2015 Outlook: Data Privacy and Security in the United States, the European Union and Hong Kong

Companies and organizations face an ever-expanding set of statutes and regulations regarding consumer privacy, data protection and cybersecurity. Legal standards continue to evolve—and differ—in all major markets, raising particular challenges for multinational businesses.

Here we review key elements of the evolving legal landscape facing companies in the United States, the European Union and Hong Kong in 2015.

United States

DEVELOPMENTS IN LITIGATION AND ENFORCEMENT

We saw several significant developments in data breach litigation and enforcement in 2014, including the ruling by a federal district court in New Jersey that upheld the FTC’s authority over data security in *FTC v. Wyndham Worldwide Corp*. Federal district courts in Minnesota and New Jersey addressed the obligations that companies suffering data breaches might owe to shareholders and banks, respectively. And courts across the United States grappled with whether customers and employees of companies affected by data breaches, whose records may have been compromised but have not been misused, can establish standing under Article III of the US Constitution or sufficiently allege that they suffered cognizable harms under relevant state laws.

These decisions are only the beginning: data-breach lawsuits continue to proliferate and will surely prompt new judicial opinions in the coming year. Moreover, with district court decisions now in the books, appellate courts are likely to weigh in on important issues. Significantly, the Third Circuit recently heard oral arguments in Wyndham’s appeal of the order upholding the FTC’s data security enforcement efforts, a case that could have ramifications for public enforcement and private litigation, and even legislation.

While data breach incidents dominate the headlines, more conventional privacy claims continue to spur litigation. Plaintiffs continue to target companies under the Fair Credit Reporting Act for their use of consumer data in the employment process; courts have certified class actions under zip-code collection statutes, such as California’s Song-Beverly Act; and cases under the Telephone Consumer Protection Act, which governs unsolicited and automated telephone calls and texts, have survived summary judgment and are leading to class
settlements—sometimes substantial ones—and potentially trials.

More recently, class actions have emerged under the Video Privacy Protection Act (VPPA), a little-known statute that prohibits video service providers from disclosing customers’ video preferences. In 2014, several courts addressed the scope of the VPPA, including who qualifies as a videotape service provider, what qualifies as personal identifying information and what practices violate the Act. The continued evolution of the VPPA could loom large in privacy law, as more companies offer streaming video content and enhanced user profile capabilities. And, in January 2015, the FTC issued its long-awaited report on the “Internet of Things,” recommending best practices that (if not followed) could pave the way for enforcement actions and, thereafter, private litigation.

Last, but perhaps most significant, the federal circuits continue to split on whether bare allegations of a federal statutory violation, without any actual harm, are sufficient to satisfy the standing requirements imposed by Article III of the US Constitution. Many privacy class actions involve allegations that a business violated a federal statute—such as the Fair Credit Reporting Act or the VPPA—but do not contend that the plaintiff suffered any concrete or tangible harm apart from experiencing the statutory violation. These class actions, combined with the data breach lawsuits described above, underscore the importance of this ongoing debate in the privacy context (and beyond). Indeed, the issue is currently pending in Spokeo, Inc. v. Robins, in which the company has petitioned the US Supreme Court for review of a Ninth Circuit’s decision authorizing claims under FCRA even when the plaintiff has not suffered actual harm. (Mayer Brown represents the petitioner.) The Supreme Court has asked the Solicitor General’s office to express its views on whether review should be granted, signaling the importance of the issue presented by the petition.

REGULATORY OUTLOOK

Federal and state regulatory agencies continued to increase their engagement on privacy and cybersecurity issues in 2014. Many announced plans to increase their regulatory activities in 2015. Whether these agencies will coordinate their efforts or will burden companies with conflicting mandates or “best practices” remains to be seen. What we do know is that these agencies will be active. Consider the following three examples:

- Last year saw the federal financial regulators substantially increased their engagement on cybersecurity issues. For example, the Federal Financial Institutions Examination Council (FFIEC) expanded its awareness campaign and issued specific recommendations for financial institutions based on its assessment of cybersecurity practices. This year is sure to see further expansion of federal financial regulators’ efforts in this field, including through their use of supervisory authorities to examine the cybersecurity practices at financial institutions. Numerous open questions about these examinations remain, including whether the examinations will enhance the security of those institutions; whether the regulators will impose de facto standards on subject entities; and how effectively those regulators will leverage the expertise and assets of other government entities. Of course, supervisory examinations are confidential, meaning that these questions may go unanswered for some time.

- The Office of Civil Rights at the Department of Health and Human Services has expressed its concern about the increasing number of data breaches involving the compromise of information protected by the Health Insurance Portability and Accountability Act (HIPAA). That office has primary authority for enforcing HIPAA’s privacy protections and
has made clear that it plans to press forward with its enforcement efforts in 2015. How those efforts will relate to the anticipated HIPAA assessments remains to be seen.

- In December 2014, the National Institute for Standards and Technology (NIST) issued an update on its Cybersecurity Framework that discussed the adoption and public awareness of that “living document.” NIST concluded that the “Framework core mappings are being used to demonstrate alignment with standards, guidelines, best practices, and, in some cases, to regulatory requirements. The Framework is also being used as a strategic planning tool to assess risks and current practices.” NIST acknowledged that it was too soon to update the Framework, and indicated that it would engage in further efforts to improve awareness of the Framework. Notably, NIST did not indicate how it expected regulatory agencies to use the Framework in 2015, leaving continuing uncertainty about the role of that document in any future regulatory activity.

European Union

TRANSFER OF DATA TO THE US: A RE-EVALUATION OF THE SAFE HARBOR REGIME

By the end of 2015, we may see a judgment from the European Court of Justice (ECJ) that has a substantial impact on the way in which data is transferred to the United States. The court will consider whether Member State data protection authorities will be able to disregard the “Safe Harbor” regime and make their own assessment of adequacy of data protection in relation to US companies. This question was submitted to the ECJ on July 16, 2014 by the Irish High Court on the back of a case brought before it by Maximillian Schrems (a Viennese data activist and law student) against Facebook.

In the case heard by the Irish High Court, Schrems argued that Facebook Ireland’s transfer of EU citizens’ data to the United States was in contravention of data protection law. The Irish High Court ruled that the Irish data protection commissioner had correctly dismissed Schrems’ complaints because Facebook was a Safe Harbor participant. Notwithstanding, the Irish High Court ruled that it did not have the authority to assess the adequacy of Safe Harbor, and therefore referred the question to the ECJ. This has given rise to an opportunity for the re-
evaluation of the Commission’s 2000 decision that created Safe Harbor.

DATA PROTECTION REGULATION

EU Member States have now agreed to conclude negotiation regarding the EU Data Protection Draft Regulation. It is now looking like there is a real possibility the Data Protection Regulation will be enacted in 2015, which, on the basis of the currently envisaged two-year implementation period, would see it implemented in 2017. Some of the major developments are as follows:

- The Right to be Forgotten (Article 17): Data subjects will have the right, under certain conditions, to request deletion of their personal data.
- The Right to Data Portability (Article 18): Data subjects will have the right to obtain a copy of all personal data relating to them in a structured and commonly used electronic format.
- Privacy by Design and Default (Articles 23 & 33): Data controllers must implement data processing systems that are in accordance with the draft legislation.
- Breach Notification (Articles 31 & 32): Data controllers must inform the relevant data protection authority of a personal data breach within 72 hours of their becoming aware of it.
- Appointment of Data Protection Officers (Articles 35 & 36): Organizations will be required to appoint a Data Protection Officer where that organization: (i) is a public authority or body; (ii) is carrying out the processing of more than 5,000 data subjects; (iii) is conducting processing activities such as regular and systematic monitoring or profiling of data subjects; or (iv) is processing special categories of data as its core activity.
- Introduction of the One-Stop Shop (Articles 54 & 73): The one-stop shop system will designate a lead data protection authority for data controllers established in more than one member state.
- New Penalties (Article 79): The cap for fines will be increased to €100m or 5 percent of global annual turnover.

THE REVISED TECHNOLOGY TRANSFER BLOCK EXEMPTION REGULATION AND TECHNOLOGY TRANSFER GUIDELINES

The European Commission has adopted a revised block exemption for technology transfer agreements (TT-BER). The new regime reduces the scope of the automatic block exemption for certain types of clauses and opts for a case-by-case assessment instead. Technology transfer agreements that have been concluded by April 30, 2014, and that are in compliance with the old TT-BER, will remain exempted until April 30, 2015.

PAYMENT SERVICES

The recast Payment Services Directive is expected to be adopted at European levels during 2015. By creating a single market standard across the European Union, trust and accessibility will be enhanced, while supporting technological innovation. The new legislation will aim to ensure markets are open to the benefits of advancing technology in the payments industry, while concurrently addressing the associated risks.

TRANSPARENCY OF CLINICAL DATA: THE EUROPEAN MEDICINES AGENCY’S NEW POLICY

On October 2, 2014 the board of the European Medicines Agency (EMA) approved the EMA’s policy on publication of clinical data for medicinal products for human use. As a response to demand for greater transparency in public health and pharmaceutical research and development, the policy facilitates the non-commercial use of the data—e.g., for consideration and analysis by academics and healthcare professionals. The document also ensures the protection of personal and commercially confidential information. The policy will be applied in steps from January 1, 2015, starting with the publication of clinical data contained in clinical reports, followed by
the publication of individual patient data, which will occur once the EMA has established structures to collect, evaluate and protect individual patient data.

Hong Kong

COMPLAINTS AND INQUIRIES
On January 28, 2015, the Hong Kong Privacy Commissioner (PC) issued his annual report for April 2013 to March 2014 (the Report) summarizing developments concerning the Personal Data (Privacy) Ordinance (the PDPO) and the Office of the PC’s activities. According to the Report, the PC received 1,888 complaints in 2013-2014. This is a 53 percent increase compared with 2012-2013. Of these, 78 percent were made against private organizations—the vast majority of which are in the banking and finance industry. Most of the complaints concerned the use of personal data without the requisite consent.

INCREASED ENFORCEMENT ACTION
The number of enforcement notices issued by the PC also rose from 25 enforcement notices in 2013 to 90 in 2014. Last year also saw the first prison sentence issued for a breach of the PDPO when an insurance agent was found guilty of knowingly making a false statement to the PC and was sentenced to four weeks in prison.

The PC also has been increasing the number of investigations initiated on its own. In 2014, the PC conducted 102 self-initiated investigations and 217 compliance checks. This is a significant increase from the 19 investigations and 208 checks conducted by the PC in 2013.

Additionally, under new provisions that came into force in 2013, the PC can now provide legal advice, mediation or legal representation for an aggrieved person. However, of the 17 requests made in 2013-2014, only one was granted legal assistance, and seven were refused (the rest were either withdrawn or are still being considered).

CROSS-BORDER TRANSFERS
Section 33 of the PDPO is Hong Kong’s only data privacy law. It prohibits the transfer of personal data out of Hong Kong except in specific circumstances—such as the transfer of data to a country that is on the “white list” of jurisdictions that the PC considers to have laws that protect personal data to a level commensurate with the PDPO. Most of Section 33’s provision have yet to come into force.

In 2013, the PC surveyed 50 jurisdictions and recommended to the government a white list of countries with protection laws substantially similar to the PDPO. Additionally, as an interim step, on December 29, 2014, the PC issued guidance on the transfer of personal data out of Hong Kong, to help data users prepare for the eventual implementation of Section 33. While Section 33 still has not fully come into force, companies should start to build into their standard personal information collection statement a tick box enabling the data subject to indicate their specific consent to the cross-border transfer.

APPS AND TECHNOLOGY
The PC received 1,702 complaints in 2014, 12 percent of which were in relation to the use of information and communications technology. This was an increase of 122 percent in the number of complaints relating to information and communications technology when compared with 2013.

The PC’s focus on mobile apps and technology is nothing new, but it is definitely an area that warrants continued oversight. In November 2012 the PC issued an information leaflet titled Personal Data Privacy Protection: What Mobile App Developers and their Client should Know, which was then followed by a Best Practice Guide on Mobile App Development issued in November 2014. The PC has also carried out investigations into mobile apps, the most well-known of which was in relation to the mobile app “Do No Evil,” which was found to infringe
the PDPO (discussed below). Continuing this focus, in January 2015 the PC launched a new privacy awareness campaign targeted at mobile app developers.

**PRIVACY MANAGEMENT PROGRAM**

The PC has encouraged organizations to embrace personal data protection as part of their corporate governance responsibilities, rather than merely treating it as a legal compliance issue. In February 2014, the PC published the Privacy Management Programme: A Best Practice Guide, which the government and 25 companies pledged to implement.

The PC considered the Privacy Management Program to be an interim substitute for the Data User Returns Scheme (the DURS). The DURS provisions enable the PC to specify certain categories of data users that must periodically provide returns to the PC, setting out prescribed information (e.g., the type of personal data held, the purposes of collection, etc.). However, the DURS has never been activated, as no such categories of data users have ever been specified by the PC.

**FOCUS ON THE BANKING INDUSTRY**

The Report highlights that the majority of private-sector complaints were made against organizations in the banking and finance industry, which was actually one of the first classes of data users that would have been obligated to file data user returns with the PC under the DURS. Although the plans for the introduction of the DURS were shelved in favor of the less-prescriptive Privacy Management Program, the guidance note issued by the PC in the last quarter of 2014 shows that the finance industry continues to be a prime industry of focus.

In 2014, the PC, the Hong Kong Monetary Authority (the HKMA) and the Securities and Futures Commission (the SFC) were particularly concerned with threats posed to banks by cybersecurity issues. In January and November 2014, respectively, the SFC issued a Circular to all Licensed Corporations on Internet Trading, Reducing Internet Hacking Risks followed by a Circular to all Licensed Corporations on Internet Trading Information Security Management and System Adequacy (the SFC Circulars). The SFC Circulars reminded licensed corporations that they must comply with Chapter 18 and Schedule 7 of the SFC Code of Conduct (which relate to obligations for ensuring the integrity and security of the company’s electronic trading system), and also made specific suggestions on security control techniques and procedures (e.g., secure coding, login controls and firewalls). The SFC Circulars also highlighted the major design and control deficiencies discovered by the SFC following its review of selected licensed organizations. These major deficiencies included the absence of any formal IT management polices or procedures for disaster recovery, monitoring of suspicious websites and the absence of independent or qualified IT and security risk management functions.

On October 14, 2014, the HKMA also issued a Circular on Customer Data Protection (the HKMA Circular), which focuses on the methods of control to help banks prevent and detect loss or leakage of customer data and procedures for addressing and reporting such incidents. The HKMA expects all authorized institutions to complete a critical review of the adequacy and effectiveness of their existing controls and procedures by the first quarter of 2015.

**THE YEAR AHEAD**

The PC has stated that for 2015, the areas it will specifically focus on shall include the following:

- The use of mobile apps and their implications on personal data privacy protection;
- Continuing to assist organizations in administering the Privacy Management Programs;
The protection of personal data contained in public registers maintained by the government;

A survey on the public’s perception of the PC and various topical privacy issues; and

Assisting the Bills Committee in the deliberations of the Electronic Health Record Sharing System Bill.

Several of these areas have already received attention from the PC. In August 2013, for example, the PC published a report regarding the mobile app “Do No Evil,” which allows public access to a database of millions of records of litigation and bankruptcy cases that the app maker compiled. The PC found that the app was in serious breach of the PDPO and issued an enforcement notice against the developer. The PC also issued Guidance on Use of Personal Data Obtained from the Public Domain.

Interestingly, the PC has not identified the introduction of Section 33 (restrictions on the cross-border transfer of personal data) in its list of areas that it will specifically focus on for 2015. Another notable omission by the PC is any reference to the introduction of a binding corporate rules (BCR) regime like they have in Europe.

TAKEAWAYS

The PC’s proactive approach is expected to continue throughout 2015. Organizations should likewise take a proactive approach to data privacy compliance. Waiting for a problem to arise may be too late, and may result in an enforcement notice, fines, imprisonment of individuals and reputational damage to the company.

For more information about this topic, please contact any of the following lawyers.

Marcus A. Christian
+1 202 263 3731
mchristian@mayerbrown.com

Rebecca S. Eisner
+1 312 701 8577
reisner@mayerbrown.com

Daniel Gallagher
+44 20 3130 3537
dgallagher@mayerbrown.com

Gabriela Kennedy
+852 2843 2380
gabriela.kennedy@mayerbrownjsm.com

Karen H. F. Lee
+852 2843 4452
karen.hf.lee@mayerbrownjsm.com

Stephen Lilley
+1 202 263 3865
slilley@mayerbrown.com

Mark A. Prinsley
+44 20 3130 3900
mprinsley@mayerbrown.com

Lei Shen
+1 312 701 8852
lshen@mayerbrown.com

Evan M. Wooten
+1 213 621 9450
ewooten@mayerbrown.com

Oliver Yaros
+44 20 3130 3698
oyaros@mayerbrown.com

Mayer Brown is a global legal services organization advising many of the world’s largest companies, including a significant portion of the Fortune 100, FTSE 100, DAX and Hang Seng Index companies and more than half of the world’s largest banks. Our legal services include banking and finance; corporate and securities; litigation and dispute resolution; antitrust and competition; US Supreme Court and appellate matters; employment and benefits; environmental; financial services regulatory & enforcement; government and global trade; intellectual property; real estate; tax; restructuring, bankruptcy and insolvency; and wealth management.

Please visit our web site for comprehensive contact information for all Mayer Brown offices. www.mayerbrown.com

Any advice expressed herein as to tax matters was neither written nor intended by Mayer Brown LLP to be used and cannot be used by any taxpayer for the purpose of avoiding tax penalties that may be imposed under US tax law. If any person uses or refers to any such tax advice in promoting, marketing or recommending a partnership or other entity, investment plan or arrangement to any taxpayer, then: (i) the advice was written to support the promotion or marketing (by a person other than Mayer Brown LLP) of that transaction or matter; and (ii) such taxpayer should seek advice based on the taxpayer’s particular circumstances from an independent tax advisor.