Locke Lord LLP

PRIVACY & CYBERSECURITY NEWSLETTER

INTERNATIONAL EDITION

NOVEMBER 2015

NOTE FROM THE EDITOR: Welcome to our November 2015 newsletter. Privacy, data protection, and cyber security continue to evolve rapidly. In recent weeks, we have seen the U.S.-EU Safe Harbor invalidated, the concept of "personal information" in the U.S. continue to evolve and expand, influential regulator movements in multiple sectors in the UK and abroad, and ongoing efforts in the public and the private sectors to develop cybersecurity standards. Virtual (cloud) and traditional IT, mobile computing, the volume and contextual uses of data, and the proliferation of Internet-connected devices continue to outgrow legal frameworks and to outpace the ability of companies to fully assess and address the associated risks. Nonetheless, cybersecurity risk management has found its way into corporate governance, and widespread attention is being given to fundamental information security practices and respect for privacy laws.

IN THIS ISSUE

Locke Lord LLP

Locke Lord's Privacy & Cybersecurity Newsletter provides topical snapshots of recent developments in the fast-changing world of privacy, data protection, and cyber risk management. For further information on any of the subjects covered in the newsletter, please contact one of the members of our privacy and cybersecurity team.

OUR AUTHORS:

Natasha Ahmed
Associate
London
+44 (0) 20 7861 9048
nahmed@lockelord.com

Theodore P. Augustinos
Partner
Hartford
860-541-7710
ted.augustinos@lockelord.com

Karen L. Booth
Associate
Hartford
860-541-7714
karen.booth@lockelord.com

Wing L. Cheung
Partner
Hong Kong
+852 3465 0688
wcheung@lockelord.com

Bart W. Huffman
Partner
Austin
512-305-4746
bhuffman@lockelord.com

Sean Kilian
Associate
Dallas
214-740-8560
skilian@lockelord.com

John Kloecker
Of Counsel
Chicago
312-443-0235
jkloecker@lockelord.com

Molly McGinnis Stine
Partner
Chicago
312-443-0327
mmstine@lockelord.com

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

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

Thomas J. Smedinghoff
Of Counsel
Chicago
312-201-2021
tom.smedinghoff@lockelord.com

Philippa Townley
Associate
London
+44 (0) 20 7861 9041
ptownley@lockelord.com

Tammy Ward Woffenden
Partner
Austin
512-305-4776
twoffenden@lockelord.com

Vita Zeltser
Senior Counsel
Atlanta
404-870-4666
vzeltser@lockelord.com

Yasemin Yanar
Associate | Gunalcin Law Firm
Istanbul
yasemin.yanar@gunalcin.av.tr

California Amends Breach Notification Law: Unique New Refinements and Requirements

The California legislature has again amended the state's breach notification statutes to impose new and unique requirements and refinements, adding further complexity to the patchwork of breach notification requirements. Through three bills described below, California has expanded the definition of "personal information," clarified the meaning of "encryption" for purposes of the notification safe harbor, and specified formatting requirements for notices to affected individuals. The amendments, which extend to companies (Cal. Civ. Code § 1798.82) as well as government agencies (Cal. Civ. Code § 1798.29), will take effect January 1, 2016.

Continuing Expansion of "Personal Information"

Senate Bill 34 expands the definition of "personal information" triggering breach notification requirements to include "[i]nformation or data collected through the use or operation of an automated license plate recognition system." This addition, unique among other states' definitions of "personal information" in breach notification statutes, is likely in recognition of ever-increasing collection of information about driver practices, which can reveal significant amounts of historical location information. It remains to be seen whether other states will follow California's lead as a number of states have done since California expanded the definition of "personal information" to include online account credentials in 2013, as we reported here.

Senate Bill 34 also requires reasonable security procedures and practices with respect to automated license plate recognition ("APLR") information, and implementation of a usage and privacy policy satisfying specific requirements with respect to such data. Further, Senate Bill 34 provides for a civil cause of action with respect to violations of such requirements.

Refinement of Encryption Safe Harbor

In what appears to be a continuing effort to encourage a sufficient level of encryption of personal information, and to narrow applicability of California's existing encryption safe harbor to those encryption methodologies generally accepted in the field of information security (a breach of encrypted data does not currently trigger a notification obligation under California law), Assembly Bill 964 provides a definition of "encryption," as circumstances where information is rendered "unusable, unreadable, or indecipherable to an unauthorized person through a security technology or methodology generally accepted in the field of information security."

Specific Individual Notice Formatting Requirements and Model Form

Senate Bill 570 imposes new, specific requirements for the form of breach notification letters issued to affected individuals, including a requirement that such notifications be titled "Notice of Data Breach"; use no smaller than 10-point font; and include the following headings for existing required disclosures: "What Happened," "What Information Was Involved," "What We Are Doing," "What You Can Do," and "For More Information." Senate Bill 570 also provides a model form of breach notification, use of which shall be deemed to be compliant with the new specific formatting requirements. The model form appears intended to provide individuals affected by a breach with a standardized presentation of information so that they can more easily determine what course of action to take following a breach.

Entities experiencing a multi-state breach impacting California residents will likely turn to California's form to fulfill the requirements of the various states' breach notification statutes, subject to the other states' specific content requirements. Potential discord may arise if other states follow suit, unless adopt they model forms that are consistent with that provided in Senate Bill 570.

In addition, Senate Bill 570 specifies requirements for "conspicuous" website notice, where substitute notice is either permitted (over 500,000 individuals are to be notified and/or cost of notice exceeds $250,000) or required (insufficient contact information). Effective January 1, 2016 such website notice must be posted for a minimum of 30 days and satisfy specific format requirements designed to call attention to the notice.

NAIC Cybersecurity Bill of Rights: The Awkward New Guest at the Data Breach Law Party

On October 14, 2015, the NAIC's Cybersecurity (EX) Task Force adopted a Cybersecurity Bill of Rights, an aspirational, well-intended document outlining the rights insurance consumers should (or could? or might? this point remains uncertain) expect with regard to their personal information in the hands of insurance companies, insurance agents, and any of their vendors. The document, now in queue for a vote by the NAIC Executive Committee, has not enjoyed a warm reception among industry groups and data privacy lawyers for a number of reasons. Concerns include the Bill's divergence from prevailing laws and regulations on important issues, and the resulting uncertainties, which could raise the cost and risk of compliance, and thereby the cost of cyber insurance coverage increasingly sought by insurance companies, agents, and their vendors to defray their exposure as a result of a data breach. As the Bill purports to bestow upon consumers of insurance products new rights and entitlements in the event of a data breach, it overlaps and creates potential inconsistencies with the data breach laws adopted by 47 of the 50 states (plus Washington DC, Puerto Rico, and other U.S. jurisdictions).

If adopted by the NAIC, the Bill is intended to be melded into existing related NAIC model laws with the expectation that those amended provisions would then be picked up by various state legislatures or state departments of insurance to amend relevant portions of their respective state insurance codes or regulations.

This Bill joins a very crowded gathering of existing and proposed measures at nearly every level of government and industry, seeking to do something – anything – about the mushrooming problem of sensitive personal information leaking (or being siphoned) seemingly uncontrollably from the electronic coffers of entities of every stripe, or simply being lost, misplaced, or misdirected by those entities.

Unfortunately, this Bill does not fit in well with the crowd it seeks to join. In enumerating six general "rights" of an insurance consumer, the Bill goes both too far and not far enough. The wording of the "rights" lacks sufficient surgical precision in defining the types of incidents that should fall within the scope of the Bill, and does not account for the practical (and in some cases, legal) realities of a data breach incident response. As a result, the Bill overburdens insurance companies and producers, while not adding meaningfully to the protection of consumers. A few illustrative examples are discussed below.

The Bill requires that a consumer receive a notice from the insurance company, agent, or any down-stream business "if an unauthorized person has (or it seems likely they have) seen, stolen, or used your personal information." (Right #4.) Unlike most existing breach notification requirements, the Bill does not contemplate exceptions to this requirement for situations where there is not a reasonable likelihood of harm to the consumer. Without such a "likelihood of harm" exception, consumers could be notified of incidents that would not likely harm them and so they would be confused and alarmed unnecessarily, and for no benefit. Most commentators,

including regulatory and enforcement agencies, have recognized the dangers of over-notification, including a desensitization that can numb notice recipients to the risks presented by potentially more harmful incidents. Likewise, the insurance company, agent, or down-stream business would be subjected to substantial unnecessary expenses, liability, and reputational risk for a no-harm, no-foul incident. Creating a mandatory notice requirement simply where an unauthorized person seems likely to have seen personal information is a substantial expansion of what constitutes a data breach under most existing legal regimes governing data breach notices without improving the protection of consumers.

There is a further requirement in the Bill that the consumer data breach notice letter is sent "never more than 60 days after a data breach is discovered." The inflexibility built into this requirement ignores, for example, cases where law enforcement or other agencies may be involved, and may request or require delayed notifications while their investigation proceeds.

As another example, consumers affected by a data breach are required under the Bill to receive at least one year of identity theft protection paid for by the insurance company or agent involved in the breach. (Right #5.) This blanket requirement does not account for the many types of breaches where identity theft protection would be of no value to the consumer. For example, while entities suffering a breach involving credit card data or a breach where there is no likelihood of harm sometimes voluntarily offer identity theft protection to potentially affected individuals, such protection is not required under most existing laws and regulations. Nevertheless, the Bill would create an expectation of entitlement that increases costs and exposures, without a corresponding benefit to the consumer.

Certainly, this well-intended Bill is a step in the right direction in trying to bring consistency and uniformity within the insurance industry on the issue of cybersecurity and data protection, but there is work yet to be done to achieve effective consumer protection in the face of the realities of cyber threats and garden variety data loss being experienced by companies in the insurance industry with increasing regularity. We continue to monitor the developments on this front.

U.S.-EU Safe Harbor Scheme Declared Invalid

The Court of Justice of the European Union (the "CJEU"), Europe's highest court, declared last month that the U.S.-EU Safe Harbor Scheme is invalid. The CJEU also declared that national supervisory authorities are free to challenge findings of the European Commission (the "Commission") that a third country ensures an adequate level of protection for personal data transferred to that country. On 16 October 2015, the Article 29 Working Party issued a statement in which it confirms that "transfers that are still taking place under the Safe Harbor decision after the CJEU judgment are unlawful" and urges businesses to "reflect on the eventual risks they take when transferring data and [to] consider putting place any legal and technical solutions in a timely manner to mitigate those risks."

The Article 29 Working Party has advised that whilst it continues to analyse the impact of the CJEU judgment on the alternative mechanisms for the transfer of personal data outside the EEA, the data protection authorities consider that Standard Contractual Clauses and Binding Corporate Rules can still be used. Ten days later, however, the German federal and state supervisory authorities released a position paper stating that they will no longer approve transfers to the U.S. on the basis of Binding Corporate Rules.

On 6 November 2015, the Commission published a Communication in which it discusses the use of alternative bases for transfers of personal data to the U.S. after the CJEU's decision. The Commission echoes the Article 29 Working Party's position that the Standard Contractual Clauses and Binding Corporate Rules (as authorised by the relevant data protection authorities ("DPAs")) can still be relied on for the transfer of personal data outside the European Economic Area (the "EEA"). The Commission states that data exporters and importers can also rely on other contractual arrangements as approved by the relative DPAs on a case by case basis, and on the derogations listed in Article 26(1) of Directive 95/46/EC (the "Directive"), which include transfers that are necessary for the performance of a contract between the data subject and the data controller, transfers in respect of which the data subject has given their unambiguous consent, and transfers that are necessary or legally required on important public interest ground of to establish, exercise, or defend legal claims.

In the Communication the Commission draws a distinction between reliance upon these alternative bases, as compared with reliance on a finding by the Commission that a third country (i.e. a country outside the EEA) ensures an adequate level of data protection: Where the Commission has made a finding of adequacy in respect of a third country, it can be assumed that the data importer in that third country to which personal data is transferred is under an obligation to comply with an adequate system of data protection legislation, and so the safety of the transferred personal data will be adequately protected. On the other hand, when the personal data is transferred to a third country on the bases of the alternative transfer methods, the data exporters and importers are themselves responsible for ensuring that the transfers comply with the requirements of the Directive. As such, the Commission draws attention to the central role of the DPAs, who "as the main enforcers of the fundamental rights of data subjects . . . are both responsible for and empowered to supervise data transfers from the EU to third countries, in full independence."

During this period of uncertainty it is imperative that businesses currently relying on Safe Harbor for the transfer of personal data to the U.S. take immediate steps to put in place alternative mechanisms to ensure that the transfers are legal. For practical guidance on the immediate or near-term actions that businesses can take in order to minimize their exposure, please see our recently published Quick Study "Safe Harbor Ruling: Company Considerations and Near Term Strategies."

OCR Expected to Strengthen HIPAA Enforcement in 2016

Two recent reports issued by the Office of Inspector General ("OIG") for the U.S. Department of Health and Human Services ("HHS") recommended that HHS's Office for Civil Rights ("OCR") should fully implement a permanent audit program and strengthen its follow-up procedures relating to breaches of Protected Health Information ("PHI"). *See OCR Should Strengthen Its Oversight of Covered Entities' Compliance with the HIPAA Privacy Standards*, OEI-09-10-00510 (2015); *OCR Should Strengthen Its Followup of Breaches of Patient Health Information Reported by Covered Entities*, OEI-09-10-00511 (2015) ("OIG Reports").

The OIG Reports highlight weaknesses identified in OCR's HIPAA oversight and enforcement activities and suggest that OCR's current program is primarily reactive and does not proactively assess possible noncompliance with HIPAA. The OIG noted that OCR's investigation efforts depend on covered entities' self-reporting of breaches as well as responding to complaints, tips, or media reports about breaches. In addition to recommending that OCR move forward with implementation of its permanent audit program, the OIG recommended that OCR improve its ability to search for and track prior breach reports filed by entities in order to identify those that may have systematic problems with HIPAA compliance. The

OIG wants OCR to not only track large breaches but also smaller breaches that could indicate patterns of noncompliance.

In its responses to the OIG Reports, OCR noted that it is committed to ensuring strong privacy protections for individuals' identifiable health information and ensuring that covered entities and their business associates comply with requirements of the Breach Notification Rule. In its September 23, 2015 response to the OIG recommendations (attached to OEI-09-10-00510), OCR stated that it is moving forward with a permanent audit program that would include periodic audits. OCR believes that Phase 2 of this program will be implemented in early 2016. This phase will test the efficacy of a combination of desk reviews of an entity's policies as well as on-site reviews. The phase will target specific areas of noncompliance and will also directly target business associates. Over the next few months, OCR is expected to update audit protocols; refine the pool of potential audit subjects; and implement screening tools to assess size, entity type, and other information about potential audit subjects.

OCR is also updating its electronic document management system and investigations tracking system to enhance its audit program. According to a September 23, 2015 response to the OIG's recommendations (attached to OEI-09-10-00511), OCR now has the capacity to track entities' historical breach reports, including information relating to breaches affecting fewer than 500 individuals, to help OCR identify covered entities' history of compliance. With this capacity, OCR may now become more proactive with enforcement efforts against entities that experience repeated breaches, whether large or small. OCR plans to develop a standardized process that will require all OCR investigators to consistently check for prior breaches submitted by covered entities and their business associates when initiating an investigation.

With OCR's imminent launch of Phase 2 of their HIPAA audit program, both covered entities and business associates should watch for additional outreach and educational resources issued by OCR, including new audit protocols and other compliance guidance, to help prepare for a potential audit. Covered entities and business associates should also review their own internal processes, including conducting routine security risk assessments, reviewing privacy and security policies and procedures, and undergoing HIPAA compliance training.

Which Way is the "Wyndham" Blowing? Cyber Regulation after *FTC vs. Wyndham*

Does the Third Circuit's recent decision in *FTC v. Wyndham Worldwide Corp.* usher in a new era of enforcement by the FTC and other federal agencies regarding cybersecurity practices? Regardless of the answer, it is important to note what this new decision does *not* do. It does not set a judicial standard for adequate cybersecurity practices. And it did not rule on the merits on the FTC's substantive allegations. Instead, the federal appellate court decision opines only on the principle of the FTC's authority to regulate cybersecurity practices under the "unfair practices" prong of its statutory authority – and not the sufficiency of its allegations, a topic that will go back to the district court.

In this case, the FTC sued Wyndham, alleging that the company's conduct in connection with several system intrusions was an "unfair practice" as defined by the FTC and that its privacy policy was deceptive. The district court denied Wyndham's motion to dismiss, and allowed interlocutory appeal of two issues: whether the FTC (1) has authority under Section 5 of the FTC Act to regulate cybersecurity practices, and (2) provided adequate notice of what it considers "unfair" in this area. The Third Circuit affirmed – greenlighting in principle the FTC's authority to police cybersecurity practices, but not opining on the propriety of any particular standard or whether Wyndham violated such a standard.

The appellate court decision validates the FTC's tough stance on the scope of its regulatory authority. This ruling and the reality of ever-increasing cyberattacks and risks will likely embolden agencies at the federal and state levels to take more action. Because cybersecurity has attracted increasing public attention, various agencies will want to be seen as vigilantly protecting personal data and critical business and organizational information and operations.

Agencies have used and will continue to use existing regulations to flex their muscles. New regulations are certain to emerge. Some rules and laws invoked to enforce cybersecurity standards may not even have the word "cyber" in them – as evidenced, for example, by the FTC's reliance on the unfair and deceptive practices language of its statutory authority. In addition, there may be more pressure for consensus about and refinement of baseline standards against which to measure an entity's cybersecurity.

This dynamic underscores the need for a business or organization to stay up to date on both formal and informal agency guidance in order to steer clear of costly enforcement actions. It is important for any business or organization to know what agency or agencies regulate it and be familiar with their pronouncements. This is particularly the case since the nature of an agency's authority and its interest in invoking it can vary. An agency's position or possible stance on cybersecurity can take the form of regulations, informal publications and guidance, press releases about recent settlements and consent decrees, and resources available on agency websites. These sources can provide guidance as to the agency's expectations for data security. Trade associations also provide and serve as resources to help determine what laws and regulations impact a particular industry.

All businesses and organizations have many powerful reasons to identify their assets vulnerable to cyberattack and to bolster their cybersecurity systems and procedures. Beyond its direct holding, this *Wyndham* decision signals the increased role that regulations from multiple stakeholder agencies will undoubtedly play in the data security decisions that businesses and organizations will and must make.

Development of Cybersecurity Information Sharing Standards

As the Obama administration continues to direct attention to cybersecurity, The University of Texas at San Antonio ("UTSA") recently won an $11 million dollar grant to develop standards for so-called "Information Sharing and Analysis Organizations" ("ISAOs"). ISAOs are voluntary organizations that collect cybersecurity threat information and share it among their members, with an eye towards preventing and responding to cybersecurity attacks. They are an extension of the sector-specific concept of Information Sharing and Analysis Centers ("ISACs"), which already exist in the aviation, communications, financial services, health, oil and gas, and other sectors of critical infrastructure. For example, the recently-formed Legal Services ISAO offers threat sharing services to law firms. The state of Virginia has also announced its intention to form the first state-level ISAO.

In February 2015 President Obama issued Executive Order 13691 to encourage the formation of ISAOs, and to open the process for the Department of Homeland Security (DHS) to select an organization to develop standards for ISAOs. How will ISAOs interact with their members, each other, and the government? As the selected organization, UTSA will develop standards for ISAOs' contractual agreements, business processes, operating procedures, technical means, privacy protection, and more. These standards will provide

groups who wish to form an ISAO with a model and best practices to follow. Additionally, ISAOs will be able to self-certify to these standards, allowing organizations who wish to join an ISAO the ability to assess its capabilities and trustworthiness.

The standards development process will be open to review and comment from both public and private stakeholders. In July 2015 PricewaterhouseCoopers ("PwC") published a study that offers a preview of the issues that stakeholders will likely want the standards to address. PwC identifies six key issues that can be summarized as follows: (1) recognition of the need to share information, (2) trust among membership, (3) flexible governance, (4) timely and valid intelligence, (5) clearly-defined operational and technical processes, and (6) addressing, where possible, concerns that sharing information can create legal liability. (Notably, although liability concerns are not directly addressable through ISAO standards, they should be kept in mind because they are likely to remain a significant barrier to participation.)

It has been said that sharing accurate and timely cybersecurity threat information is a "necessity, rather than a 'nice to have.'" UTSA's work in developing standards will be very important to the use of ISAOs as a vehicle to help fill that need.

Opt-in System Introduced in Turkey for Commercial Electronic Communications in E-commerce Law

Turkey's solid and rapidly expanding e-commerce market volume reached 18.9 billion Turkish Liras as of the end of 2014. The Turkish e-commerce sector accounts for 1.6% of the country's overall retail sector. Even though this number is well below the 4.5% average of emerging countries, the steady growth percentages over the years have proven the potential in the market.

According to the data provided by TÜSİAD (Turkish Industry & Business Association) and TÜBİSAD (Turkish Informatics Industry Association) the market volume growth average between the years 2008 and 2012 was 35.5%, and this promising growth was maintained in 2013 and 2014 despite the slower economy. However, the need for regulation in the sector was overlooked by the authorities until very recently. The first sector-specific piece of regulation, the Law on Regulation of Electronic Commerce ("E-commerce Law"), was prepared in parallel with the EU Directive on E-Commerce (numbered 2000/31/EC). It came into force on May 1, 2015.

The E-commerce Law regulates the general rules and principles of the relationship between service providers and customers in e-commerce platforms. It also includes an obscure clause on protection of personal data in the sector, pursuant to which service providers are responsible for the protection of the retained personal data and the data cannot be shared by third parties without the prior consent of the data subject.

Significantly, the E-commerce Law also introduced an opt-in permission system in Turkey with respect to unsolicited electronic communications for direct marketing purposes. Before this law, such unsolicited electronic communications were only loosely regulated in Turkey – they were permitted provided that recipients were granted an easy and free-of-charge opportunity to opt out at the time of first communication. When considered in conjunction with the absence of a legislative framework in Turkey regarding the protection of personal data, personal information of the data subjects was easily accessed and regularly used without reasonable limitations. In this environment, commercial use of electronic communication as a means of direct advertising had become almost unsettling. Because of the wide range of advertising and solicitation topics, the discomfort experienced by consumers was not limited to the e-commerce sector, as would be expected.

Now, the Regulation on Commercial Communication and Commercial Electronic Messages ("Commercial Communication Regulation") has been published, and it came into effect on July 15, 2015. The Commercial Communication Regulation is prepared based on the E-commerce Law in order to eliminate the uncertainties of the law and shed some light on the implementation.

Under the new set of rules, any kind of commercial electronic communication – including by means of automated calling machines, telefaxes, e-mails, or text messages to the recipients – is banned unless prior consent is received. In addition, recipients that consented to communication must be permitted to opt out at any time and without specifying any reasons. Further key points that should be taken into consideration are as follows:

- The opt-in permission system will not apply to B2B relationships; however, businesses are permitted to use an opt-out option at any time.
- Consent means the recipient's explicit consent. Silence of the recipient cannot be interpreted as consent.
- There are no formal requirements for obtaining the prior consent of the recipient. Such consent can be obtained in writing or by using any form of electronic communication. However, if the consent is obtained in writing it must bear the signature of the recipient and if it is obtained through electronic communication then it should include a declaration of positive intent.
- Consent cannot be actively requested by sending an electronic mail or text message to the recipient or deemed obtained through disclaimers and/or general terms and conditions.
- An opt-out option must be specified in each electronic communication with the recipient.

Recipients can resort to the complaints procedure in case they are faced with unlawful electronic communication and failure to comply with the new law. Violations of the E-commerce Law (and the Commercial Communication Regulation) are punishable by administrative fines.

Weltimmo v Hungarian DPA: Landmark Verdict on the Meaning of "Established"

In the case of Weltimmo s.r.o. v Nemzeti Adatvédelmi és Információszabadság Hatóság, the Court of Justice of the European Union ("CJEU") handed down a landmark judgment in October 2015 on data protection legislation, tackling the issue of jurisdiction when a company is headquartered in one EU country and operates its business in another. The ruling has extended the meaning of "established" as to a company under EU Directive 95/46/EC to include "real and effective activity" through stable arrangements. The decision is likely to have important implications for companies operating across multiple EU countries.

The key facts of the case surround Weltimmo, a company registered in Slovakia, which runs a property advertising website concerning Hungarian properties and processes the personal data of the advertisers. When the fees for this service were not paid by many advertisers, Weltimmo forwarded the personal data of the advertisers to debt collection agencies. After receiving complaints from these advertisers, the Hungarian Data Protection Authority ("NAIH") fined Weltimmo HUF 10 million (approximately €32,000) for breaching Hungarian law transposing EU Directive 95/46/EC.

Weltimmo appealed the fine before the domestic courts in Hungary, claiming that the NAIH was not competent, under Article 4 of Directive 95/46/EC, to apply the Hungarian Data Protection Law to a company established in Slovakia, a different Member

State. The Hungarian Supreme Court referred the case to the CJEU, who ruled in the NAIH's favour.

This ruling is pivotal as it allows data protection legislation of a Member State to be applied to a foreign company that has representatives in that country and operates a service in the native language of that country, despite being headquartered in a different country.

Going forward this decision will impact multi-jurisdictional companies who have chosen to headquarter their business in a particular European country (such as Facebook has done in Ireland) with the understanding that they would only be subject to the data protection laws of that country. Now these companies will also be answerable to the authorities of other Member States in which they operate a "real and effective activity" and are accordingly deemed to have an "establishment" in that territory.

SEC Releases Guidance on Examination of Broker-Dealer and Investment Advisor Information Security Practices; NYSE Releases Cybersecurity Guide

The Security and Exchange Commission's Office of Compliance Inspections and Examinations (the "OCIE") recently announced its 2015 Cybersecurity Examination Initiative, which describes the focus of the OCIE's examination of cybersecurity practices within the securities industry and "encourage[s] registered broker-dealers and investment advisers to reflect upon their own practices, policies, and procedures with respect to cybersecurity."

The Cybersecurity Examination Initiative provides guidance as to the key topics that the OCIE will evaluate in the course of its examinations, as follows: governance and risk management (general information security practices, enterprise efforts to address information security, role of information security leadership), access rights and controls (what personnel have access to what information), data loss prevention (adequacy of efforts to prevent unauthorized access or misuse), vendor management (diligence in selection, contingency, and change management plans), training (employees and other personnel having access to information), and incident response (handling of past incident and plan to handle future incidents). The announcement also provides a helpful checklist of documents that would likely be requested in connection with a cybersecurity review.

Just a week after the Cybersecurity Examination Initiative announcement, the SEC instituted a settled administrative proceeding (*In re R.T. Jones Capital Equities Mgmt.*, No. 3-16827 (SEC Sep. 22, 2015)) ordering an investment advisor to cease and desist insufficient information security practices in the wake of an information security breach. The SEC's pursuit of a proceeding against *R.T. Jones* underscores the SEC's interest in this topic and provides additional guidance as to what the SEC may look for with respect to information security, including, in R.T. Jones's case, alleged failures to implement appropriate written policies, employ a firewall to protect customer information, encrypt customer information, and establish procedures to respond to a security incident. The SEC's order found that R.T. Jones violated Rule 30(a) of Regulation S-P under the Securities Act of 1933. Presumably because R.T. Jones had actually acted with a fair amount of diligence in handling the security incident, and there was no indication of financial harm, the matter was settled with a fairly small penalty of $75,000.

Separately, in a more generally-applicable context, the SEC recently released guidance titled "Navigating the Digital Age – The Definitive Cybersecurity Guide for Directors and Officers" (the "Cybersecurity Guide," available here), noting that "No issue today has created more concern within corporate C-suites and boardrooms than cybersecurity risk." The Cybersecurity Guide provides nearly 300 pages of guidance and materials for directors and officers seeking to understand how to improve their companies' cybersecurity practices, drawing on the expertise of an impressive array of industry players. At the end of the day, however, this guide is just another example of regulators' and the public's expectation that companies will give cyber risk their full attention and address it commensurate with other risks to company assets and operations. The risks of digital data and digital systems are pervasive.

Responsibly assessing and addressing cyber risks is vital to protecting ongoing business operations and digital assets, and is an accepted requirement in order to avoid significant liabilities for misuse or inadequate security of legally protected data. Matters of such importance cannot be ignored or simply delegated to a company's information technology department.

Recent Cases Highlight Importance of Compliance with Hong Kong Privacy Law

The use of personal data in direct marketing without the customer's consent and without fulfilling legal prerequisites has resulted fines issued by the Hong Kong Office of the Privacy Commissioner of Personal Data ("PCPD"). First, the September 9, 2015 conviction of Hong Kong Broadband Network Limited ("HK Broadband") conveyed a strong message to organisations engaging in direct marketing activities that requests from consumers must be complied with and the use of consumers' personal data be respected. HK Broadband was convicted of failure to comply with the requirement from a data subject to cease to use his personal data in direct marketing, in violation of section 35G(3) of the Personal Data (Privacy) Ordinance (the Ordinance). The conviction resulted in a fine of HK $30,000 to HK Broadband, which was the first such fine imposed since the Ordinance was amended to allow for fines of up to HK $30,000 (fines had been limited to HK $10,000; as amended, violations may also give rise to a term of imprisonment of up to 3 years). The action arose when an individual complained that although the complainant had opted out receiving direct marketing from HK Broadband – and HK Broadband had acknowledged that opt-out – an HK Broadband employee nonetheless left a voicemail for the complainant that included promotion of services. This conviction underscores the importance of maintaining comprehensive processes, not just to receive individual's opt-out requests, but also to effectively preclude employee attempts to provide individuals having opted out with direct marketing.

Second, and just five days after the HK Broadband conviction, a storage service provider, Links International Relocation Limited, was fined HK $10,000 for its failure to take specified steps under the Ordinance, including obtaining the customer's consent before using his personal data for the purposes of direct marketing. Under the law, it is an offence for organizations to fail to take specified action to notify individual consumers before using personal data in direct marketing.

The past few months have seen important appointments in the public sector on privacy. Stephen Kai-yi Wong was appointed the new Privacy Commissioner for Personal Data. Mr. Wong succeeded Allan Yam-wang Chiang, who completed his five-year term on 3 August 2015. In addition, on September 25, the government announced the appointment of two new members and the re-appointment of six incumbent members to the Personal Data (Privacy) Advisory Committee for a term of two years with effect from 1 October 2015.

Breaches, Damned Breaches and Their Statistics

Interesting conclusions about data breach costs emerge from two new studies, the 2015 Ponemon Institute's Cost of Cyber Crime Study: Global and the 2015 NetDiligence® Cyber Claims Study. While the phrase alluded to in our title and popularized by Mark Twain might invite general skepticism about statistics, these two well-regarded studies leave no doubt that both data breaches and the average cost of addressing them are on the rise.

The Ponemon report found that the current year's average internalized cost for a cyber crime suffered by a U.S. entity is $15 million, an almost 20% increase over the prior year's average. The costs vary with the size of the breached entity, the number of records, the nature of the infiltration, the type of information affected, and the duration of the breach and the remediation.

The NetDiligence® report found that "hackers were the most frequent cause of loss" and that there was "insider involvement in 32% of the claims submitted" to insurers. The authors also noted that more claims are being submitted to insurers. The average claim payout from an insurer to an insured entity was $674,000, with more than 75% of the amount associated with crisis services (forensics, notification, credit/identity monitoring, legal guidance, and public relations). According to the report, costs for an insured organization are up to 30% lower than for an uninsured entity.

While the Ponemon Institute examined the costs of a breach and not who pays for it, the recent NetDiligence® report focused on the portion of breach costs and exposure covered and paid for by insurers. With different methodologies and purposes, information from the two reports is not intended to match up. However, both reports reveal ever-increasing numbers of cyber incidents, significant costs or potential exposure, and confirmation that the scope and effects of breaches can be wide-ranging.

The Ponemon study examines its field-based research, including interviews of senior-level personnel, of more than 500 organizations in seven countries. The NetDiligence® study is based on information from insurance underwriters about covered claims arising from data breaches and their costs.

UK Information Commissioner's Office Assesses Nuisance Calls Fines

The Information Commissioner's Officer ("ICO") has issued a fine of £200,000, its largest ever penalty for nuisance calls, to Home Energy & Lifestyle Management Ltd. ("HELM"), a green energy company. HELM was investigated after the ICO received hundreds of complaints from consumers concerning automated marketing calls received from HELM.

The ICO discovered that HELM had made over 6 million automated calls as part of its 'free solar panels' marketing campaign without the consent of the consumers, in breach of the Privacy and Electronic Communications (EC Directive) Regulations 2003. ICO's Head of Enforcement Steve Eckersley has been quoted as saying that:

> This company's ignorance of the law is beyond belief. It didn't even bother to find out what the rules were and its badly thought out marketing campaign made people's lives a misery. The monetary penalty is for a significant amount because of the clear failings of the company, and the number of people affected by its deliberate and unlawful campaign. … It should be a warning to other companies to think before they launch into a campaign. Direct marketing campaigns can be run within the law with a little thought and there's plenty of advice available to companies in the ICO's website.

California Enacts Electronic Communication Privacy Statute, Connected Television Privacy Statute

The California legislature recently enacted the California Electronic Communications Privacy Act ("CalECPA") (Senate Bill 178), which provides greater protections against governmental searches for persons' electronic communications. The enactment of CalECPA follows judicial recognition, in the Fourth Amendment context, that modern technologies allow for far greater amounts and more sensitive types of information to be accessed and searched in manners not contemplated in decades past.

Under CalECPA law enforcement agencies will be required – subject to certain exceptions, such as consent of the individual whose communications are at issue, or to prevent death or serious physical injury – to obtain a warrant or court order to compel production of or access to "electronic communications," which is defined broadly as "transfer of signals, writings, images, sounds, data, or intelligence of any nature in whole or in part by a wire, radio, electromagnetic, photoelectric, or photo-optical system" from an electronic communication service provider.

CalECPA also requires warrants and court orders compelling access or disclosure of electronic communications to set out with particularity the information subject to the warrant or order and the relevant time period, and to provide for sealing of any information or materials other than those specified.

Separately, California has enacted an innovative law designed to protect the privacy of information collected through connected televisions. Assembly Bill 1116 prohibits the enablement of voice recognition features within connected television devices without the specific consent of the user of that device. Assembly Bill 1116 also precludes use of information collected through voice recognition features for advertising purposes, and prohibits the compulsion of a manufacturer to build voice recognition features for investigative or law enforcement uses.