Locke Lord LLP

PRIVACY & CYBERSECURITY NEWSLETTER

INTERNATIONAL EDITION

FEBRUARY 2015

NOTE FROM THE EDITOR: The recent combination of Locke Lord and Edwards Wildman created a law firm of 1,000 lawyers in 23 cities around the world. Within those ranks, the already strong privacy and cybersecurity practices of the two firms have combined into a practice that offers an impressive breadth and depth of experience within this ever-evolving and increasingly critical area. Our newly combined Privacy & Cybersecurity Practice consists of more than 40 lawyers across the U.S. and in London, Hong Kong, and Istanbul. See page 3 for more information.

IN THIS ISSUE

Locke Lord LLP

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

OUR AUTHORS:

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

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

David L. Anderson
Counsel
Los Angeles
310-860-8710
danderson@lockelord.com

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

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

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

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

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

Robert Courtneidge
Global Head of Cards & Payments
London
+44 (0) 20 7861 9019
rcourtneidge@lockelord.com

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

Ellen Giblin
Counsel
Boston
617-239-0484
ellen.giblin@lockelord.com

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

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

Locke Lord and Edwards Wildman Combination Creates Industry-Leading Privacy & Cybersecurity Practice

The recent combination of Locke Lord and Edwards Wildman created a law firm of 1,000 lawyers in 23 cities around the world. Within those ranks, the already strong privacy and cybersecurity practices of the two firms have combined into a practice group that offers an impressive breadth and depth of experience within this ever-evolving and increasingly critical practice area. We help clients protect and manage personal data as well as proprietary and other information assets, and other cyber risk exposures. We guide them in meeting their legal, regulatory and contractual obligations concerning the collection, use, transmission, storage, and destruction of data and in mitigating cybersecurity risks. We also represent clients in privacy-related litigation, including class action defense, in jurisdictions throughout the U.S., and in regulatory proceedings in the U.S. and UK.

Our newly combined Privacy & Cybersecurity Practice Group consists of more than 40 lawyers across the United States, and in London, Hong Kong, and Istanbul. With a range of backgrounds in insurance, finance, retail, healthcare, energy, intellectual property, and litigation, among others, our team provides advice that takes into account the standards and practices of the industries and legal frameworks in which our clients operate, as well as laws and regulations of countries on a worldwide basis.

Solving the Legal Challenges of Trustworthy Online Identity

In this age of phishing, hacking, identity fraud, and other forms of cybercrime, answering two simple questions – "Who are you?" and "How can you prove it?" – is fast becoming a critical requirement for online business activities.

In fact, this issue of online identity was elevated to a key priority by the White House a few years ago when it released its *National Strategy for Trusted Identities in Cyberspace* ("National Strategy"). With this document, the Administration began the process of tackling the difficult problem of facilitating a trustworthy online identity management capability.

While there are many different approaches to identity management, they all involve three basic processes: (1) one-time identification, (2) issuance of a credential to reflect that identity information, and (3) authentication of that identity information on multiple occasions with multiple different parties.

Driver's licenses provide a familiar offline example. Issued by a state following completion of an identification process, a driver's license is a credential that a wide variety of relying parties can use to verify the identity of an individual. The association of the identity information in the license with an individual presenting himself in person is authenticated by comparing the picture on the license to the physical person. And this single identity credential can be used in situations involving many different relying parties. Common examples include the TSA agent who uses the driver's license to verify the name of a person seeking to enter an airport boarding area, and a bartender who uses it to verify the age of a person ordering a drink.

The vision of the National Strategy is to extend this concept to the digital world so that businesses and government agencies can rely on an identification process performed and identity information provided by any one of several third-party private sector identity providers. This would allow individuals and businesses to use a single digital identity credential of their choosing to conduct online transactions with numerous enterprises, just as an individual might use a driver's license for a variety of different offline transactions.

Achieving this goal requires building identity systems that are secure (*e.g.*, protected against falsification or hacking), where identity credentials are interoperable (so that one credential can be used with numerous relying parties), that address privacy concerns (so that individuals will be in control of their personal information), where participation is voluntary (so it doesn't turn into a national ID card), and that are cost-effective and easy to use. It also requires balancing individual privacy concerns against the need for trustworthy online identity verification mechanisms.

This requires, of course, implementation of appropriate software and communication technologies. But it also requires adherence by all participants (*e.g.*, subjects, identity providers, and relying parties) to a common set of rules, including technical standards, operational requirements and legal rules sometimes referred to as a *trust framework*.

Like Visa payment card rules, a *trust framework* is a master set of contract-based rules that governs the operation of the system and the performance of the parties. It specifies the technical and operational requirements, makes them legally binding on and enforceable against the participants, defines and governs the legal and privacy rights, responsibilities and liabilities of the participants, and clarifies the legal risks parties assume (*e.g.*, warranties, liability for losses, risks to the privacy of their personal data). It may also specify enforcement mechanisms, termination rights and measures of damages, penalties, and other forms of liability.

A foundational issue for any identity system, *trust framework* is protecting the privacy of personal information, since by its nature any form of identity management typically involves the collection (by an identity provider) and disclosure (to a relying party) of some personal information about a subject. This requires ensuring that the information identity providers collect about subjects during the identification process, and disclose to relying parties during the authentication process, is verified, maintained in an accurate form, kept confidential, not shared with third parties, and not otherwise misused or exposed to unauthorized individuals.

The National Strategy views the privacy issue as a key one. It argues that identity *trust frameworks* must offer individuals better means of protecting their privacy by establishing clear rules and guidelines that address not only the circumstances under which participants in an identity system may share information, but also the kinds of information that they may collect and how that information may be used.

The other primary legal concern of importance to the participants in any identity system is determining who will bear the risks associated with faulty identification or authentication, failure of technology, and other problems or failures of performance that might lead to unauthorized access through identity fraud or mistake.

Concerns regarding liability represent a key barrier to private sector adoption of interoperable identity management solutions. The U.S. National Strategy anticipates that liability issues will be best addressed by contractual agreement among the participants, and this is the approach we see with the credit card and electronic

payment system models. At the same time, the National Strategy also recognizes that legislation may be ultimately necessary to address some of those concerns. The EU recently adopted such legislation, and Virginia has recently introduced legislation to do the same.

Trustworthy online identity management is critical to cybersecurity and e-commerce. And solving the privacy and liability issues is key to making it work.

Standing in Data Breach Cases – Still a Moving Target

Where do we stand on standing in data breach cases? It depends on which court you ask. In December 2014, two courts considered whether plaintiffs alleged sufficient injury in their complaints involving well-known data breaches – and reached different results on standing. In a case against Target Corporation (No. 14-md-2522, D. Minn.), the court held that the plaintiffs had alleged a concrete and particularized injury, traceable to Target's conduct, based on allegations of "unlawful charges, restricted or blocked access to bank accounts, inability to pay other bills, and late payment or new card fees," and therefore had standing to sue. In contrast, in a case against P.F. Chang's China Bistro (No. 14-cv-4787, N.D. Ill.), allegations of overpayment for P.F. Chang's services, fraudulent charges to a debit card, inability to accrue reward points, and "increased risk of identity theft" were insufficient to confer standing.

The two recent cases illustrate the types of alleged injuries plaintiffs claim they have suffered from the theft of their personal identifying information. These two cases and other recent decisions demonstrate that there are divisions in the courts on standing issues. When personal information is breached by a hacker targeting a favorite retailer, restaurant, bank, or doctor's office, whether the victim has standing to sue in federal court remains a definite "maybe" depending on the jurisdiction and the nature of any specific out-of-pocket damages allegedly incurred.

Federal Trade Commission Guidance on the Internet of Things

On January 27, 2015, the FTC released its Staff Report on the so-called "Internet of Things" (IoT) – the ability of everyday objects (from refrigerators to wearable devices) to connect to the Internet and send and receive data. In addition to the Staff Report, the FTC released a guidance document entitled "Careful Connections: Building Security in the Internet of Things" ("Guidance").

The Staff Report focuses on the growing nature of the number of IoT devices – approximately 25 billion connected devices in 2015 and up to 50 billion by 2020 – and the many benefits and risks associated with the devices. Highlighted risks include those associated with enabling unauthorized access and misuse of personal information, facilitating or enabling attacks on other systems, and new risks to personal safety.

The Staff Report reiterates the significance of Fair Information Practice Principals of security, data minimization, notice, and choice.

1. SECURITY. The Staff Report encourages "security by design," emphasizing that companies should build security into their devices at the outset. This process includes: (a) conducting a privacy or risk assessment; (b) minimizing the data collected and retained; and (c) testing security before launch. The Staff Report also emphasizes the importance of proper training of staff, retaining vendors with appropriate security practices, using multi-layered security, reasonable access controls, and monitoring and patching products after release.
2. DATA MINIMIZATION. The report also discusses the greater risk associated with collecting large amounts of data and retaining it for long periods of time. The FTC suggests that companies should consider options with respect to how to minimize data, such as not collecting data at all, collecting only the data necessary, collecting less sensitive data, or de-identifying data.
3. NOTICE AND CHOICE. The FTC recognizes that notice and choice can be difficult with connected devices. Echoing recommendations in the FTC's 2012 Privacy Report, the report notes that companies are not generally compelled to provide notice and choice for practices consistent with the context of the transaction or the company's relationship with the consumer. Companies should generally obtain express, informed consumer consent for unexpected collection of volumes or types of data. Regardless of the method, the FTC emphasized that privacy choices should be clear and prominent and not buried in long documents.
4. LEGISLATION. The FTC recommends that Congress enact federal data security legislation to strengthen the FTC's existing data enforcement tools and to provide notification to consumers when there is a security breach. The Staff Report did not recommend that this legislation be limited to the IoT, but rather that it should be technology-agnostic. In the absence of this legislation, the FTC indicates that it will continue to rely on its existing enforcement tools (FTC Act, FCRA, COPPA, etc.) to ensure that IoT companies consider privacy and data security when developing new devices.

The FTC-released Guidance which provides that while there is no "one size fits all" checklist to guarantee the security of connected devices, companies should still take reasonable steps to ensure the security of both the devices and the data collected by the devices. Like the Staff Report, the Guidance emphasizes the importance of "security by design"; but the Guidance also promotes a culture of security, using multi-layered security, and common-sense recommendations such as refraining from shipping IoT devices with default passwords (which become readily known shortly after a product is released).

The Guidance also recommends designing products with authentication in mind and protecting the interface between the product and other devices or services. The Guidance recommends setting the more secure option as the default option on a product rather than setting the default on the least secure option, as this helps ensure protection for inexperienced users.

The Guidance also suggests "just in time" notices to better educate consumers about safe use of the product, with easy access to security settings, and that firms should think through how

updates to the product may be handled over time and planned obsolescence. Lastly, the Guidance recommends that companies stay informed of the latest security threats and vulnerabilities and communicate clearly with customers.

UK Information Commissioner's Office (ICO) Reviews Google's Privacy Policy

The ICO is the UK's independent authority set up to uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals. The ICO has recently ordered Google to sign a formal undertaking to improve the information it provides to individuals about how it collects personal data in the UK.

It is well known that Google acquires vast amounts of personal data, and the ICO has found that the search engine has been too vague in its descriptions as to how it uses personal data gathered from its web services and products. As a result of the ICO's investigation, Google has stated that it will now provide unambiguous and comprehensive information regarding data processing, including an exhaustive list of the types of data processed by Google and the purposes for which data is processed. Google's commitments are consistent with the requirements of the UK Data Protection Act 1998 (DPA).

This undertaking enforced by the ICO marks a significant step forward following a lengthy investigation. Google's commitment to making changes to its privacy policy will improve the information that UK consumers receive when using its online services and products. Overall, the ICO hopes that this decision will highlight to all online organisations the requirement to comply with data protection law. Ensuring that personal data is processed fairly and transparently is a key requirement of the DPA. The ICO hopes that the detailed agreement Google has signed setting out its commitments will encourage other organisations to follow suit.

The ICO has already worked with Google to ensure a significant number of changes to its policy. The search engine must now make the agreed further changes by 30 June 2015 and take additional steps over the next two years. The ICO plans to update its Privacy Notices Code Practice later in 2015 to provide organisations with further guidance about how to provide effective privacy information, particularly in online and mobile environments.

UK Information Commissioner's Office (ICO) Receives Power to Audit National Health Service

The ICO has welcomed a change in legislation which came into effect on 1 February 2015 enabling it to audit National Health Service (NHS) bodies to check for compliance with the UK Data Protection Act 1998. The ICO now has the authority to assess the compliance of a number of bodies within the NHS, including NHS foundation trusts, GP surgeries, NHS Trusts, and Community Healthcare Councils. According to the ICO, the remit of the ICO's new powers will not extend to private companies providing services within public healthcare.

Whilst the ICO has the power to fine organizations that breach data protection laws, its objective has over time become more proactive than reactive: encouraging organizations to solve the problem before a breach occurs is the ICO's end goal.

Previously, the ICO could impose audits only on government departments, and only public authorities, ISPs, and telecommunication companies have been under a legal duty to notify breaches. Now the ICO will be able to audit and review how the NHS handles patients' personal information, and can review related areas including security of data, records management, staff training, and data sharing.

There is no doubt that the NHS holds some of the most sensitive personal information available, and in recent times it has been under scrutiny in relation to the way in which it safeguards the security of that information. Issues with procedures and training have contributed to a number of data security breaches, including, for example, the theft of a laptop from an unlocked store room at the headquarters of NHS Central London's strategic health authority in 2011, which contained details of 8.3 million patients.

The ICO first issued a financial penalty to the NHS of £70,000 in 2012 after personal information was sent to the wrong patient. Since then, the ICO has issued fines totaling £1.3m to organizations within the NHS.

Legislative Initiative: The Rhode Island Identity Theft Protection Act of 2015

President Barack Obama recognized in a speech he gave at the Federal Trade Commission on January 12th that identity theft poses a direct threat to the financial security of Americans.

President Obama acknowledged, "We're introducing new legislation to create a single, strong national standard so Americans know when their information has been stolen or misused. Right now, almost every state has a different law on this, and it's confusing for consumers and it's confusing for companies – and it's costly, too, to have to comply with this patchwork of laws. So under the new standard that we're proposing, companies would have to notify consumers of a breach within 30 days."

During the last decade there has been similar proposed legislation to harmonize the 50 states and the territories within one federal data breach notification law. To date, no such law has passed. According to the FTC's Consumer Sentinel Network Data Book for 2013 (2014), the CSN received over 2 million consumer complaints in 2013, and identity theft complaints accounted for 14% of all complaints. Government documents/benefits fraud (34%) was the most common form of reported identity theft, followed by credit card fraud (17%), phone or utilities fraud (14%), and bank fraud (8%). Other significant categories of identity theft reported by victims were employment-related fraud (6%) and loan fraud (4%).

Rhode Island's legislative leadership took action to protect the personal information of Rhode Island residents. Senator Louis P. DiPalma and Representative Stephen R. Ucci, the sponsors of the Identity Theft Protection Act of 2015 (S0134), noted in a Rhode Island State House Press Release, "Technology has come a considerable distance in the last decade, and it's time for the state's identity theft statute to be brought up to date as well." The release noted the pair introduced the legislation to craft a bill that would better protect citizens from identity theft and govern the steps that businesses and other entities must take to safeguard their systems and prevent the theft of personal information whether in electronic or paper format from their systems.

"Our current identity theft law was a step in the right direction at a time when we didn't have much on the books defining the crime and seeking to prevent it. But in the decade that's passed, new technology has developed, hackers have become more adept, and we've identified some weaknesses in the law that we needed to address. This bill is aimed at giving Rhode Islanders better protection in a rapidly changing world of technology," said Senator DiPalma.

Representative Ucci stated, "Data breaches, unfortunately, are a widespread problem, and we need to learn from the experience of recent years to strengthen and clarify this law so it truly prevents identity theft and so businesses and others storing individuals' information know clearly what their responsibilities are."

The legislation addresses ambiguities in the existing law by repealing it and redrafting it to:

- clarify that municipal agencies are subject to its provisions;
- specify that those whose information was subject to the breach be notified no later than 15 calendar days after its discovery and listing which information must be included in that notice;
- require that the entity notify the Rhode Island Attorney General and major credit reporting agencies immediately, and that the entity must cooperate and share threat information with all federal, state, or municipal law enforcement agencies investigating the breach; and
- define "personal information" protected by the act to include medical information, health insurance information, and email addresses when acquired with their passwords or other access codes.

The most remarkable addition is the new data security requirements. Now any agency or person that stores, collects, processes, maintains, acquires, uses, owns or licenses personal information about a Rhode Island resident shall be required to implement and maintain a risk-based information security program which contains reasonable security procedures and practices appropriate to the size and scope of the organization, the nature of the information, and the purpose for which the information was collected in order to protect the personal information. Many of the safeguarding requirements in the new legislation are similar to the current Massachusetts Data Security Regulations found at 201 CMR 17, especially regarding vendor management. Additionally, the legislation broadens a provision that allows an entity subject to the law to be deemed compliant with notification requirements if the entity maintains its own similar security breach procedures or the entity is already in compliance with similar federal laws.

Currently, each violation under the existing data breach notification law could draw up to a $100 civil penalty, not to exceed a $25,000 total. The legislation increases the civil penalties for violating the chapter. The bill would eliminate the limit on the total fines, and allow each violation to be subject to fines of $100 to $200 per record, if the violation was reckless and up to the higher amount, if the violation is knowing and willful.

The legislation was developed after a workshop on strengthening the law organized in September by the Rhode Island Corporate Cybersecurity Initiative, a part of the Pell Center Cyber Leadership Project, supported by the Verizon Foundation and housed at the Pell Center for International Relations and Public Policy at Salve Regina University in Newport.

New Jersey Imposes Unique Encryption Requirements

Effective August 1, 2015, New Jersey will require health insurance carriers authorized to issue health benefit plans in New Jersey to encrypt personal information that they store electronically. The new law (P.L. 2014, c. 88, codified at N.J. Stat. Ann. §§ 56:8-196 - 56:8-198) is unique relative to existing data security requirements, as follows:

- The new requirement defines "personal information" expansively to include an individual's name and address (without other data), as well as other more sensitive data typically subject to data security requirements.
- The new law applies to such data when residing on desktops and other computer systems designed to allow end users to access computerized information, software, programs or networks, and when transmitted across public networks. In contrast, existing state encryption requirements (such as Massachusetts and Nevada) only require encryption of data residing on mobile or portable devices, data in flight, or data otherwise transferred outside the control of the company.
- The requirement is absolute; unlike most other existing requirements (including HIPAA), it is not subject to risk assessments, reasonableness, or technical feasibility, but rather mandates encryption or "any other method or technology rendering the information unreadable, undecipherable, or otherwise unusable by an unauthorized person" for all companies subject to the law, specifying that mere password protection is not sufficient.

This unique encryption requirement applies to licensed health insurance companies, HMOs, medical service corporations, and other entities licensed to issue health benefit plans in New Jersey. In preparation for the effective date of this new requirement, each such company should review its data security safeguards and protocols for compliance. Given the expansive definition of personal information and the extension of the encryption requirement to all computer systems and programs accessible by end users, many companies will likely need to extend their existing encryption technology to cover additional systems and data.

Particularly given the recent announcement of a high profile breach involving a health plan affecting tens of millions of Americans, this New Jersey legislation may well inspire similar legislative initiatives in other states. Therefore, carriers in all

jurisdictions should monitor legislative and regulatory initiatives imposing similar encryption requirements that may be expected to follow. As the health insurance industry is by no means the only industry threatened by attacks on the privacy and security of personal information, companies in every industry should consider extending the scope of current encryption practices for risk mitigation, and be vigilant in monitoring legislative developments for new encryption requirements that may be inspired by this unique New Jersey requirement.

Current UK Thinking on Cybersecurity

2014 contained a series of high profile data breaches, including the recent Sony breach in relation to the Hollywood film release of The Interview. It is expected that globally 2015 will focus further on fighting privacy and cybersecurity issues.

In the U.S., after a year of significant privacy and information security regulatory enforcement, litigation, and legislative activity at both the federal and state levels, President Obama has recently announced the proposal of new cybersecurity legislation (as further discussed elsewhere in this newsletter). The proposal includes (i) the promotion of cybersecurity information sharing including targeted liability protection, (ii) federal legislation intended to simplify and standardise data breach reporting requirements, and (iii) legislation aimed at protecting student information by prohibiting companies from selling student data for non-educational purposes.

Similarly, in the UK, David Cameron announced on 16 January 2015, new measures to guide UK businesses to combat cybersecurity challenges. The new measures include a revised version of the "10 Steps to Cyber Security" guide on how to stop common cyber-attacks, and improved cybersecurity information and advice for businesses. The UK government's National Cyber Security Programme has been developing a variety of policies and goals to improve the country's strength and resilience. Furthermore, there is ongoing discussion in the EU in respect of a proposal for a Cyber Security Directive concerning measures to ensure a high common level of network and information security across the EU.

Overall, and certainly in the UK, the industry consensus is that businesses should stop worrying primarily about *preventing* intruders getting into their computer networks, but concentrate instead on minimizing the damage they cause *when* they do. Experts believe the answer is to focus efforts on effectively detecting security breaches and then responding as speedily as possible. However, it must be stressed that whilst increased recognition of security at board level within a firm is reassuring, it is important that this information is filtered down to those who manage the business and that internal training programs are devised in order to ensure privacy and cybersecurity are properly deployed.

One important technique to make life harder for hackers is "network segmentation." This involves separating one part of the network from another in such a way that if hackers get on to the network they only get access to the data in that segment and no more. The downside of this method is that it may be inconvenient for employees on a day to day basis and productivity would potentially suffer. Improvements in encryption methods, if integrated with network segmentation, will undoubtedly be valuable for companies because, although they are not insurmountable, together they certainly present a considerable obstacle which will hamper a hacker's progress and could be enough to make them look elsewhere.

NIST, White House Continue Efforts to Enhance Cybersecurity Awareness and Protections

The National Institute of Standards and Technology (NIST) and the White House continue efforts to improve private sector security and increase sharing of information about potential cybersecurity threats. Most recently, the NIST released its Update on Cybersecurity Framework in December of last year, updating NIST's Cybersecurity Framework of February 2014, and the White House released draft legislation that would provide private sector entities with greater protections and resources when sharing threat information.

The NIST Update presents commentary from the private sector concerning use of the Cybersecurity Framework. Comments ranged from the difficulties and uncertainty of using the Framework as a benchmarking tool (and possible regulatory consequences) to a more practical consideration of how NIST may be able to help entities better use the Framework.

Specific concerns were noted regarding:

- the "high-risk area" of authentication solutions;
- streamlining "indicator sharing," including through solutions to overcome legal barriers;
- supply chain assessments;
- the state of the cybersecurity workforce; and
- privacy and civil liberty issues arising in connection with information sharing.

The Update does not attempt to specifically address all of these concerns, and states that no new version of the Framework should be expected at least within the next year. However, the Update does indicate that NIST will continue to support the development of resources to help organizations address their concerns.

The White House has renewed its push for Congress to take action on the significant cybersecurity issues that have become increasingly apparent in the past year. Part of this effort includes draft legislation designed to allow for better information sharing between private entities and the federal government. This draft legislation includes measures to promote and facilitate private-sector sharing of cybersecurity threats with each other through "private information sharing and analysis organizations" (standards for which are to be set by a collection of federal agencies) and also with law enforcement and government agencies. The legislation would include liability protection for information shared with the National Cybersecurity and Communications Integration Center or with private information sharing and analysis organizations.

The White House's proposed legislation (like the Update on Cybersecurity Framework) recognizes the importance of privacy and civil liberties issues relating to information sharing. Federal departments and agencies would be required to develop guidelines for the appropriate limitation, destruction, anonymization and safeguarding of information that could identify specific individuals.

Cybersecurity is Key Initiative for National Association of Insurance Commissioners

Even your grandmother is talking about cybersecurity, so you know it's got to be important. In the world of insurance, the wheels are in motion at the NAIC – the National Association of Insurance Commissioners – to get a better handle on cybersecurity risks. In November 2014, the NAIC formed the Cybersecurity (EX) Task Force to monitor emerging cyber risks and their impact on the insurance industry, determine whether any regulatory action may be required, and generally coordinate issues related to insurance and cybersecurity.

This is the NAIC's key initiative for 2015, and one of their expressed goals is to propose additional guidance to insurance examiners reviewing insurance companies' practices for cybersecurity risks. To that end, the NAIC is considering collecting information from insurers writing cybersecurity coverage to learn more about this new and quickly evolving market. More to come on this from the NAIC later this year, so stay tuned.

Cybersecurity Issues Receiving Attention at Highest Level in the U.S.

The Obama Administration could not be more clear that cybersecurity issues will continue to receive priority attention at the highest levels of government. President Obama emphasized the importance of cybersecurity during his State of the Union address, with special consideration for the need to balance and protect privacy interests. On February 13, 2015, the Administration hosted a Summit on Cybersecurity and Consumer Protection at Stanford University, which featured keynote remarks by and the announcement of a new Executive Order from President Obama, as well as participants including cabinet secretaries and major industry leaders in areas of technology and critical infrastructure.

It was viewed as inevitable that the President would address cybersecurity as a top priority, given a number of recent incidents that have shed light on threats posed to the nation's economy, defense and critical infrastructure. These incidents have included breaches suffered by major retailers, North Korea's believed involvement in a hack against Sony, and direct attacks and theft affecting our most sensitive information (such as a security incident suffered by a major defense contractor). President Obama has remarked that cybersecurity issues are an "urgent and growing danger" and "one of the most serious economic and

national security challenges we face as a nation" where "foreign governments, criminals and hackers probe America's computer networks every single day."

The Summit was a real-time example of the need for public and private participation in the initiative to bolster security and improve resilience to cyber attacks. The impressive panels of leaders spoke about the need to address weaknesses in cyber security, to ensure that private industry would not be left to address these issues alone, to remain cognizant of privacy and civil liberties.

The Executive Order, announced at the Summit, emanates from the agenda for enhanced sharing of threat information. The Executive Order clearly places the Department of Homeland Security in a leadership role (to the relief of a public wary of the National Security Agency) and provides for the use of Information Sharing and Analysis Organizations to facilitate cyber threat information sharing within the private sector.

Balance will be key in the measures advanced and proposed by the Obama Administration (some criticized that the President's proposals might actually harm cybersecurity efforts by criminalizing activities of so-called "white hat" hackers). In addition, as the President acknowledged, the private sector expects some measure of liability protection and associated standards to facilitate government cooperation, and, while the Administration can take executive branch action and can sponsor work on standards, it cannot legislate the boundaries of liability associated with the use and sharing of information. Avivah Litan of Gartner recently posited: "There's no meaningful intelligence sharing because of all the lawyers. There's always the threat of lawsuits."

This should be a monumental year with respect to the government's awareness and emphasis on cybersecurity. The incidents are too vivid to ignore. The Obama Administration clearly recognizes the need to capitalize on the advantages of global connectivity and the new age of information technology while also cooperating with each other and the government to ensure that our concern for safety appropriately parallels our concern for growth. Along the way, we might even get a national data breach law.