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 4 April 2009

Commentary

News

BNA International Inc., a subsidiary of The Bureau of National Affairs, Inc., U.S.A.

Publishing Director:
Andrea Naylor

Editors:
Jacqueline Gazey and Nicola McKilligan

Commissioning Editor: **Shelley Malhotra**
Production Manager: **Nitesh Vaghadia**

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, 29th Floor, Millbank Tower, 21-24 Millbank, London SW1P4QP, U.K. Tel. (+44) (0)20 7559 4800; fax (+44) (0)20 7559 4880; 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: 29th Floor, Millbank Tower, 21-24 Millbank, London SW1P 4QP, England. Tel. (+44) (0)20 7559 4801; Fax (+44) (0)20 7559 4840; 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 April edition of the World Data Protection Report.

This month's edition is once again packed with all the latest in global data privacy news ranging from an update on the Dutch view of viral marketing using social networking sites and the latest on European Model contracts for data processors, to the first of our updates on the controversial changes which are expected to the German Federal law this Autumn.

The new German law will introduce, amongst other things, the first U.S.-style security breach notification law in Europe and over the next few months we will be carefully tracking developments in Germany and asking our expert commentators for their views on how business should prepare for the new law.

Here in the U.K. comments have just closed on the draft version of the new British standard for Managing Personal Information (previously entitled a Standard for compliance with the Data Protection Act). Comments on the Standard were favourable, with many commentators welcoming practical advice on setting up an organisational infrastructure for data privacy. In fact, the way that privacy compliance is managed in an organisation is becoming the most important factor in whether it achieves an adequate level of data privacy compliance which is why we have also included a brief update in this edition on the growing role of the global privacy professional, most of whom are no doubt devotees of the WDPR!

Best wishes for April 2009.

Nicola McKilligan

Co-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

The debate is over; Massachusetts issues its final regulations for personal information security

By Robin Campbell, Special Counsel, and Kris Meade, Partner, Privacy Group, Crowell & Moring LLP. They can be contacted at: rcampbell@crowell.com and kmeade@crowell.com

On February 12, 2009, the Office of Consumer Affairs and Business Regulation for the Commonwealth of Massachusetts issued final regulations, implementing its security breach notification statute. The regulations mandate privacy and security standards for all organisations that own, license, store or maintain personal information about Massachusetts residents. Virtually every company that has employees or customers in Massachusetts will be affected by these regulations, as will other organisations, including institutions of higher education, that house information on students and other individuals. These state regulations are the first of their kind in the U.S. and mirror some of the requirements of the more robust European data protection laws. They likewise mirror regulations implementing the federal Gramm-Leach-Bliley Act, which pertain to banking and financial institutions, and may provide a glimpse into what's next for state legislatures across the U.S.

The original deadline for compliance with the new regulations was January 1, 2009. The Massachusetts Office of Consumer Affairs and Business Regulation (OCABR) extended that deadline to May 1, 2009. The OCABR said that "in light of intervening economic circumstances," it delayed the deadline to "provide flexibility to businesses that may be experiencing financial challenges brought on by national and international economic conditions". After receiving numerous complaints that businesses would not be able to comply, even with the extended deadline, the OCABR held a public hearing on January 16, 2009 to discuss additional time for compliance. Although the purpose of the hearing was to evaluate the effective date, there was again much debate over the substantive requirements. The result was a final set of regulations that softened the requirement relating to certification of third party service providers, to ease the administrative burden on businesses. The new deadline for compliance with all aspects of the regulations is January 1, 2010.

The new regulations build on the Massachusetts security breach notification law, which mandated the development of the regulations to "safeguard the personal information of residents of the commonwealth". The objectives of the regulations, as set forth in the breach law, are to,

"insure the security and confidentiality of customer information in a manner fully consistent with industry standards; protect against anticipated threats or hazards to the security or integrity of such information; and protect against unauthorized access to or use of such information that may result in substantial harm or inconvenience to a consumer."

Personal information is defined for these purposes as,

"a resident's first name and last name or first initial and last name in combination with any one of more of the following: social security number; driver's license number or state-issued identification card number; or 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".

Most importantly, the new regulations add teeth to a key requirement of many security breach notification laws – that organisations ensure "reasonable and adequate security" – by delineating specific technical security measures that any covered organisation must adopt, including:

- secure user authentication protocols
- secure access control measures
- encryption of all transmitted personal information that travels across public networks and wirelessly (to the extent technically feasible)
- reasonable monitoring of systems for unauthorised use or access
- encryption of all personal information stored on laptops or other portable devices (nothing about feasibility on this one)
- up-to-date firewall protections and OS patches
- reasonably updated versions of system security agent software which must include malware, patches and virus definitions
- education and training of employees on the proper use of the computer security system and the importance of personal information security

The Massachusetts regulation also mandates a comprehensive, written security program applicable to all personal information. The written program must include:

- designation of a person responsible for the program
- an assessment of risks and safeguards to limit those risks
- policies that address employee handling of personal information outside of business premises
- disciplinary measures for violations of the program
- measures to prevent access to personal information by terminated employees
- limitations on the collection, retention of, and access to personal information
- a description of the location of personal information within the organisation
- restrictions on physical access to personal information

- a plan to monitor and upgrade the program regularly
- at least annual reviews of the scope of the program
- a process to document responses to any security breach

In addition, the initial set of regulations required verification that third party service providers who handle personal information have adequate safeguards and a *written certification* that the service provider has a written, comprehensive information security program that is in compliance with the provisions of 201 CMR 17.00 *before* that service provider could access personal information. As revised, the regulations now require:

> *Taking all reasonable steps to verify that any third-party service provider with access to personal information has the capacity to protect such personal information in the manner provided for in 201 CMR 17.00; and taking all reasonable steps to ensure that such third party service provider is applying to such personal information protective security measures at least as stringent as those required to be applied to personal information under 201 CMR 17.00.*

The change is subtle, and while on its face it appears to lighten the load on those outsourcing the handling of personal information to third party service providers, the effect is very much the same. While there is no longer a "written certification" requirement before a service provider can access personal information, there remains a requirement that an entity takes *all* reasonable steps to verify that the service provider can protect personal information in accordance with the new Massachusetts regulations. Wouldn't the first step in that process be a contractual requirement that the service provider follow the Massachusetts standards, including all of the security requirements listed above? An entity must not only verify the capacity of a service provider to protect data, but must also ensure that security measures, at least as stringent as those in this regulation, are actually being applied to such personal information. Compliance with this section would seem to require both specific contractual obligations on any service provider handling personal information and audit rights to ensure that those contractual obligations are being met. Semantics aside, the need for oversight of third party service providers remains and now there is a specific technical standard against which the service providers' practices can be judged.

Those doing business in Europe, or in the health care or financial services industries, should be well on their way to compliance with the new regulations. Others may need to take a closer look at their privacy and security standards to ensure that they are ready for the new Massachusetts regulations when they take effect on January 1, 2010.

The rise of the global privacy professional

By J. Trevor Hughes, CIPP, Executive Director, IAPP.

Trevor Hughes of the International Association of Privacy Professionals contends that an international community of privacy professionals is the key to improved compliance and global understanding.

Let's think back 10 years. Social networking meant getting together with colleagues after work, Street View was a term realtors used, and 9-11 hadn't happened yet. By today's standards, data privacy issues were few. But they did exist. The Internet and its faithful cookie had recently emerged. Consumers were anxious about using credit cards online. The need for management of privacy issues existed.

In those earliest of days, law firms may have had one partner well-versed in privacy and organisations were just beginning to think about compliance with the emerging number of data protection laws. A relatively small group of professionals found themselves charting the mostly unmapped territory of data privacy, and their need for resources and collaboration was great. The International Association of Privacy Officers emerged from that need in 2000, creating a community for these professionals, who were blazing a trail that others—many others—would eventually follow.

The profession and its international association (renamed the International Association of Privacy Professionals (IAPP) in 2002), has grown in breadth and numbers steadily. After nearly a decade, the data privacy field has evolved to one where law firms dedicate entire practice units to the issue and privacy officers occupy a place in the C- suite at many organisations. Today, 29 IAPP employees serve more than 6,000 members—privacy professionals from 47 nations across the world.

One thing is certain: the privacy profession is not going away. It is no corporate fad. No passing fancy of the dot com era. It is here to stay and will continue to grow worldwide because privacy professionals are critical to the competent management of data in the information economy. They are information sentinels in a world where trust is constantly tested and where the stakes for privacy blunders are continually raised.

And each time the stakes are raised, the bar is set higher.

More than 3000 IAPP members today hold the IAPP Certified Information Privacy Professional credential. Credentials go a long way in demonstrating a high level of privacy understanding and issue-spotting capabilities. We're seeing an increased demand for these professional assets. More and more, employers ask for such credentials in privacy job descriptions, and regulators and standards bodies have recognised the need to have certified data privacy officers.

But credentials are only one part of the mix.

Advancing the privacy profession requires collaboration. We must work together across geographic, cultural, even industry lines, to expand awareness, forward knowledge and maximize our effectiveness. Data and data protection know no boundaries. The technologies that challenge both will continue to pervade. Working in silos will not advance our cause or our profession. If we are to be effective, we must work together.

  WDPR ISSN 1473-3579

To this end, the IAPP has partnered with the German Association for Data Protection and Data Security (*Gesellschaft für Datenschutz und Datensicherung*), the French Association of Data Protection Correspondents (*AssociationFrancaise des Correspondants aux Donnees Personnelles*), and has developed an affiliate relationship with colleagues in Australia and New Zealand—the IAPP ANZ. Just last month we introduced the IAPP Canada, a dedicated entity to serve Canada's sophisticated and growing privacy profession. These connections, and others to come, bring together privacy professionals in ways that contribute to the overall betterment of the professionals, therefore the profession.

We look forward to expanding offerings for European privacy professionals, as well. A certification credential will be a key component of those offerings, as will an event, to be held in conjunction with the 31st International Data Protection Conference in Madrid later this year. An esteemed group of European privacy experts is guiding these efforts.

One may wonder to what end we extend these efforts.

Professionalism is not about the amount of knowledge we have or clout we wield. It is about standardising and improving our approach to solving problems in our field with a community of people who are working to the same end.

The data privacy field, much as it has matured, is still new. Yet our work impacts the majority of the world's citizens. Attaining and sustaining a high standard demands engagement in the broader community and requires constant learning, sharing experiences with peers, and forging connections with others who, day in and day out, work through similar issues, except maybe in a different province, nation, or time zone. It is our shared responsibility to continue to build this profession.

Privacy pros are the guardians of trust in the information economy and the benefactors of our good work are many.

News

ASIA PACIFIC

Privacy Awareness Week: May 3–9, 2009

Privacy Awareness Week (PAW) is the annual promotion of privacy by the Asia Pacific Privacy Authorities (APPA). This year PAW will be held from May 3–9.

In Australia, the Commissioner's Office will be launching a web portal aimed at young people and a young adult magazine. The Office will also be launching the 2009 Australian Privacy Awards and Medal, in addition to producing new guidance and holding seminars throughout the week.

The Canadian Privacy Commissioner will be using PAW to promote awareness of its new website, http://www.youthprivacy.ca an interactive site offering advice to youngsters on how they can protect their personal information online and shape their online identity. The Office will also be launching the 'My Privacy and Me' National Video Competition inviting young people to create a public service announcement on privacy.

The Hong Kong Privacy Commissioner is planning several events including a meeting of the Data Protection Officers' Club and the launch of the Personal Data Privacy Campaign for Medical Practitioners.

As part of PAW, the New Zealand Privacy Commissioner's Office has launched two new sections on its website, 'Interpreting the privacy principles' to help make interpreting and applying the privacy principles easier and the 'Privacy Officer Forum', an online space for Privacy Officers to discuss privacy issues with their counterparts. In addition, it will also launch a new video entitled, 'Think before you upload' aimed at the youth sector to encourage them to think about the information they post online. There will also be a series of events.

For further information on these events and activities and those of the other APPA members, visit http://www.privacyawarenessweek.org/paw/

BELGIUM

Viral marketing sterilised

In June 2008, the President of the Commercial Court of Huy had to consider the use of viral email marketing in a case of an operator of an online dating agency suing a competitor for unfair trade practices. The case is one of the first in Belgium and provides a warning to organisations considering this practice. [See also in this issue, Commentary, *Netherlands: Online networks of acquaintances as a marketing tool*].

Viral dating

The offending organisation ran an online dating agency and used its existing user base to collect data about other potential customers. It did this in two ways:

- users registering for the first time on the online dating site were asked if the site could access their personal mailbox so as to review their address book and extract email addresses contained within it; and
- a specific section of the site, called 'Make Some Noise', invited users to enter email addresses of their friends in exchange for a higher popularity-rating on the site.

The third parties whose email addresses had been collected automatically received emails advertising the website with an invitation to join it.

Privacy and unfair competition law

The operator of a rival dating site filed for an injunction claiming this was an unfair trading practice. In particular, the collection of emails in this manner, and their subsequent use for advertising, were infringing the Law

of December 8, 1992 on privacy protection in relation to the processing of personal data.

The defendant claimed that no such infringement took place. First, it alleged that it was not a data controller in respect of the advertising emails as they were sent by the site's users. Instead it considered its role was limited to the provision of a technical tool allowing its users to send such emails like any web-based email service. Secondly, it argued it had a legitimate ground to process personal data on the basis of Article 5 (f) of the privacy law. This permits data controllers to process data if it is necessary for their legitimate interest and is not outweighed by data subjects' prevailing privacy rights.

The judge rejected both arguments, considering that the emails were sent directly from the dating site's mail server and that the privacy rights of the addressees outweighed those of the dating site. The collection of data in this way from unsuspecting addressees infringed their fundamental rights, especially as they had not been asked for their prior consent.

And anti-spam laws?

The rival operator claimed that this marketing technique also infringed Article 14 of the Law of March 11, 2003 on certain legal aspects of information society services *i.e.* that "*the use of electronic post for advertisement is prohibited without prior, freely given, specific and informed consent from the addressee of the messages*".

The judge again rejected the defendant's claim that the emails were sent by its users, considering that both direct use and indirect use of the email addresses in this manner without prior consent amounts to spamming. In this case, the method used was unacceptable and prior consent should have been obtained from the addressees by less intrusive means.

Conclusion

This judgment is among the first to address viral marketing in Belgium and prohibits two practices which are widely used by so-called web 2.0 applications. Although the judge did not prohibit the usage of viral marketing *per se*, he made it clear that such use must comply with relevant data protection laws.

By Guillaume Couneson, Associate, and Tanguy Van Overstraeten, Partner and Global Head of the Privacy Practice, Linklaters. They can be contacted at: guillaume.couneson@linklaters.com and tanguy.van_overstraeten@linklaters.com This article was first published in the Linklaters TMT newsletter.

CANADA

Identity Theft Bill

The Minister of Justice and Attorney General for Canada re-introduced identity theft legislation at the end of March 2009. The proposed Identity Theft Bill would create three new offences, all of which carry a maximum five year prison sentence and are as follows:

- Obtaining and possessing identity information, with the intent to use the information deceptively, dishonestly or fraudulently in the commission of a crime;
- Trafficking in identity information; and
- Unlawfully possessing or trafficking in government-issued identity documents.

Additional changes would include creating new offences for fraudulently re-directing a person's mail and giving courts the power to order an offender to pay restitution to a victim of identity theft where the victim has incurred expenses in trying to restore their identity.

A copy of the proposed legislation is available at: http://www.parl.gc.ca

Commissioner launches DPI website

The Privacy Commissioner has launched a website to discuss the privacy issues surrounding deep packet inspection (DPI). DPI is a computer network packet filtering system that can detect *e.g.* viruses, pre-defined key words, protocol non-compliance, spam, *etc.* The website features a series of essays written by experts and is aimed at generating public discussion and awareness about DPI.

The Commissioner's Office decided to do research into DPI after receiving several complaints. It was seen as an opportunity to launch a public awareness campaign and discuss the implications.

The site provides an overview of DPI and how it can be used for purposes such as behavioural advertising, monitoring Internet traffic and surveillance.

The website address is: http://dpi.priv.gc.ca/

No appeal for Radwanski acquittal

Ontario's Attorney General has decided against appealing the decision to acquit Former Privacy Commissioner, George Radwanski. Radwanski was found not guilty of fraud and breach of trust earlier this year after he and his former chief of staff, Art Lamarche were formally charged in March 2006.

Justice Paul Belanger of the Ontario Court of Justice said the prosecution failed to show Radwanski's behaviour was outside the Ottawa norm. He did however acknowledge that the $24,000 worth of expenses claimed by Radwanski during his three years as Commissioner were extreme.

Lamarche was convicted of breach of trust for authorising an improper $16,000 vacation pay-out to Radwanski, but Belanger ruled no fraud was involved.

  WDPR ISSN 1473-3579

CANADA AND THE UNITED STATES

Accounting institutes release draft framework for comment

The American Institute of Certified Public Accountants and the Canadian Institute of Chartered Accountants released a draft document for public comment, proposing changes to their Generally Accepted Privacy Principles – a generic privacy framework. Comments were due by April 15, 2009.

For more information, visit: http://www.aicpa.org/ or http://www.cica.ca

EUROPEAN UNION

Working Party investigates Data Retention Directive implementation

The E.U. Working Party for data protection (Article 29 Working Party) is launching an investigation into compliance at national level by telecom providers and ISPs in meeting the requirements of national traffic data retention legislation (implementing the requirements of the e-Privacy Directive 2002/58/EC and the Data Retention Directive 2006/24/EC).

The investigation will be conducted via an initial questionnaire focusing on 10 areas where retention of traffic data is significant, followed by onsite investigations.

The primary aim of the investigation is to examine whether data protection requirements are being met and if so, how they are being met within the telecoms sector for each Member State. The results of the investigation will be evaluated at E.U. level and by the Member States and could lead to guidance being issued to help improve compliance in this area.

For further information, visit: http://ec.europa.eu/justice_home/fsj/privacy/news/index_en.htm

EC appoints DLA Piper for e-commerce legislation review

DLA Piper's Belgian office has been instructed by the European Commission to review all the legal areas which govern online services including data protection, child safety, electronic payments and consumer protection.

The aim of the study is primarily to review the problems experienced by businesses and consumers operating in an online environment; particularly, the issues of diverging legislation across E.U. Member States, how businesses can best adhere to the strict requirements of the E.U. data protection legal framework and how that framework could be updated to meet the expanding e-commerce marketplace.

The study will be conducted over the coming months and presented to the Commission in time for it to launch its official review of the E-Commerce Directive which is expected to take place in October 2009. DLA Piper will be assisted by experts from around the world including Ian Walden, Professor of Information and Communications Law, at Queen Mary University, London and Lawrence Lessig, Professor of Law at Stanford University.

EC's Data Protection Unit releases guidance questions and answers

The European Commission has released a set of questions and answers to help companies understand the legal aspects of transferring personal information outside the European Union and European Economic Area. The guidance is particularly aimed at small and medium sized businesses and is available at:

http://ec.europa.eu/justice_home/fsj/privacy/docs/international_transfers_faq/international_transfers_faq.pdf

HONG KONG

Privacy Commissioner concerned by use of CCTV in taxis

The Privacy Commissioner has voiced his concerns about the taxi industry's proposal to install CCTV in taxis. He has made it clear that he does not support such a move, considering it an intrusive method of preventing crime. The Commissioner has called for less privacy intrusive measures to be considered first.

NEW ZEALAND

Privacy Commissioner welcomes Privacy Bill

The Privacy Commissioner, Marie Shroff, has welcomed the first reading of the Privacy (Cross-border Information) Amendment Bill, commenting,

> "New Zealand business is operating in a global data processing economy and our data protection law needs to be recognised as stacking up internationally- . . .Our privacy law must keep pace so that New Zealand businesses can take advantage of opportunities in the digital age."
>
> "This is especially important in the current global economic climate. The changes in this Bill should help to secure a finding from the European Union that New Zealand law offers an adequate standard of data protection, thus opening up trading opportunities with Europe."

The Bill includes provisions to:

- help ensure New Zealand's privacy law meets the requirements set by its international trading partners;
- remove an anomaly which prevented people living overseas from accessing their personal information held in New Zealand;

- provide the Privacy Commissioner with mechanisms to cooperate with other privacy authorities when dealing with, or transferring, privacy complaints; an issue which has been prioritised by both APEC and the OECD.

UNITED KINGDOM

Government fails to meet deadline on ICO's powers

The U.K. Government has failed to meet its own deadline for bringing in the Information Commissioner's new powers to fine companies for data protection breaches. Although the Ministry of Justice has reaffirmed its commitment to bring in these powers, there is no explanation about why the government failed to meet the deadline or when it is planning to introduce the secondary legislation required to enact the ICO's new powers.

The Criminal Justice and Immigration Act 2008 amended the Data Protection Act and introduced a power for the Information Commissioner to impose civil monetary penalties on data controllers that knowingly or recklessly commit serious contravention of the data protection principles (including security).

IAB draws up self-regulatory guidelines

The U.K. Internet Advertising Bureau has created a set of self-regulatory guidelines on behavioural advertising. The guidance establishes a set of good practice principles and frequently asked questions. Critics of the guidelines are already arguing that they do no go far enough to address privacy concerns and put too much onus on the individual. (See also in this issue, Commentary, *Online behavioural advertising: key players seek to calm the storm.*)

The guidelines are available from http://www.youronlinechoices.co.uk/

Government drops data sharing proposals

The U.K. Government has confirmed that it is dropping its controversial plan to share data between government departments. Clause 152 of the Coroners and Justice Bill was met with fierce opposition from all sides of the political spectrum and the Information Commissioner's Office.

UNITED STATES

FTC to enforce Red Flag Rules

The Federal Trade Commission (FTC) is planning to enforce its Red Flag Rules as of May 1, and has launched a website to help organisations comply with the requirements. The Rules have been drawn up to reduce the problem of identity theft and require financial institutions to create and implement a written identity theft prevention scheme.

The site provides guidance to help organisations develop an identity theft programme including tips on how to recognise identity theft and how to prevent it. There are also articles available for downloading by companies to use as part of an awareness building exercise.

The original deadline was extended from November 1, 2008 to May 1, 2009 because companies were not ready for the Rules to come into force. It is thought that the FTC will take a case by case approach when it comes to enforcing the Rules.

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

  WDPR ISSN 1473-3579