


## IN THIS ISSUE

- 2  [Our Authors](#)
- 3  [Retail Tracking Update: Privacy Guidance Following Nomi Technologies](#), by Sean Kilian
- 3  [EU Data Protection Regulation: Final "Triologue" Negotiations are off to a Good Start](#), by Alan Meneghetti, Natasha Ahmed, and Philippa Townley
- 3  [Data Breach Plaintiffs Bag a Win on Standing—Seventh Circuit Finds Against Neiman Marcus](#), by Molly McGinnis Stine, John F. Kloecker, and Charles M. Salmon
- 4  [Significant Amendments to Connecticut and Nevada Breach Notifications and Data Security Laws](#), by Theodore Augustinos and Karen Booth
- 4  [Cyber Risk Governance in the Digital Age](#), by Bart Huffman
- 5  [Identity Management: Push to Adopt Legislation Heats Up](#), by Thomas J. Smedinghoff
- 5  ["Everything Old is New Again" – Issues in Recent Cyber Insurance Litigation](#), by Molly McGinnis Stine and John F. Kloecker
- 6  [At Last! Canadian Breach Notification has \(Almost\) Arrived](#), by Laura L. Ferguson
- 6  [Addressing Public Information Act Concerns in Dealing With Governmental Entities](#), by Brian O'Reilly and Charles Salmon
- 7  [Facebook Wins First Round of European Class Action Privacy Battle](#), by Alan Meneghetti, Natasha Ahmed, and Philippa Townley
- 7  [Shocking? – Insurers Consider Potential Aggregate Risks from a Power Grid Attack](#), by Molly McGinnis Stine and John F. Kloecker
- 8  [Turkey Officially Permits the International Transfer of Personal Data in Telecommunications Sector](#), by Yasemin Yanar
- 8  [Lack of Privacy Awareness Among Children in Hong Kong](#), by Wing L. Cheung

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](mailto:nahmed@lockelord.com)



**Molly McGinnis Stine**  
Partner  
Chicago  
312-443-0327  
[mmstine@lockelord.com](mailto:mmstine@lockelord.com)



**Theodore P. Augustinos**  
Partner  
Hartford  
860-541-7710  
[ted.augustinos@lockelord.com](mailto:ted.augustinos@lockelord.com)



**Alan Meneghetti**  
Partner  
London  
+44 (0) 20 7861 9024  
[ameneghetti@lockelord.com](mailto:ameneghetti@lockelord.com)



**Karen L. Booth**  
Associate  
Hartford  
860-541-7714  
[karen.booth@lockelord.com](mailto:karen.booth@lockelord.com)



**Brian L. O'Reilly**  
Associate  
Austin  
512-305-4853  
[boreilly@lockelord.com](mailto:boreilly@lockelord.com)



**Wing Cheung**  
Partner  
Hong Kong  
+852 3465 0688  
[wcheung@lockelord.com](mailto:wcheung@lockelord.com)



**Charles M. Salmon**  
Associate  
Austin  
512-305-4722  
[csalmon@lockelord.com](mailto:csalmon@lockelord.com)



**Laura Ferguson**  
Associate  
Houston  
713-226-1590  
[lferguson@lockelord.com](mailto:lferguson@lockelord.com)



**Thomas J. Smedinghoff**  
Of Counsel  
Chicago  
312-201-2021  
[tom.smedinghoff@lockelord.com](mailto:tom.smedinghoff@lockelord.com)



**Bart W. Huffman**  
Partner  
Austin  
512-305-4746  
[bhuffman@lockelord.com](mailto:bhuffman@lockelord.com)



**Philippa Townley**  
Trainee Solicitor  
London  
+44 (0) 20 7861 9041  
[ptownley@lockelord.com](mailto:ptownley@lockelord.com)



**Sean Kilian**  
Associate  
Dallas  
214-740-8560  
[skilian@lockelord.com](mailto:skilian@lockelord.com)



**Yasemin Yanar**  
Associate | Gunalcin Law Firm  
Istanbul  
[yasemin.yanar@gunalcin.av.tr](mailto:yasemin.yanar@gunalcin.av.tr)



**John Kloecker**  
Of Counsel  
Chicago  
312-443-0235  
[jkloecker@lockelord.com](mailto:jkloecker@lockelord.com)

## Retail Tracking Update: Privacy Guidance Following Nomi Technologies

There is currently a widespread effort to quantify everything, from steps, to sleep, to [batted ball exit velocity](#). Fifteen years ago, TV host Jeremy Clarkson [tested](#) an innovative new supercar that could quantify your driving habits. At the time, Clarkson glibly quipped that the car's technology allowed you to "compare your drive home from work with the drive home last night." Today, that type of data is regarded as so useful that some companies will give you the technology for free. Of course, if we can quantify driving habits, we can quantify shopping habits. Indeed, by using mobile location analytics, retailers gain valuable insight by comparing a customer's "checkout dwell time" with the checkout dwell time last night. The problem is that customers are even less eager to be quantified than Clarkson was.

Mobile location analytics (MLA) works by placing sensors inside stores and using them to interact with the Wi-Fi and Bluetooth functions of smartphones. The resulting data is de-personalized and aggregated into [analytics](#) that tell retailers about customers' walking paths, high-traffic areas, the duration and frequency of customer visits, the impact of advertising, and more. Retailers can use this data to help optimize their store layouts, place products, and adjust staffing levels. However, a recent FTC action highlighted the privacy concerns that temper widespread MLA use.

In April 2015, the FTC [settled](#) a complaint against Nomi Technologies, Inc., the first of its kind against an MLA provider. The [complaint](#) alleged Nomi's privacy policy misrepresented that consumers would have the ability to opt out of MLA "at any retailer using Nomi's technology." In practice, according to the FTC, consumers were not actually provided a means to opt out in person. Instead, consumers – who had no clear notice that they were being tracked in the first place – could only opt out by visiting Nomi's website.

Not surprisingly, consumers generally disapprove of being tracked. A 2014 [survey](#) showed that 77% of shoppers disapproved of in-store tracking, and [businesses](#) also cite consumer privacy concerns as stalling their adoption of MLA. Currently, the law does not directly protect consumer privacy from the type of data collection used by MLA providers.<sup>1</sup> Instead, protection for both consumers and businesses comes in the form of privacy policies and codes of conduct that provide consumers notice and choice.

The most prevalent [code of conduct](#) is promulgated by the Future of Privacy Forum. In contrast to the *Nomi* case, participating companies only commit to taking "reasonable steps" to ensure there is in-person signage at stores where MLA is used. More concretely, they commit to providing detailed privacy notices on their websites. They also maintain a centralized procedure for consumers to opt out of MLA across all participating companies, although [some groups](#) advocate for an opt-in consent model.

In light of *Nomi* and the uncertain state of MLA privacy law, the best protection for businesses is to adopt a notice and choice privacy policy, and actually follow it in practice.

<sup>1</sup> Aside from invasion of privacy torts, [theories of legal protection](#) include violations of federal wiretap laws, state unfair business practices statutes, and state constitutional rights to privacy. [The Location Privacy Protection Act of 2014](#), which was not enacted, would have criminalized the collection of a device's geolocation information without the consent of its owner. Additionally, in early 2015, The GPS Act was re-introduced in the [House](#) and the [Senate](#). It would criminalize the interception of geolocation information pertaining to another person.

## EU Data Protection Regulation: Final "Trilogue" Negotiations are off to a Good Start

Following the European Parliament's adoption of a [General Approach](#) to the long-awaited draft Data Protection Regulation (DPR) last month, negotiations over the regulation's final form have now commenced. These negotiations between the European Commission, the European Parliament, and the EU Council of Ministers (Council) are known as the "Trilogue process." This represents the final stage of the European negotiations, which means the regulations are on track for being put in place by the end of the year.

The first trilogue meeting took place on June 24, 2015. In a [statement](#) from Czech Commissioner Vera Jourová from the European Commission, it was reported that: "Today we send a strong message to tomorrow's European Council meeting on the Digital Single Market: We are on track to adopt the data protection reform in 2015." The Commissioner provided reassurance that:

[W]e all agree on a number of critical elements that form the foundation of this reform:

- A single set of rules on data protection, valid across the EU. Not 28;
- Reinforced rights to put people back in control over their data;
- The same rules for companies from the EU and from outside the EU; and
- A strong and effective one-stop shop mechanism to simplify the lives of companies and citizens.

Final adoption of the DPR is expected by the end of 2015, which will then come into force in European member states two years later.

## Data Breach Plaintiffs Bag a Win on Standing—Seventh Circuit Finds Against Neiman Marcus

In what is sure to be a widely cited data breach standing [decision](#), the U.S. Court of Appeals for the Seventh Circuit found that increased risk of future harms from a data breach are sufficient to confer standing to sue upon affected individuals and reversed a district court's dismissal of a putative data breach class action for lack of standing. In *Remijas v. Neiman Marcus Group, LLC*, No. 14-3122 (7th Cir. Jul. 20, 2015), the appellate court addressed customer claims arising from the 2013 cyberattack on Neiman Marcus stores, which exposed credit card information of about 350,000 customers. The district court had dismissed the claims for lack of standing, holding that none of the damages alleged by the plaintiffs alleged an injury in fact sufficient to confer Article III standing under *Clapper v. Amnesty Int'l USA*, 133 S. Ct. 1138 (2013).

The Seventh Circuit reversed, noting that in light of the uncontested fact that the breach exposed the plaintiffs' personal data, the risk that the data will be misused by the hackers "is immediate and very real" (citing *In re Adobe Sys., Inc. Privacy Litig.*, No. 13-CV-05226-LHK, 2014 WL 4379916, at \*8 (N.D. Cal. Sept. 4, 2014)). Therefore, the court reasoned, the Neiman Marcus victims "should not have to wait until hackers commit identity theft or credit-card fraud in order to give the class standing, because there is an 'objectively reasonable likelihood' that such an injury will occur." While basing its holding on the increased risk of future injury from identity theft, it is noteworthy that the Seventh Circuit found the other categories of alleged injury to be "more



problematic.” For example, the court expressly declined to hold that alleged “overpayment” – i.e., a premium price that plaintiffs allegedly paid for store goods with expectation of increased security – was an injury in fact sufficient to allege standing.

The *Neiman Marcus* decision is the first federal appellate decision on the issue of standing to assert data breach claims since *Clapper*, and is therefore likely to be widely cited and parsed by both plaintiffs and defendants in such cases. In the short term, the decision may have implications for the dismissal of data breach claims in other cases, such as *Lewert v. P.F. Chang’s China Bistro, Inc.*, No. 14-cv-4787 (N.D. Ill. Dec. 10, 2014), which is currently on appeal to the Seventh Circuit following a district court finding that “an increased risk of identity theft [was] insufficient to confer standing” on plaintiffs. And, in the longer term, the *Neiman Marcus* decision will join the line of prior cases in creating the legal framework for data breach class actions. Although data breach plaintiffs will certainly champion this decision, other cases have found there to be no standing and each new case will need to be considered under its particular facts, allegations, and applicable law.

## Significant Amendments to Nevada and Connecticut Breach Notifications and Data Security Laws

Nevada and Connecticut recently enacted amendments to breach notification and data security requirements that are relatively unique among existing state laws, thus imposing new compliance obligations upon companies doing business in these states, as further described below.

Nevada’s [Assembly Bill No. 179](#) expands the definition of “personal information” subject to Nevada’s data security, encryption, and breach notification requirements to include online account credentials, medical identification number, health insurance identification number, and driver authorization card number.

The Nevada amendment is unique due to its expansion of Nevada’s already significant encryption requirement, which mandates encryption of personal information transferred electronically outside of the business for companies doing business in the state that are not subject to the Payment Card Industry Data Security Standards (“PCI-DSS”). Nevada continues to require companies that accept payment cards to comply with PCI-DSS, including its encryption obligations. As such, companies that do not accept payment cards are subject to different, and in some ways more burdensome, encryption requirements under Nevada law than those that do accept credit and debit cards. For these companies, Nevada now sets a new standard for state encryption requirements of general applicability by mandating encryption of online account credentials, medical identification number, health insurance identification number, and driver authorization card number – personal data not subject to the encryption obligations under Nevada’s existing law or the Massachusetts data security regulations.

Further, in addition to encryption, the Nevada amendment requires “reasonable” data security, as well as breach notification, for this expanded set of personal information. With respect to breach notification, AB 179 follows a trend started by California in 2013, as reported [here](#), in requiring notice for breach of online account credentials. Unlike California, however, Nevada does not allow for an alternative notification format option with respect to breaches of online account credentials. Assembly Bill 179, which took effect July 1, 2015, requires compliance with the new obligations by July 1, 2016.

Connecticut recently amended its breach notification statute pursuant to [Public Act No. 15-142](#), effective October 1, 2015, to require that breached entities offer “appropriate identity theft prevention services and, if applicable, identity theft mitigation services” to affected Connecticut residents whose Social Security numbers were exposed in the breach. The Connecticut amendment requires such offering at no cost for a period of not less than 12 months, although a representative of the Connecticut Attorney General’s Office has publicly indicated that they will continue to expect two years of the identity theft prevention services when Social Security numbers are compromised. Public Act 15-142 further specifies that the breached entity must provide affected individuals with “all information necessary for such resident to enroll in such service or services and shall include information on how such resident can place a credit freeze on such resident’s credit file.”

Connecticut’s amendment follows a similar amendment to California’s breach notification law, reported [here](#), arguably requiring by statute an offering that has been expected, and generally offered, in connection with breaches exposing Social Security numbers or other information particularly at risk for identity theft, for some time. Public Act 15-142 also limits the “without unreasonable delay” standard for notification letters to no more than 90 days after discovery of a breach, unless a shorter time is required by federal law, and imposes new requirements that health insurance companies must maintain a comprehensive information security program, and certify that it complies with such requirement. New information security requirements are also imposed on state contracting agencies and their contractors.

## Cyber Risk Governance in the Digital Age

It has taken a while for companies to realize the value of digital assets, and it is also taking a while for companies to digest the significance of digital risks. In the digital economy, virtually all aspects of business rely to some degree on computer technology, records, networks, and service providers.

In the reality of business today, cyber risk goes to the heart of things and is much more than just the concern of Information Technology or Compliance. As stated in the [Cybersecurity Questions for CEOs](#) document published by the Department of Homeland Security’s United States Computer Emergency Readiness Team (“US-CERT”):

Cyber threats constantly evolve with increasing intensity and complexity. The ability to achieve mission objectives and deliver business functions is increasingly reliant on information systems and the Internet, resulting in increased cyber risks that could cause severe disruption to a company’s business functions or operational supply chain, impact reputation, or compromise sensitive customer data and intellectual property.

Cyber risks cover the full spectrum, including litigation, regulatory, reputational, business interruption, financial, intellectual property, and tangible and intangible asset protection concerns. Moreover, cyber attacks are pervasive and cannot realistically be avoided entirely, so it is as important for companies to be ready as it is for companies to be secure. Indeed, three of the five core threat-addressing functions as set forth in the National Institute of Standards and Technology (“NIST”) [Framework for Improving Critical Infrastructure Cybersecurity](#) – Identify, Protect, Detect, Respond, Recover – are applicable because cyber attacks are expected to occur.

Cyber risk governance involves meaningful engagement of the Board and executive leadership within a framework that facilitates relevant input, strategy formulation, and decision making. Relevant input includes risk identification and assessment, but must also include reports from an appropriate oversight team, which, again, should consist of more than IT. As the US-CERT guidance for CEOs aptly states further:

Cybersecurity is NOT implementing a checklist of requirements; rather it is managing cyber risks to an acceptable level. Managing cybersecurity risk as part of an organization's governance, risk management, and business continuity frameworks provides the strategic framework for managing cybersecurity risk throughout the enterprise.

Primary areas of concern will vary for different organizations. Resource constraints will almost always require that initiatives be prioritized and undertaken in sequence over a period of time. For almost any business, "hot" topics are likely to include business continuity, oversight of service providers, cyber insurance, incident response preparedness, and information sharing.

Although much more remains to be said and done in this area, it seems inevitable that prudent cyber risk governance and management will eventually be taken as seriously as prudent governance and management of fiscal affairs.

## Identity Management: Push to Adopt Legislation Heats Up

Businesses and governments are beginning to recognize the critical importance of online identity management, as [previously reported](#), and as a result we are starting to see a strong push for legislation governing this topic. At least two jurisdictions have enacted significant identity management legislation within the past year, and in July 2015 the United Nations Commission on International Trade Law ("UNCITRAL") approved a project to develop international legal rules to facilitate cross-border online digital identity management.

Key to online identity management is building a legal framework of predictable and enforceable rules designed to ensure proper functioning and trustworthy identity systems. Much like the Visa or MasterCard rules that govern credit card systems, identity system rules will ideally provide a structure to govern the operation of an identity system. They include the technical specifications and operational rules and requirements necessary to make the system functional and trustworthy, and the legal rules that define the rights and legal obligations of the parties and facilitate enforcement where necessary.

The source and content of those rules, and the method of assuring each participant that all of the other participants are following those rules, have provided some of the key challenges for developing economically viable identity systems. Consequently, there has recently been a great deal of legislative activity in this area. But as might be expected, the EU and the U.S. are pursuing somewhat different approaches.

The EU took the lead, beginning with the July 2014 adoption of its [eIDAS Regulation](#), to address federated identity transactions. The EU eIDAS Regulation focuses on identity systems that issue credentials for use in online transactions with public sector bodies. Its key goal is mutual recognition of such credentials in cross-border public sector transactions – *i.e.*, to enable individuals who have an identity credential issued in one EU member state to use that same credential to access online public services in another member state.

The eIDAS Regulation does not require that identity systems be government-operated. Accordingly, credentials issued by an EU member state, under a mandate from the member state, or independently of the member state (e.g., by the private sector) but recognized by the member state, are all acceptable. However, they must also comply with the applicable technical specifications, standards, and procedures regarding assurance levels set out in the implementing act currently being developed. And the Regulation holds member states and identity providers liable for damage caused by a negligent failure to comply with its obligations under the Regulation.

A few months after the EU Regulation was adopted, the state of Virginia became the first U.S. state to adopt rules by enacting its own Electronic Identity Management Act, which can be found [here](#) and [here](#). That legislation, which took effect on July 1, 2015, takes a very different approach. It provides for the creation of a Virginia Identity Management Standards Council, which is tasked with developing Identity Management Standards. And unlike the EU approach, the Virginia statute grants immunity from civil liability to trust framework operators and identity providers that comply with the requirements of those Identity Management Standards. It also provides for the regulation of identity management trustmarks designed to evidence trustworthy systems.

These legislative initiatives represent very divergent approaches. Yet there is a general recognition that identity management is a global issue, and that interoperability across national boundaries is critical. Accordingly, in the spring of 2015 the [American Bar Association Identity Management Legal Task Force](#), and the countries of Austria, Belgium, France, Italy, and Poland (with support from the EU Commission), all submitted proposals to UNCITRAL [recommending](#) that it undertake a project to develop "a basic legal framework covering identity management transactions, including appropriate provisions designed to facilitate international cross-border interoperability." At its July 2015 meeting UNCITRAL agreed to move forward with such a project.

As we saw with its prior work in the area of electronic commerce, UNCITRAL provides an international forum capable of developing a harmonized set of globally accepted rules governing identity management. Such rules can be adapted domestically by countries to promote a universal approach to identity management law, and can also be extended globally (to facilitate cross-border identity transactions) through an international convention.

Given the cross-border nature of e-commerce and associated identity management requirements, and in light of the level of interest in identity management legislation to facilitate the development of a trustworthy identity management ecosystem, it is important that new legislative efforts adopt appropriate approaches and are sufficiently harmonized so that such legislation does not present a barrier to the use of identity in online transactions.

## "Everything Old is New Again" – Issues in Recent Cyber Insurance Litigation

Early days still for coverage litigation about cyber risks – whether under cyber insurance policies or other types of policies. This is not surprising given the relatively short history of cyber risks and even shorter history of cyber-specific policies. Also, a number of claims described as "cyber claims" are paid or privately negotiated between insurers and insureds, resulting in a dearth of published decisions.

But the ball is rolling now. Three recent cases illustrate the evolving issues in cyber-related insurance litigation. In *Universal American Corp. v. Nat'l Union Fire Ins. Co.*, N.Y. Slip Op. 05516, 2015 WL 3885816 (June 25, 2015), New York's highest court affirmed summary judgment for the insurer, National Union, where the alleged losses resulted from authorized entry into the systems of the insured, a health care insurance company. Specifically, health care providers authorized to access the insured's systems submitted fraudulent claims to certain of the insured's health insurance plans. The policy provision at issue covered losses for fraudulent entry to the insured's systems or data, and fraudulent change of a computer program or data. The trial court granted summary judgment to National Union on grounds that the rider applied only to "unauthorized" access to the insured's systems. The New York Court of Appeals affirmed, noting that the rider was not ambiguous and "does not extend as far as providing coverage for fraudulent claims which were entered into the system by authorized users."

In *Travelers Property Cas. Co. v. Federal Recovery Servs., Inc.*, No. 2:14-CV-170 TS (D. Utah May 11, 2015), a Utah federal district court held there was no coverage for and no duty to defend in connection with a lawsuit concerning the refusal of the insured, a payment processing company, to return certain credit card and bank account information to its customer. The court said the insured's cyber errors and omissions policy did not respond because there was no allegation in the complaint against the insured that the insured "withheld the data because of an error, omission, or negligence."

Finally, in a recently filed coverage action regarding third party lawsuits alleging a health care data breach, the insurer sought a declaration that its cyber policy does not respond because the insured breached its warranty to follow the data and privacy protection procedures and risk controls that it identified on its policy application. *Columbia Cas. Co. v. Cottage Health Sys.*, No. 2:15-cv-03432 (C.D. Cal., filed May 7, 2015). The case was dismissed without prejudice on July 17, 2015, based on the insurer's failure to follow the alternative dispute resolution provision in the policy prior to filing its complaint. But the issue of the insured's alleged noncompliance with warranties about its internal cybersecurity processes was not resolved by the dismissal, and the same issue is likely to be raised in other cases.

The three cases highlight three "fault lines" – these and others set the stage for future disputes over the scope of cyber-related insurance coverage: (1) what constitutes fraudulent or unauthorized access to a system for purposes of a cyber-related loss; (2) whether a loss or threatened liability is due to intentional or negligent activity; and (3) to what extent will an insured's risk control and mitigation practices be put on trial when an insurer disputes a cyber-related claim. These and other key coverage issues are familiar in the insurance arena in other contexts. There are or may also be coverage issues unique to this burgeoning new area. Regardless, longstanding insurance principles and prior insurance case law over the years will play a critical role in any litigation and in any published decisions. Given the massive expansion in cyber risk underwriting in recent years, the potential for large and aggregated losses inherent in cyber risks, and the widely varying policy language, it seems inevitable that courts will be forced to address these issues with increasing frequency.

## At Last! Canadian Breach Notification Has (Almost) Arrived

June 18, 2015 marks another step forward for a country with already strong privacy laws, with the long-awaited passage of

the Digital Privacy Act in Canada. [The Digital Privacy Act](#) amends Canada's existing privacy framework, the [Personal Information Protection and Electronic Documents Act](#) ("PIPEDA"). The new law provides for mandatory breach notification and penalties for failure to notify, and revises certain provisions regarding consent.

The breach notification requirements and penalties will not become effective until regulations are issued. Once effective, PIPEDA will require notification when there is a "real risk of significant harm" to the individual. Although breach notification is a welcome change that promises to increase compliance with the existing framework, the Digital Privacy Act's addition of exemptions from the existing consent requirements gives businesses some slack on the protection of information such as business contact information and personal information in the context of business transactions.

On a related note across the sea, a breach notification law was also passed recently in the [Netherlands](#).

## Addressing Public Information Act Concerns in Dealings with the Government

When dealing with a governmental entity it is important to account for the possibility that information shared with that entity may be subject to disclosure under state and/or federal open records acts (e.g., the federal [Freedom of Information Act](#) or state public information acts; collectively "PIAs"). In Texas, for example, the [Public Information Act](#) (the "Texas PIA") provides that information that is written, produced, collected, assembled, or maintained under a law or ordinance or in connection with the transaction of official business by or for a governmental entity is subject to disclosure upon request. PIAs typically provide important exceptions to public disclosure requirements for certain types of information about private entities, including, as may be applicable, competitive or bidding information, trade secrets, and commercial or financial information. Appropriately contracting and dealing with governmental entities will allow for the greatest possible protection of information shared.

Of particular concern in the PIA context is competitors' or adverse parties' ability to obtain information about a private entity that was shared with a public entity subject to a PIA. There are methods to protect against these abuses and certain steps may be taken to reduce the chance that information could be prematurely released.

PIA-related issues may also arise where a private entity is required to provide personal information to a governmental entity, as may the case where a governmental agency examines an entity's books and records in connection with an engagement. As demonstrated in the Texas Attorney General's [Public Information Handbook 2014](#), a number of exemptions may be applied to exclude personal information from PIA requirements (including: Social Security numbers, certain e-mail addresses, information about public officials and peace officers, student information protected by federal statute, payment card information, information held by municipalities about minors, and information concerning "the most intimate aspects of human affairs"). Private entities should carefully limit information they share with public entities to that which is minimally necessary, develop a clear and documented understanding of the exclusions from PIA disclosure requirements applicable to that information, and appropriately designate those types of information when disclosed to governmental entities.



Further, as private entities increasingly implement programs to protect critical information, detailed documentation of their information security measures itself becomes more of a concern. In the wrong hands, such information may well act as a road map for hackers, and that exact type of information may be subject to regulatory examination or disclosure requirements. The sensitivity of such information has been recognized in the context of information relating to governmental entities; for example, the Court of Appeals for the District of Columbia Circuit has [held](#) that information relating to certain Department of Homeland Security practices relating to telecommunications handling issues is not subject to requests under the Freedom of Information Act, and [California's PIA](#) excludes public entities' "information security" records from its disclosure requirements if disclosure might reveal vulnerabilities. The law is not clear cut as to exclusions that may be available for information security materials of private entities, but there is no good reason why such information should not be protected from public disclosure. As with personal information, private entities should carefully limit disclosure of information, document agreements with respect to PIA treatment of that information, and appropriately designate materials to provide for the greatest possible protection from PIA disclosures.

In any case, private companies that wish to protect information must be prepared to act quickly. For example, upon receipt of a request under the Texas PIA, a governmental entity must promptly produce the public information or within 10 days seek an attorney general decision on whether exceptions apply to the requested information. In many instances a government employee will not know whether certain information is confidential and should be protected, unless it is appropriately and clearly marked as such when provided to the governmental entity. Governmental entities may defer to the private entity's designation and refrain from releasing the marked documents without first seeking an attorney general decision.

A sample provision governing PIA-treatment of information is provided as follows:

[PRIVATE ENTITY] acknowledges that all information provided to the [PUBLIC ENTITY] is subject to the [APPLICABLE PIA]. The [PUBLIC ENTITY] cannot guarantee that information received from [PRIVATE ENTITY] will remain confidential if a request for such information is made under the [APPLICABLE PIA]. However, in the event that the [PUBLIC ENTITY] receives a request for any of the information provided by [PRIVATE ENTITY] that is clearly marked confidential or proprietary (or otherwise sensitive and protected), then the [PUBLIC ENTITY] shall notify [PRIVATE ENTITY] in writing in accordance with the requirements of the [APPLICABLE PIA] and will, if requested by [PRIVATE ENTITY], ask for a decision from the Open Records Division of the Office of the Attorney General regarding whether the information may be excepted from disclosure under the [APPLICABLE PIA]. The [PRIVATE ENTITY] bears the burden of demonstrating to the satisfaction of the Attorney General's Office that the information relates to a [TYPE OF INFORMATION EXCLUDED FROM DISCLOSURE REQUIREMENTS] that the disclosure of such would cause substantial competitive harm to the [PRIVATE ENTITY].

It is important to keep an eye on statutory deadlines surrounding a request under the PIA. Attorneys General strictly enforce the deadlines set forth in the statute. Upon notification of a PIA request, quickly securing counsel and preparing an argument asserting the relevant exceptions is critical in order to maintain the confidentiality of your sensitive and protected information.

## Facebook Wins First Round of European Class Action Privacy Battle

Facebook has won its latest class action case in a long-running legal battle involving 25,000 European Facebook users. The class action was led by Austrian law student and privacy campaigner Max Schrems, and alleged that Facebook breached European privacy laws. The Austrian court held that they lacked jurisdiction to hear the case, which sought €500 compensation for each claimant, totalling €12.5m.

Mr. Schrems alleges that Facebook illegally tracked its users' browsing habits via software installed on other web pages, and provided information to U.S. intelligence agencies, amongst other violations.

Facebook has welcomed the rejection with their [statement](#): "This litigation was unnecessary and we're pleased that the court has roundly rejected these claims." Yet the ruling is an isolated victory for the social network, which is facing lawsuits across Europe over the way it handles its users' personal data.

Mr. Schrems is undeterred by this ruling and plans to appeal against the decision. In a [statement](#) by Schrems' lawyer, Wolfram Proksch, he responded: "This finding by the court is really very strange. Unfortunately it seems like the court wanted to forward this hot potato to the higher courts."

The court has thrown the case out on procedural grounds rather than on its material facts, referring it on to a higher tribunal. A further 55,000 people have registered to take part in a second round, if the lawsuit proceeds.

## Shocking? – Insurers Consider Potential Aggregate Risks from a Power Grid Attack

In the fast-developing cyber insurance marketplace, insurers have closely considered the possible risks and have analyzed the potential aggregation of such risks. While not the only topics of interest to insurers, these two are spotlighted in a new report that focuses on the hypothetical prospect of a cyber attack on the U.S. electric power grid and the potential type, volume, and geography of losses across multiple lines of insurance coverage.

The study, co-authored by the University of Cambridge Centre for Risk Studies and Lloyd's, is based on a scenario in which 93 million people in 15 states in the eastern U.S. are without power due to a cyber attack. The study attempts to quantify losses to productivity, trade, and consumption, including projected losses that would follow from such an outage, including interruptions to public safety and transportation systems, water supply, and effects on tourism, social unrest, damage to food and other perishables, and trade and commercial activities as ports and other transportation facilities shut down.

The study estimates that the economic losses to the U.S. economy would range from \$243 billion to over \$1 trillion over a five-year period. The insured losses from such an event would total more than \$70 billion, the study estimates. According to the U.S. Department of Energy, there have been at least 15 suspected cyber attacks on the U.S. electricity grid since 2000.

Major blackouts have ample precedent in the U.S. The August 2003 blackout that affected large areas of the Midwest and Northeast U.S. and parts of Canada (not related to a cyber attack) affected 50 million people, many of whom were without power for two days. Losses from the 2003 blackout are estimated to be in the range of \$7 to \$10 billion.

What is unknown is the extent to which a blackout caused by a cyber attack on the scale contemplated by the University of Cambridge/Lloyd's study, if it occurred now, would affect the increasingly broad scope of automation and online devices that depend on the grid for power, and trigger multiple lines of coverage across a wide range of industries. The study notes that there is a "short history of claims experience [for cyber losses] available to calibrate the likelihood of future risk." And while "there have been large individual business losses attributed to cyber attacks there have so far been no examples of catastrophe-level losses from a widespread cyber attack have a severe impact on many companies all at once . . . . The greatest concern for insurers [] is that the risk itself is not constrained by the conventional boundaries of geography, jurisdiction or physical laws." (p. 25.)

The authors are careful to say they are not saying or predicting that such a massive attack will occur. (p. 7.) Instead, they stress that "we believe that it is representative of the type of extreme events that insurers should assess in order to understand potential exposures" (p. 43) and that the report is intended to be "useful and challenging" to the insurance industry. (p. 7.) The recent study has been broadly publicized. It will almost certainly be part of continuing discussion about power grid vulnerability in the public domain, among utilities, and in the government. However, it will also spur further debate and analysis about the aggregation risk to the insurance community, including the cyber insurance marketplace, due to insureds' dependence on the power grid.

The University of Cambridge/Lloyd's study is available [here](#).

## Turkey Officially Permits the International Transfer of Personal Data in Telecommunications Sector

In 2012 Turkey's telecommunications sector regulator, the Information Technologies and Communication Authority ("ICTA"), issued a new regulation on the Processing of Personal Data and Protection of Privacy in the Electronic Communications Sector ("e-Privacy Regulation") which introduced minimum security requirements and limitations for data retention and — most important of all — prohibited the international transfer of personal data. The e-Privacy Regulation was enacted by ICTA based on the authority to regulate the procedures and principles of data protection and data retention in the telecommunications sector, granted to it by Article 51 of the Electronic Communications Act ("ECA").

After a series of amendments and postponements, the e-Privacy Regulation became effective on July 24, 2013, but the effective date of Article 4 prohibiting the international transfer of personal data without any exceptions was postponed until January 1, 2014. Then, in April 2014, only three months after the e-Privacy Regulation became fully effective, the Turkish Constitutional Court ruled that Article 51 of the ECA was in violation of the Turkish

Constitution and therefore was void. The ruling was based on the constitutional principal that fundamental rights and freedoms can only be limited with laws and not with other legal acts with lower status – i.e., that the framework of the procedures and legal principles must first be regulated by act of law. The absence of a framework law on the protection of personal data in Turkey was underlined by the Constitutional Court. The ruling became effective on January 26, 2015, as a result of which Article 51 of the ECA was automatically annulled; however, certain disagreements on the validity of the e-Privacy Regulation remained and, accordingly, the status of the law on the international transfer of personal data was unclear for some time.

The arguments have now been silenced by the Turkish National Assembly when an omnibus bill created a new Article 51 for the ECA on April 15, 2015. Under the new law, Article 51 has been amended in conformity with the Constitutional Court's ruling and the most significant regulations of the e-Privacy Regulation were transferred to Article 51 itself. Unlike the blanket prohibition of the previous (annulled) regulation, the new Article 51 permits the international transfer of personal data, provided that the data subjects' explicit consent is obtained.

## Lack of Privacy Awareness Among Children in Hong Kong

A child's digital footprint is now taking shape from a very young age and children do not have the capacity to engage with the Internet in a safe manner in all circumstances.

On May 19, 2015, the Office of the Privacy Commissioner for Personal Data ("PCPD") [announced](#) the results of a study conducted in October 2014 that reveal a lack of privacy awareness among children in Hong Kong. The PCPD is especially concerned about children's privacy issues related to the use of social networking sites and other online activities. The study highlighted that the lack of awareness among children and their parents or guardians and teachers may pose a serious risk, and that parents, teachers, and schools seldom provide support to children concerning privacy protection.

Not unlike other organizational data users, schools have to comply with the Personal Data (Privacy) Ordinance. Schools need to develop internal codes of practice to ensure that the requirements prescribed by the Ordinance are met. Just as parents teach their children basic safety rules for the physical world, they should also teach their children basic safety rules for the virtual world.

The PCPD has developed a thematic website called "[Youth Privacy Portal](#)" which is a one-stop portal for youngsters to learn about personal data privacy and for teachers to prepare related materials. [Practical tips](#) are available for parents to instill in their children the concept of personal data protection and respect for each other's privacy.

---

Practical Wisdom, Trusted Advice.

**Locke  
Lord**<sup>LLP</sup>

[www.lockelord.com](http://www.lockelord.com)

Atlanta | Austin | Boston | Chicago | Dallas | Hartford | Hong Kong | Houston | Istanbul | London | Los Angeles | Miami | Morristown  
New Orleans | New York | Orange County | Providence | Sacramento | San Francisco | Stamford | Tokyo | Washington DC | West Palm Beach

---

Locke Lord LLP disclaims all liability whatsoever in relation to any materials or information provided. This brochure is provided solely for educational and informational purposes. It is not intended to constitute legal advice or to create an attorney-client relationship. If you wish to secure legal advice specific to your enterprise and circumstances in connection with any of the topics addressed, we encourage you to engage counsel of your choice. If you would like to be removed from our mailing list, please contact us at either [unsubscribe@lockelord.com](mailto:unsubscribe@lockelord.com) or Locke Lord LLP, 111 South Wacker Drive, Chicago, Illinois 60606, Attention: Marketing. If we are not so advised, you will continue to receive brochures. Attorney Advertising (072915).

© 2015 Locke Lord LLP