BNA International

World Data Protection Report

International Information for International Businesses

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

Volume 9, Number 7 July 2009

Commentary

Databases: treasure or curse? In many ways databases are the backbone of our society. From client relationship management systems and lists of preferred customers, to health records or national databases of offenders they are seen as extremely useful tools allowing businesses and government to quickly access information that allows them to make decisions and coordinate their actions. Page 5

Amendments to the Indian Information Technology Act: implications for Australian corporations The Indian Government is in the process of finalising regulations to clarify the operation of various new provisions under the recent Information Technology (Amendment) Act 2008. Michael Pattison reports on the legislation, and on the implications for Australian corporations. Page 7

Administration proposes new Federal Consumer Financial Protection Agency Addressing the Obama Administration's proposals to reform financial regulation in the US, Barney Frank (D-MA), Chairman of the House Financial Services Committee, has promised to report legislation which would create a new Consumer Financial Protection Agency (CFPA) before the House adjourns for its August recess at the end of July 2009. Page 13

Privacy and social networking In June 2009 the Article 29 Data Protection Working Party, an independent European advisory body on data protection and privacy set up under Article 29 of Directive 95/46/EC ("WP-29"), rendered an opinion on privacy law implications of social networking ("WP-163"). In its WP-163, the WP-29 defines a social network service as "online communication platform which enable individuals to join or create networks of like-minded users" and categorises them as being information society services, as defined in Article 1 paragraph 2 of Directive 98/34/EC as amended by Directive 98/48/EC. The WP-163 stresses that the key phenomenon of social networks lies in the fact that users are asked to provide sufficient information about themselves in order to create a thorough personality profile or description and that moreover such information can be distributed to others. Page 25

News

Karen Curtis's tenure as Commissioner extended for another year Karen Curtis has been appointed for a further one year term as Federal Privacy Commissioner. Page 21

Article 29 Working Party releases opinion on social networking The Article 29 Working Party has released its opinion on social networking and how European data protection laws apply to social networking services. Page 22

Article 29 Working Party holds discussions with WADA The Article 29 Working Party held further discussions with representatives from the World Anti-Doping Agency (WADA) about the International Standard for the Protection of Privacy and Personal Information. Page 32

Submissions by Authors: The Editors of *World Data Protection Report* invite readers to submit for publication articles that address issues arising out of the regulation of data protection, either on a national or transnational level. Articles with an appeal to an international audience are most welcomed. Prospective authors should contact Andrea Naylor, World Data Protection Report, BNA International Inc, 1st Floor, 38 Threadneedle Street, London EC2R 8AY, U.K. Tel. (+44) (0)20 7847 5800; fax (+44) (0)20 7847 5880; or e-mail: anaylor@bna.com. If submitting an article by mail please include an electronic copy of the article in a recognised software.

World Data Protection Report is published monthly by BNA International Inc., a subsidiary of The Bureau of National Affairs, Inc., Washington, D.C., U.S.A. Administrative headquarters: 1st Floor, 38 Threadneedle Street, London EC2R 8AY, England. Tel. (+44) (0)20 7847 5801; Fax (+44) (0)20 7847 5858; e-mail marketing@bnai.com. In the U.S. call toll-free on: 1-800-727-3116.

Subscription price: U.K. and rest of world £725; Eurozone €1, 175; U.S. and Canada U.S. $1,245. Additional copies of this publication are available to existing subscribers at half price when they are sent in the same envelope as a standard subscription.

Website: *www.bnai.com*
ISSN 1473-3579

Welcome to the July edition of the World Data Protection Report. This issue features a special report by Vinod Bange and Jennifer Sumpster of Speechley Bircham LLP. Drawing on recent high profile cases in the UK and Canada, they discuss the data privacy implications of the misuse and poor management of databases and the ramifications for business and customers.

As the popularity of social networks and blogs increases, our regular contributor, Dr Michael Schmidl of Baker & McKenzie examines privacy and social networking in light of recent guidance from the EU's Article 29 Working Party. Maria Giannakaki of Karageorgiou & Associates comments on whether Internet bloggers in Greece are entitled to privacy after a retiring Greek Supreme Court prosecutor issued his controversial opinion on the matter.

While the conflict between privacy and security continues, Malcolm Crompton of Information Integrity Solutions provides us with his opinion on the ongoing fallacy that we must compromise privacy for the sake of security.

And, of course, there is our usual digest of data privacy news from around the world as well as articles on the latest developments in France, India, the UK and US.

We hope you enjoy this issue!

Shelley Malhotra
Commissioning Editor

Please contact us with your opinions or suggestions or if you would like to write for us, by phone on: +44 (0) 7720 774224 or by email at nmckilligan@europp.co.uk, or jgazey@europp.co.uk

Topical Summary

Legislation and Guidance

Personal Data

Country Checklist

Asia Pacific

Australia

Canada

Costa Rica

European Union

France

Greece

Hong Kong

India

Italy

Japan

Macau

Malaysia

Spain

Sweden

Switzerland

United Kingdom

United States

  WDPR ISSN 1473-3579

Legislation and Guidance

Databases: treasure or curse?

July's issue of WDPR opens with a special feature by Vinod Bange, Partner and Jennifer Sumpster, Solicitor, at Speechly Bircham LLP

In many ways databases are the backbone of our society. From client relationship management systems and lists of preferred customers, to health records or national databases of offenders they are seen as extremely useful tools allowing businesses and government to quickly access information that allows them to make decisions and coordinate their actions.

There have however, been a number of recent high-profile headlines both in the UK national press and in this publication concerning databases that have shown these "useful tools" for business and government to be capable of breaching data protection laws and in some cases a dangerous invasion of privacy for members of the public.

In this article we draw together three of the recent database horror stories, and discuss what can be learnt in the customer context to ensure that databases are safe and beneficial to businesses and consumers alike.

The lesson

Construction industry workers database: built on unsafe foundations.

Investigations by the UK Information Commissioner's Office revealed a database containing the personal details of 3,213 construction industry workers. The information that was held on the database included trade union membership and disciplinary history leading to the widely held assumption that subscribing employers, including many household name construction companies, used such information to effectively "blacklist" workers within the construction industry.

The database was reportedly compiled and maintained by Ian Kerr, trading as the Consulting Association over the past 15 years. On payment of an annual subscription of £3,000, construction companies were able to add to the database, and they could also access details on individual workers for an additional fee of £2.20 per request.

The ICO investigation revealed that Mr Kerr had not given the construction workers included on the database any "fair-processing" information as required under the Data Protection Act 1998, and had not notified his data processing activities to the Information Commissioner.

As a result of their findings the ICO has seized the database and has ordered Mr Kerr and the Consulting Association to cease trading. It has also taken the extremely unusual step of opening a hotline for those construction industry workers who think they may have been included on the database.

It is not only Mr Kerr who should be mindful of the ICO's actions – each of the subscribing companies must consider their own obligations under the Data Protection Act and also under anti-discrimination and other employment legislation. The ICO has taken an extremely dim view of this particular database, and all those who have used it should think very carefully about how they can regain the respect and confidence of their employees and other members of the industry.

This is a perfect example of how *not* to manage and exploit a database: Mr Kerr's actions may be considered reprehensible indeed, but perhaps more alarming were the actions of the companies who ignored their own data protection and employment law obligations and used the information gained from the database to make or influence employment decisions.

The lesson, quite simply, is this: the rights of data subjects whose personal data are included within a database must not be ignored no matter how lucrative or useful that database appears to be.

Data privacy matters have been a specialist focus of Vinod's practice for 12 years. He has particular experience in all aspects informational law, data protection, risk management, audit and implementation projects, global data flows, non-compliance risks and breach incidents as well advising on databases, marketing, customer profile and insight. His client sectors include financial services, retail, technology, healthcare and pharmaceutical. Vinod has been involved in UK, European and international industry and legislative consultation process on data protection and e-commerce laws.

Jennifer Sumpster is in the Data Privacy Group and specialises in data protection compliance issues including monitoring systems for compliance with ethics, money laundering and anti-corruption laws across the EU and internationally as well as advising clients from a diverse range of industries on internal data protection and information security policies and data breach management. She has a particular interest in children's privacy and regularly advises on the data privacy issues that arise when aiming a product or a service at children, particularly in the e-commerce environment.

The authors can be contacted at: vinod.bange@speechlys.com and jennifer.sumpster@speechlys.com

The warning

ContactPoint and the Rowntree Report: children's database destined for the naughty-corner?

There has been much talk over recent months around the introduction by the UK government of a nationwide database containing details of all children and young people under the age of 18 in the UK. This database is known as ContactPoint.

ContactPoint has caused a lot of uncomfortable feeling amongst human rights campaigners and children's charities alike and some organisations, such as the Joseph Rowntree Reform Trust (usually vocally in favour of data policies aimed at protecting vulnerable groups) have called for it to be scrapped in its entirety due to concerns over breaches of data protection and human rights laws and huge fears over the security of the information.

The government commissioned Deloitte & Touche LLP to investigate and report on data security issues surrounding the ContactPoint database. Whilst the full report has never been made public, the executive summary[1] made some fairly alarming observations such as:

"*It should be noted that risk can only be managed, not eliminated, and therefore there will always be a risk of data security incidents occurring*"

This may be a fairly predictable comment that many of us as lawyers will have echoed with our own clients in our advisory capacities, but when it is put in to context, and we remember the type of data that is involved here it is hardly surprising that outrage ensued.

Deloitte's report also determined that:

"*The degree of reliance on a hierarchy of self-certifications over a connecting organisation's security processes poses a significant risk to ContactPoint and its assets.*"

This is chilling indeed considering the number of high-profile security breaches government departments have been at the centre of in recent times, especially given that this database will hold the names, addresses, dates of birth, parent's details, school details, GP details and the contact details of many other individuals and organisations that will be involved, in some way or another, with the care of the child. Any threat to the security of this information, however slight or unavoidable, will clearly bring the majority of us out in a cold sweat, and the potential implications of this information falling into the wrong hands hardly bear thinking about.

Amid a storm of heavy criticism, ContactPoint was launched earlier this year and has been rolled out to a test group of local authorities in England.

There is no doubt that the government's rationale behind the implementation of such a database is extremely compelling: who indeed would argue that any measure which seeks to avoid future tragedies such as that of Victoria Climbié, or "Baby Peter" by plugging communication gaps between care providers is a very good thing, but it is important to remember that a blanket "public interest" justification for the disregarding of fundamental security considerations is not acceptable.

It will be extremely interesting (and a little frightening) to see how ContactPoint's security measures hold up now that the system is live.

Whilst there is no "opt-out" option for parents, one alternative that is available to parents who are concerned about these security risks, and who consider that their child may be at risk of significant harm if their whereabouts were known, is that in certain circumstances they can apply to "shield" information relating to their child's location and any parental details. This is rather a double edged sword, however, as the following advice from one borough council illustrates:

"It is important that you understand, that by requesting a record to be shielded you are informing the authorities that you feel a child/young person is at risk of harm, and if you currently have no professionals involved with your family, the request could generate professional involvement."

The guidance states that "shielding" of data should only occur if *not* shielding the data would place a child at risk of significant harm. It is clear that it could be argued that any child on the ContactPoint database could be placed at risk of significant harm if their details were seen by the "wrong" person (indeed what harm to a child would not be "significant" in this context), and so shielding could be seen by some to be a sensible option even if there was no immediate risk to the child, however in the same advice leaflet, the council makes it very clear that:

"*It is not appropriate to simply shield a record where there is an opposition to ContactPoint in principle.*"

Even if parents were able to shield their child's data if there was no immediate risk of abuse or other harm, this particular council makes the rather sinister inference that in requesting shielding, this is an indicator to the council that a child is at risk, and so this would effectively be a red flag necessitating the involvement of social services or other health care professionals. It seems that this is a rather large leap in logic, and one that perhaps should not be taken in such a sweeping way, not least because the involvement of social services in cases where such action is not necessary is a huge waste of resources, and would divert essential services away from where they are critically needed.

What then are the alternative options available to parents who do not want their children's (or indeed their own) details included on the ContactPoint Database? It may take a challenge to this system in front of the courts before we have any clarity on this issue.

The clear warning from this case is that no matter how genuine the principle and compelling the need for a database, consideration must be paid to the context of the database and its contents. The urgency to meet a particular need, for example to fill communication gaps, must not be balanced against fundamental requirements to protect and secure data: both are valid concerns that seek to protect our information, and in the case of Con-

  WDPR ISSN 1473-3579

tactPoint to protect society's most vulnerable citizens, and both require equal consideration.

The balance?

Databases in a customer context: passengers should be entitled to information from airlines (but it's no substitute for a cold beer!)

For most data protection practitioners the majority of databases occupying our time concern customer data. We have seen in the examples outlined above how things can go horribly wrong in HR and public sector contexts, but what of customer databases? Here we draw an example from our cousins across the pond: enter Air Canada.

Back in 2005 an Air Canada passenger was involved in an incident during a short-haul flight following his insistence that he be permitted to consume the beer that he and his companion had brought on board. The passenger apparently did not know that by drinking his own beer onboard he would be contravening the Canadian Aeronautics Act – and did not take too kindly to the manner of the flight attendant who informed him of this fact. An incident ensued which resulted in the passenger being dubbed "unruly" by the flight captain, and he was detained by the police for questioning when the plane landed. No charges were ever brought against him.

The passenger later applied to the airline for copies of the reports relating to the incident. The airline refused, citing solicitor-client privilege. The Federal Privacy Commissioner of Canada has now commenced an action against the airline.

The background to this case means that the outcome will be particularly interesting: as this case is being heard, the Canadian government is finalising new regulations which will:

"enhance the ability of air carriers to prepare reports on certain types of disruptive behaviour"

The new regulations would require airlines to prepare reports on certain types of disruptive behaviour and to make these reports and related statistics available to the Canadian government on request.

As a result of the heightened concerns about air-security which the new Canadian regulations seek to address, the Canadian Commissioner considers that it is "*critically important*" that passengers have a right to access information an airline has collected about them, especially in cases where they seek to correct the record.

The outcome may also have implications that reach beyond Canada to the air-travel industry in general. Airlines commonly use lists and databases of unruly and disruptive passengers – often for extremely sound reasons but despite the usefulness and the compelling need for such databases, again it is important that data protection principles are adhered to.

The lesson to be learned from the three examples outlined here (and the other countless "database-nasties" lurking in the shadows) is this: databases can be incredibly useful tools, especially in a customer context and businesses need databases to operate efficiently and profitably. But it is important to remember that no compelling need or sound justification for the existence of a database means that data protection obligations and security measures can be ignored.

Databases can be a "treasure" not only for businesses, but also, ultimately, for customers if a more efficient and profitable business means better products or services but this can only be achieved if the databases are managed in a manner compliant with data protection and other related principles.

NOTES

[1] The executive summary can be found here: http://www.parliament.uk/deposits/depositedpapers/2008/DEP2008-0502.pdf

Amendments to the Indian Information Technology Act: implications for Australian corporations

By Michael Pattison, Partner, at Allens, Arthur Robinson.

In brief: The Indian Government is in the process of finalising regulations to clarify the operation of various new provisions under the recent Information Technology (Amendment) Act 2008. Michael Pattison reports on the legislation, and on the implications for Australian corporations.

Michael Pattison can be contacted at: Michael.Pattison@aar.com.au

How does it affect you?

The recent Information Technology (Amendment) Act 2008 will:

- require Indian service providers who handle 'sensitive personal data' on their computer systems to maintain 'reasonable security practices and procedures'; and
- provide some legislative backing for data protection obligations under Indian law.

Australian corporations who have (or are contemplating) commercial outsourcing arrangements with Indian

service providers will still need to implement rigorous provisions in their agreements to protect personal data.

Introduction

The Information Technology (Amendment) Act 2008 (the "Amendment Act") introduces new provisions into India's existing Information Technology Act 2000 (the "IT Act") to deal with issues such as data protection, cybercrime, ISP liability and electronic signature authentication. The Indian Ministry of Communications and Information Technology (MIT) recently issued draft rules in relation to the Amendment Act for public comment, and has also sought the input of the Indian IT industry body, NASSCOM, and its related industry self-regulatory organisation, the Data Security Council of India (DSCI), on how the new statutory concepts of 'reasonable security practices and procedures', 'personal information' and 'sensitive information' should be defined and applied. Finalisation of these regulations is the last step of notification required for commencement of the Amendment Act.

Background

The Bill was passed by the Indian Parliament on December 23, 2008 and subsequently assented to by the President on February 5, 2009. Despite the relatively low-key passage of the Bill through the Parliament, much of the Indian media coverage focused primarily on the cybercrime (interception powers) aspects of the Amendment Act.

Relevance to Australian corporations

Australian corporations with commercial outsourcing arrangements with offshore Indian service providers will be most interested in the data protection aspects of the new legislation. Among other new requirements, under Section 43A of the Amendment Act, a body corporate that possesses or handles 'sensitive personal data' on computer systems that it owns or controls is liable for negligence where its failure to implement and maintain 'reasonable security practices' causes 'wrongful loss or wrongful gain' to a person. The definitions both of 'sensitive personal data' and of 'reasonable security practices' make reference to practices and information that may be prescribed by the government in consultation with industry professional bodies.

NASSCOM and DSCI recommendations

The reference to prescribed government practices in the Amendment Act has required the MIT to seek industry consultation on the appropriate frames of reference for these definitions.

On April 2009, NASSCOM and the DSCI prepared their recommendations for the draft rules after consultation with their members. In relation to the Section 43A definitions, NASSCOM and the DSCI advise that:

- 'reasonable security practices' be, in effect, a self-declared written and implemented policy by which an organisation will state the security standard it adopts (which may be a combination of ISO 27001 and OECD Security principles). An organisation will need to document procedures setting out its selected security controls and how they are implemented. In the event of any security breach, an organisation will need to demonstrate that it conforms with its own policy procedures and that the security controls were commensurate with the assets being protected;

- 'personal information' be information relating to a person who can be identified directly or indirectly by reference to an identification number or by one or more specific factors in relation to that person's physical, economic, cultural, physiological or mental details. This is consistent with the definition of 'personal data' in Article 2a of the EU Privacy Directive 95/46; and

- 'sensitive personal information' be defined to include data pertaining to health or sex information, but excluding data references to racial or ethnic origin, political or religious beliefs, which, by contrast, are included in the corresponding definition in the EU Privacy Directive.

Existing Australian privacy laws permit the transfer of personal information to a recipient outside Australia, provided that the transferring organisation reasonably believes that the overseas recipient is subject to a law, scheme or contract that is substantially similar to Australian privacy law. As a consequence, Australian corporations are generally advised to make sure their offshoring contracts stipulate data privacy compliance provisions that are consistent with, and not less than, those that apply under Australian law.

The new Indian regulations may simply require self-regulation by service providers, which may involve less onerous security standards. Accordingly, it is recommended that Australian corporations engaged in offshoring arrangements review and continue to ensure that their contracts expressly set out rigorous data privacy and data security practices and standards.

What next?

We will continue to monitor this discussion and the finalisation of the rules that will apply to the commencement of the Amendment Act.

Privacy on the Internet and bloggers' identity

By Maria Giannakaki, Attorney at Law and Vassilis Papadopoulos, Trainee Lawyer Karageorgiou & Associates Law Firm, Athens.

A legal opinion issued by the retiring public prosecutor of the Greek Supreme Court, stipulating that blogs are means of public expression and consequently the identity of Internet bloggers is not subject to the privacy of telecommunications, raises several questions and objections by the competent Greek authorities and legal experts.

The legal opinion

According to the legal opinion of the public prosecutor, the privacy of electronic communications does not protect communications through the Internet and "external communication data" such as names and other personal data used to identify the user of electronic communication services, as well as traffic data (data referring to the routing, duration, time and volume of the communication, the location and terminal of the equipment *etc*) and location data (data indicating the geographic position of the terminal equipment of the user). Based on the above, the prosecutor concluded that telecommunication service providers bear the obligation to give access to communications of private individuals or organisations to prosecuting, investigative and police authorities as well as Judicial Councils and Courts, without prior authorisation by a Public Prosecutor of the competent Authority. In addition to the above, he suggested that Internet service providers should give access to both external data and content of the communication, while providers for services other than Internet should give access only to traffic data, not to the content of electronic communications.

This legal opinion, issued following a request by the police department for criminal proceedings against computer crime, leads to the lifting of anonymity of Internet blogs and if applied it may result in criminal prosecution of bloggers not only for serious felonies, but also for regulatory offences such as defamation. According to the President of the Hellenic Data Protection Authority ("DPA") this legal opinion is a cause for legal concerns for the reason that it does not comply with the Law 3471/2006, implementing the EU Directive 2002/58 regarding the processing of personal communication data.

The authors can be contacted at: giannakaki.m@dsa.gr and v_papado@hotmail.com

General framework: legal interception

According to the Greek legislation on privacy in the telecommunication sector and in the light of the legal opinion no 79/2002 of the Greek Data Protection Authority, privacy covers the external data of communication (telephone numbers, subscribers names, contact details, IP addresses *etc*) and the content of communication. With regard to the content of the communication, article 19 of the Greek Constitution and article 4 of the Law 2225/94 are applicable. "External communication data", are qualified as personal data and therefore the Law no 2472/1997 with regard to personal data collection and processing and Law no 3471/2006 with regard to the privacy in the telecommunication sector are applicable.

Content of the communication

Article 19 of the Greek Constitution, protecting freedom of correspondence and communication provided for two legal causes of lawful interception:

a. the protection of national security; and

b. investigation of crimes.

Law 2225/94 with regard to disclosure of private communications describes the procedure for lawful interception for each of the abovementioned causes.

With regard to national security, only judicial, administrative, military, police or other public authorities may submit an application before the Public Prosecutor, if the issue of national security comes within the scope of their competence.

With regard to investigation of crimes, lawful interception is permitted only for specific offences provided by penal law (*e.g.* treachery, falsification of currency, explosions *etc*) and is permitted only against targeted suspects involved in a crime under investigation or against persons used by suspects as contacts or liaisons.

In very urgent matters, the Public Prosecutor or examining magistrate may themselves order lawful interception, but they are obliged to submit the issue to the Council within three days. If the Council does not approve the order of the Public Prosecutor or examining magistrate the decision for lawful interception is abolished.

External communication data

According to Article 4 of the Law 3471/1997 implementing Directive 2002/58/EC on the protection of privacy in the electronic telecommunications sector,

> "any use of electronic communications services offered through a publicly available electronic telecommunication network, as well as the pertinent traffic and location data shall be protected by the principle of confidentiality of telecommunications. The with-

drawal of confidentiality shall be allowed only under the procedures and conditions provided for in Art. 19 of the Constitution".

Therefore, listening, taping, storage or other kinds of interception or surveillance of communications and the related data is prohibited, except when legally authorised.

Binding character of public prosecutor's legal opinion

According to Article 25 of the Law 1756/1988, the public prosecutor of the Greek Supreme Court renders a legal opinion with regard to "legal issues of wide public interest", on the interpretation and implementation of the penal law. His legal opinion is an "official interpretation" of the law but it is not an "authentic interpretation". Only the Greek Courts by virtue of their decisions have the authority to give "authentic interpretations" of the laws and for that reason the legal opinion of the prosecutor does not have a binding character for Greek Courts. Moreover, the legal opinion does not have a binding character towards other prosecutors due to the principle of independence of the prosecution service.

Conclusion

Following the aforementioned analysis, we may conclude that the legal opinion includes a misinterpretation of the conditions for lawful interception without taking into consideration the European legislation regarding personal data protection and privacy in the telecommunication sector, which has been implemented in the Greek legislation.

From a practical point of view, conditions of lawful interception are very strict and not flexible. Police authorities often handle cases that may involve serious criminal offences, especially with the use of computers or through the Internet, which are not included in the list of offences for which the anonymity can be lifted according to the Law 2225/1994. In such urgent cases, crimes cannot be prevented or electronic traces may be lost during the process of application for lawful interception. However, the abuse of the right of privacy of communications and the lifting of the protection of personal data cannot be a solution. On the contrary, a better protection may be accomplished through the addition of offences to the list of crimes for which communication privacy may be lifted.

Following a proposal of the Hellenic Authority for the Communication Security and Privacy, the Greek Penal Code and the Law 2225/94 was relatively recently amended and the offence of pedophilia was added to the offences for which lawful interception may be permitted. Other offences that may also be added to Article 4 of the Law 2225/94 are those described in Articles 370A, 370B and 370C of the Greek Penal Code, regarding violation of communications privacy and computer crimes.

ICO publishes privacy notices code of practice

By James Castro-Edwards, Solicitor, and Vinod Bange, Partner, Speechly Bircham LLP.

On June 12, the UK Information Commissioner's Office launched its Privacy Notices Code of Practice. The Code is intended to assist organisations which collect and process personal data to draft more user-friendly privacy notices. The Code is a clear signal from the ICO that existing privacy notices, which are confusing and written in legal jargon are unacceptable.

Background

The Code follows the ICO's crackdown on misleading small print of February this year. Research conducted by the ICO revealed that half of consumers do not understand what they are signing up to when they fill in online and paper forms. The ICO research revealed widespread consumer cynicism in relation to privacy notices, with consumers believing that privacy notices were drafted to confuse them and simply serve as a licence for companies to sell individuals' personal information. In response to the findings of the research, the ICO expressed concern that "*too many companies baffle customers with a lengthy and unnecessary 'legalese'*". The research also revealed the following findings:

- consumers wanted to see clearer ways of opting out of receiving marketing, less jargon and a clear explanation of how their personal information would be used;
- half of consumers surveyed suggested that larger text should be used instead of the customary 'small print'; and
- almost three quarters of the UK population did not properly read or understand privacy notices.

As well as calling for organisations to improve their privacy notices, the ICO urges individuals to take the time to read and understand privacy notices in order to understand how their personal data will be used and to avoid being bombarded by marketing material they have

The authors can be contacted at James.Castro-Edwards@speechlys.com and Vinod.Bange@speechlys.com.

  WDPR ISSN 1473-3579

not asked for. In response to the survey, Information Commissioner Richard Thomas said,

> "Too many privacy notices involve too much small print and too much confusing gobbledegook. Privacy notices are an important way to inform individuals and ensure that organisations are open about how they use personal information. But no one should need a magnifying glass or a lawyer to find out what will happen to their information, and what their choices are and what their rights are. Too many privacy notices are written to protect organisations, rather than to inform consumers. What chance do people have if privacy notices are written in complex legalese? How can you make an informed decision without understanding what you are signing up to? Organisations should only collect the minimum of personal information and they must explain what they will do with it in clear, plain language."

The ICO was not alone in its condemnation of current practices surrounding the use of privacy notices. Television broadcaster and consumer champion, Nick Ross, expressed his support for the campaign, recognising that data controllers that hide dubious privacy and marketing practices behind legal jargon or small print are a widespread problem.

The Code places the responsibility firmly with data controllers for explaining in a clear manner exactly what will be done with individuals' personal data. The underlying message in the Code is that organisations must use personal information in a way which people would expect.

At the same time, the ICO has made it very clear that individuals should take the time to read privacy notices, in order that they understand exactly what they're permitting companies to do when their personal data is collected. The ICO also published a leaflet aimed at individuals explaining the protection they should expect in privacy notices and what they can do if they feel their information has been misused.

The guidance contained in the Code

The Code is aimed at organisations that process personal data. As a starting point it recommends that plain English is used rather than "legalese or technical language". It also emphasises that the duty to actively communicate a privacy notice is the strongest where a data subject is unlikely to expect the processing undertaken by the data controller in respect of their data, or where the data collected is particularly sensitive. Sensitive personal data is defined by the Data Protection Act 1998 and includes data relating to an individual's health, sexual life, religious or philosophical beliefs or criminal record. The Code goes on to explain that an organisation which only processes personal data in an obvious way may not need to actively draw data subjects' attention to its privacy notice.

The Code explains the purpose of a privacy notice, mainly to satisfy the first principle of the DPA. However, the ICO points out that a privacy notice drafted in legal language solely to cover the legal obligations of the data controller is unlikely to satisfy the objectives of the Code. The Code is aimed at all organisations which collect information about individuals. The ICO gives a number of examples:

- organisations which ask people to fill in their names, addresses and health information on an official form;
- information about shoppers from their loyalty card transactions;
- call centres which record and retain calls made by customers; and
- analysis of consumers' online purchasing habits to send out targeted special offers and recommendations to those same consumers.

The Code explains what information must be included in a privacy notice under the DPA, and goes on to explain the necessity of fairness and transparency in drafting a privacy notice. It also recommends that in situations where data controllers use data for a variety of reasons, rather than having a single "catch all" policy it may be advisable to have a number of policies which are tailored to their data subjects. The Code does not give any specific examples, but this would cover, for example, a privacy notice used to inform potential recruits as well as potential customers about the way their information will be processed. The Code goes on to emphasise the necessity for transparency, and explain the difference between transparency and consent. While valid consent requires transparency from the data controller, a detailed description of processing and disclosure, no matter how transparent does not in itself amount to consent.

The Code explains that there is no requirement to "actively communicate" a privacy notice where the collection in use of personal data is obvious, for example where individuals requesting a service cannot receive the service unless they provide personal data such as their name and address. However, even in cases where the use of personal data is obvious, the ICO still recommends that organisations have a privacy notice in place, for those data subjects who wish to understand more about the ways in which their information is possessed. Active communication involves taking positive action to provide the privacy notice to a member of the public, for example by sending a letter, reading from a script or sending a copy of the privacy notice by email. The Code goes on to say that where data is collected from data subjects and the data controller subsequently decides to process the data in another manner, consent from the data subject should be actively sought. In practice, this will involve contacting the affected data subject and may require opt-in consent for the data subject's approval of the new purpose, depending upon the circumstances.

The ICO recognises the value to data controllers in data

sharing with third parties. However because of the risks to individuals by collating different data sets about them, information such as the names of the third parties to whom data is disclosed should be given when the data is collected. In particular those organisations which collect personal data expressly with the intention of selling that on to unspecified third parties must make this very clear to the data subject. The Code says that where data is collected for one purpose and subsequently used for another purpose, which was not revealed to the data subjects, the data controller may well be in breach of the DPA.

Drafting privacy notices

Transparency

The Code makes it very clear that the primary purpose of a privacy notice is to inform data subjects about the uses of their data in a clear and transparent manner. It is not to indemnify an organisation against claims from data subjects.

Same media

The guidance also recognises that privacy notices are not just limited to online privacy policies, but extend to oral notices, printed notices or notices conveyed by way of poster as well as privacy policies in electronic form. The Code suggests that the medium through which personal data is collected is also used to transmit the privacy notice, so in a face to face meeting where individuals' details are collected by the data controller, the individual should be informed orally of the privacy notice during the meeting. Where the circumstances in which personal information is collected make it impossible to transmit the privacy notice, data controllers must ensure that they do not process data in a way that would be unexpected by the data subject.

Layered

The Code recommends a "layered" approach, where the basic information is readily accessible, as most data subjects are unlikely to read the whole policy. However, a layered policy would also include more detail which the interested data subjects can find by for example following a link.

Vulnerable groups

The Code also recommends that where a privacy notice is aimed at a vulnerable group, for example children, it is drafted in such a way that it is understandable by the vulnerable data subject. It recommends that privacy notices are reviewed on an ongoing basis to reflect and changes in the data processing activities of the data controller.

Practical examples

The Code gives a number of practical examples of good and bad privacy notices. Most of the given examples of bad privacy policies will not be unfamiliar to readers. For example, a large block of small print text containing legal language is considered as bad practice, in particular when compared with simple language, clear font and style. Explanations of why information should be provided (such as providing a phone number to assist with an insurance claim) are encouraged, along with honest explanations of the outcomes of choosing not to provide certain information. However, practices such as implying the provision of certain information is mandatory when in fact it is not, referring generally to "third parties" rather than identifying those individuals or entities and using confusing language are regarded as bad practice. Practices such as referring to the DPA and the use of official sounding or legal language are discouraged since this is off-putting to users, while clear, straightforward guidance and helpful advice are encouraged.

Comments

The Code is likely to apply to the vast majority of privacy notices currently in use, and will be useful to even those organisations that have genuinely tried to make their privacy notices as clear, transparent and user-friendly as possible. The ICO has made it very clear that a privacy notice is not to protect the data controller but to protect the data subject. The ICO is not alone in its view that most existing privacy notices are inadequate and do not achieve their intended purpose. In May of this year the London School of Economics and Political Science in conjunction with 80/20 Thinking published its report for the Working Group on Consumer Consent. The Report commented on the fact that for consent to be valid, the data subject should be properly informed by the data controller as to how the data subject's data would be processed. The Report notes that privacy notices are inherently complex and difficult to follow for users. Many studies show that individuals simply never read them. However, both the Report and the Code place emphasis on individuals to take the time to read privacy notices. Data subjects are urged to actually read privacy notices in order to fully understand the purposes for which their data will be processed. Though clearly, individuals are unlikely to take an interest until organisations adopt a more user-friendly approach in drafting privacy notices. In the US earlier this year, government research into the way that bank customers best understand privacy and information sharing policies revealed that the solid text format used by most policies is ineffective in achieving its intended aim, when compared to alternative approaches. The research commissioned by the US government created fake notices, typical of those currently used by US banks and found that the tabular notice format was the most effective at helping users to understand its content.

  WDPR ISSN 1473-3579

Clearly, organisations that collect personal data and process it in a manner which may not be readily apparent or readily obvious to data subjects should take the recent guidance to heart. While organisations which rely on privacy notices may be reluctant to revisit them, the ICO suggests that by being transparent and honest with data subjects, an organisation will benefit.

A good privacy notice increases trust and improves the relationship with the people companies collect information about. A good privacy notice also:

- gives a competitive advantage by reassuring data subjects that their privacy is a serious issue;
- encourages people to provide more valuable information by instilling confidence that it will be used properly;
- allows customers to indicate their marketing preferences which may encourage them to respond more positively; and
- decrease the risk of queries, complaints and disputes about the data controllers use of the data subjects' personal information.

The Code is not legally binding, however in his introduction to the Code, Information Commissioner Richard Thomas says,

> "I will take its standards into account when for example, I receive a complaint that information has been collected in an unreasonably way".

Accordingly, if an organisation that was being investigated by the ICO had failed to follow the guidance, that organisation would have done itself no favours in demonstrating a desire to comply with the DPA.

Benefits aside, it will be interesting to see if, following the publication of the Code, the Information Commissioner takes enforcement action against organisations which rely on incomprehensible privacy policies to license sharp practice with consumers' personal information. Prudent data controllers would then do well to revisit their privacy policies in the light of the new guidance.

Administration proposes new Federal Consumer Financial Protection Agency

By Heidi Salow, Of Counsel and Micah Thorner, Associate, DLA Piper.

Addressing the Obama Administration's proposals to reform financial regulation in the US, Barney Frank (D-MA), Chairman of the House Financial Services Committee, has promised to report legislation which would create a new Consumer Financial Protection Agency (CFPA) before the House adjourns for its August recess at the end of July 2009.

This proposed new agency would be authorised to concentrate in one agency many of the consumer protection powers over mortgages and credit cards that now are spread across as many as 10 federal regulators. The Obama Administration proposal is set forth in a Department of the Treasury report, "Financial Regulatory Reform: A New Foundation".

The Report reflects the Obama Administration's view that a broad reorganisation of the way the government regulates its financial system and protects consumers is necessary because consumer protection has allegedly taken a back seat to other aspects of bank regulation. This view follows the issuance, in the waning months of the Bush Administration, of strong credit card regulations by the Federal Reserve Board, compounded by the recent enactment of legislation that threatens to dramatically alter the existing business model that has historically governed the credit card industry.

The CFPA would be charged with ensuring that consumers have clear information about the financial products or services they purchase, as well as protecting them from any deception they might encounter when purchasing such products. The proposed legislation suggests that the agency could accomplish these objectives by requiring lenders to make safer, "plain vanilla" products clearly available to consumers, while stepping up

Heidi Salow is Of Counsel in the Communications, Privacy and eCommerce group at DLA Piper a global law firm with over 67 offices in 38 countries. Ms Salow has been handling cutting-edge privacy and data security, intellectual property and e-commerce issues for most of her career. Her practice includes transactional, legislative, and compliance work for Fortune 500, mid-sized and start-up companies.

She also regularly advocates on public policy and legislative matters before the Federal Trade Commission, Federal Communications Commission, state legislatures, and members of Congress. Her clients come from a variety of industries including the telecommunications services, education, hotel/hospitality, medical and consumer products industries. She can be contacted at: Heidi.Salow@dlapiper.com

Micah Thorner is an Associate in the Communications, Privacy and eCommerce group at DLA Piper. Her practice focuses primarily on international data protection regimes and compliance with federal privacy and data security laws. She counsels clients on ways to manage international data flows, particularly mechanisms for US companies to comply with the EU Data Directive. She can be contacted at: Micah.Thorner@dlapiper.com

scrutiny on alternative products. The agency would be empowered to issue new regulations requiring financial disclosure documents to "balance communication" of the relative merits of the products or services, "prominently disclose significant risks and costs," and communicate those risks and costs in a "clear, concise, and timely" manner. In short, the Administration proposes a reform of financial services regulations that purport to integrate the consumer perspective, by rule, into the marketing and sale of financial services and products.

These reforms have many legislators and businesses very worried. Some of their key concerns about the proposal include:

1. Broad authority over financial products.

Under the terms of President Barack Obama's plan, the new agency would have sweeping authority over providers of financial products, including banks and credit card companies. The authorisation language in the proposal is very broad and so the precise impact of any forthcoming regulations is difficult to gauge. Nonetheless, many in the financial services industry have expressed grave concerns about whether this proposal will add yet another layer of regulation and whether the federal government, in the form of CFPA, will soon be dictating the terms of the products the industry offers – for example, the rate and fees that can be charged to credit card customers – and whether rules that are virtually unreviewable could meaningfully alter their business models and threaten their economic viability. In addition, given the broad language used to define the concepts of financial services and products in this new proposed statute, and the extensive delegation of authority provided to this new agency by the contemplated legislative provisions, it is possible that jurisdiction may be asserted over products and services not traditionally seen to be within the scope of conventional financial services and products. One consequence of being subject to such jurisdiction would include the possibility of non-recognition of an agreement to arbitrate.

2. New regulator with less knowledge

The proposal removes responsibility for consumer protection from the existing federal banking agencies and Federal Trade Commission and sequesters it in a new federal agency with no other defined purpose other than to "promote transparency, simplicity, fairness, accountability, and access in the market for consumer products or services." The CFPA would be charged with protecting consumers of credit, savings, payment, and other consumer financial products and services, except for investment products and services currently regulated by the SEC. The FTC would retain authority for dealing with fraud, remain the lead agency for data security and have backup authority for the CFPA. The new agency, however, would become responsible for privacy protection related to financial products, services and transactions.

Because the CFPA's supervisory, examination and enforcement authority would extend to all persons and entities covered by the statutes it implements, as well as by statutes with no or limited rule-writing authority (such as the Fair Credit Reporting Act [FCRA] or Gramm-Leach-Bliley Act [GLBA]) all federal and state chartered depository institutions, bank affiliates and other non-banking institutions would fall within its jurisdiction despite the new agency's limited knowledge of financial regulations issued across multiple federal agencies. In other words, critics contend, the new agency would have enforcement authority without the necessary technical and institutional expertise to successfully protect consumers. It should be added that enforcement authority for this new agency not only contemplates the ability to litigate free of the Justice Department in federal courts, but also to represent itself before the United States Supreme Court following notice to the US Attorney General.

Because most, if not all, financial services products would be regulated by one agency, it is possible that such a structure would give the CFPA only some of the information it would need for effective regulation, making the whole system weak and inefficient.

3. New disclosure standard creates uncertainty for financial services companies

In March 2007, eight federal regulators (the Board of Governors of the Federal Reserve System, the Commodity Futures Trading Commission, the Federal Deposit Insurance Corporation, the Federal Trade Commission, the National Credit Union Administration, the Office of the Comptroller, the Office of Thrift Supervision and the Securities and Exchange Commission) requested comment on a model privacy form (Model Form) that financial institutions would be able to use for their privacy notices to consumers, as required by GLBA. The agencies made clear that use of the Model Form (expected to be finalised in August) would be entirely voluntary but would allow entities to qualify for a safe harbor. Achievement of safe harbor status would depend on vigorous adherence to the content and format requirements set forth in the proposed rule, however. The information contained in the proposed Model Form is highly standardised, permitting very little variation among entities' disclosures about their information sharing practices.

The Administration's proposal would potentially limit the ability of financial service providers to obtain this safe harbor by using the Model Form. The Administration's Report proposes that the CFPA enact regulations:

- making all mandatory disclosure forms clear, simple and concise;

  WDPR ISSN 1473-3579

- requiring that disclosures and communications with customers be clear and reasonable; and
- allowing the CFPA to use technology to make disclosures more dynamic and relevant.

The plan would require financial service providers to present disclosures that are "technically compliant, non-deceptive and reasonable". To satisfy this new standard, marketing materials, notices (including privacy notices) and other consumer communications would have to identify any significant product risks, and a provider that failed to meet this duty would be subject to action by the CFPA. When introducing a new product or service, a provider would risk liability – even for using a model form – unless the provider obtained a "no action letter" or waiver from the CFPA.

In light of these specific proposals for consumer notices and communications, it is unclear at this early juncture whether the proposed Model Form will become obsolete.

Conclusion

Given the role that abusive and overly complex exotic mortgage products played in sparking the financial crisis, at first glance an independent agency dedicated to consumer financial protection might not seem terribly radical. But the true impact of such a new federal bureaucracy, operating with a singular purpose yet in the absence of any true institutional context, lies in the many details to be unveiled as the legislative process evolves. Already, many serious questions have arisen, with answers yet to come.

A copy of the report is available from: http://www.finreg21.com/content/financial-regulatory-reform-a-new-foundation-1

Privacy, data breach protection and notification laws: changes to US privacy laws

By Gregory T. Casamento, Partner, New York, Brian T. Casey, Partner, Atlanta, Patrick J. Hatfield, Partner, Atlanta and Vita E. Zeltser, Associate, Atlanta, Locke Lord Bissell & Liddell.

The overwhelming majority of individual states in the US require those who own, license, store or maintain personally identifiable information of that state's residents to provide notice to those residents when their personally identifiable information has been breached.[1] Navigating the patchwork of each state's notification laws and compliance with those laws in the event of a breach do not come cheap. Studies show that, on average, a data breach in a US company costs $202 per lost record in associated lost business costs, as well as notification compliance costs.[2] One can imagine that the cost for a non-US company would be even higher, given the additional costs and burdens of compliance over international territories. Notwithstanding the multitude of laws intended to protect residents' personally identifiable information, the associated costs of compliance both pre-breach and post-breach, and the reputational injury that occurs, major data security breaches in the US are commonplace. News of employees engaging in the unauthorised review of employee personnel, customer or patient records, stories of stolen or lost laptops containing the names, addresses, federally issued Social Security numbers and credit card numbers of customers or employees, and criminal investigations of sophisticated hackers accessing customer or employee information through cyber-piracy to serve as sobering reminders that in the era of digitised personal information and portable electronic devices, data security breaches occur with alarming frequency. Thus, it comes as no surprise that the laws governing the safeguarding of personally identifiable information and data security breach notification requirements are expanding in scope and stringency as the US federal, state and related governmental agencies attempt to respond to this reality and their residents' concerns about the protection of personally identifiable information.

Gregory A. Casamento focuses his practice on business, commercial, insurance and intellectual property litigation and technology transactions. Mr. Casamento has significant experience litigating trademark infringement claims, technology, contract and restrictive covenant disputes, and insurance issues for his clients before both State and Federal Courts.

Brian T. Casey is a co-leader of Locke Lord's Insurance Practice Group, and a member of the firm's Corporate, Capital Markets and Healthcare Practice Groups. Mr. Casey focuses on corporate, M&A, and regulatory matters for corporate clients in the insurance, financial services and health care industries.

Patrick J. Hatfield co-chairs the Firm's Technology Transactions Group. Throughout his legal career, Mr. Hatfield has focused on financial services, intellectual property and technology, gaining valuable experience as in-house counsel.

Vita E. Zeltser focuses on general corporate and corporate governance matters, preparation and negotiation of commercial contracts, commercial lending and debt financing, and mergers and acquisitions.

Massachusetts Security Breach Regulations: a sign of what's to follow?

The state of Massachusetts, for example, has taken a significant step to address data security through the efforts of the Massachusetts Office of Consumer Affairs and Business Regulation ("MCA"). The MCA recently enacted a regulation, effective January 1, 2010, (the "Massachusetts regulation") setting stricter security standards for the protection of all Massachusetts residents' personally identifiable information and broader notification requirements for the breach of such information. These standards include specific encryption requirements for all persons that own, license, store or maintain personally identifiable information in both electronic and paper form about Massachusetts residents.[3] The term "Massachusetts Resident" in the regulation indicates that any company or entity, whether located in Massachusetts, another state, or even outside the United States, that owns, licenses, stores or maintains a Massachusetts Resident's personal information is subject to the Massachusetts regulations.[4] While presently many US states require pre-breach security measures and post-breach notification requirements to safeguard personally identifiable information, those measures are not as comprehensive as those that will become mandatory under the Massachusetts regulation.[5] The substantive details of the Massachusetts Regulation, the Massachusetts notion of "residency" and its effect on non-US holders of personally identifiable information (defined as collectors, users, sellers, or holders of personally identifiable information) is discussed more fully below.

Federal legislation

The US Senate has also responded to the call for additional protections on personally identifiable information, though moving at a much slower pace than Massachusetts. A proposed federal bill sponsored by Sen. Dianne Feinstein (D-CA), titled the Data Breach Notification Act ("Senate Bill 139"), would require all federal agencies and persons engaged in interstate commerce who are in possession of data containing sensitive personally identifiable information to disclose any breach of such information. The federal bill provides that once it is passed into law, it "shall supersede. . . any provisions of law of any [s]tate relating to notification by a business entity engaged in interstate commerce or an agency of a security breach," subject to some exceptions for victim protection assistance provided by state laws.[6] This bill has been in the Senate Committee on the Judiciary since January 6, 2009, and no action has been officially reported on it since that date, so given the passage of time it is possible that this bill may not become law during the current congressional term.

Most recently, on April 30, 2009, the US House proposed the Data Accountability and Trust Act ("House Bill 2221"),[7] which contains certain information security safeguards aimed at protecting computerised data containing personal information and, like Senate Bill 139, requires a nationwide data security breach notification in response to a breach. The House bill was recently amended and recommended for full committee vote of the House Energy and Commerce Committee.

The trend continues

The Massachusetts regulation and the two proposed federal bills constitute a drastic expansion of security and notification obligations and requirements, and both are the bellwether for future laws and regulations in the data security management and breach notification areas.[8] Therefore, the key requirements of the Massachusetts regulation and the proposed federal bills will be discussed in greater depth below to provide non-US based holders of personally identifiable information a better understanding of how to prepare to meet the upcoming data management and security challenges associated with handling personally identifiable information. If either the proposed Senate or (as seems more likely to be the case) House legislations are enacted, they would preempt current state notification laws, creating a uniform national standard for data breach notification.

Massachusetts: written comprehensive information security program requirement

The new Massachusetts regulation, 201 CMR §§ 17.01 – 17.04, referred to as the "Standards for the Protection of Personal Information of Residents of the Commonwealth," provides the minimum standards to be met in connection with the safeguarding of personally identifiable information contained in both paper and electronic records. The regulation requires all persons that own, license, store or maintain personally identifiable information about a Massachusetts resident to develop, implement, maintain and monitor a comprehensive written information security program to safeguard that information.[9] The program must be consistent with industry standards, and must contain administrative, technical and physical safeguards to ensure the security and confidentiality of personal information. Although the regulation provides that the information security program's scope will depend on the size, scope, and type of business at issue, the amount of available resources and stored data and the need for security and confidentiality, the regulation provides a list of specific elements the information security program must contain, including:

1. designating a specific employee to maintain the information security program,

2. identifying and assessing reasonably foreseeable internal and external risks,

3. developing security policies in connection with records that are transported outside the business premises,

  WDPR ISSN 1473-3579

4. imposing disciplinary measures for violations,

5. preventing terminated employees from accessing records by immediately terminating their access to physical and electronic records,

6. verifying that third-party service providers adhere to equally stringent security measures,

7. limiting the amount of sensitive personal information collected and retained,

8. identifying the electronic media that contain personal information,

9. placing reasonable restrictions on records containing personal information,

10. regularly monitoring the information security program,

11. reviewing the scope of the program at least annually, and

12. documenting all responsive actions taken. [10]

The regulation also contains computer system security requirements that require, among other measures, securing user authentication protocols such as user IDs and reasonably secure passwords, placing restrictions of access to the personally identifiable information to those with a need to know basis to perform job duties, education and training for employees, and similar security measures. The regulation also requires, to the extent technically feasible, encrypting all transmitted records containing personal information that will travel across public networks, encrypting all data containing personal information to be transmitted wirelessly, and encrypting all personal information stored on laptops or other personal devices.

The broad implications of the regulation to non-US businesses and other entities handling personally identifiable information cannot be understated. The technical requirements of the regulation go beyond any current state laws and will require companies to rewrite their IT playbook and specifically, their data security management and data breach response plans. Moreover, the fact that the regulation applies to records stored in both paper and electronic form should provide incentive for those holders who have been waiting to convert paper records to electronic records. Finally, because the regulation applies to information about employees who are Massachusetts residents, even entities that do not engage in transactions with consumers and are otherwise exempt from the requirements of the US Federal Trade Commission's ("FTC") Red Flags Rule,[11] will need to adopt a written comprehensive information security program to meet the standards. These changes are significant and non-US based holders of personally identifiable information should plan, adopt and test their revised information security programs now, so that those programs meet the regulation's standards on January 1, 2010.

The Massachusetts regulation protects the personal information of all "residents" of Massachusetts. Unfortunately, the term "resident" is not defined anywhere in the Massachusetts statutes. Indeed, there is no formal procedure for establishing a legal residence in Massachusetts and the definition of "resident" varies depending on the context in which the term is used. Voter registration, automobile registration, a driver's licence, the appearance of a person's name on a city or town street list, and rent, utility, mortgage or telephone bills normally provide tangible proof of residence. Regardless of context, though, "resident" appears to be a broadly defined term. Massachusetts regulators elected use of the term "resident" instead of "citizen" in the data protection regulations, thus evincing intent to protect a broader range of individuals subject to jurisdiction. Citizenship is not equated with residence but with "domicile," which is defined as the place where an individual has his "true fixed home and principal establishment, and to which, whenever he is absent, he has the intention of returning." [12] "Citizen" is a more restrictive term than "resident," and the terms are not interchangeable and signify different classes of people – the case of "residents" being a much broader class of people. [13]

For a non-US Company that has experienced a security breach, trying to determine which individuals whose information may have been compromised by the breach are protected by the Massachusetts regulation will present some challenges in light of the absence of clear authority for the establishments of residency in this context. If the person affected by the breach is an employee, the company would look to the state to which the employee pays income taxes, the state which the employee indicates in his home address, the state of the employee's driver's licence, or other similar indicators. If the affected person is a customer or patient, that person's home address on file with the company, or other information, such as the state of the person's automobile registration or driver's licence, or any other state-specific information the company may have on record, could also be used as a guide to determine residency. Assuming any one of these factors points to a Massachusetts residency, the company may seek to err on the side of caution and provide breach notification to such individuals as a precautionary measure.

Federal Data Breach Notification Act

Senate Bill 139, the proposed Federal Data Breach Notification Act, requires any federal agency or business entity engaged in interstate commerce that uses, accesses, or collects sensitive personally identifiable information to (a) provide notice to any US resident whose information may have been accessed or acquired following the

discovery of a security breach; and (b) provide notice to the owner or licensee of any such information that the agency or business does not own or license. As noted above, the federal bill provides that once it is passed into law, it "shall supersede. . . any provisions of law of any [s]tate relating to notification by a business entity engaged in interstate commerce or an agency of a security breach," subject to some exceptions for victim protection assistance provided by state laws.[14] Senate Bill 139 exempts: (1) agencies and business entities from notification requirements for national security and law enforcement purposes; (2) security breaches where the agency or business conducts a risk assessment that concludes there is no significant risk of resulting harm, provides the results of the risk assessment to the Secret Service and the Secret Service does not respond within 10 days with a written directive requiring notification; and (3) business entities that utilise a security program that blocks the use of sensitive personally identifiable information and provides notice of a breach to affected individuals. Under certain circumstances, the Secret Service, the FBI, the Postal Inspection Service, and State Attorneys General must be notified of the data security breach. Senate Bill 139 includes appropriations for costs incurred by the Secret Service to investigate and conduct risk assessments of security breaches. Certain violations are punishable by civil penalties, and the US Attorney General and State Attorneys General may bring a civil action against any business entity that violates Senate Bill 139. Senate Bill 139 further amends the Fair Credit Reporting Act to require agencies to include a fraud alert in the file of a consumer that submits evidence of compromised financial information to a consumer reporting agency. The text of Senate Bill 139, as currently drafted, is likely to undergo significant revisions, and as of the date of this article, the proposed Act had been forwarded to the Senate Committee on the Judiciary.

Federal Data Accountability and Trust Act

On April 30, 2009, House Bill 2221 was proposed with bipartisan sponsorship in the US House of Representatives. It was amended and forwarded to the full House Commerce Committee on June 3, 2009. The proposed bill requires the FTC to promulgate regulations requiring each person engaged in interstate commerce and that directly or through a third party owns or possesses data in electronic format containing personal information to establish and implement policies and procedures regarding information security practices for the treatment and protection of personal information, including destruction of such information. Additionally, the proposed bill contains data security breach notification requirements applicable to any person engaged in interstate commerce that owns or possesses data in electronic format containing personal information.

House Bill 2221 notification requirements are largely similar to those currently in force in most states, with some substantive modification. The bill requires notices of a data breach to be sent to all affected US citizens or residents and to the FTC. If health information is breached, the Secretary of Health and Human Services is to be notified. The bill also contains special provisions not otherwise found in state laws for telecommunications carriers, cable operators, information services and interactive computer services providers. Notifications are to be made in written form or by email, under certain circumstances, as is currently permitted in most states. The notification must contain a description of the personal information acquired, a summary of the recipient's rights to free credit reports, and contact information for the company sending the notices, the credit reporting bureaus, and the FTC. Importantly, House Bill 2221, as proposed, has several major limitations that are similar to limits already in existence in some but certainly not all current state laws and regulations. First, it exempts from the notification requirement persons who determine that there is no reasonable risk of identity theft, fraud, or other unlawful conduct resulting from the breach. Second, the bill provides that encryption of data in electronic form, and other technologies the FTC may later identify, establishes a presumption that no reasonable risk of identity theft, fraud or other unlawful conduct exists following a breach. The presumption may be rebutted by facts showing that the encryption may be compromised. Third, the bill requires that, subject to some limitations, companies who must send breach notification letters must, upon request of individuals whose information was breached, provide at no cost to the individuals, consumer credit reports for two years. Finally, the bill allows the FTC to post notices of data security breaches on its website, thus magnifying the publicity given to a breach.

House Bill 2221, as proposed, grants enforcement authority to the FTC, and grants state attorneys general the right to bring civil actions against violators, with penalties up to $5,000,000. As with Senate Bill 139, House Bill 2221 as currently drafted, is likely to undergo significant revisions.

In summary, as the law of privacy and data security continues to evolve, it becomes clear that non-US holders of personally identifiable information will need to plan ahead to respond to the challenges posed by a continuously evolving legal and regulatory landscape to meet these challenges, including the Massachusetts regulation, which takes effect on January 1, 2010 .

Contingency planning

In addition to complying with the specific laws requiring particular security measures to be in place, companies are encouraged to develop a response plan in advance of an actual security incident. Even with the best security measures in place, however, many companies will face the unpleasant experience of having to navigate

   ISSN 1473-3579

through these various laws to determine the applicable notice obligations. A security incident may occur within a company's own IT infrastructure or at the facilities of one of its IT/outsourcing suppliers. A basic contingency plan will help a company respond thoughtfully and quickly. That contingency plan should, at a minimum, identify who within the company and within its advisors should be brought together immediately following the first indication of an incident. The first response team should include the necessary IT and security representatives as well as representatives from the legal and compliance departments who are familiar with the regulatory landscape in the relevant jurisdictions. The relationship manager from significant IT/outsourcing suppliers should also be named in the communication tree to expedite evaluating incidents involving such suppliers. For more information on information security breach or loss notification laws, preparing breach or loss remediation plans, legally compliant breach notices or any of the other issues discussed in this article, contact the authors listed on the first page or any member of Locke Lord's Technology Transactions Group.

NOTES

[1] The definition of personally identifiable information varies by state, but at the US federal level is often defined as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific individual, including any — (A) name, [a federally issued] Social Security number, date of birth, official [s]tate or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number; (B) unique biometric data, such as fingerprint, voice print, retina or iris image, or other unique physical representation; (C) unique electronic identification number, address, or routing code; or (D) telecommunication identifying information or access device." See 18 USC. § 1028(d)(7). A few examples of state laws protecting this information are: California – Cal. Civ. Code § 1798.82; Georgia – O.C.G.A. § 10-1-910 et seq.; Illinois – 815 Ill. Comp. Stat. 530/1 et seq.; Louisiana – La. Rev. Stat. § 51:3071 et seq.; La. Admin Code. tit. 16, pt. III, § 701; Massachusetts – Mass. Gen. Laws ch. 93H, § 1 et al.; New York – N.Y. Bus. Law § 899-aa; Texas – Tex. Bus. & Com. Code § 48.001 et seq.; Washington, D.C. – DC Code Ann. § 28-3851 – 3853.

[2] This figure accounts for an average of $139 lost business costs per record lost, as well as unbudgeted out-of-pocket spending on incident detection and investigation, notification of victims, and related expenses and costs. Ponemon Institute, LLC 2008 Annual Study: Cost of a Data Breach, http://download.pgp.com/pdfs/whitepapers/Ponemon_COB_2008_US_090201.pdf (last accessed July 6, 2009).

[3] The Massachusetts regulations, known as the "Standards for the Protection of Personal Information of Residents of the Commonwealth," define personal information as "a Massachusetts resident's first name and last name or first initial and last name in combination with any one or more of the following data elements that relate to such resident: (a) [S]ocial [S]ecurity number; (b) driver's license number or state-issued identification card number; or (c) financial account number, or credit or debit card number, with or without any required security code, access code, personal identification number or password, that would permit access to a resident's financial account; provided, however, that "Personal information" shall not include information that is lawfully obtained from publicly available information, or from federal, state or local government records lawfully made available to the general public." 201 CMR 17.02.

[4] See 201 CMR 17.01 ("This regulation implements the provisions. . . relative to the standards to be met by persons who own, license, store or maintain personal information about a resident of the Commonwealth of Massachusetts. . .").

[5] For example, Since October, 2008, Nevada's breach notice law requires all Nevada businesses to encrypt all electronic transmissions (other than faxes) of a consumer's personal information if the information is sent outside the secure system of the business. Nev. Rev. Stat. 570.970 (2005).

[6] S. 139, 111th Cong. § 10 (2009).

[7] H.R. 2221, 22th Cong. (2009).

[8] The health information technology section of the American Recovery and Reinvestment Act of 2009 that President Obama signed on Tuesday, February 17, 2009 (the "HITECH Act") contains numerous provisions affecting health privacy and security, electronic health information and updates to the Health Insurance Portability and Accountability Act ("HIPAA"). Among these changes were new notification requirements for breaches of privacy, security or integrity of personal health information (PHI). On April 16, 2009, the US Federal Trade Commission issued the proposed Health Breach Notification Rules regarding breach notification requirements for vendors, their related entities and third party service providers when electronic health information is breached. Once finalised, these rules would apply to breaches that are discovered on or after September 18, 2009. On April 17, 2009, the Department of Health & Human Services issued guidance regarding technologies and methodologies that can be used to render PHI unusable, unreadable, or indecipherable to unauthorised individuals and, in effect, provides covered entities and their business associates with an optional safe harbor from the new data security breach notification requirement. HIPAA covered entities and business associates, as well as the new entities that are covered under the new FTC rules, should be prepared to comply with breach notification requirements that are being finalised.

[9] 201 CMR 17.01.

[10] 201 CMR 17.03(3).

[11] The FTC's Red Flags Rule, which will be enforced by the FTC as of August 1, 2009, requires entities subject to the FTC's jurisdiction to adopt written identity theft prevention policies – or, essentially, pre-breach security measures.

[12] See *Valentin v. Hospital Bella Vista*, 254 F.3d 358, 366 (1st Cir. 2001).

[13] See *McMorris v. TJX Companies, Inc.*, 493 F. Supp. 2d 158, 162 (D. Mass 2007).

[14] S. 139, 111th Cong. § 10 (2009).

The authors can be contacted at: Gregory T. Casamento, 212-812-8325, gcasamento@lockelord.com; Brian T. Casey, 404-870-4638, bcasey@lockelord.com; Patrick J. Hatfield, 404-870-4643, phatfield@lockelord.com; Vita E. Zeltser, 404-870-4666, vzeltser@lockelord.com

The Security versus Privacy paradox: a virulent fallacy under challenge

By Malcolm Crompton, Managing Director at Information Integrity Solutions [IIS].

How often have you heard somebody argue that there has to be a trade off between security and privacy?

The argument usually runs something along the lines that in order to keep you secure, you have to give up some aspect of your privacy. For example, you must exhibit a lot of evidence of identity before completing a transaction or joining a group or organisation.

This fallacy has been challenged vigorously many times with some of the most cogent reasoning coming from the Information and Privacy Commissioner of Ontario, Ann Cavoukian. She directly challenged the trade off concept in her 2002 paper "Security Technologies Enabling Privacy (STEPs): Time for a Paradigm Shift"[1] and followed up with "The Security-Privacy Paradox: Issues, Misconceptions and Strategies" in 2003[2]. The Commissioner first began drawing attention to the fallacy in 1995 in "Privacy-Enhancing Technologies: The Path to Anonymity"[3], a ground breaking paper published with her Dutch counterparts.

For all the effort that has gone into the challenge, the fallacy has lived on. But the tide is turning. On May 29, the US President released the 60-day Cyberspace Policy Review.[4] Item 10 in the Near Term Action Plan put forward by the review calls for the nation to:

"Build a cybersecurity-based identity management vision and strategy that addresses privacy and civil liberties interests, leveraging privacy-enhancing technologies for the Nation."

Read the US President's remarks at the time of the release[5] and count how many times he remarks on the importance of getting privacy AND security right.

Why is this relevant to such campaigns as National E-Security Awareness Week which took place in Australia in June?[6]

Because if nothing else, the two concepts do inform each other. Here is an example: it is possible to improve the security settings in your organisation by intelligently applying privacy principles such as those seen in the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data[7], the APEC Privacy Framework[8] and many laws worldwide. For example, consider the National Privacy Principles (NPPs)[9] in the Privacy Act of Australia[10]. In particular, consider the security guidance supplied by the following NPPs:

NPP1, The Collection Principle: "An organisation must not collect personal information unless the information is necessary for one or more of its functions or activities." From a security perspective, the less personal information you collect, the less there is to keep secure and the less to lose. And the less attractive your data sets are to those who want to steal it. An additional bonus: this should also reduce your data handling costs.

NPP2, The Use and Disclosure Principle: "An organisation must not use or disclose personal information about an individual for a purpose (the secondary purpose) other than the primary purpose of collection unless" certain limited exceptions apply. This is totally in line with the 'need to know' adage in any security framework.

NPP3, The Data Quality Principle: "An organisation must take reasonable steps to make sure that the personal information it collects, uses or discloses is accurate, complete and up-to-date." One of the most significant weaknesses in any organisation's security framework is its ability to ensure not only that new staff and contractors are properly provisioned with resources when they commence, but are also DE-provisioned when they leave.

NPP4, The Data Security Principle: "An organisation must take reasonable steps to protect the personal information it holds from misuse and loss and from unauthorised access, modification or disclosure." and "An organisation must take reasonable steps to destroy or permanently de-identify personal information if it is no longer needed. . ." Enough said!

And so it is possible to work your way through the NPPs in this way.

But in a sense, that is old news. Take emerging technologies and business processes such as the urge to make more use of cloud computing than is already happening with search, data storage, email etc. The perspective in "It's 6 O'Clock - Do You Know Where Your Cloud's Data Center Is?"[11] that was carried in Information Week on June 2, 2009 is well worth reading.

Even if all this guidance is applied well, data losses will happen even in the best run organisation. What to do then? Again, it is possible to plan a response based on the hard-learned lessons of recent years from the losses of personal information.

Malcolm Crompton can be contacted at: MCrompton@iispartners.com. IIS is a specialist privacy consultancy; its services include privacy impact assessments, privacy thought leadership and advice and strategy. Information about IIS is available at www.iispartners.com. Malcolm regularly blogs on www.Openforum.com.au. An earlier version of this article first appeared on the Open Forum.

  WDPR ISSN 1473-3579

The 2009 Data Breach Investigations Report[12] , a study conducted by the Verizon Business RISK Team provides plenty of surprising insights as to where the security weaknesses in many organisations might really be. The Office of the Privacy Commissioner of Australia has also published a "Guide to handling personal information security breaches".[13] At IIS, we have published a Privacy Breach Check List.[14] The check list provides immediate help in the first 24 hours of a major data loss and suggests what to do as matters unfold over the first week and what to think about in the longer term.

In short, Security AND Privacy go hand in hand, neither by itself sufficient, both informing the other.

And the discussion will continue. The 31st International Conference of Data Protection and Privacy will be held in Madrid in November.[15] Like many of its predecessors, it will be supported by a number of very challenging preconferences. One will be *Privacy by Design: The Definitive Workshop*, which will be held on Monday, November 2 2009 at the Hotel Melia Castilla in Madrid. Participants will hear from a global cross-section of privacy leaders who will describe their real-life experiences and plans for the use of Privacy by Design. Participants and speakers will include Ann Cavoukian, the Privacy Commissioner of Ontario, Canada, Yoram Hacohen, Head of Israeli Law, Information and Technology Authority, Peter Hustinx, the European Data Protection Supervisor, Dr. Jacques Bus, Head of Unit for Trust and Security in ICT Research at the European Commission, Dr. Alexander Dix, Data Protection and Freedom of Information Commissioner for Berlin, Germany and the Honourable Pamela Jones Harbour, US Federal Trade Commissioner.

The fallacy may continue, but there is a good chance it will be seen in more realistic light soon.

NOTES

1 http://www.ipc.on.ca/english/Resources/Discussion-Papers/Discussion-Papers-Summary/?id=245

2 http://www.ipc.on.ca/english/Resources/Discussion-Papers/Discussion-Papers-Summary/?id=248

3 http://www.ipc.on.ca/images/Resources/anoni-v2.pdf

4 http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf

5 http://www.whitehouse.gov/the_press_office/Remarks-by-the-President-on-Securing-Our-Nations-Cyber-Infrastructure/

6 http://www.business.gov.au/Business+Entry+Point/News/National+Esecurity+Awareness+Week.htm

7 http://www.oecd.org/document/18/0,2340,en_2649_34255_1815186_119820_1_1_1,00.html

8 http://www.apec.org/apec/news___media/2005_media_releases/161105_kor_minsapproveapecprivacyframewrk.MedialibDownload.v1.html?url=/etc/medialib/apec_media_library/downloads/taskforce/ecsg/pubs/2005.Par.0001.File.v1.1

9 http://www.privacy.gov.au/publications/npps01.html

10 http://www.comlaw.gov.au/comlaw/management.nsf/lookupindexpagesbyid/IP200401860

11 http://www.informationweek.com/cloud-computing/blog/archives/2009/06/its_6_oclock_do.html

12 http://www.verizonbusiness.com/resources/security/reports/2009_databreach_rp.pdf

13 http://www.privacy.gov.au/publications/index.html#G

14 http://www.iispartners.com/downloads/2006-07-Security-breach-checklist.pdf

15 http://www.privacyconference2009.org

News

ASIA PACIFIC

Highlights from the 31st APPA meeting

The Asia Pacific Privacy Authorities held their 31st Forum in Hong Kong, June 11–12, 2009.

APPA members reported on national and international developments, in particular, there were discussions about how to deal with the privacy challenges surrounding new technologies and the security issues posed by portable storage devices. The Working Group for Privacy Awareness Week also reported on the success of the 2009 Privacy Awareness Week held in May. It was agreed that the Privacy Awareness Week for 2010 will also take place during the first week of May.

Other topics discussed included data breach notification developments in Asia Pacific and an update on the APEC Privacy Framework. Discussions were also held about how best to deal with the privacy implications of electronic health records.

The 32nd APPA meeting will be held during the first week in December, 2009 in Adelaide, Australia.

For more information about the outcomes from the Forum, visit:

http://www.privacy.gov.au/international/appa/hongkong-communique.html

AUSTRALIA

Karen Curtis's tenure as Commissioner extended for another year

Karen Curtis has been appointed for a further one year term as Federal Privacy Commissioner. Her term has been extended so she can oversee the transition period where her Office assumes responsibility for Freedom of Information and Privacy to become the Office of the Information Commissioner (OIC).

The OIC will include two new posts; an Information Commissioner and a separate Freedom of Information Commissioner. The Australian government has allocated AUS$20.5 million over a four year period to establish the new information agency. Karen Curtis's one year term starts from July 12, 2009.

Closing date for Australian Privacy Awards nominations

The closing date for nominations for the Australian Privacy Awards is August 6, 2009. The awards are split into four categories; Large Business, Small to Medium Businesses, Community and NGOs and government agencies. There is also a 'Grand Award' for an outstanding nomine from the categories listed above and the Australian Privacy Medal which is awarded to an individual who has made a significant contribution to privacy in Australia.

Winners will be presented with their awards at a Gala dinner on 12th November 2009.

More information is available from: http://www.privacy.gov.au/about/awards/index.html

CANADA

Telemarketers served with notices for breaching do-not-call list rules

The Canadian Radio-television and Telcommunications Commission (CRTC) has served 'Notices of Violations' on two telemarketers for breaking the rules relating to Canada's do-not-call list.

The CRTC has not released any details about the telemarketers who have thirty days to either pay a fine or contest the Notices before a CRTC panel,

> "Canadians who have registered on the National DNCL have noticed a reduction in the number of telemarketing calls and faxes they receive," said Leonard Katz, the CRTC's Vice-Chairman of Telecommunications. "Although most telemarketers are abiding by the rules, we will use the enforcement tools at our disposal to promote compliance. The Notices of Violation we have issued serve as a warning to telemarketers that we will not look the other way if they break the rules and invade the privacy of consumers."

The CRTC has faced much criticism from privacy advocates, consumer groups and the Canadian press since it launched the Do Not Call lists in September 2008. There were complaints that even after registering with the list, consumers were still receiving unwanted calls. The CRTC was further criticised for failing to enforce the rules and not taking action against telemarketers.

More information is available from: http://www.crtc.gc.ca/eng/home-accueil.htm

Canadian MPs call for changes to privacy law

A Canadian House of Commons Committee has called for the Federal privacy law to be updated to address new technologies and DNA collection. There were also calls for the Privacy Commissioner to be given a much clearer mandate for educating the public about privacy. In its report, the Committee acknowledged that there was a need to overhaul the Privacy Act. However, in the short term, it advocates adopting the 12 quick-fix measures proposed by the Federal Privacy Commissioner, Jennifer Stoddart as an interim solution. The MPs also recommended reviewing the law every five years.

The Privacy Act has not been revised (substantially) since coming into effect 26 years ago, before the emergence of new technology such as biometric scanning.

COSTA RICA

Data protection law for Costa Rica

The Costa Rican government has voted in favour of Costa Rica having its own data protection law. A bill was voted on by the Legal Matters Committee of the Legislative Assembly. It will be referred to as the Law on Individuals' Protection against Personal Data Treatment. The Law will aim to ensure the respect for individuals' rights and the protection of their personal data. The Law also makes reference to the rights of legal persons, includes definitions for key terms such as personal and sensitive personal data and establishes a set of basic data protection principles.

A copy of the bill is available in Spanish from: http://www.asamblea.go.cr/proyecto/16600/16679.doc

EUROPE

Article 29 Working Party releases its Annual Report for 2008

The Article 29 Working Party has released its Annual Report for 2008. The Report provides an overview of the issues dealt with by the Working Party in 2008. It also addresses developments in Member States, EEA countries and European Bodies.

A copy of the report will be available from: http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/annual_reports_en.htm

Article 29 Working Party releases opinion on social networking

The Article 29 Working Party has released its opinion on social networking and how European data protection laws applies to social networking services. WP163 is analysed in detail in this issue in *Privacy and social networking* by Michael Schmidl.

The opinion is available at: http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/index_en.htm

  WDPR ISSN 1473-3579

FRANCE

French Senate issues report on privacy rights in the digital age

The French Senate has issued a report entitled, *La vie privee a l'heure des memoires numeriques* on the right to privacy in the digital age. The report addresses the threat to privacy posed by the emergence of new technologies and the privacy implications for younger generations posed through the prevalent use of social networking sites and so forth.

Interestingly the report recommends making it mandatory for organisations with fifty or more employees to have a Data Protection Officer, creating a mandatory data breach notification requirement, expanding the CNIL (French data protection authority) to include a network of regional offices and increasing its financial resources. The report also refers to changing the French constitution to include privacy rights.

For an update on data privacy developments in France, please see the article in this issue, *Recent developments in personal data protection in France* by Héléna Delabarre and Sabine Deloges .

A copy of the report is available in French at: http://www.senat.fr/noticerap/2008/r08-441-notice.html

HONG KONG

New guidance for estate agents

The Estate Agents Authority and the Office of the Privacy Commissioner have jointly launched guidance entitled, 'Proper Handling of Customers Personal Data by Estate Agents'. The aim of the guidance is to raise awareness amongst estate agents about how to protect their clients' personal data.

The guidance is available from both the Commissioner's and EEA's websites:
http://www.eaa.org.hk/publications/documents/privacy.pdf
http://www.pcpd.org.hk/english/publications/infor_book.html

MALAYSIA

Data protection bill on its way

The Personal Data Protection Bill is due to be introduced for its first reading before Parliament in October 2009. The Bill which has been finalised by the Attorney General's Department will be presented before Parliament alongside the Credit Reference Agencies Bill prepared by the Finance Ministry. The Bill was drafted after consultation involving representatives from the public and private sectors, government departments and industry representatives. It includes provisions to safeguard the personal data of individuals as well as penalties for failure to comply.

SPAIN

Spanish DPA to host Commissioners' conference

The Spanish Data Protection Authority is hosting this year's International Conference for Data Protection and Privacy Commissioners. The conference is taking place in Madrid between November 4–6, 2009. There will be meetings either side of the conference hosted by organisations such as the International Association of Privacy Professionals and the European Privacy Officers' Network.

The themes for the 31st International Conference include 'privacy versus security', the 'conflict between intellectual property and privacy' 'privacy by design' and protecting minors' privacy when faced with technological advances.

At this event, the Commissioners are also hoping to reach an agreement on 'International standards for the protection of privacy and personal data'. Preparatory work has already gone into developing the standards. Spanish and Basque Data Protection Authorities have already co-hosted meetings in Barcelona and Bilbao to work on drafting the standards. The meetings have included representatives from 18 data protection authorities around the world.

For more information about the conference, visit:http://www.privacyconference2009.org/privacyconf2009/home/index-iden-idweb.html

UNITED KINGDOM

Notification fee will increase to £500 for some organisations

The Ministry of Justice is introducing a two tier fee structure for the annual notification requirements whereby organisations pay £35 to the Information Commissioner's Office.

Organisations (data controllers) will either fall into Tier 1 or Tier 2 according to the fee structure. Tier 2 organisations are those obliged to pay the new £500 fee. These organisations have 250 or more members of staff and a turnover of £25.9 million or more, as well as all public authorities with 250 or more members of staff. Tier 2 specifically excludes any data controller that is a charity or a small occupational pension scheme. Organisations that fall into the Tier 1 category will continue to pay the £35 fee. They are organisations which do not meet the conditions specified above, charities and those running a small occupational health scheme.

The new two tier system is due to come into effect from October 1, 2009. It follows the consultation that was car-

ried out by the Ministry of Justice between July and August 2008 about the proposed tiered fee structure.

For more information, consult the Data Protection (Notification and notification fees) (Amendment) Regulations 2009 and its accompanying Explanatory Memorandum which are available from: http://www.opsi.gov.uk/si/si2009/em/uksiem_20091677_en.pdf

http://www.opsi.gov.uk/si/si2009/pdf/uksi_20091677_en.pdf

For a copy of the consultation, visit: http://www.justice.gov.uk/consultations/consultations-closed-withresponse.htm

ICO clarifies data protection myths surrounding photos at school events

The Information Commissioner's Office has sought once again to clarify the data protection myth surrounding parents taking photos of their children at school events such as sports days.

Deputy Commissioner, David Smith, said,

> "We recognise that parents want to capture significant moments on camera and we want to reassure them and other family members that whatever they might be told data protection does not prevent them taking photographs of their children and friends at school events. Photographs taken for the family photo album are exempt from the Act and citing the Data Protection Act to stop people taking photos or filming their children at school is wrong."

The ICO has produced guidance explaining that the Act probably does not apply to many situations involving photos taken at schools.

The guidance is available from: http://www.ico.gov.uk

ICO puts out tender for a research project

The Information Commissioner's Office is inviting interested parties to tender for a three month research project to develop a business case for persuading organisations to invest in proactive privacy protection. The aim is to help organisations devise proper costings and expenditure for having privacy safeguards in place.

Jonathan Bamford, Assistant Commissioner, said,

> "We are aware that one of the barriers to more proactive privacy protection within organisations is the absence of a soundly argued business case for expenditure. However, organisations can no longer afford to ignore data protection and CEOs need to wake up to the risks and responsibilities that come with vast data collection. Data protection needs to be taken as seriously as health and safety by those at the top of the corporate structure.
>
> It is important that this report produces a financial rationale that stands up to the scrutiny of those unfamiliar with data protection requirements or wider privacy concerns, whilst reinforcing the fact that data protection has become a matter of corporate and financial governance."

The deadline for interested parties to submit bids was July 20, 2009. Further details are available at: http://www.ico.gov.uk/about_us/research/invitations_to_tender.aspx

UNITED STATES

Spammers fined $3.7 million

The Federal Trade Commission has been successful in its enforcement action against an international spam ring operating out of Canada and St. Kitts. The ring violated the Can-SPAM Act and the US SAFE WEB Act. The ring was accused of illegally sending email messages which promoted weight loss products and pills claiming to reverse the ageing process. The FTC alleged that the spammers sent emails using false addresses and misleading subject headings to entice people to read the emails. They also failed to provide an opt-out link or a postal address.

The FTC settled with three defendants, a US company and two individuals based in the US and Australia respectively in May 2008 but was unable to reach an agreement with five remaining defendants based in Quebec, Canada. The remaining defendants have been fined $3.7 million, their proceeds from their illegal activities.

The case is the first time the FTC launched an enforcement action using the US SAFE WEB Act designed to protect consumers affected by cross-border fraud and deception.

For more information, visit: http://www.ftc.gov

  WDPR ISSN 1473-3579

Personal Data

Privacy and social networking

By Dr. Michael Schmidl, Maître en Droit, LL.M. Eur.

In June 2009 the Article 29 Data Protection Working Party, an independent European advisory body on data protection and privacy set up under Article 29 of Directive 95/46/EC ("WP-29"), rendered an opinion on privacy law implications of social networking ("WP-163"). In its WP-163, the WP-29 defines a social network service as "online communication platform which enable individuals to join or create networks of like-minded users" and categorises them as being information society services, as defined in Article 1 paragraph 2 of Directive 98/34/EC as amended by Directive 98/48/EC. The WP-163 stresses that the key phenomenon of social networks lies in the fact that users are asked to provide sufficient information about themselves in order to create a thorough personality profile or description and that moreover such information can be distributed to others.

The social network providers offer the corresponding tools, which not only allow the sharing of directly private information but also of subjects of interest to the user such as their favourite music, films or actors. All this information allows the social network providers to tailor advertising campaigns to the respective user groups. In light of the fact that many children and minors are using social network services WP-163 emphasises the importance for social network providers to make sure that the corresponding user group is adequately protected *inter alia* by means of age verification, informed consent, awareness as well as training campaigns, limiting the scope of collected data and its purposes, separation of communities of children and adults.

The WP-163 also deals with questions relating to the applicability of the European Data Protection Directive 95/46/EC and contains measures, which social network providers should implement in order to abide by the legal principles contained in the European privacy framework.

The most important question of whether European privacy laws apply to the social network providers established outside Europe is not analysed. Instead the WP-163 refers to its WP-148 on search engines in which the WP-29 has extensively examined under what circumstances European privacy laws may be applicable. The use of cookies on the social network users' computers in order to improve or customise the services is almost the rule and correspondingly a very frequent reason for applying European privacy laws to social network providers outside Europe. The reason for this effect of cookies is that they enable the social network provider to collect data without the users' interaction. The users' computers are thus turned into technical means under the control of the provider, which is sufficient to trigger the applicability of the privacy laws at the users' locations.

On this basis the WP-163 deals with identifying the data controller in the framework of social network services. The statement that the social network providers are to be regarded as responsible data controllers is not surprising, especially if and to the extent they actively process the users' data for their own business purposes but also since they provide all the network and user management functionality. The third-party providers of applications accessible for users of social networks can also qualify as data controllers, for example as regards the user data. The most interesting phenomenon, however, is the concept of users being qualified as additional data controllers. Although all users collect, process and use personal data about other users they are exempted of the application of privacy law as a consequence of the so-called "household exemption", if their data processing activities occur simply in the course of a purely personal or household activity. This exemption does not apply, however, where a user acts as company representative in the social network in order to promote the company's activities, commercial, political or other goals or if a company uses the service as a professional collaboration platform. As a consequence the full set of data controller obligations apply. WP-163 lists further typical examples of when data controller rules have to be applied to users.

WP-163 also deals with the importance of restrictive so-called "privacy-friendly" default settings (*e.g.*, on what data can be searched and found from inside the network or from outside by means of search machines), since such settings will most likely be left unchanged by the majority of the users, and with the importance of sufficient information and warnings to users regarding the impact on their privacy if they upload personal data. According to the WP-163 users do especially have to be informed about planned direct marketing measures, data sharing with third parties, the risks for providing own data (especially sensitive data) and the potential illegality of providing third parties' data on social networks. The WP-163 recommends that the social network provider should also give information (*e.g.*, on its website) on how to access a complaint facility, which could inter alia deal with the users' rights of access, correction and deletion. Another aspect of "privacy-friendly" settings

Dr Schmidl is a partner of Baker & McKenzie Partnerschaft von Rechtsanwälten, Solicitors und Steuerberatern, Munich and member of the firm's Information Technology Group. Dr. Schmidl is a specialised attorney for IT-Law and a lecturer for Internet law at the University of Augsburg. The author may be contacted at: Michael.Schmidl@bakernet.com

can be seen in the definition of maximum time periods for which data of inactive users is retained and in the deletion of users who have terminated their accounts. Moreover, the service provider has to enable data subjects to use the service with a pseudonym rather than with their real name.

In addition to these topics the WP-163 emphasises that any kind of direct marketing targeted at the users of the network must comply with the corresponding legal requirements, especially as regards the use of cookies and the technique of behavioural targeting. As per the WP-163 the social network providers do not have to fulfil data retention requirements applicable to providers of electronic communication services provided in Article 2 c) of the Framework Directive (2002/21/EC). This may be seen differently if they provide additional services that fall under the scope of an electronic communications service such as a publicly accessible email service. Another interesting aspect the working paper deals with is the handling of invitations to join the network directed at third parties by users of a networking system. Such invitations can be exempted from direct marketing restrictions for email if they are merely personal communications (*i.e.* no incentive is given to either sender or recipient, the provider does not select the recipients of the message, the identity of the sending user must be clearly mentioned, the sending user must know the full content of the message that will be sent on his behalf).

In many respects the WP-163 is similar to a June 2008-decision of the German Düsseldorfer Kreis ("GDK"), a panel in which the German Federal States' data protection authorities reach agreement on the uniform application of the FDPA. The GDK's decision contains a list of key obligations for the operators of social networks (for details on the GDK's decision, please refer to an article written by the author which appeared in the May 2008 issue of the WDPR).

A copy of WP-163 is available in English at: http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/wpdocs/2009_en.htm

Recent developments in personal data protection in France

By Héléna Delabarre, Partner, of the IP-Media-New Techonologies department in NomoS and Sabine Deloges, Associate, in the IP-Media-New Technologies department in NomoS.

The CNIL, the French Data Protection Authority, published its 2008 Annual Report on May 13, 2009.

The CNIL Annual Report is very extensive as it simultaneously provides a presentation of all the work carried out by this authority in 2008 (in all French business sectors where issues relating to personal data protection arise) and also announces the major projects that CNIL intends to particularly focus on in 2009.

This report is thus an opportunity for the CNIL to officially present and update its whole "policy" on personal data protection. Notably, this policy has an even greater scope as the Chairman of the CNIL is currently the Chairman of the Article 29 Working Group.

The report consequently deals with extremely varied issues, such as, for example, the CNIL's opinion on particular bills for which its "opinion" has been requested (this was the case with the "Creation and Internet" bill introducing the "graduated response" mechanism to deal with illegal downloads by net surfers), its (highly reserved) position on processing used by the French intelligence services to consolidate highly varied information about people whose collective or individual activities may undermine public safety or even the conditions under which pharmacists could have automated and integrated access to any prescriptions and drug purchases made by their customers at any chemist's in the country.

We have chosen to review a selection of issues from this report which are likely to affect private sector companies operating in France.

We will also consider the CNIL's position on online targeted advertising which made the news at the beginning of this year following a report made public on March 26, 2009. This report, wholly focused on targeted advertising, analyses the profiling methods implemented and developed by different Internet players for advertising purposes (website designers, community platforms, advertising sales agencies, search engines) and formalises the CNIL's recommendations concerning the protection of net surfers' privacy.

Video surveillance in companies

Video surveillance, which constitutes personal data processing (personal data in this case being the image of a person likely to be identified), is subject to two sets of rules in France, which are often poorly understood by companies. Therefore, the CNIL notes that this dual regulation is very poorly applied, which is all the more worrying as the use of this type of system is constantly increasing (this is also linked to the French government's desire to triple the number of video surveillance systems in public places by 2011).

Video surveillance systems in "places open to the public" are governed by the Act of January 21, 1995 subject to obtaining prior authorisation from the Prefect (authority representing the State in each region).

Video surveillance systems used in "places not open to

Héléna Delabarre and Sabine Deloges can be contacted on: HDELABARRE@nomosparis.com and SDELOGES@nomosparis.com

  WDPR ISSN 1473-3579

the public" on the other hand, fall under the Data Protection Act of January 6, 1978 (amended by the Act of August 6, 2004) and are subject to an obligation to be declared in advance to the CNIL. The same applies for all video surveillance systems, regardless of where they are used, combined with biometric control systems such as facial recognition or files allowing individuals to be identified directly.

Many companies which deal with the public as part of their business find it hard to distinguish between the concepts of places that are open and those that are not open to the public: a supermarket which receives several hundred visitors everyday is legally the private property of the company which owns it but clearly constitutes a "place open to the public" in which the installation of video surveillance systems must be authorised by the Prefect. The same applies for the local grocer's shop which only receives a few customers. Companies may be more reluctant on the other hand when they have to decide which category their building car park falls under, which may have hundreds of employees passing through every day (in this case, this is a place "not open to the public"). Many companies must apply the two regulations. For example, a business which owns supermarkets will be subject to the Act of January 21, 1995 for video surveillance systems installed in its shops whereas cameras installed in the entrance hall of the building containing the company's offices will be subject to the Act of January 6, 1978.

The non-application of these regulations (even due to a failure to understand. . .) constitutes a criminal offence that could subject the person responsible to a fine of up to €300,000.

It is subsequently preferable that these regulations are clarified and above all unified within a single regulation, which the CNIL lists among its wishes in its report by proposing that all video surveillance systems fall under its power. This measure is also desired by a parliamentary committee appointed to make proposals on this issue.

Requests to amend particular personal data processing techniques before their effective implementation

Under Article 22 of the Act of January 6, 1978, the person responsible for the automated processing of personal data shall declare such processing to the CNIL before its implementation.

When this prior declaration is registered and even beforehand, when asked by companies for an "opinion", the CNIL may have to "encourage" companies to modify the processing they intend to carry out.

The recent examples provided below, expressly mentioned in the CNIL's report, show that this right to interfere occurs essentially in high-tech sectors: telecoms, biometry and the Internet.

Google Streetview service

Following the CNIL's recommendations, this service could only be launched in France after being modified to take into account the authority's recommendations. This service allows pictures of towns to be displayed using a 360° navigation system. The CNIL asked Google to set up an automatic blurring of car registration plates and of the faces of people who might appear in the pictures since the vehicle owners and individuals whose image appears are not able to express their prior consent to this use of their personal data, contrary to the principle deriving from Article 7 of the Act of January 6, 1978.

Displaying of advertisements on mobiles via Bluetooth technology

The CNIL demanded the modification of the conditions for sending advertising messages to customers' mobile phones: messages sent from Bluetooth terminals integrated into advertisement hoardings set up in public places (train stations, public roads, concert halls, discos, etc.). This service initially provided that the mobile phone owners in the signal coverage area whose Bluetooth was activated could have adverts sent to them, which again raised the problem of obtaining the prior agreement of the subscriber to consult their personal data used to send such advertising.

The CNIL asked that the advertising should only be sent to subscribers who had expressed their desire to receive them, for example when their telephone comes within a few centimetres of panels integrating Bluetooth terminals.

Venous network recognition system

Biometry is at the heart of the CNIL's concerns due to the highly rapid development of the techniques used and their naturally very intrusive character. The CNIL states in its report that it worked closely with one of the designers of the first systems of physical or logical access control relying on venous system recognition by making specific recommendations, for his attention, about the guarantees that must accompany the implementation of this type of technique. This again confirms that it is preferable for any company wishing to develop technologies or new techniques likely to raise personal data issues that they make the CNIL a partner in their thought process within the company, before the product is designed.

Online targeted advertising

In a report made available to the public on March, 26 2009, the CNIL focused on e-marketing tools for online targeted advertising. It analysed the profiling methods implemented and developed by the leading Internet companies for advertising purposes (website publishers, community platforms, advertising sales agency and search engines) to provide proposals concerning the protection of net surfers' privacy.

Targeted advertising is today widely displayed on websites since it offers a more efficient marketing communication tool for advertisers allowing them, as its name suggests, to target distinct categories of consumers according to different criteria (*e.g.* age, gender, city, occupation, leisure, sites visited, words entered).

In its report, the CNIL notices the existence of different Online Targeted Advertising methods (customised, contextual or behavioural advertising) based on more or less detailed information. According to the CNIL, the performance of these new e-marketing tools implies a significant risk concerning the respect of net surfers' freedom and privacy: "These developments make me afraid of a systematic profiling of net surfers, without their knowledge, as well as a risk for the "bargaining" of their individual profiles between content providers and advertisers".

For websites, these new methods of advertising distribution bring new revenue sources and improve net surfers' browsing on the pages they visit in offering them customised advertisements based on their tastes and their interests.

Indeed, the functioning of targeted advertising is based on the collection and the combination of the net surfers' data in connection with their navigation and behaviour on the Internet in order to build their consumer profiles, via cookies, which may contain a unique identifier for each user.

On this particular issue, the CNIL states in its report that "data which are in the profiles such as age, gender or location are personal data *insofar as they relate to this identifier*". This analysis is not approved by the different leading Internet companies which consider, on the contrary, that browsing data collected and stored in cookies are not identifying to the extent that they cannot be linked to the real identity of net surfers.

By way of this legal qualification, the CNIL considers that French data protection regulation is fully applicable to online targeted advertising processing and provides for better information about the use of their data and how to opt-out. This position is also the one adopted by the Article 29 Working Group in its Opinion 1/2008 dated April 4, 2008 regarding data protection related to search engines.

In addition, the CNIL wishes to collaborate with the "Forum des Droits de l'Internet"[1] to develop a code of conduct for professionals and recommends creating a "Computer and Liberty label", which would be assigned to websites which are respectful of their net surfers' personal data.

Inspections of companies and penalties

Companies are particularly sensitive to the law enforcement aspect of the CNIL's work which is the focus of a considerable part of its Annual Report.

The record of inspections and penalties provided in the CNIL's Annual Report is an opportunity to draw companies' attention to the conditions and cases under which they may be subject to an inspection by the CNIL, possibly followed by a penalty.

First, it should be remembered that this independent administrative authority has benefited, (since the Act of August 6, 2004 amending the Data Protection Act of January 6, 1978) from an independent power to impose penalties. The penalties range from providing formal notices to a definitive ban on continuing to use a process, as well as a decision to impose pecuniary sanctions, if necessary accompanied by an order for publication.

The Conseil d'Etat (French High Administrative Court) furthermore accepted in a decision of February 19, 2008[2] that this own power to impose penalties today makes the CNIL a real "court" within the meaning of Article 6.1 of the European Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR). As a result, the CNIL must ensure it respects the fundamental principle of fair trial as laid down in the ECHR, in particular in relation to the independence of the court and the requirement of a hearing in the presence of both parties.

This Conseil d'Etat decision also required the CNIL to use its power to impose penalties only after a formal notice explicitly stating the alleged facts and the applicable laws.

The CNIL's independent power to impose penalties continues to co-exist with the legal power to impose penalties as most breaches of the regulation concerning the personal data protection (non-declaration of a processing, unfair personal data collection, failure to respect the right to object to market research, illegal "sensitive" data collection", *etc.*) also constitute criminal offences.

Faced with a particularly serious breach of the rules on the personal data protection, the CNIL may decide to hand over the case to the public prosecutor's office to institute criminal proceedings but, given the facts, it should be noted that this right is seldom used and it prefers to use its own power to impose penalties.

The CNIL's Annual Report confirms that instituting sanction proceedings is generally preceded by an inspection by the CNIL's agents.

Inspection

The CNIL report states that no sector is exempt from this inspection power which in practice is carried out in three different ways:

1. The inspection of a company may firstly be decided as part of an annual inspection programme determined by the CNIL according to the set of themes it wishes to focus its work on in the given year.

   Therefore, in 2008, the CNIL inspected electronic voting methods, one of the priorities of its annual inspection programme being to visit private and public organisations using this voting method in order to check whether the regulation on personal data is respected during electronic voting operations (anonymous voting, secret ballot, security measures ensuring the personal nature of voting, *etc*).

2. The inspection of a company may also be undertaken by the CNIL after it receives a complaint which leads the CNIL to carry out checks on the company concerning the facts that have been complained about by the complainant.

3. Finally, a company which is subject to a formal notice by the CNIL and which responds positively to the

  WDPR ISSN 1473-3579

CNIL's formal notice by making commitments in this regard, has good reason to think that it will be the subject of an inspection by the CNIL aimed at making sure that the measures requested in the formal notice have been effectively implemented by the company.

The CNIL decides at its sole discretion whether the inspection will be carried out only "on evidence", *i.e.* based on documents and supporting documents provided by the company, or "on site", *i.e.* during visits by the CNIL's agents to the company. These agents are authorised to have direct access to personal data processing in order to check the implementation conditions.

Companies must in any case remember that inspections are substantially increasing and the CNIL is pleased to report a 33 percent rise in the number of inspections carried out in 2008 compared with the previous year.

Penalties

The full table of penalties, published by the CNIL in its 2008 report, shows that the companies that were prosecuted come from varied lines of business such as services (trade, Internet advertising sales agencies, telephone marketing, distance selling) and were prosecuted for equally diverse reasons:

- Failure to respect the right to object and the right of access;
- Non-declaration of files;
- Improper entry in a file;
- Breach of a security obligation;
- Excessive duration for the storage of collected data;
- Collection of sensitive (racial or ethnic) data in conditions in breach of the law.

Furthermore, it should be noted that some of the companies saw their penalty increased as there was a lack of "cooperation" and "transparency" with the CNIL during the inspection.

As stated above (see the decision of the Conseil d'Etat of February 19, 2008), the CNIL cannot initiate sanction proceedings without providing prior formal notice to the company.

In the majority of cases, companies comply with the CNIL's demands as soon as they receive the formal notice and the CNIL closes the case without imposing penalties (that was the case in 2008 for 84 out of 126 companies who received a formal notice).

However, if they refuse to comply with the formal notice, or worse, if they fail to reply, the CNIL may have to impose a penalty in a reasoned decision and after holding a hearing with both parties present. The measures the CNIL is authorised to take as penalties are expressly provided by the Act of January 6, 1978 and are highly diverse: warning, injunction to suspend processing temporarily or definitively, financial penalties of up to €300,000, and publication of the decision. However, an examination of the financial penalties imposed in 2008 shows that their amount remains moderate and does not exceed €30,000.

The CNIL's relative leniency with regard to financial penalties is a sign that this authority also intends to teach companies a lesson but it is clear that as the years go by that such leniency is becoming rarer and the penalties are increasing.

NOTES

[1] The FDI is a French agency. Its purpose is to enhance the relationships and dialogues between the different stakeholders (administration, industries, and users) involved in Internet activities in order to encourage concerted actions about legal or business issues and practices.

[2] Summary judgment, Conseil d'Etat, February 19, 2008.

Connectivity's mobile phone directory is privacy friendly, says ICO. But is it?

By Dominic Hodgkinson, Solicitor correspondent, Calleja Consulting Ltd.

On June 18, 2009 Connectivity (a start-up company financed by venture capital companies 3i and Esprit Capital Partners) launched a new 118 phone directory service – for mobile phone numbers of private individuals. The initiative has taken two years to launch and has been the target of strong criticism from MPs and civil rights campaigners that it invades individuals' privacy. However, the Information Commissioner's Office has confirmed that Connectivity's mobile phone directory is privacy friendly and the 118 800 service is now up and running.

Dominic Hodgkinson can be contacted at info@callejaconsulting.com

Background

There are approximately 42 million mobile phone numbers issued by UK mobile phone service providers. Under the Universal Services Directive[1] , the UK must provide a comprehensive telephone directory (the BT Phone Book) that must include mobile phone numbers, supplied by UK mobile phone service providers, provided that each user agrees to his number being included. However, even if every user agreed to his mobile number being included there are still two drawbacks to the BT Phone Book's directory of mobile phone num-

bers: pay-as-you-go mobile phone users do not have to provide their personal details when they sign up and the person registered with the mobile phone might not be the user; accordingly, the BT Phone Book cannot be a complete record of mobile phone numbers.

On July 13, 2007 *The Times* announced that Connectivity was about to launch a new mobile phone directory consisting of private individuals' telephone numbers; it stated that Connectivity recognised the privacy concerns associated with such a directory and had put safeguards in place, including contacting every mobile user on its list to ask their permission to be included in a directory.

Two years later, Connectivity launched the service which lets customers search for 16 million mobile phone numbers by entering the name, surname and town of the mobile phone user they would like to contact. For £1, Connectivity will send a text to the user or try to connect both parties by dialling the user's number and asking whether they are prepared to take the call; if they accept, the caller is put through paying a connection charge of 69p and a call charge of 14p per minute.

Data protection and e-privacy

Connectivity's mobile phone directory must comply with the Data Protection Act 1998 and The E-Privacy Regulations[2]. The Act provides that personal data (mobile phone numbers and user names are personal data) must be processed in accordance with the eight data protection principles.

The first principle provides that personal data must be processed fairly and lawfully and only if one of the conditions in Schedule 2 is met; the only relevant condition in Schedule 2 will be that the user has given his consent to the processing.

The second principle provides that personal data must be obtained only for one or more specified purposes, and shall not be further processed in any manner incompatible with that purpose(s).

Review of Connectivity's service under UK law

Connectivity's website states that,

> "Our mobile phone directory is made up from various sources. Generally it comes from companies who collect mobile telephone numbers from customers in the course of doing business and have been given permission by the customers to share those numbers."

Privacy campaigners have raised the issue that although customers of online businesses do sometimes tick the box permitting their contact details to be shared there are two potential issues with Connectivity's claim above that persons on its list have consented to their details being stored on its directory.

The first is that the language accompanying an online box permitting a customer's contact details to be shared is usually put in terms of, for example 'companies offering similar goods and/or services' which wouldn't necessarily incorporate a mobile phone directory; accordingly, the customer technically hasn't given his consent to his contact details being included in such a directory, in which case Connectivity's service is breaching the first data protection principle.

The second is that if the customer hasn't given his consent to his details being shared for the purpose of inclusion in a mobile phone directory, then his personal data is being processed in a manner that is incompatible with the original purpose he did consent to, so Connectivity's service is also breaching the second data protection principle.

Shona Forster, 118800's Marketing Director commented that,

> "We are accessing data in the same way that lots of other companies do for marketing purposes; the difference is that we don't use that data for marketing purposes."

> This is the point – if the customer has agreed that his data may only be processed by persons other than the original data collector for 'marketing purposes', then Connectivity is now proposing to use the data for purposes other than marketing.

Furthermore, the E-Privacy Regulations provide that a mobile phone user's personal data shall not be included in a directory unless that user has, free of charge, been informed by the collector of the personal data of the purposes of such a directory, and given the opportunity to agree to such inclusion.

ICO approval

The ICO commented that Connectivity's service is,

> "...privacy friendly in that it will only connect people when the recipient agrees to take the call and even then it will do so without divulging their number."

However, the ICO also went on to say that,

> "We made it absolutely clear to Connectivity that it should not use numbers where there was any doubt about whether the consumer was happy for their information to be used in this way."

Comment

Recital 11 of the Universal Services Directive states that,

> "Users and consumers desire comprehensive [telephone] directories and a directory enquiry service covering all listed telephone subscribers and their numbers (including fixed and mobile numbers) and want this information to be presented in a non-preferential fashion."

Consumers probably do want a mobile phone directory that might be more comprehensive than, or at least an alternative to, the BT Phone Book. However, concerns raised by privacy campaigners that Connectivity may have breached UK data protection and e-privacy laws in the way that it has compiled its list of mobile phone us-

  WDPR ISSN 1473-3579

ers remain seemingly unresolved – unless Connectivity has, as stated in the Times, July 2007 report, contacted all 16 million mobile phone users whose numbers it acquired.

Connectivity's website FAQs on '*Your questions about privacy*' and announcements to date do not really address this issue; rather, they tend to focus on the fact that the mobile phone user's details remain private at all times and that not even Connectivity staff can access mobile numbers in the directory.

Furthermore, the ICO would appear to have put the ball back in Connectivity's court: it agrees with Connectivity that aspects of its service are privacy friendly but goes on to state that it is Connectivity's responsibility to confirm that all of its subscribers are happy for their details to be entered into the directory, which is the whole point – have all of Connectivity's directory subscribers agreed that they are happy to be included?

For now, the point remains slightly academic as Connectivity's service isn't fully functional – their website home page states that,

> "We hope you find what you want on our website. However, the 118 800 phone service is still being tested and we know it's not yet perfect. So if something's not quite right, we are really sorry but we are working hard to sort things out as quickly as we can."

And, in the most recent twist to the story, Connectivity has suspended its online service, owing to the high number of requests it has received from persons on the directory list seeking to remove their contact details – which has increased speculation that Connectivity didn't correctly obtain consent from 'subscribers' to its directory list.

NOTES

[1] Directive 2002/22/EC of the European Parliament and of the Council of March 7, 2002 on universal service and users' rights relating to electronic communications networks and services.

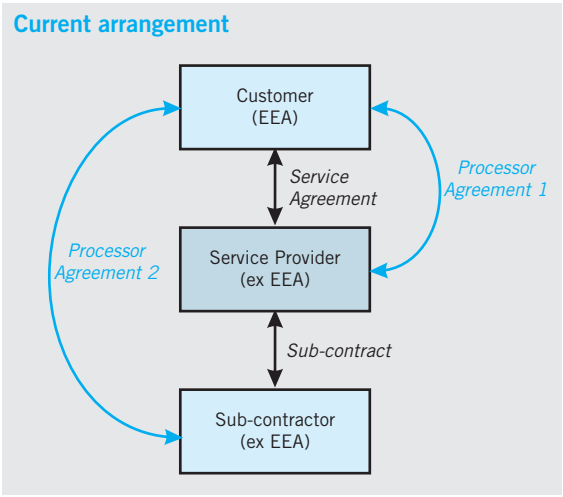
[2] The Privacy and Electronic Communications (EC Directive) Regulations 2003/2426.

Plans to amend model clauses for use in global outsourcing transactions

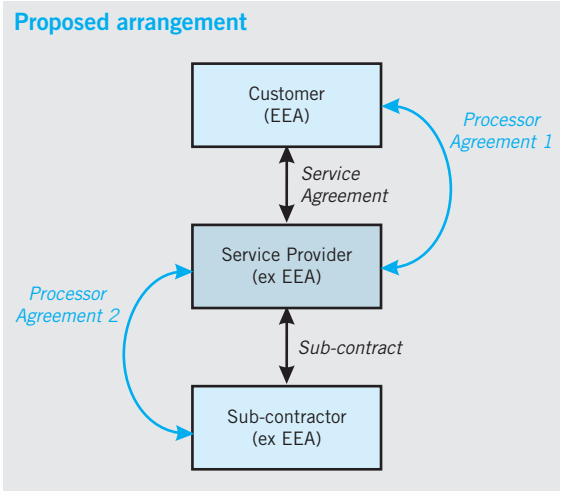
By Cameron Craig

The diagrams that featured in this article last month were inaccurate in that the wording in the bottom boxes should read 'sub-contractor' rather than 'customer'. The correct diagrams are as shown. The author apologises for any confusion.

Current arrangement



Proposed arrangement



News

EUROPE

Article 29 Working Party holds discussions with WADA

The Article 29 Working Party held further discussions with representatives from the World Anti-Doping Agency (WADA) about the International Standard for the Protection of Privacy and Personal Information (as previously reported in the WDPR). The discussions took place at the Working Party's 71st plenary session in Brussels, June 16–17, 2009.

Although the Working Party acknowledged the efforts made by the WADA in adapting the Standard to meet European data protection requirements (the WADA has previously adapted the Standard in line with recommendations made by the Working Party), it would still like to see further changes made. The issues outstanding remain the same – the whereabouts rule, the grounds for processing, the publication of sanctions rulings and retention periods. The Working Party is open to further discussions to ensure the Standard fully complies with EU data protection legislation.

Further information is available at: http://ec.europa.eu/justice_home/fsj/privacy/news/docs/pr_16_06_09_en.pdf

ITALY

Trial of Google executives postponed until September 2009

The trial of four Google executives has been postponed until September 29, 2009 because the translator failed to attend.

As reported in the June issue of the WDPR, the four executives had been granted a fast track trial by a Milanese court. They stand accused of privacy violations, for allowing a video showing a teenager with Downs Syndrome being bullied by classmates, to be posted on Google Video back in 2006.

The four executives being prosecuted are David Drummond, Google's Chief Legal Officer; Peter Fleischer, its Global Privacy Officer; George Reyes, the former Chief Financial Officer; and Arvind Desikan, the former Head of Google Video Europe.

Google removed the video within a day of being informed about it and helped the police to arrest the bullies shown in the video.

Italian prosecutors filed criminal proceedings against Google last year, arguing that Google failed to do enough to prevent the video from being uploaded in the first place and then for taking too long to remove the video.

JAPAN

Google forced to reshoot Streetview images in Japan

Google has said that is will reshoot pictures taken for its Streetview service in Japan after complaints about privacy. Google is to begin re-shooting images lowering the height of its car mounted cameras by 16 inches after complaints were made about its cameras capturing images over fences in private homes.

Opponents of Streetview had previously campaigned unsuccessfully for Google to be refused the right to launch Streetview in Japan over concerns about privacy.

Streetview does not violate privacy according to the Japanese government

The Japanese government has ruled that Google's Streetview service does not violate the rights of Japanese citizens providing that that there are safeguards in place to blur people's faces and licence plates. This was the decision reached by an advisory panel set up by the Internal Affairs and Communications Ministry.

In addition to the use of blurring technology, the panel also called for the cameras to not to be mounted above a certain level on Streeview cars when they capture images and for Google to ensure that the cameras do not enter private properties when capturing images.

Google launched its Streetview service across 12 Japanese cities last August and has since attracted a huge amount of criticism in Japan and worldwide.

MACAU

Data protection awareness rises

Data protection awareness is on the rise in Macau according to local government officials. At the 'Breach of Data – Problems and Solutions' Conference held in Macau following on from the 31st Asia Pacific Conference held in Hong Kong in June 2009, Florinda Chan, Secretary for Administration and Justice paid tribute to the work of the Macau Office for Personal Data Protection. The Office has made concerted efforts to promote data privacy and educate the public on data privacy matters.

The Office was established in 2007 to enforce the Personal Data Protection Act and related legislation. Since its creation, local residents' awareness of privacy matters has risen after the Office took steps to educate the public on the importance of privacy to their daily lives. She also acknowledged the importance of international cooperation in developing strategies for data protection

  WDPR ISSN 1473-3579

through organisations such as APPA. Macau officials attended the 31st APPA Forum as observers.

More information about the Macau Office for Personal Data Protection is available from: http://www.gpdp.gov.mo/en/

SWEDEN

Swedish regulators probing location based services

Swedish regulators are looking into how location-based information is sold by mobile phone operators to service providers. The Swedish Data Inspection Board (Swedish Data Protection Authority) and the Swedish Post and Telecom Agency are jointly investigating location-based services to ensure individuals' privacy rights are fully protected.

The Agency has sent questionnaires to operators enquiring about what information is transferred to service providers, how the information is protected and how consent for sharing the data has been obtained initially from subscribers. They are also looking into how mobile phone numbers are used.

The regulators are aiming to analyse the responses during the autumn with a view to publishing their findings in a report by the end of October 2009.

SWITZERLAND

Commissioner seeks assurances from Google over Streetview

The Swiss Federal Data Protection Commissioner has asked Google to improve its privacy practices before it can launch its Streetview services in Switzerland. The Commissioner has called for Google to use the same blurring technology to be used in Switzerland as it is uses in other European countries to obscure faces and licence plates.

The Commissioner intervened after receiving complaints from data privacy groups that Google was not offering the same level of privacy protection for Swiss citizens compared with the rest of Europe, by not using its blurring technology for images captured in Swiss cities.

The Commissioner's Office is planning to monitor the situation to check images are being blurred. Google has also insisted that it will respect individuals' rights.

Commissioner seeks assurances from Google over Streetview

The Swiss Federal Data Protection Commissioner has asked Google to improve its privacy practices before it can launch its Streetview services in Switzerland. The Commissioner has called for Google to use the same blurring technology to be used in Switzerland as it is uses in other European countries to obscure faces and licence plates.

The Commissioner intervened after receiving complaints from data privacy groups that Google was not offering the same level of privacy protection for Swiss citizens compared with the rest of Europe, by not using its blurring technology for images captured in Swiss cities.

The Commissioner's Office is planning to monitor the situation to check images are being blurred. Google has also insisted that it will respect individuals' rights.

UNITED KINGDOM

Future head of MI6's details on Facebook

The wife of Sir John Sawers, the next head of MI6, posted family details and photos including one of Sir John on Facebook. Details included the location of their London flat and information about their children and Sir John's parents. She posted the information without any privacy protection on her account which made it accessible to all of Facebook's users.

As are result, diplomats and civil servants are being warned about posting information on social networking sites.

Phorm loses BT as a customer

Phorm suffered a blow this month as British Telecom decided not to continue using its Webwise system for behavioural targeted advertising. It follows huge controversy surrounding BT's secret trials testing the system on its customers in 2006 and 2007 without having first sought their consent. While BT has claimed that its decision not to continue is cost based, it is probably more to do with customer opposition in having their Internet browsing patterns profiled to deliver personalised advertising. Phorm has sought to play down BT's decision despite BT being one of its key partners in helping to develop the technology.

ICO finds Manchester City Council guilty of breaching DPA

The Information Commissioner has found Manchester City Council guilty of breaching the Data Protection Act following the theft of two laptops from the town hall. Neither of the laptops were encrypted or securely fixed to desks to prevent theft. One held information relating to employees at local schools. The Council's Chief Executive has signed a formal undertaking to ensure that removable devices are used to hold minimal personal

data and that all laptops and other such devices are encrypted and secured to desks to avoid theft, or locked away.

A copy of the undertaking can be downloaded from: http://www.ico.gov.uk/what_we_cover/data_protection/enforcement.aspx

UNITED STATES

Retail chain TJX settles security breach charges

TJX, the owner of TJ Maxx stores has settled charges with 41 states over a security breach in 2007 which exposed customers' financial data. Unauthorised parties were able to gain access to TJX's computer network and obtain credit card information and personal data on customers.

The retail chain has agreed to pay $9.75 million to the 41 states and to implement a robust and effective data security program to protect customer information to help avoid a similar breach in the future. As part of the settlement, TJX will regularly report to the states' Attorneys General on their data security program after third party audits.

The states have agreed to use the payment under the settlement as follows:

- $5.5 million to be used by the states for data protection and consumer protection;
- $1.75 million is to reimburse the costs and fees of the investigation;
- $2.5 million for the Attorneys General to fund a Data Security Trust Fund to help with enforcement efforts and policy development for data security and protecting personal information.

The 41 states participating in the agreement include California, Florida, Hawaii, Massachusetts, New Hampshire, New Jersey, New York and Washington.

  WDPR ISSN 1473-3579

World IP & Communications Library

What it is

From one resource, keep updated and research global developments in IP and communications law and regulation. This is the best means available to obtain the latest data and authoritative guidance on issues such as global protection and exploitation of IP, data protection and privacy, Internet governance, regulation of e-commerce and domain names.

The World IP & Communications Library allows you to draw upon - as a single database - BNA International´s core IP and Communications Regulation services

What it helps you to do

- Transform your ability to find information and analysis of developments in international IP and communications law and regulation
- Get to the heart of IP-related legal, legislative, and regulatory news and trends from around the world, including important late-breaking developments in protection and enforcement.
- Obtain news and expert analysis of global developments affecting communications and emerging from the convergence of technologies
- Monitor developments in IP law and communications regulation worldwide - and understand compliance implications.
- Gain an insight into how key issues are being handled in different jurisdictions - for example: internet governance, domain names, defamation, liability, data protection, dispute resolution and copyright infringement.
- Receive comprehensive coverage of domain name resolutions
- Cut the time it takes to find text of new regulations, enforcement actions and other key legal documents

Major Topics Covered

- Internet governance
- Copyright infringements
- Dispute resolution reports
- Domain names
- Design rights
- Patentability of software and business methods
- Unfair competition
- Telecommunications
- Media Law
- Information Technology
- Regulation
- E-Commerce
- Security & Surveillance
- Privacy
- Appellations of origin
- Computer software
- Data privacy
- Databases
- Geographical indications
- Global information network
- Industrial designs
- Information infrastructure
- Integrated circuits
- Online information
- Passing-off
- Patents
- Service marks
- Trade secrets
- Trademarks
- Utility models

Category
Subscription Services

Subcategory
International IP Communications and Technology

Formats Available
Web service, with print included for component services

Frequency of Publication
Component services are updated monthly

BNA International
38 Threadneedle Street, London,EC2R 8AY
Telephone: + 44 (0)20 7847 5801 Fax: + 44 (0)20 7847 5858
E-mail: marketing@bnai.com Web Site: www.bnai.com/tax

Privacy & Security Law Report

Category

Subscription Services

Subcategory

U.S. related Corporate Law and Business

Formats Available

Web

Frequency of Publication

Weekly

What this service is

BNA's Privacy & Security Law Report provides comprehensive weekly coverage of the latest breaking legal, regulatory, legislative, and judicial news in the privacy and security fields, including U.S. and global developments affecting finance, health, data protection, and consumers.

What it helps you do

- Keep up with HIPAA, Gramm-Leach-Bliley, CAN-SPAM Act, Fair Credit Reporting Act, USA PATRIOT Act, Fair and Accurate Credit Transactions Act, EU Data Directive, and dozens of other privacy/security-related laws and regulations, plus hot topics and emerging issues.
- Read in-depth analysis from experts in numerous articles on privacy and data and information security, written by some of the nation's top attorneys.
- Follow recent privacy/security-related court rulings, including updates on key litigation and settlements.
- Review the latest legislation pending in Congress and the nation's state houses, especially in the bellwether state of California.
- Rely on BNA for tracking the progress of new privacy/security-related bills, updates on Federal Register notices of proposed and final agency rules, summaries of the latest GAO reports dealing with privacy and security, and news of regulatory enforcement actions.
- Depend upon BNA's legal editor/reporters to cover major conferences and teleconferences you might otherwise miss.

BNA International
38 Threadneedle Street, London,EC2R 8AY
Telephone: + 44 (0)20 7847 5801 Fax: + 44 (0)20 7847 5858
E-mail: marketing@bnai.com Web Site: www.bnai.com/tax