounts of personal data processed by these services. Online transactions including access to e-banking services, private sector medical records and online shopping are few examples of services that may be subject to personal data breaches causing significant risks to a large number of European citizens. Limiting the scope of these obligations to publicly available electronic communications services would only affect a very limited number of stakeholders and thus would significantly reduce the impact of personal data breach notifications as a means to protect individuals against risks such as identity theft, financial loss, loss of business or employment opportunities and physical harm."

The Council's Common Position will now be debated in the European Parliament.

Will there be mandatory breach notification in the EU?

Since 2008 PL&B has surveyed data protection authorities in 21 countries about their attitudes towards data breach laws What constitutes a security breach, to whom should notification apply, and what should companies do? PL&B researcher **Amy Norcup** explains.

Question 1: To what extent do existing data security provisions place obligations on organisations to notify authorities of data breaches?

In the absence of breach notification laws, European countries rely on comprehensive data protection laws, civil and criminal legislation to sanction those organisations that fail to uphold the protection of personal data, but there is no obligation to notify. Whilst some EU regulators require, at the very least, data breach incidents to be recorded, others have no way of knowing exactly how much personal data is being lost and by which organisations. Of course, it is the rising number of data breaches and the lack of an obligation to notify the regulatory authorities or the affected individuals in existing data security provisions throughout the EU that has acted as the impetus for change in European law.

Question 2: What are the current breach notification guidelines and expectations from the Data Protection Authorities (DPAs) across Europe?

DPAs in Europe offer "general" advice and guidance on what to do before, during and after a data breach occurs. In the main, guidance and expectations are centred on general data protection provisions which require organisations to adopt appropriate measures which will prevent the "unauthorised access, unlawful processing, accidental loss, destruction and damage to personal data". Such measures include:

1. Adopting data breach security policies
2. Making regular detailed assessments of risks posed to personal data
3. Enforcement of new policies to tighten processes and reduce the likelihood of data going missing
4. Maintaining strong relationships with key personnel
5. Notification to the affected individuals and the regulatory authorities.

Even though notification is not mandatory, the majority of DPAs would expect companies to inform them of a breach. However, not all DPAs would expect data subjects to be informed in the first instance. At the very least, organisations are required to cooperate and work with the authorities to prevent and reduce the impact of a breach which "may"

include notifying data subjects in the long-term. At the core of regulatory advice and guidance of those DPAs surveyed, identifying a good wider data breach strategy is the main step to be taken by organisations.

Question 3: What are the driving factors behind introducing new legislative breach notification requirements into the EU?

The rising number of data breach incidents over the past three years has been the main driving force behind proposals to extend the E-privacy directive and introduce a new 'legal' notion of notification into Europe. Some countries in the EU do not consider there to be a demand in their country for notification requirements, as data breach incidents are either unheard of, or at such a low level, that they can be managed. However, for those countries where breaches are prevalent, new provisions are necessary in order to:

1. Increase the protection of personal data
2. Make organisations more accountable for data security
3. Force organisations to improve security standards
4. Restore confidence in data controllers by data subjects.

PL&B's survey has also revealed that there is a clear difference in the driving factors for legislation between larger and smaller jurisdictions. Whilst the "lack of" notification provisions in one larger country is a problem, for a small EU Member State, something other than notification is required to ensure that the relationship between regulators and businesses can be restored and encourage unity in working together to prevent breaches in the first place.

It remains to be seen the extent to which "notification" provisions alone, beginning with the proposed amendments to the EU E-privacy Directive, will improve protection, accountability and confidence for data subjects.

Question 4: How long will it be before we would see national notification requirements? Which countries are likely to be the first to implement such a measure?

Modifying the E-privacy directive is just one regulatory option available in Europe. Both DPAs and companies have considered further options including:

1. Amending the general EU Data Protection Directive
2. Making modest amendments to national laws
3. Introducing broader breach management strategies at a company level
4. Continuing to improve internal systems within the public and private sector.

The difference in opinion of the EU level authorities on the scope of notification in the E-privacy directive indicates that it is not clear to what extent notification should be imposed. Nevertheless, as the European compromise on this matter draws nearer in May, it will be more apparent that in the not-too-distant future the 27 Member States will need to implement such a provision for certain organisations. Results of the PL&B survey suggest that it is likely that those countries which are experiencing the largest rise in data breaches will be the first to integrate breach notification principles into their existing policies, if not introduce a specific law to govern this area.

Question 5: What enforcement powers are available to Data Protection Authorities related to breach notification?

DPAs already encourage voluntary notification and the majority have the capacity to impose financial penalties, audit and make certain blocking orders as to the specific actions of organisations when they are informed or discover for themselves that a data breach has occurred. The majority of DPAs surveyed were mostly happy with their existing powers but several authorities did think that "some form" of notification was a good idea. In some cases, DPAs wanted to be able to increase the level of fines they can impose for more serious breaches and others simply require the power to conduct audits and inspections to ensure that security standards are at an appropriate level. Whilst mandatory notification orders are not common in the countries surveyed, DPAs did express concerns as to how they would react to an increasing number of notifications. Many considered that an increase in manpower and resources would be necessary to deal at the correct level with breach notification.

• *A full report of the views of all 21 countries is available from Privacy Laws & Business. See www.privacylaws.com/Documents/data_breach_conference.pdf.*

Japan, continued from p.8

This incident is the largest recent personal information data leak in the Japanese financial sector. The injured customers may have a cause of action against MUFJ based on a tort negligence theory, however, because there is little economic incentive in Japan for possible plaintiffs to band together in a class action suit, large scale litigation against MUFJ is unlikely. On the regulatory side, the Financial Services Agency ("FSA"), the arm of the Ministry of Finance that regulates MUFJ, has demanded a report of the incident from MUFJ and may very well conduct a privacy inspection of MUFJ in the near future. In addition, the Japan Securities Dealers Association, a self-governing organisation to which MUFJ belongs, stated that it will examine whether MUFJ broke the Association's rules.

The FSA has promulgated privacy guidelines that interpret and expand upon the main privacy law of Japan, the Personal Information Protection Law. The FSA Privacy Guidelines call for an employer in the financial field to contract with its employees regarding non-disclosure of personal information, train employees about the company's security measures and confirm employees' compliance with security measures. The FSA Privacy Guidelines also call for a data controller in the financial field to take physical and technical precautions to prevent a data leak. If the FSA chooses to investigate this incident and publicise its findings, such a report would be useful for other financial institutions that are eager to strengthen their security precautions and avoid a public relations fiasco of the kind the MUFJ currently finds itself in.

• *Yoshiyuki Omori and Eric Kosinski, White & Case LLP (Tokyo). See www.whitecase.com/tokyo.*

Your Newsletter Subscription **Includes**

1. Six Newsletters a year
The *Privacy Laws & Business (PL&B) International* Newsletter, published since 1987, provides you with a comprehensive information service on data protection and privacy issues. We bring you the latest privacy news from 50 countries – new laws, bills, amendments, codes and how they work in practice.

2. Helpline Enquiry Service
Subscribers may telephone, fax or email us with their questions such as: contact details of Data Protection Authorities, the current status of legislation and amendments, and sources for specific issues and texts.

3. email updates
We will keep you informed of the latest developments.

4. Index
Subscribers receive annually a cumulative Country, Subject and Company index. Multiple headings include advertising, data security, Internet, police, transborder data flows and sensitive data. The index is updated after every issue on our website www.privacylaws.com.

e-Newsletter

Electronic Option
The newsletter is available, for an additional enterprise licence fee, in PDF format for uploading onto your Intranet or network. This format enables you to see the Newsletter on any computer on your network as it appears in the paper version. It allows you to print out pages at any location.

Privacy Laws & Business has clients in over 45 countries, including 25 of the Global Top 50, 24 of Europe's Top 50, 25 of the UK's Top 50 in the Financial Times *lists; and 10 of the Global Top 20 in the* Fortune *list.*

Privacy Laws & Business also publishes the United Kingdom Newsletter, *a publication which ranges beyond the Data Protection Act to include the Freedom of Information Act and related aspects of other laws.*

Newsletter Subscription Form

Subscription Packages

(Please add 15% VAT to prices for the PDF format within the EU)

❑ **Print** ❑ **PDF** (please tick preferred delivery format)

❑ Send a FREE sample of the *UK/International* newsletter

❑ *PL&B International* Subscription **£375**

❑ *UK/International* Combined Subscription **£595**
or an extra **£310** for existing UK subscribers)

❑ Special academic rate – 50% discount on above prices

Multiple Subscription Discounts

❑ 2-9 copies: 30% discount (indicate no. of copies ...)

Intranet Enterprise Licence (inc. up to 10 printed copies)

❑ *PL&B International* **£1,875**

❑ *PL&B UK* **£1,425**

❑ Both *International/UK* newsletters **£2,975**

❑ I wish to receive *PL&B's* FREE email news service

Data Protection Notice: *Privacy Laws & Business* will not pass on your details to third parties. We would like to occasionally send you information on data protection law services. Please indicate if you *do not* wish to contacted by: ❑ Post ❑ email ❑ Telephone

Name:

Position:

Organisation:

Address:

Postcode: Country:

Tel:

email:

Signature:

Date:

Payment Options

Address of Accounts (if different):

Postcode:

❑ Purchase Order

❑ Cheque payable to: *Privacy Laws & Business*

❑ Bank transfer direct to our account:
Privacy Laws & Business, Barclays Bank PLC,
355 Station Road, Harrow, Middlesex, HA1 2AN, UK.
Bank sort code: 20-37-16 Account No.: 20240664
IBAN: GB92 BARC 2037 1620 2406 64 SWIFTBIC: BARCGB22
Please send a copy of the transfer order with this form.

❑ American Express ❑ MasterCard ❑ Visa

Card Name:

Credit Card Number:

Expiry Date:

Signature: Date:

I am interested in:

❑ Consultancy/Audits
❑ In-House Presentations/Training
❑ Recruitment Service

Please return to: Newsletter Subscriptions Department, Privacy Laws & Business, 2nd Floor, Monument House, 215 Marsh Road, Pinner, Middlesex HA5 5NE, UK, Tel +44 20 8868 9200
Fax: +44 20 8868 5215, email: sales@privacylaws.com 22/04

www.privacylaws.com

Guarantee

If you are dissatisfied with the newsletter in any way, the unexpired portion of your subscription will be repaid.