Locke Lord LLP

Data Protection NEWSLETTER

May 2014

Locke Lord's Data Protection Newsletter provides topical snapshots of recent developments in the fast-changing world of data security in the United States and Europe. For further information on any of the subjects covered in the newsletter, please contact one of the members of our data protection team.

Alan Meneghetti
Partner, London
T: +44 (0) 20 7861 9024
ameneghetti@lockelord.com

Patrick J. Hatfield
Partner, Austin, Texas
T: (512) 305-4787
phatfield@lockelord.com

Bart W. Huffman
Partner, Austin, Texas
T: (512) 305-4746
bhuffman@lockelord.com

Topics:

1. European Parliament votes through EU data protection reforms

The first major reforms to EU's data protection legislation since 1995 have been approved by an overwhelming majority in the European Parliament on 12 March 2014.

The 1995 Data Protection Directive (95/46/EC), which currently sets out the minimum standards for data protection that the 28 EU Members States have based their national laws on, was created before the internet was even in widespread use. The cry for reform stems from the apparent inconsistencies between the current patchwork of national laws, the need for a more powerful enforcement of data protection and the rapidly evolving technology of today.

Some of the key features of the draft Data Protection Regulation include:

- One continent, one law: a single, pan-European law for data protection will be established, the benefits of which are estimated at €2.3 billion per year.
- The right to be forgotten: the obligation on data controllers to delete personal data when requested by the data subject provided that there are no legitimate grounds for retaining it.
- One-stop-shop: companies operating in the EU Single Market will only have to deal with one supervisory authority, rather than 28, making it simpler and cheaper for companies to do business in the EU.
- Fines: data protection authorities will be able to fine companies up to 5 per cent (on the current wording of the draft Regulation) of their global annual turnover for non-compliance with EU rules.
- Easy access: A right to data portability which will make it easier for data subjects to transfer their personal data between service providers.

There have been mixed responses to the reforms. EU Justice Commissioner, Viviane Reding, who proposed the reforms is clearly still a strong supporter of them in her statement:

"The message the European Parliament is sending is unequivocal: This reform is a necessity, and now it is irreversible… Data Protection is made in Europe. Strong data protection rules must be Europe's trade mark. Following the U.S. data spying scandals, data protection is more than ever a competitive advantage."

In contrast, concerns have been raised by the Finance & Leasing Association and other industry specialists over rushing into force legislation that poses a threat to credit industry data processing and the on-lender's ability to lend responsibly and prevent fraud. Moreover, Digital Europe, a lobbying group that represents 10,000 companies, including some of the world's largest consumer-electronics companies has commented:

"This will put Europe at a disadvantage to other parts of the world that are embracing the new technologies."

Whether a final agreed draft is ready during 2014 remains to be seen. If it is, and on the current drafting, the Regulation would come into effect in each Member State two years after it was published in the *Official Journal of the European Union* (OJEU). Sometime in the latter part of 2016 or early 2017, therefore, we shall see the true impact of the Regulation on data protection in the EU.

2. Edward Snowden and the latest U.S. National Security Agency reforms

On 27 March 2014, U.S. President Obama released proposals to reform the way the National Security Agency (NSA) collects data from phone calls in the United States. The reforms are a response to the allegations made by former NSA contractor Edward Snowden in June 2013 regarding the bulk collection and monitoring of phone calls by the NSA. The details of the proposed legislation remain unclear.

The NSA's domestic policy to systematically collect data about American's calling habits, known as the "President's Surveillance Program", was introduced by President Bush shortly after the 9/11 terrorist attacks. Snowden's exposure of the alleged extent of the surveillance amplified momentum for reform of the NSA's activity.

On 27 March 2014 and following months of discussion, the Obama administration formally released proposals which will likely end the NSA's bulk collection of all U.S. phone data. The new proposal requires the government to apply for a court order to access records held by telecom companies for up to 18 months (previously 5 years), which will only be released once the Foreign Intelligence Surveillance Court (FISC) have granted access. The government must prove that there is "reasonable suspicion" that a phone number is connected to a terrorist. Once granted approval by the FISC, telecom companies will provide metadata and technical support to the NSA.

The Obama administration has said it plans to renew the current NSA programme for at least another 90 days until Congress passes the new bill. The current surveillance program is due to expire in mid-2015.

3. Backlash over Facebook acquisition of WhatsApp

Facebook has acquired WhatsApp for $19 billion, in the biggest internet deal in over a decade, raising privacy concerns from users of the messaging service. Privacy activists have raised the issue of whether Facebook will be able to get their hands on WhatsApp's database of phone numbers and other personal data of its 450 million users.

The Deputy Director of Big Brother Watch, Emma Carr, told the IB Times: "This case highlights exactly why Data Protection Laws are out of date. Many customers of WhatsApp will feel let down that they provided their data in good faith on the basis that it would not be shared with a third party."

Mark Zuckerburg has confirmed that WhatsApp would continue to operate independently. Nonetheless, the Electronic Privacy Information Center (EPIC) and the Center for Digital Democracy (CDD) have requested that the U.S. Federal Trade Commission (FTC) investigate the acquisition and confirm whether Facebook can access WhatsApp's store of user personal data. The FTC will determine whether the acquisition can continue and what, if any, conditions will be imposed.

The FTC complaint highlighted that following Facebook's acquisition of Instagram in 2012, they altered the Instagram Terms of Service so that it could access the photo app users' data. Consequently, there is little faith that the social networking giant will not do the same again. The complaint reads that: "Whatsapp users could not reasonably have anticipated that by selecting a pro-privacy messaging service, they would subject their data to Facebook's data collection practices".

4. Morrisons under fire following theft of payroll data

The UK's fourth-largest supermarket retailer has had to publicly apologise to employees and convince customers their data is safe, following a security lapse which saw around 100,000 of its employees' personal data published online. A Morrisons' employee has been arrested in connection with the theft and publication of the confidential data.

Staff salaries, bank account details and addresses were published online and also sent anonymously on a disc to a local paper in Yorkshire.

The *Guardian* has reported that a Morrisons' employee has been arrested on suspicion of making or supplying an article for the use of fraud, under section 7 of the Fraud Act 2006.

Cyber protection company Clearswift has said that the situation demonstrates the need for businesses to be increasingly vigilant against internal security threats. Additionally, V3 reports that ICO have confirmed they will be investigating the "potential data breach".

If the European Parliament's draft data protection law is enacted (See article 1 of this newsletter), companies such as Morrisons could be subject to fines of up to 5 per cent of their global turnover for such data breaches.

5. "Ignorance is no excuse" for British Pregnancy and Advisory Service who have been fined £200,000 for exposing clients

The Information Commissioner's Office (ICO) has fined the British Pregnancy and Advisory Service (BPAS) £200,000 after details of almost 10,000 people seeking advice on abortion, pregnancy and contraception were revealed to a hacker. The ICO considered that the failure of the BPAS to detect a problem with its system was a serious breach of the UK Data Protection Act 1998.

Through outsourcing the online booking service to a third party, BPAS was unable to closely monitor the security of confidential client details. The ICO investigation revealed that the charity "didn't realise" its website was storing the names, addresses, dates of birth and telephone numbers of those who had requested the advice. The Deputy Commissioner and Director of Data Protection responded that even in these circumstances "ignorance is no excuse".

BPAS also breached the Data Protection Act by storing data for five years longer than was necessary for its purposes (see *Principle 5 of the UK DPA 1998*).

The BBC has reported that BPAS chief executive Ann Furedi condemned what she regarded as a disproportionately high fine. Citing the fact that BPAS themselves were a victim of internet crime, Furedi considered the fine to be unfair to impose on a charity which "spends any proceeds on the care of women who need our help". BPAS intend to appeal the fine.

The hacker was prevented from publishing the information after it was recovered by the police following an injunction obtained by the BPAS.

6. £100,000 fine for Kent Police as confidential interview tapes found abandoned

The ICO have fined Kent Police in the UK £100,000 for leaving confidential information, including copies of interview tapes, in the basement of a former police station. The information is thought to have been left at the site when the building was vacated in July 2009.

The highly sensitive information included interviews with victims, informants and convicted criminals dating back to the 1980s. The tapes were discovered by the new business owner of the site previously occupied by the Gravesend Police Force, who "was planning on watching them for entertainment". A Kent Police spokesperson emphasised that no sensitive information had been lost in the incident.

However, ICO head of enforcement Stephen Eckersley condemned the breach as a serious lack of oversight and information governance, the impact of which would have been "enormous and damaging" had the information fallen into the wrong hands.

Kent Online have reported that, since this incident, Kent Police have committed to reviewing its policies to ensure complete compliance with the Data Protection Act, and to reduce the possibility of further data leaks.

7. ECJ declares Data Retention Directive invalid

On 8 April 2014 the European Court of Justice (ECJ) declared the EU Data Retention Directive 2006/24/EC invalid. It has been held that the directive "interferes in a particularly serious manner with the fundamental rights to respect for private life and to the protection of personal data" (Articles 7 and 8 of the European Charter of Fundamental Rights of the European Union).

The Directive attempts to harmonise Member States' national legislations regarding the retention of data by telecommunication providers for the prevention and prosecution of crime and terrorism; the intention being to resolve legal and technical differences between the patchwork of national provisions. Although the ECJ did recognise that the directive principally serves legitimate public interests of public security, it concluded that it is disproportionate, causing a more serious interference with fundamental rights to respect private life and the protection of personal data than is necessary to achieve its objectives.

The main criticisms the ECJ cites for its conclusion include:

- The Directive generalises all individuals, all means of electronic communication and all traffic data without any differentiation.
- The Directive insufficiently defines the severity of the crimes that would justify such interference of fundamental rights, failing to lay down any objective criterion.
- The lack of safeguards to ensure effective protection of the data against the risk of abuse.
- No requirements for review by a court of administrative body prior to accessing the data
- The data retention period sets no distinction between the categories of data
- It does not require the data to be stored within the EU, failing to ensure that the control of compliance by an independent authority, as is required by the European Charter of Fundamental Rights.

The invalidity ruled by the ECJ applies from the day the Directive came into force, which means that the situation after the decision is that it is as if the Directive never existed. The decision will impact all types of data processing, including international data transfers and storage.

8. ICO issues guidance on privacy in mobile apps

The ICO has published guidance to help mobile app developers comply with the DPA 1998 and to ensure their users' privacy is protected. App developers have now been urged to take a privacy by design approach, ensuring privacy protections are in place from the outset.

The International Law Office reported that the guidance follows a YouGov survey commissioned by the ICO issued in December 2013, which found that 49 per cent of app users had decided not to download an app as a result of privacy concerns. The guidance, therefore, is aimed at helping app developers to understand their data protection responsibilities and earn the trust of their users.

The guidance urges app developers to be have answers to the following questions:

- Will you app deal with personal data?
- Who will control the personal data collected?
- What data will you collect?
- How will you inform your users and gain consent?
- How will you give your users feedback and control?
- How will you keep your data secured?
- How will you keep your app tested and maintained?

The guidance also sets out some other important legal considerations, such as, reminding developers of apps involving communication that they should comply with the rules regarding consent to marketing under the Privacy and Electronic Communications Regulations.

In promoting a privacy by design approach, the ICO is primarily encouraging app developers to consider privacy issues at all stages of the development, to ensure they are fully compliant with the DPA 1998.

9. Microsoft cloud wins EU privacy approval

The EU's Article 29 Data Protection Working Party has confirmed that Microsoft's enterprise cloud contracts comply with EU Data Protection law. It is hoped by Microsoft that this development reduces the number of national authorizations required to allow the international transfer of data (depending on the national legislation).

In the Working Party's review of Microsoft's MS Agreement[1] and Standard Contractual Clauses , they have concluded that Microsoft's contractual commitments meet the requirements of the EU's model clauses, Standard Contractual Clause 2010/87/EU.

Companies that agree to Microsoft's contracts will now be able to use Microsoft cloud to move data more freely from Europe to the rest of the world.

Brad Smith, General Counsel and Executive Vice President of Legal and Corporate Affairs at Microsoft, wrote in his Microsoft blog: 'Starting July 1, we will ensure that all our enterprise customers benefit from this privacy recognition through our standard agreements. The EU approval requires that customers execute a short, standardized addendum to their current agreements in order to take advantage of this new recognition, and we will create a very simple process to facilitate this.'

10. Google pays its biggest EU fine of €1 million in Italy for Street View privacy breaches.

Reuters has reported that the €1m fine imposed on Google was due to the vehicles it used for collecting footage for Street View not being recognizable enough whilst roaming the streets of Italy. The issue the Italian data protection watchdog raised was that this violated the privacy rights of citizens caught on camera without their knowledge or consent.

Google has previously faced a number of privacy lawsuits in Europe and the United States relating to Street View, but this is their largest penalty yet, *Bloomberg* reports. In imposing such a high fine, the Italian watchdog confirmed the search engine operator's "consolidated revenue of over $50 billion" was taken into account. This can be seen as a warning, particularly to large, lucrative companies, of the severity of data protection fines that can be imposed.

In response, Google has already taken steps to make their cars used to collect data more easily identifiable, and by publishing the locations to be visited by the Street View cars on its website and the local media.

[1] Enterprise Enrollment Addendum Microsoft Online Services Data Processing Agreement ("MS Agreement") and its Annex 1 Standard Contractual Clauses (processors).

11. French data protection agency is granted online inspection powers under new French law

Privacy Laws & Business reported that a new French law allows the CNIL to carry out remote online investigations and react to any violations of the French Data Protection Act on the internet. If an infringement is detected, the CNIL's President can decide whether to issue an injunction.

A CNIL spokesperson has confirmed that "this new law also allows us to check how individuals are informed of the use of their data, how their consent is collected when it's necessary and how cookies and tracking tools are employed."

The CNIL has emphasized that the new online investigations will only apply to freely accessible data, and does allow the CNIL to override companies' security measures to gain access to their information systems.

This new power is in addition to the CNIL's existing powers to conduct on-site inspections, document reviews and hearings. Moreover, if CNIL considers that a criminal offence has been committed, it can notify the Public Prosecutor and can publicize any sanctions imposed.

12. PCI Security Standards Council update - action required before 1 January 2015

The PCI Security Standards Council[2] published an updated version of the Payment Card Industry Data Security Standards (PCI DSS) at the end of 2013, applicable to all entities involved in the payment card process, including merchants that accept payment cards. The new version, Version 3.0, became effective on 1 January 2014, and companies will have one year to become compliant.

An updated version of the Payment Application Data Security Standards, applicable to certain software vendors and others who develop card payment applications, were also issued by the PCI. PCI DSS compliance is required by all merchant agreements, and constitutes a critical step in mitigating the risks for data security breaches.

The new Data Security Standards require, among other activities, merchants who accept payment via payment cards (debit cards or credit cards) to have in place written information security procedures (or WISP) addressing specified topics, including how the merchant manages its vendors having access to payment card data. Merchants who outsource the payment processing activities to third parties must still implement a WISP addressing how the merchant manages vendors.

[2] An organisation that develops standards for payment card security.

13. Deceptively simple?

In the absence of broadly-applicable federal privacy legislation, the primary driver of privacy and data security enforcement in the United States comes from a few words that likely weren't meant to regulate privacy or security. The Federal Trade Commission (FTC) regulates generally in the privacy and data security area pursuant to Section 5(a) of the FTC Act (15 U.S.C. §45(a)), which grants the FTC authority to take action against "unfair or deceptive acts or practices in or affecting commerce."

Pursuant to this authority, the FTC has deemed companies' acts with respect to privacy- or security-related disclosures to be "deceptive" and/or "unfair" when those companies have failed to live up to promises made to consumers. E.g., *In re Epic Marketplace, Inc.*, FTC File No. 112 3182 (Mar. 13, 2013) (failure to disclose practice of "history sniffing" in privacy policy). More recently, the FTC has used its "unfairness" authority to initiate enforcement actions against companies have failed to provide for "reasonable and appropriate security." *E.g., In re HTC Am., Inc.*, FTC File No. 122 3049 (Jun. 25, 2013); see also *In re LabMD, Inc.*, FTC File No. 102 3099 (Aug. 28, 2013).

Sounds simple? Some (including LabMD, Inc., noted above) have pushed back, saying that it goes too far to say that authority to regulate "unfair" commercial practices includes the authority to impose baseline information security standards. Others say that the flexibility of authority based on "unfair or deceptive" acts or practice is the kind of flexibility that is called in this rapidly-evolving information economy.

14. California's latest contribution to privacy law

Industry and federal legislators are still dancing with the issue of data collection and use by third party companies on commercial websites (sometimes referred to as "observer" collection – typically involving analytics, or ad servers or other digital marketing service providers). Meanwhile, California, in typical form, has forged ahead with an actual disclosure requirement. Because most websites have visitors from California, the law has a national effect.

California Assembly Bill No. 370 amended California's Online Privacy Protection Act by requiring commercial website operators to make disclosures in their privacy policies relating to their online tracking practices. Briefly summarised, Bill No. 370 requires a commercial website operator to disclose:

- how the operator responds to web browser "do not track" signals or other mechanisms that provide consumers the ability to exercise choice regarding the collection of personally identifiable information about their online activities over time and across third-party websites or online services, if the operator engages in such collection; and

- whether other parties may collect personally identifiable information about consumers' online activities over time and across different websites when consumers use the operator's website or service.

This is an interesting law. Although analytics and digital marketing firms are well aware of browser-based "do not track" methodology, many (if not most) of the commercial website operators (who engage those analytics and digital marketing firms) aren't really sure whether or even how to respond. Yet, the mandate requires commercial website operators to think about "do not track," and it also requires them to specifically inquire whether their third-party "observer" service providers are going to use the information they collect for targeted marketing purposes on other sites.

California has historically been a leader in privacy and data security legislation (including in areas such as data breach notification, payment card data, and mobile privacy). Here, the primary contribution may be simply be a requirement of added thought.

15. The Federal Trade Commission and the "Internet of Things"

The Federal Trade Commission (the primary U.S. privacy regulator) hosted a workshop a few months ago entitled "The Internet of Things—Privacy & Security in a Connected World." The workshop focused on the ubiquitous collection of data in the modern world and steps that might be needed to protect consumers' privacy and security, including discussions of the possible inadequacy of the traditional "notice and choice" privacy framework.

In a sense, the privacy and security issues associated with sharing information among numerous devices is next in a logical progression from the recent focus on ever-increasing service provider handling of personal information. In addition to the FTC, other state and federal agencies and standard-setting bodies (including the National Institute of Standards and Technology) are recognizing that control systems, sensors, and the like must be taken into account along with traditional information systems in any sophisticated information/cyber security program.

Most fundamentally, the "Internet of Things" captures the concept of a highly-connected world in which devices connected to the Internet include phones, cars, home automation and security systems, utility meters, and even commodity-measuring tools for items such as milk and light bulbs.

Several recurring themes emerged as takeaways from the workshop:

- *The viability of Fair Information Practice Principles (FIPPs) notice and choice:* The FTC continues to evaluate the current, traditional FIPPs approach to privacy notice and choice. There are inherent limitations of such an approach in a world where information is collected about consumers ubiquitously, often without any user interfaces. Ultimately, solutions may involve standardized disclosures and notices in connection with use (as opposed to collection) of information.

- *The importance of the context in which information is collected:* For example, data generated by a home automation system to control a coffee pot may be inappropriate for marketing purposes.

- *Consumer awareness and "privacy by design" considerations:* Consumers underestimate how information collected about them might be used in a harmful manner. For example, consumers may not appreciate that information collected by their utility provider could indicate what types of devices they use, when they use those devices, and when they are home or on vacation. On the flip side, automation technology developers may not adequately emphasize and invest in information security in the midst of rapid innovation, market pressures, and the difficulty of predicting the myriad potential uses of the information generated or obtained.

Inadequacy of mere notice-and-choice aside, the "Internet of Things" will be a good test of how much we learned from the experience of adapting privacy and data security concerns to the now-burgeoning mobile app market.

Return to **TABLE OF CONTENTS**