Locke Lord LLP

Data Protection NEWSLETTER

July 2014
Int'l Ed.

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.

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

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

Michael Fung
Partner, Hong Kong
T: +852 3465 0618
mfung@lockelord.com

Stephen K.P. Lo
Of Counsel, Hong Kong
T: +852 3465 0682
slo@lockelord.com

Laura Ferguson
Associate, Houston
T: 713-226-1590
lferguson@lockelord.com

Topics:

Locke Lord LLP

Data Protection NEWSLETTER

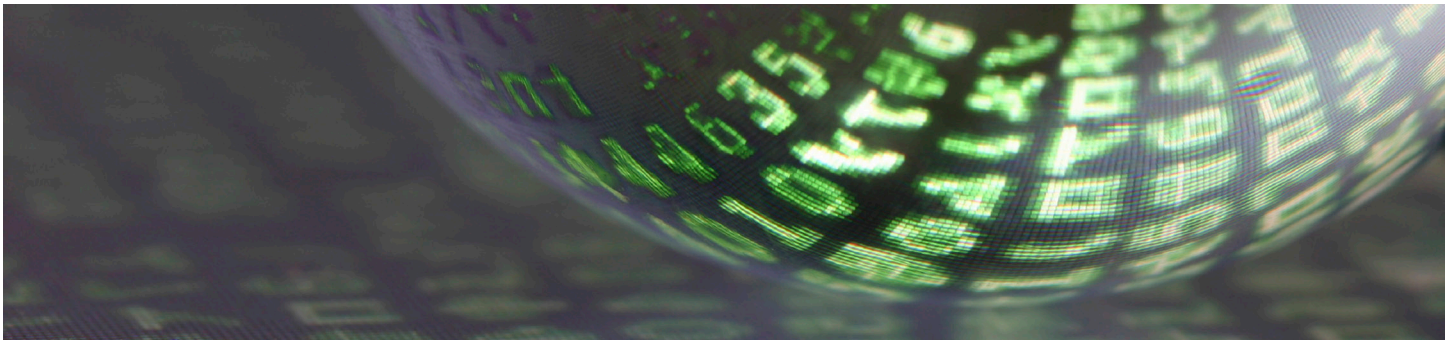
July 2014
Int'l Ed.

Charles M. Salmon
Associate, Austin
T: 512-305-4722
csalmon@lockelord.com

Philippa Townley
Trainee Solicitor, London
T: +44 20 7861 9041
ptownley@lockelord.com

David Dyer
Summer Clerk, Austin
T: (512) 305-4724
ddyer@lockelord.com

Topics: (cont)



1. U.S. State Data Breach Law Update – Kentucky Joins the List and Florida Raises the Bar

Kentucky has finally passed a data breach law, increasing to 47 the number of states in the infamous patchwork of U.S. state data breach laws. Now, only Alabama, New Mexico and South Dakota do not have data breach laws.

Drawing on various features of other state data breach laws, the Kentucky law is applicable only to electronic data breaches, requires prompt notification to affected individuals (but no regulator notification), and is triggered when the unencrypted personal information of a Kentucky resident has been or is reasonably believed to have been acquired by an unauthorized person. Service providers are specifically required to provide notice of a data breach to data owners, and the law includes special restrictions on the processing of student data by cloud computing providers.

More recently, Florida has just repealed its data breach law in favor of a new law, the Florida Information Protection Act of 2014, that includes unique requirements and a tight notification period (30 days after discovery, absent an extension from the Florida AG).

The Florida law provides that, upon request of the Florida Department of Legal Affairs, a company that experiences a breach (presumably, of more than 500 individuals, such as would trigger a regulatory notice requirement) must produce:

1. A police report, incident report, or computer forensics report.
2. A copy of the policies in place regarding breaches.
3. Steps that have been taken to rectify the breach.

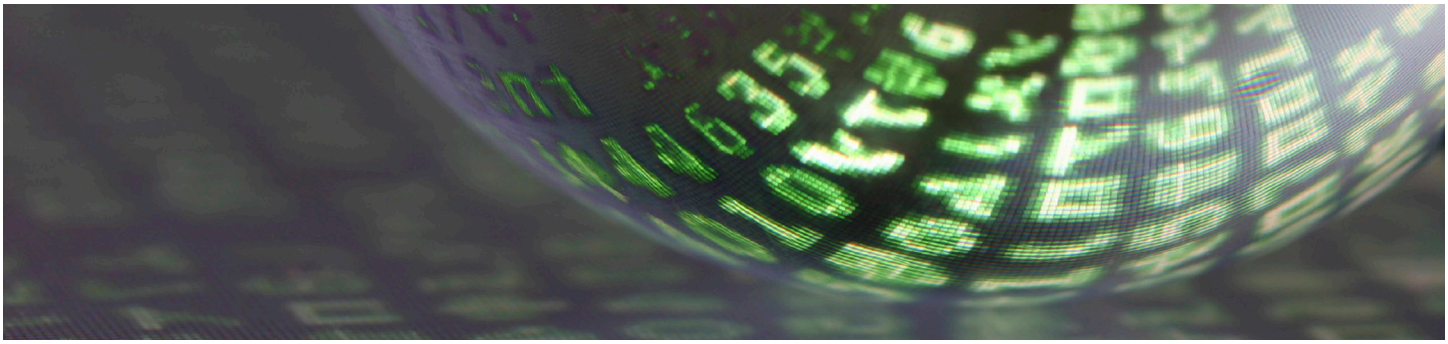
For companies that have employees, customers, or consumer marketing contacts in Florida, the establishment of a security incident response plan has become even more of a good idea.

Adding to the relatively small list of states (such as Massachusetts and California) that specifically require the implementation of information security measures, the Florida law includes a general requirement that companies "take reasonable measures to protect and secure data in electronic form containing personal information." Also, in keeping with the trend, and like the new Kentucky law, the Florida law expressly requires that service providers (called "third party agents") notify data owners "as expeditiously as practicable, but no later than 10 days following the determination of the breach of security or reason to believe the breach occurred."

As companies must generally comply with the highest bar of the various state laws, the new Florida law has significant compliance implications.

2. New EU Data Protection Law on Track for 2015

Speaking at Privacy Laws and Business conference on 1 July, the European Data Protection Supervisor, Peter Hustinx, confirmed that the data protection



regulation, which creates a statutory 'right to be forgotten' and brings non-EU entities within the scope of EU law, is now on an "irreversible road" for agreement in 2015.

One of the issues surrounding the new EU data protection law is whether it will be in the form of a regulation, and therefore immediately effective on Member States, or a directive, which would require national laws to implement it.

The Law Society Gazette reports that the next step in the 'trialogue' process is to reach a consensus between the European council of ministers. This is likely to involve a battle with the UK, who has made their objections to a regulation, and preference of a directive, quite clear. The information commissioner, for example, has emphasised the need to *"engage with partners all around the world. We cannot pull up the drawbridge on the rest of the world, either the European or the UK. We're dealing with a global phenomenon, there need to be global solutions."*

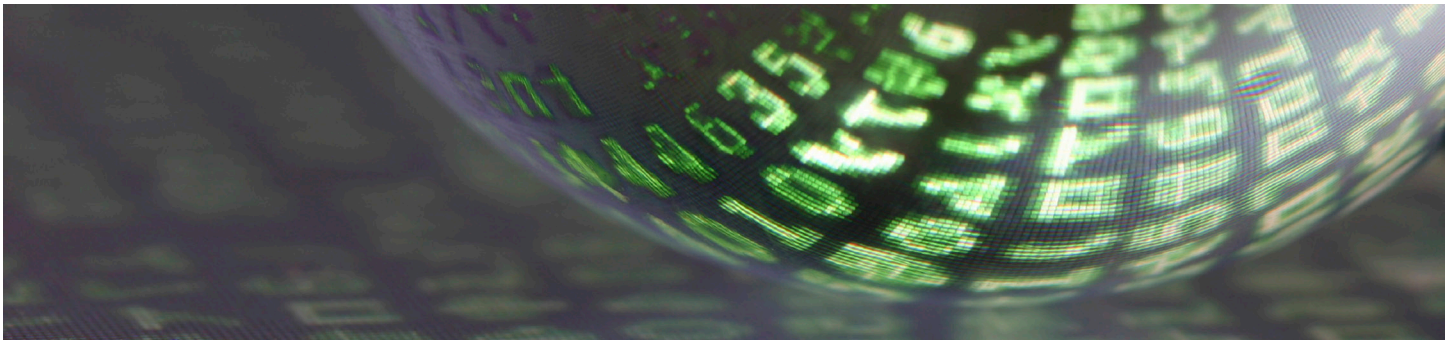
Hustinx, however, has reportedly affirmed that UK objections to a regulation are unlikely to have any an impact, given that voting in the Council will be done by qualified majority.

3. Mobile App "Privacy Sweep" – Collaboration Between Hong Kong Privacy Commissioner and Global Privacy Enforcement Network

The Office of the Privacy Commissioner for Personal Data in Hong Kong ("PCPD") has collaborated with the Global Privacy Enforcement Network in conducting a Privacy Sweep exercise to assess corporate data users in their collection and use of personal data on mobile applications.

The PCPD will look at how an app explains to consumers why it wants the data it collects and what it will do with it. It will also examine the types of permissions an app is seeking and whether those permissions exceed what would be expected based on the app's functionality.

The Privacy Commissioner for Personal Data has said: *"Mobile apps are ubiquitous and have transformed business operations and our lives. However, many app developers are often unaware of the privacy implications of their work. As revealed in the Hong Kong Sweep of 60 apps last year, transparency in terms of privacy policy was generally inadequate. Only 60 per cent of the apps provided Privacy Policy Statements ("PPS") but they were all provided in the developer's websites and few explained the purpose for accessing each type of data stored on smartphones. In several cases, the PPS was not provided until after the users had installed the apps. Appropriate advice has been given to the organisations concerned to ensure no excessive collection of personal data and that consumers are clearly informed about the types of personal data an app collects and uses and why that data is needed."*



"Improving privacy and data protection in the use of apps remains a key area of focus for PCPD in 2014. A two-pronged approach will be taken, covering both professional and public education as well as enforcement. We hope to see an improvement in privacy protection in this year's Sweep. We encourage app developers to embrace privacy to build user trust and gain a competitive advantage in business. The results of this year's Sweep will be compiled and made public by this fall. We do not rule out having to take enforcement action when warranted."

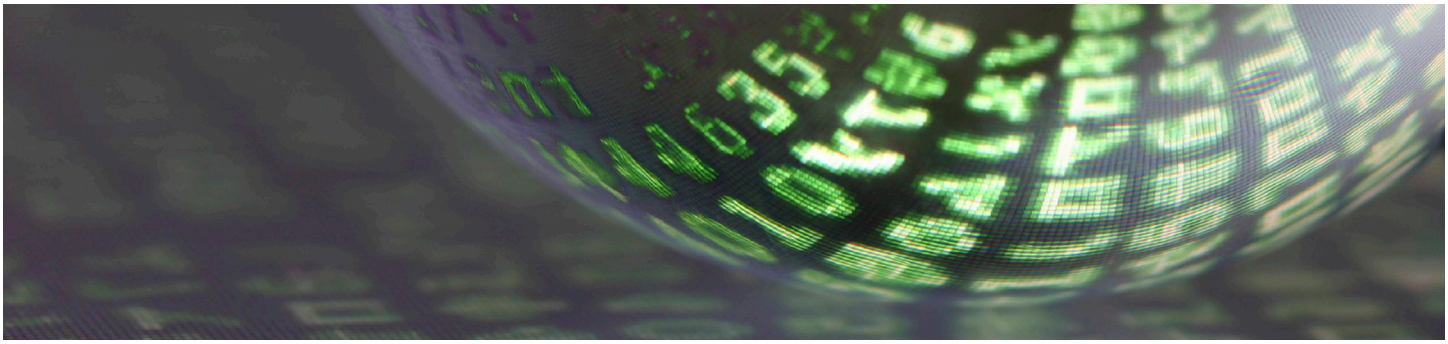
4. Canada's New Anti-Spam Law

Canada has finally implemented a law approved over three years ago that is a real game-changer for companies that conduct electronic marketing in Canada. The "Fighting Internet and Wireless Spam Bill," commonly known as the "Canadian Anti Spam Law" or "CASL," took effect on July 1, 2014. In contrast to the U.S. CAN-SPAM law, CASL is an opt-in regime, requiring some form of consent before messages are sent (in addition to offering an unsubscribe mechanism), and CASL applies to a broad swath of electronic messages, including e-mail, SMS/text messages, and some social media communications.

The law may be enforced by the Canadian Radio-Television and Telecommunications Commission, the Commissioner of Competition, and the Privacy Commissioner. Companies that market into Canada would be well-advised to make efforts to comply (and to ensure that their marketing vendors are complying) right away, as hefty penalties are available. In 2015, the reach of the law will expand to cover installation of apps and other "computer programs" on devices. Beginning in 2017, private rights of action will be available.

CASL prohibits sending "commercial electronic messages" to "electronic addresses" in Canada without express or implied consent, sender identification information, and an unsubscribe mechanism. Consent may be implied from an existing business relationship, but the period of such implied consent may be limited. Companies' electronic marketing platforms will need to track express consents, transaction history (and any other implied consent details), and unsubscribe requests.

Several Canadian governmental resources are available to assist with interpretation of CASL, including a CASL website and bulletins such as those found here and here.



5. Privacy Comes at a Cost: The U.S. Supreme Court's Opinion in Riley v. California

In Riley v. California, a cell phone search-and-seizure opinion delivered by Chief Justice Roberts for a unanimous Court last month, the U.S. Supreme Court squarely recognized, and afforded special protection to, the ubiquitous use and storage of voluminous electronic data of many different types on mobile devices today. The opinion holds that, without a warrant, law enforcement generally may not search the content of a cell phone that has been taken from an arrested individual.

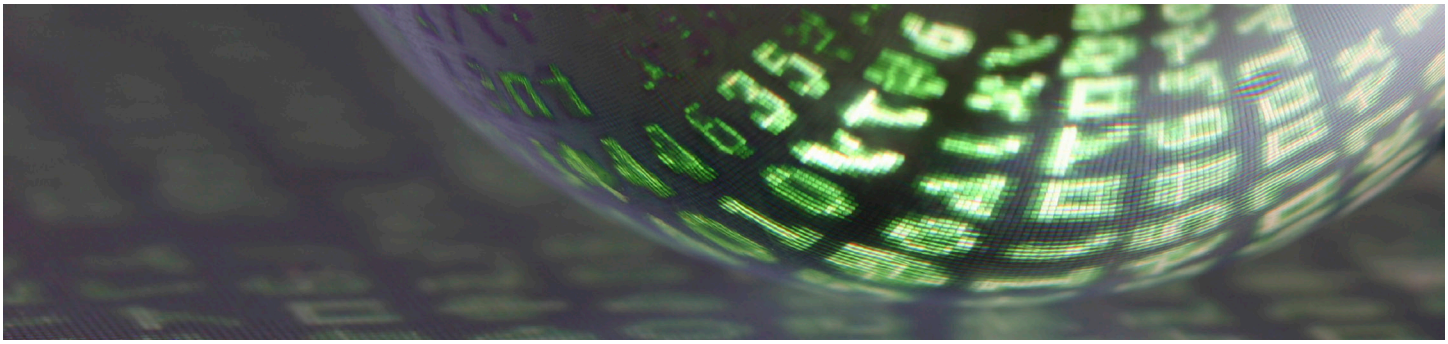
This landmark decision required a distinct departure from a trilogy of U.S. Supreme Court decisions permitting the search of property found on or near an arrestee under the "incident to an arrest" exception to the requirement of a warrant under Fourth Amendment jurisprudence. Those decisions were grounded in the interests of officer safety and preservation of evidence, a limited intrusion on individual privacy, and, in one decision, the unique characteristics of the arrest of an individual in an automobile.

Harking back to Learned Hand's observation in 1926 that "it is 'a totally different thing to search a man's pockets and use against him what they contain, from ransacking his house for everything that may incriminate him,'" today's Court observed that, "[i]f his pockets contain a cell phone, however, that is no longer true."

The Court described information obtainable through the search of a cell phone (browsing histories, app selection and usage, etc.), which Riley's brief had argued implicated First Amendment concerns for freedom of expression and freedom of association. The Court reasoned:

> The storage capacity of cell phones has several interrelated consequences for privacy. First, a cell phone collects in one place many distinct types of information – an address, a note, a prescription, a bank statement, a video – that reveal much more in combination than any isolated record. Second, a cell phone's capacity allows even just one type of information to convey far more than previously possible. The sum of an individual's private life can be reconstructed through a thousand photographs labelled with dates, locations, and descriptions; the same cannot be said off a photograph or two of loved ones tucked into a wallet. Third, the data on a phone can date back to the purchase of the phone, or even earlier. A person might carry in his pocket a slip of paper reminding him to call Mr. Jones; he would not carry a record of all his communications with Mr. Jones for the past several months, as would routinely be kept on a phone.

The Court made a point (in a footnote) of stating that this decision, which concerns only the question of a search incident to an arrest, does not address "the question whether the collection



or inspection of aggregated digital information amounts to a search under other circumstances."

Although the Court made clear that warrantless search of a cellphone may still be permissible under the "exigent circumstances" doctrine, the Court blunted conceded, "We cannot deny that our decision today will have an impact on the ability of law enforcement to combat crime. … Privacy comes at a cost."

In part out of the Court's "general preference to provide clear guidance" to law enforcement with straightforward rules, the Court declined to limit its holding with, for example, a rule that a cell phone search without a warrant would be permissible whenever the police officer has a reasonable belief that the cell phone has evidence of the crime for which the arrest has been made. As the Court noted, "[i]t would be a particularly inexperienced or unimaginative law enforcement officer who could not come up with several reasons to suppose evidence of just about any crime could be found on a cell phone." There is at least a little bit of irony in that.

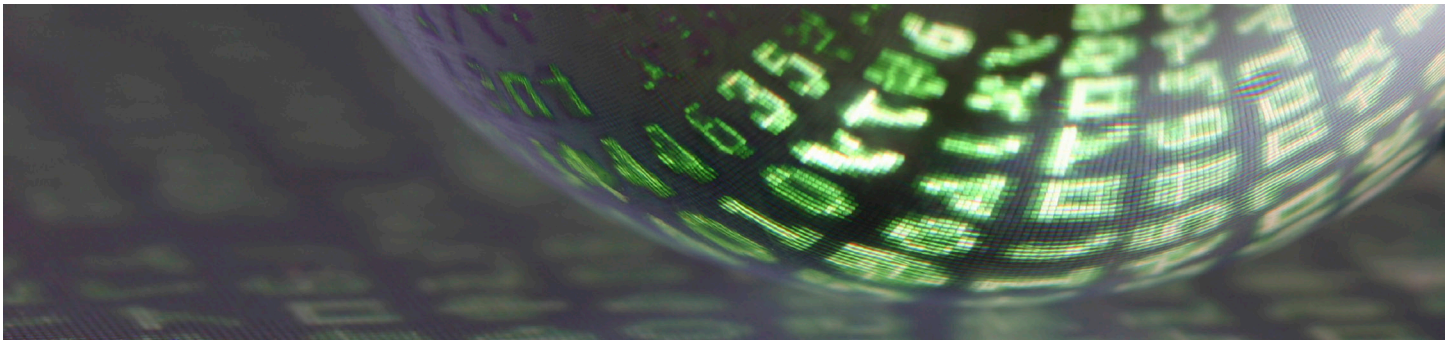
6. British Government's Continued Insistence on Telecom and ISP Data Retention Notwithstanding Ruling of EU Court of Justice

The British Government could face High Court legal action for continuing to force telecoms and internet providers to retain customer data, despite the EU Data Retention Directive being overturned.

In April this year, the Data Retention (EC Direction) Act of 2009, which required member states to store citizens' telecoms data for a minimum of six months and a maximum of 24 months, was declared unlawful by the Court of Justice of the European Union and overturned. The Directive required telecoms companies to retain records of customer phone calls and emails to help police investigate crimes.

Pedro Cruz Villalón, the court's Advocate General, is reported in the Guardian as stating that the directive constituted a "*serious interference with … the right to privacy and the right to protection of personal data.*" He also explained that there was a *"risk that the retained data might be used illegally in ways that are "potentially detrimental to privacy or, more broadly, fraudulent or even malicious."*

Despite this, the UK Government has not yet invalidated the UK implementation of the directive. Further, in June this year, the Home Office Minister, James Brokenshire made the following announcement: *"The Government continues to consider the judgment of the European Court. At the present time, we consider that the UK Data Retention (EC Directive) Regulations 2009 remain in force. Those in receipt of a notice under the regulations have been informed that they should continue to observe their obligations as outlined in any notice."*



7. Hong Kong Privacy Commissioner Condemns Recruitment Advertisements that do not Identify Employers

In Hong Kong, some organizations have been found to be in breach of the Data Protection Principle for placing job advertisements without disclosing their identities. Such advertisements are called blind ads, and solicit job applicants' personal data in an unfair manner. They could be exploited as an unscrupulous means to acquire personal data for direct marketing and fraudulent activities, thus causing nuisance and/or financial loss.

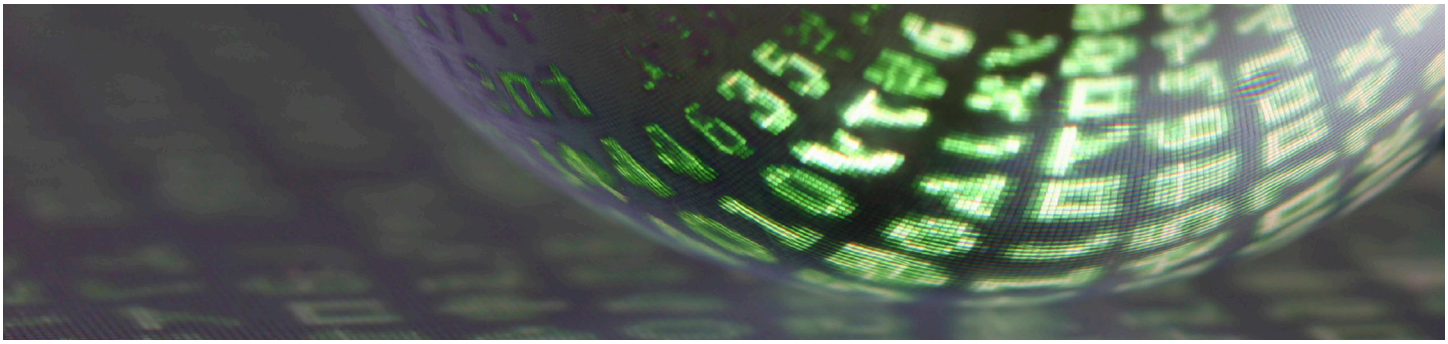
Investigation into 48 cases has been carried out. The organizations involved in all of the 48 completed cases were issued an enforcement notice by the Privacy Commissioner directing them to delete the personal data collected, unless it has to be retained for satisfying other legal requirements, or for a continuing recruitment process in which case the job applicants have to be informed and given the option to demand deletion of their personal data.

The Privacy Commissioner has said: *"A job advertisement placed by an organization serves to attract suitable candidates to fill the vacancy as well as to project its corporate image. A Blind Ad in this regard is counter-productive as it demonstrates the company's ignorance of the law and a disrespect for privacy and data protection. Employers should therefore refrain from placing Blind Ads seeking job applicants' personal data. Where there is a genuine need for employers to conceal their identity when advertising for job vacancies, they may resort to Blind Ads but use them to solicit job applicants' enquiries rather than personal data."*

8. The White House Big Data Report and a Recent Press Release on Big Data from the European Commission

The Big Data: Seizing Opportunities, Preserving Values report by the White House provides a thoughtful analysis of economic, legal, and practical issues that arise from Big Data. The report, released in May, has been frequently referenced but has not received much specific attention. That is primarily because it does not include any unusual or new positions, instead focusing on the state of current thinking as well as the need for greater interoperability on a global scale.

But it is still an excellent report, drawing on input from hundreds of stakeholders from industry, academia, privacy and civil liberties organizations, international data protection authorities, and



the federal government (including intelligence and law enforcement). It is certainly recommended reading for thinkers in the field.

The topic is vitally important and very real. As the report notes:

> We aspire to use data to solve problems, improve well-being, and generate economic prosperity. The collection, storage, and analysis of data is on an upward and seemingly unbounded trajectory, fueled by increases in processing power, the cratering costs of computation and storage, and the growing number of sensor devices embedded in devices of all kinds.
>
> Big data may be viewed as property, as a public resource, or as an expression of individual identity. Big data applications may be the driver of America's future or a threat to cherished liberties. Big data may be all of these things.

The report discusses economic, consumer, and health and safety benefits, as well as threats to privacy, possible governmental abuse, and possible discriminatory use associated with Big Data.

Notably, the report also includes a pragmatic discussion of the "de-identification," or "anonymization," concept, which is a foundational element (too often glossed over) in most uses of Big Data. As the report notes, "[i]n practice, data collected and de-identified is protected in this form by companies' commitments to not re-identify the data and by security measures put in place to ensure those protections." There is a real need for more discussion and ultimately a need for generally-accepted standards (beyond isolated examples, such as found in the U.S. Health Insurance Portability and Accountability Act) on this topic.

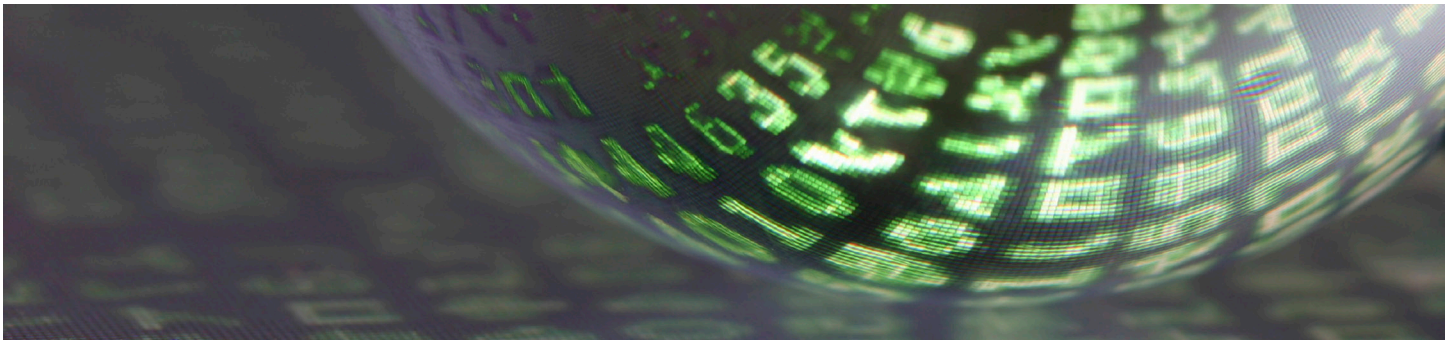
Sending a clear signal that the U.S. understands the global significance of the appropriate recognition of individual privacy rights, the report recommends, among other things:

- advancement of the White House's Consumer Privacy Bill of Rights;
- the extension of privacy protections to non-U.S. persons in connection with data held by the federal government;
- expansion of technical expertise within the federal government's "lead civil rights and consumer protection agencies;" and
- amendment of the Electronic Communications Privacy Act to ensure appropriate protection of digital content.

On the other side of the pond, the European Commission also recognizes the inevitability of the "Big Data Revolution," including the collection and use of data in connection with the "Internet of Things." On July 2, 2014, the European Commission called on national governments within the E.U. to embrace the potential of Big Data.

The Commission's press release observes that "[b]usinesses that build their decision-making processes on knowledge generated from data see a 5-6 percent increase of productivity." It highlights a frank quote from Vice-President Neelie Kroes :

> It's about time we focus on the positive aspects of big data. Big data sounds negative and scary, and for the most part it isn't. Leaders need to embrace big data.



According to the Commission, topics of particular importance in the realization of Big Data's potential are cross-border coordination, a need for more data experts and related skill resources, and de-fragmentation and simplification of the applicable legal frameworks. Proposed action items are stated as follows:

- A Big Data public-private partnership that funds "game-changing" big data ideas, in areas such as personalised medicine and food logistics.
- Create an open data incubator (within the Horizon 2020 framework), to help SMEs set up supply chains based on data and use cloud computing more.
- Propose new rules on "data ownership" and liability of data provision for data gathered via Internet of Things (Machine to Machine communication)
- Mapping of data standards, identifying potential gaps
-
- Establish a series of Supercomputing Centres of Excellence to increase number of skilled data workers in Europe
- Create network of data processing facilities in different Member States

9. Cyber Attack on World Cup Officials and Sponsors by "Anonymous" Hacking Group

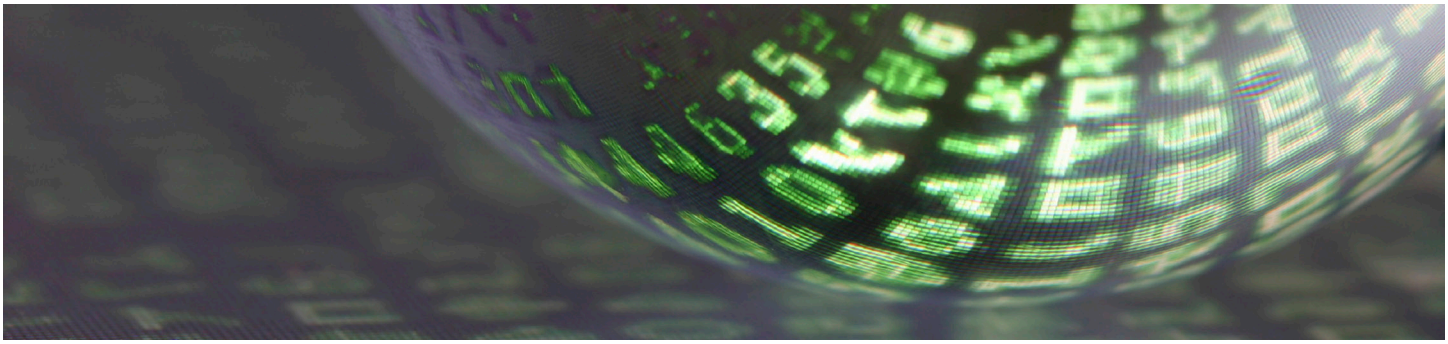
In June this year, hacking group by the name of "Anonymous" has been threatening and carrying out cyber attacks on commercial sponsors and organisers of the football World Cup in Brazil. Cyber Risk Network has reported that already hundreds of documents taken from Brazil's Foreign Ministry's computing network have been posted and dozens of confidential emails leaked.

In addition to the protesters that have taken to the streets of Brazil in the lead up to the 2014 World Cup, the cyber attack is part of a protest against Brazil's extravagant expense of hosting the World Cup, when much of the Brazil's population is reported as struggling to make a living.

A member of Anonymous who calls himself Che Commodore explained to Reuters in June that *"companies and institutions that work with a government that denies the basic rights of its people in order to promote a private, exclusive and corrupt sports event will be targeted".*

Che Commodore further warned that they had a "*plan of attack",* and potential targets included Adidas, Emirates Airline, the Coca-Cola Co and Budweiser. In response, an Emirates spokesperson confirmed to Arabian Business that the Dubai airline *"has been made aware of the potential threats and has taken the necessary measures to prepare ourselves should the need arise".*

Reuters explains how the hacktivists have used a Distributed Denial of Service (DDoS) against government sites, which essentially takes a web site down by overriding its server with multiple



access requests. Defacement of sites has also been carried out, whereby hackers manipulate the appearance of a site and insert hostile messages.

An Analysis Report by Tiger Security revealed that in the days leading up to the World Cup 55 email accounts of Brazil's diplomatic officers were hacked. The hacktavists then sent over 600 emails to employees and diplomats of Brazil's Ministry of Foreign Affairs inviting them to enter email credentials, as part of a mission to break into and steal mail and data from them, including a list of foreign dignitaries planning to attend World Cup matches. In response a Foreign Ministry spokesperson has played down the impact of the attack stating: *"The problem has been solved, nothing important has leaked out".*

10. New Personal Data Protection Act comes into Effect in Singapore

From 2 July this year, the Personal Data Protection Act (PDPA) that was passed in Singapore on October 2012 will have effect, imposing stricter rules on how companies collect and use personal data.

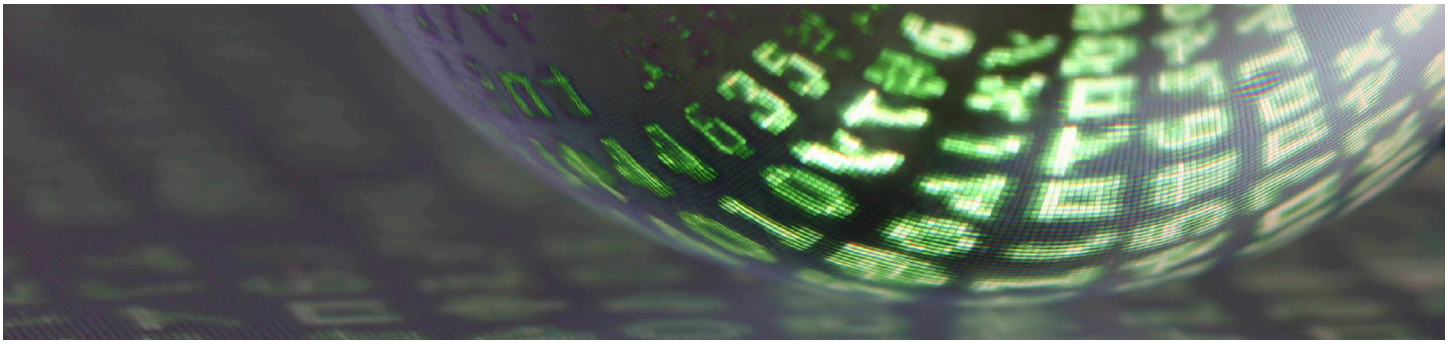
Some of the Act's provisions took effect earlier this year, for example preventing companies from sending messages to numbers that are listed on the Do Not Call registry. The remainder of the rules, however, take effect from 2 July.

Channel News Asia reported that companies that have collected data before 2 July can continue to use the data as they did before the new rules. After 2 July, however, companies will have to abide by the new rules, which require them to take further steps to protect customers, whilst giving greater power to customers.

The additional obligations on organisations and rights of customers include:

- Data Protection Officer (DPO) - companies now have to appoint a DPO;
- Consent - companies will have to tell their customers why they are collecting their data, for example, and customers will have to give their consent;
- Access and correction - individuals will be able to request access to and correction of the data that the company holds on that individual. The Regulations clarify that the request has to be made in writing to the company's DPO;
- Transfer of data outside Singapore – before transferring personal data outside of Singapore, the transferring organisation must ensure that the recipient is "bound by legally enforceable obligations to provide to the personal data transferred a standard of protection that is comparable to that under the PDPA"

In advance of the PDPA coming into effect, the Singapore Personal Data Protection Commission released the Personal Data Protection Regulations (2014) and Guidelines to clarify the obligations under the new Act.



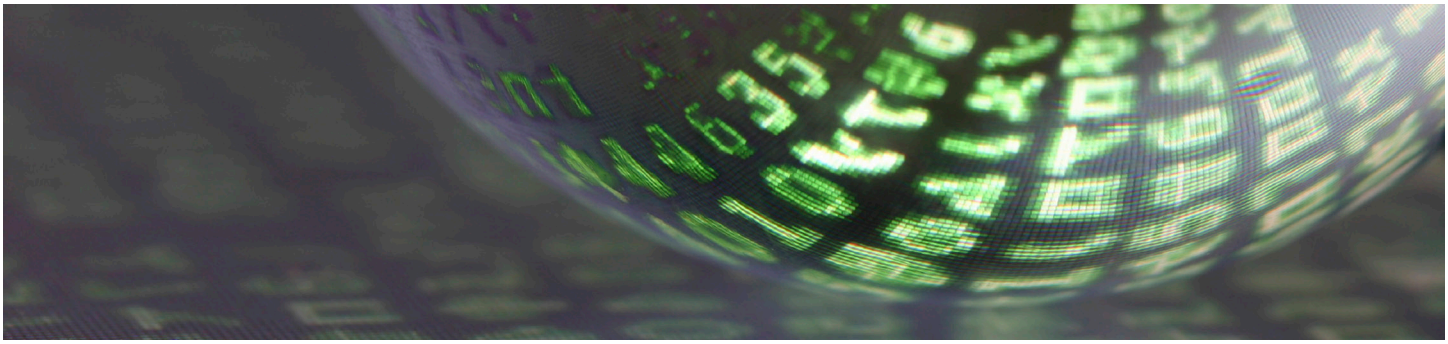
11. Heath Plan Identifiers, CHPs, and SHPs – Implications for a Company's U.S. Group Health Plan

The U.S. Department of Health and Human Services is increasing its oversight of group health plan covered entities in accordance with regulations issued as required by the Affordable Care Act. By November 5, 2014, all group health plans subject to the Health Insurance Portability and Accountability Act ("HIPAA") Privacy Rule must register for a Health Plan Identifier number ("HPID"). Small health plans (< $5M in annual receipts) have until November 5, 2015. The HPID is required for use by the plan when it (or a business associate of the plan) conducts standard transactions, such as for eligibility, health care claim status, and health care electronic fund transfers and remittance advice.

Each health plan that controls its own business activities, actions, or policies is required to register as a "Controlling Health Plan" ("CHP"). The CHP can file on behalf of any health plans whose activities it directs (called "Subhealth Plans" ("SHP")), or the employer can apply for a separate number for its SHP(s). For an employer that has multiple covered entity health plans that are part of a "wrap" plan for Form 5500 purposes (such as a major medical group health plan and a health care FSA), the employer can register the wrap plan as the CHP and the component plans would be SHPs (such that only one HPID is required).

In addition, under proposed regulations issued in January pursuant to the Affordable Care Act, a CHP must, by December 31, 2015: (1) certify that the CHP conducts standard transactions in compliance with the Transaction Rules (even if business associates conduct those transactions on the CHP's behalf); and (2) file an attestation with HHS that it obtained the required certification described in (1) and report the number of covered lives under the plan. Failure to file the certification and attestation may result in penalties of $1 per covered life per day (up to a maximum amount). Since most group health plans rely on business associates to conduct the transactions addressed by these rules, employers should review business associate agreements and administrative service agreements to determine which party is responsible for compliance with these regulations (once final), the timing for preparing the required certification, and the applicability of any indemnification provisions for the new responsibilities (since the CHP must attest to any certification prepared by the business associate).

See here for more information on the Health Plan Identifiers. For more information on the Affordable Care Act certifications, see guidance available here.



12. ICO Warns that Google Glass could Breach U.K. Data Protection Act

In the same week that Google Glass was launched in the UK in June this year, Andrew Paterson, the Senior Technology Officer for the ICO published a blog on the interplay of the device with the protections afforded to individuals under the UK's Data Protection Act 1998.

The main concern in the media over the wearable recording device appears to be the lack of notice it gives to the public that might be being filmed without their knowledge or consent. Paterson explains: *"If you are using a wearable technology for your own use then you are unlikely to be breaching the Act. This is because the Act includes an exemption for the collection of personal information for domestic purposes. But if you were to one day decide that you'd like to start using this information for other purposes outside of your personal use, for example to support a local campaign or to start a business, then this exemption would no longer apply.*

This includes making sure that people are being informed about how their details are being collected and used, only collecting information that is relevant, adequate and not excessive and ensuring that any information that needs to be collected is kept securely and deleted once it is no longer required. This is not the case for organisations, whose use of wearable technology to process personal information will almost always be covered the Act. This means that they must process the information collected by these devices in compliance with the legislation."

The blog closes by recognising the excitement of wearable technology, but warning that *"organisations must not lose sight of the fact that wearables must still operate in compliance with the law and consumers' personal information must be looked after."*

13. Europe's First Ever Cyber Security Focused Fund

London-based asset manager, C5 Capital, is launching Europe's first ever cyber security focused fund, valued at £125m, taking advantage of Europe's strong position in relation to data protection and digital security, as global concerns continue to grow.

In June this year the FT has reported on C5 Capital's announcement that the fund has already made a £8m investment in Balabit, a company that specialises in detecting insider threats, preventing employees and contractors stealing confidential data and IP from computer networks.

Research from Gartner shows that the global information security sector market is currently valued at $67bn, and will only continue to grow given the numerous high profile cyber attacks reported recently. The fund appears to be a proactive response to the growing concerns surrounding leaks of data and digital security.

Return to **TABLE OF CONTENTS**