












IN THIS ISSUE

- 2  [Our Authors](#)
- 3  [California Attorney General Defines Minimum Requirements for 'Reasonable Cybersecurity,'](#) by Thomas J. Smedinghoff
- 3  [OCR for the Win: Lincare, Inc. HIPAA Enforcement Action,](#) by Laura L. Ferguson
- 3  [A Common Standard for Evaluating Cyber Risk – Insurers Walk the Walk,](#) by Molly McGinnis Stine and John F. Kloecker
- 4  [Testing the Limits – Cyber Coverage Litigation Update,](#) by Molly McGinnis Stine and John F. Kloecker
- 4  [Rhode Island Amends Identity Theft Protection Act,](#) by Theodore P. Augustinos and Karen L. Booth
- 5  [Executive Action: Obama Administration Budgets for Cybersecurity,](#) by Sean Kilian
- 5  [President Obama Signs Cybersecurity Act of 2015 into Law,](#) by Karen L. Booth and Charles M. Salmon
- 6  [Sixth Circuit Rules 10 Weeks of Camera Monitoring from Public Utility Pole Does Not Require a Warrant,](#) by Brian L. O'Reilly and Charles M. Salmon
- 6  [Should Apple Always Have a Key to All iPhone Data? To Some iPhone Data?,](#) by Bart W. Huffman
- 7  [New Safe Harbor Agreement for EU Data Transfer Announced,](#) by Mark E. Schreiber, Alan D. Meneghetti, Natasha Ahmed and Thomas J. Smedinghoff

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



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



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



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



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



Brian L. O'Reilly
Associate
Austin
512-305-4853
boreilly@lockelord.com



Laura L. Ferguson
Associate
Houston
713-226-1590
lferguson@lockelord.com



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



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



Mark E. Schreiber
Partner
Boston
617-239-0585
mark.schreiber@lockelord.com



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



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



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

California Attorney General Defines Minimum Requirements for 'Reasonable Cybersecurity'

California has now weighed in on the definition of "reasonable" security and minimum security requirements for all businesses through the California Attorney General's [2016 Data Breach Report](#).

The Report references the legal obligation to secure information, and adopts the views that "Security is a process," that "Information security laws and regulations generally require a risk management approach," and that "This means organizations must develop, implement, monitor, and regularly update a comprehensive information security program."

More importantly, the Report adopts the Critical Security Controls for Effective Cyber Defense released by the Center for Internet Security (formerly known as the SANS Top 20) as the "minimum standard of care for personal information." According to the Report, "The 20 controls in the Center for Internet Security's Critical Security Controls define a minimum level of information security that all organizations that collect or maintain personal information should meet. The failure to implement all the Controls that apply to an organization's environment constitutes a lack of reasonable security." (Emphasis added.)

Presumably this view will guide their enforcement actions going forward and likely warrants the careful attention of entities seeking to maintain strong information security practices.

OCR for the Win: Lincare, Inc. HIPAA Enforcement Action

For the second time in history, on January 13, 2016, an Administrative Law Judge (ALJ) upheld the imposition of civil money penalties charged against a covered entity by the Office of Civil Rights in the Department of Health and Human Services (OCR) for violations of the Health Insurance Portability and Accountability Act of 1996, as amended (HIPAA). Typically, covered entities cooperate with OCR and enter into a resolution agreement that indicates the covered entities *potentially* violated HIPAA (sometimes with the payment of a resolution amount). However, Lincare refused to settle and took the position that it had not violated HIPAA because the protected health information (PHI) was "stolen" by a former employee. Evidence established that Lincare had a practice of requiring its employees to keep patient information "secured" in their vehicles so that if an office was destroyed, they still had access to the PHI. In this situation, the employee left the PHI in a car to which her husband had the keys – and then left it behind when she moved out of their marital home. The husband informed Lincare and OCR that he had the PHI in his possession. Lincare argued that the husband stole the PHI in an attempt to induce his estranged wife to return to him. The ALJ found that was no defense and stated that "under HIPAA, Respondent [Lincare] was obligated to take reasonable steps to protect its PHI from theft." In the absence of an appeal by Lincare, Lincare now owes civil money penalties of \$239,800 due to its violations of HIPAA.

You can read the ALJ's opinion [here](#) and the OCR press release [here](#).

A Common Standard for Evaluating Cyber Risk – Insurers Walk the Walk

Insurers have struggled to find a common baseline to measure cyber risks. Changes in technology, hacking and other data security risks and the shifting legal landscape concerning liability for data breaches have made the terrain particularly uncertain. Because of the unique and changing nature of cyber risks, current risk models used for pricing and measuring risk aggregation do not provide the level of confidence insurers want and need. To date, most insurers have used internally-developed and proprietary models that rely on insureds' responses to application questions that vary widely, and other data collected and stored in a non-uniform fashion. That variation, added to the continually evolving nature of cyber risks, impairs an insurer's ability to accurately (a) price the risk for insureds and (b) gauge the appropriate level of cyber risk in its overall portfolio – potentially limiting capacity.

On January 19, 2016, two leading modeling firms and the University of Cambridge, with support from a number of insurers and reinsurers, released what is hoped to be the first step in providing a common set of standards to bridge the gap between insureds, whose data security systems and capabilities vary widely, and insurers and other constituents that need a common language to evaluate cyber risks. Risk Management Solutions, Inc. (RMS), AIR Worldwide (a unit of Verisk Analytics) and the University of Cambridge's Centre for Risk Studies have collaborated to create a standardized framework that will enable insurers to track exposures with a uniform set of data elements and practices for maintaining the data. The Cyber Insurance Exposure Data Schema v1.0 released by RMS can be accessed [here](#).

The goals of the RMS schema are to (a) provide a standardized approach to identifying, quantifying and reporting cyber exposure; (b) enable the development of models for cyber risk that will be applicable to multiple users; (c) facilitate risk transfer to reinsurers and other risk partners and risk sharing between insurers; and (d) provide a framework for exposure-related dialogues for risk managers, brokers, consultants and analysts. The schema uses six categories of exposure attributes to structure information: (1) cyber peril codes, (2) geographical jurisdiction, (3) cyber loss coverage categories, (4) business sector, (5) enterprise attributes and (6) cyber risk attributes.

AIR Worldwide also released data standards to create uniform methods for collection, coding, storage and transfer of data – in the form of a cyber exposure SQL (structure query language) database and [preparer's guide](#). AIR's data standard and preparer's guide can be accessed [here](#).

The new standards will likely evolve and mature as have other attempts to categorize and standardize assessments of complex risks. But development of the RMS/AIR standards points the way to a common language to assist underwriters, investors and other constituents in tackling what has to date been an unpredictable and difficult-to-quantify risk.

Testing the Limits – Cyber Coverage Litigation Update

The growing percentage of businesses that purchase cyber security and data privacy insurance portends a growing number of claims and, inevitably, litigation over some of those claims. Wells Fargo's [2015 Cyber Security and Data Privacy Survey: How Protected Are You?](#) indicates that nearly half (44%) of companies with \$100 to \$500 million in revenue that have cyber security and data privacy insurance have filed a claim with their carriers at some point. But 96% of those companies that filed a claim are satisfied with their coverage and the insurers' handling of the claim. If the data can be extrapolated, then the remaining 4% are in or could end up in some sort of dispute resolution proceeding – small by percentage but potentially large in terms of the direct and indirect costs that can arise from cyber risk.

Recent litigation filings provide a glimpse into what types of claims are in dispute and several are noted here; however, it is important to note that these cases are still pending and no coverage decisions have been made.

One of the hottest areas of cybercrime is spoofed emails – ostensibly from an authorized corporate official – instructing an employee to transfer funds out of the company. Does the fact that the scam occurs by means of email turn the scam into a “cyber” loss? In [Ameriforge Group Inc. v. Federal Ins. Co.](#), filed on January 4, 2016 in Harris County, Texas (No. 2016-00197), the plaintiff alleges that its insurer wrongfully denied coverage under a crime policy for a spoofed email resulting in the unauthorized transfer of \$480,000. The plaintiff seeks coverage under the “computer fraud coverage” provision, asserting that the email directing the funds transfer was an “unauthorized introduction of instructions, programmatic or otherwise, which propagate themselves” through a computer system. The insurer has denied coverage on the basis (among others) that the email and unauthorized transfer do not constitute computer fraud as defined in the policy.

A battle over policy limits is the subject of another recent filing. In [New Hotel Monteleone, LLC v. Certain Underwriters at Lloyd's](#), filed on December 10, 2015 in Orleans Parish, Louisiana (No. 2:16-cv-00061), and then removed to the Federal District Court for the Eastern District of Louisiana, the insurer has asserted that the \$200,000 limit in an endorsement for “payment card industry fines” applies to all claims arising from a cyberattack against the insured. The insured claims that the full policy limits of \$3 million are available to cover its alleged losses, which include not only PCI fines but also fraudulent charge reimbursement and card replacement.

Lastly, a recently filed Illinois action seeks a declaration of no coverage under a cyber, privacy and media policy for a lawsuit alleging that two employees misappropriated trade secrets when they left a competitor to work for the insured. [Certain Underwriters at Lloyd's v. Wunderland Group, LLC](#), filed on December 15, 2015 in Cook County, Illinois (No. 15 CH 018139). The competitor's suit alleged that the two former employees violated their non-disclosure agreements by using proprietary information relating to the IT staffing market. The insured contends the suit should be covered under a provision covering misappropriation of trade secrets and other information arising from “media content” or “user generated content.”

The policy language, facts and jurisdiction will affect the outcomes in litigation or other proceedings. These recent filings illustrate that insureds and insurers present and face a wide array of arguments that will mark the legal landscape. While most claims get paid or settled, the minority of disputed claims continues to provide fodder for litigation that will help develop the body of law that both insureds and insurers can consider in their insurance transactions going forward.

Rhode Island Amends Identity Theft Protection Act

Rhode Island recently amended its 10-year-old Identity Theft Protection Act effective June 26, 2016, further defining and refining existing data security and breach notification requirements, and adding a requirement to notify the Rhode Island Attorney General of certain breaches. More specifically, the amended statute, available [here](#), makes the following changes to Rhode Island's existing information security and breach notification law:

- Modifies the requirement to implement and maintain reasonable policies and procedures to protect personal information of Rhode Island residents, now called a “risk based information security program.”
- Requires secure destruction of personal information, and prohibits its retention longer than is reasonably required to provide the services requested, to meet the purposes for which it was collected or in accordance with a written retention policy or as may be required by law.
- Requires that the Rhode Island Attorney General and major credit reporting agencies be notified of data breaches in which more than 500 Rhode Island residents are to be notified.
- Specifies that breach notification must be provided to affected individuals “in the most expedient time possible but no later than 45 calendar days after confirmation of the breach and the ability to ascertain the information required to fulfill the notice requirements.” (Current law requires notice “in the most expedient time possible and without unreasonable delay.”)
- Expands the definition of “personal information” triggering breach notification obligations to include medical information and health insurance information, tribal identification numbers and e-mail addresses with any required security code, access code or password that would permit access to an individual's personal, medical, insurance or financial account.
- Broadens the definition of “breach of the security of the system” to include “unauthorized access” in addition to “acquisition of” computerized data. (We note, however, that the breach notification requirement is still triggered by acquisition, not access.)
- Narrows the encryption exception to the breach notification requirement to 128 bit key length or greater encryption.
- Adds required content for breach notification letters to Rhode Island residents.
- No longer requires consultation with law enforcement for a data breach risk of harm determination.

Executive Action: Obama Administration Budgets for Cybersecurity

On February 9, 2016, the Obama administration released its [final budget](#), which includes a request for \$19 billion to fund the Cybersecurity National Action Plan ([CNAP](#)). The CNAP sets forth a variety of cybersecurity and privacy initiatives, the headlines of which are detailed in two executive orders released alongside the budget.

First, Executive Order [13718](#) establishes a twelve member Commission on Enhancing National Cybersecurity (Commission). In short, the Commission is charged with making recommendations to strengthen cybersecurity in the public and private sectors by studying the behavior of technology users and providers, improving awareness of cybersecurity risks and improving access to the knowledge needed to make informed risk management decisions. Specifically, by December 1, 2016, the Commission is to develop recommendations in at least five substantive areas:

- bolstering protection of systems and data, including through the advancement of identity management;
- stabilizing security in the context of the Internet of Things;
- identifying research and development initiatives that can enhance cybersecurity;
- educating and training the cybersecurity workforce in the federal government and the private sector; and
- improving cybersecurity education in the general public.

Second, Executive Order [13719](#) focuses on improving the federal government's ability to protect the privacy of those individuals about whom it collects information. To do so, it establishes the Federal Privacy Council (Privacy Council) to act as an interagency support structure and to ensure consistent implementation of privacy policy across the federal government. The Privacy Council will be composed of the Senior Agency Official for Privacy from each of twenty-four named executive departments and federal agencies. It is charged with developing recommendations for government privacy policies, coordinating privacy best practices between agencies and assessing how to meet the federal government's hiring and training needs with respect to privacy matters.

In his [Budget Message](#) President Obama recognized the need to take "bold, aggressive action" on cybersecurity by empowering government, companies and individuals while protecting privacy. Indeed, the executive actions are well-timed, as they come just one day after the [latest breach](#) of federal employees' personal information. In light of persistent cybersecurity risks, companies should monitor the recommendations of the Commission and the Privacy Council and ensure their actions are consistent with best practices.

President Obama Signs Cybersecurity Act of 2015 into Law

On December 18, 2015, President Obama signed into law the Federal Cybersecurity Act of 2015 (the Act). The long-awaited and heavily negotiated legislation recognizes the need for greater cybersecurity threat information sharing among public and private entities, encourages private entities to more freely engage in such sharing and permits private entities to take certain measures to protect themselves against cyber threats.

With respect to information sharing, the Act establishes a mechanism for sharing cybersecurity threat information among private sector entities and the federal government, with the Department of Homeland Security as the primary hub for that sharing. The Act provides broad safe harbors for private entities sharing information in accordance with its terms, exempting such entities from civil, regulatory and antitrust liability based on their sharing, and exempting shared information from the Freedom of Information Act. Further, the Act specifically provides that disclosure of cyber threat indicators or defensive measures (discussed below) to the federal government in accordance with the Act will not operate to waive privileges or protections provided by law, such as in trade secret.

The federal government's usage of information obtained pursuant to the Act is limited to specified permissible uses. In addition, prior to sharing information under the Act, nonfederal entities are required to review the information and remove any information that the sharing entity "knows at the time of the sharing" to be personal or personally identifying information not directly related to a security threat.

With respect to measures that may be taken by a private entity to protect themselves, the Act authorizes private entities to monitor and use defensive measures to protect their information systems (and those of consenting entities). However, measures commonly considered and referred to as "hacking back" are specifically excluded from the defensive measures permitted by the Act. The U.S. Department of Homeland Security has released a document titled [Guidance to Assist Non-Federal Entities to Share Cyber Threat Indicators and Defensive Measures with Federal Entities under the Cybersecurity Information Sharing Act of 2015](#) to provide "information that will assist non-federal entities who elect to share cyber threat indicators with the Federal Government to do so in accordance with the Act."

Private entities will now be able to more freely share what is often rapidly-evolving cyber threat information with one another and take defensive measures to protect themselves from those threats, avoiding circumstances where every new threat requires companies to repeatedly reinvent the wheel to protect their information and systems.

Sixth Circuit Rules 10 Weeks of Camera Monitoring from Public Utility Pole Does Not Require a Warrant

A panel of the United States Court of Appeals for the Sixth Circuit ruled earlier this month in a case styled [U.S. v. Houston](#) (No. 14-5800) that a warrant was not required under the [Fourth Amendment](#) for federal agents to gather evidence of a defendant's activities in which he, according to the court, did not have a "reasonable expectation of privacy," despite the activities taking place on private property where the defendant lived.

The case concerned allegations that the defendant illegally possessed a number of firearms. The ATF had been unable to effectively monitor defendant's activity on the property through traditional means because the rural location of the property caused those monitoring efforts (drive-by surveillance) to "st[ic]k out like a sore thumb." Thus, to monitor the defendant, the ATF directed a utility company to install a camera on a nearby public utility pole for a period of 10 weeks.

The panel found that no warrant was necessary and that the defendant's Fourth Amendment rights were not violated "when it was possible for any member of the public to have observed [the defendant's] activities during the surveillance period." The panel also expressed concern that requiring a warrant under such circumstances would lead to a technological advantage for criminals, as they would be able to one-sidedly benefit from the advance of technologies, while law enforcement could be mired in ever-evolving Fourth Amendment inquiries.

The panel made efforts to distinguish the case from concerns raised in Justice Alito's and Justice Sotomayor's 2012 concurring opinions in the Supreme Court's [U.S. v. Jones](#), which related to long-term GPS monitoring. The panel reasoned that, unlike the GPS monitoring in *Jones*, a stationary camera on a utility pole does not have the potential to monitor and catalogue every move an individual makes over a period of time, or reveal significant details about that individual's activities, beliefs and affiliations.

U.S. District Judge Thomas M. Rose of the Southern District of Ohio, sitting on the panel by designation, parted from the majority opinion on certain points, noting in concurrence that the impracticality of government monitoring was a traditional, "ordinary check" against "abusive law enforcement practices" (internal quotations and citations omitted) and noting concerns relating to monitoring of a person's home, ultimately stating that "privacy concerns implicated by a fixed point of surveillance are equal, if not greater, when it is one's home that is under surveillance."

Notably, the majority opinion of the Supreme Court in the above-referenced *Jones* case rested on traditional notions of trespass in the Fourth Amendment context, with Justice Alito (3 other Justices joining) and Justice Sotomayor each penning concurrences that analyzed evolving privacy concerns in light of technological change. The majority opinion was written by Justice Scalia, joined by only four other Justices. Given the lack of a clear, unified position at the Supreme Court, and in light of Justice Scalia's recent death, issues at the intersection of technology and the Fourth Amendment may be ripe for further consideration in coming Supreme Court terms, and may depend largely on the views of Justice Scalia's replacement on the Court.

Should Apple Always Have a Key to All iPhone Data? To Some iPhone Data?

On February 16, 2016, U.S. Magistrate Judge Sheri Pym of the U.S. District Court for the Central District of California issued an [Order](#) under the [All Writs Act](#) directing Apple Inc. to cooperate with efforts by the Federal Bureau of Investigation to access the contents of an iPhone used by Syed Farook, a deceased [alleged gunman](#) in a shooting spree that left 14 dead in San Bernardino, California.

Under the terms of the Order, Apple's cooperation is to include "reasonable technical assistance" to circumvent certain auto-erase and passcode security functionalities built into the iPhone. The Order does allow Apple to use other means to accomplish the Order's purposes, if deemed possible (with concurrence by the government).

Evidently, iPhone's recent operating systems encrypt data on the iPhone in such a manner that repeated efforts (brute force attacks) to unlock the data result in deletion of the data. This is a pretty powerful measure for protecting data against all but those who have the key.

The issue is part of a larger national security debate, in which the government is generally opposed to technology that permits individuals to encrypt or otherwise protect information using technical means that preclude governmental recovery or review. The theory, as exemplified by statutes such as the [Communications Assistance for Law Enforcement Act](#), is that the government should have the ability to retrieve and search digital data, assuming that probable cause or other legal requirements are met.

By one analogy, the concept is similar to the landlord of a building being required to unlock the suite on the 5th floor. On the other hand, digital data can be created and erased at will, so what is inherently wrong with the idea of permitting users to choose to securely encrypt certain data (as an alternative to erasing it, for example)? Indeed, Internet service providers are generally immune from claims concerning user-provided data under the [Communications Decency Act](#), so for websites that want to provide freedom to post content (even content that promotes or constitutes criminal activity), there is not much by way of legal impetus for the websites to record any usage data that could lead law enforcement to identify posters.

Perhaps the stakes are different when we are talking about strongly encrypting broad categories of data on a communications device that is used on a near-constant basis by almost 100 million people in the U.S. Still, as Apple points out below, there's no "law" against designing technology in such a manner, and the creation of an exception inevitably drives a huge chink in the armor (especially now that the matter has received so much public attention).

Soon after the Order, Apple CEO Tim Cook released a [letter](#) to Apple's customers expressing serious concerns with respect to the technical steps Apple would be required to take. In his letter, Mr. Cook describes the cooperation dictated by the Order as requiring Apple to write software that does not currently exist that would "circumvent[] several important security features, . . ." and he goes on to state that "[i]n the wrong hands, this software – which does not exist today – would have the potential to unlock any iPhone in someone's physical possession."

Mr. Cook was careful to mention that Apple has cooperated to the extent possible and legal up to the point of the Order, and he reiterated Apple's belief that the FBI agents involved are acting with good intentions. However, he also made clear Apple's position that cooperation under the terms of the Order would set a dangerous precedent:

The implications of the government's demands are chilling. If the government can use the All Writs Act to make it easier to unlock your iPhone, it would have the power to reach into anyone's device to capture their data. The government could extend this breach of privacy and demand that Apple build surveillance software to intercept your messages, access your health records or financial data, track your location, or even access your phone's microphone or camera without your knowledge.

The Order provides that Apple may apply to the court for relief within 5 days of receipt of the Order if Apple believes compliance would be "unreasonably burdensome." Although that time period has not expired as of the time of this writing, it seems likely that Apple will challenge the Order. The success or failure of Apple's efforts to resist the Order may have a significant impact on manufacturers' ability to develop and maintain security features to protect against unexpected access to customer information and the government's ability to obtain information protected by technical means under extraordinary circumstances.

New Safe Harbor Agreement for EU Data Transfer Announced

Companies are relieved that there will now be a new Safe Harbor for cross-border transfer of personal data from Europe to the U.S.

This announcement will provide a degree of certainty going forward, in particular after the upheaval which the Schrems case decision of the European Court of Justice last year produced, striking down the then-existing Safe Harbor framework. Businesses should, however, also expect a more rigorous process by the U.S. Department of Commerce to qualify for the "new" Safe Harbor certification and by the FTC to enforce it.

Both the [EU](#) authorities and the [FTC](#) issued statements on February 2 announcing the agreement highlights.

While it will take some time for the authorities to reduce these elements to detailed text and obtain formal approval, several new components of the Safe Harbor arrangements (now referred to as the EU-U.S. Privacy Shield) are already clear from the announcements.

Strong obligations on companies handling Europeans' personal data and robust enforcement.

U.S. companies wishing to import personal data from Europe will need to expressly commit to robust obligations on how personal data is processed and individual rights are guaranteed. The Department of Commerce will monitor companies' published Safe Harbor commitments for enforcement by the FTC. In addition, any company handling human resources data from Europe has to commit to comply with decisions by the various European Data Protection Authorities (DPAs).

Clear safeguards and transparency obligations on U.S. government access.

The U.S. has given the EU written assurances that access by U.S. authorities for law enforcement and national security will be subject to clear limitations, safeguards and oversight mechanisms. The U.S. has also, significantly, ruled out indiscriminate mass surveillance on personal data transferred to the U.S. under the new arrangement. To regularly monitor the arrangement there will be an annual joint review, which will also include the issue of national security access. The European Commission and the U.S. Department of Commerce will conduct the review and invite national intelligence experts from the U.S. and European DPAs to it.

Effective protection of EU citizens' rights with several redress possibilities.

Any EU citizen who considers that their data has been misused under the new arrangement will have several redress possibilities. Companies will have deadlines to reply to complaints, and European DPAs can refer complaints to the Department of Commerce and the FTC. In addition, an Alternative Dispute Resolution process to address complaints will be provided free of charge, giving real teeth to the right of redress, something which was a major concern to the EU authorities during the course of the negotiations. For complaints on possible access by national intelligence authorities, a new Ombudsperson will be created.

Of course, we will need to see what the final text of the Safe Harbor framework looks like and, ultimately, what the regulations and guidance to be issued by the Department of Commerce and FTC around this will require. In addition and, as is so often the case, the practical implementation of the framework will be crucial.

In the meantime and until the text of the new Safe Harbor framework is agreed and published, businesses can continue to rely on model clauses, consents obtained from data subjects from whom data is collected and binding corporate rules. However, the EU Article 29 Working Party (a policy body made up of EU DPA heads) has also indicated in very recent announcements that they have concerns regarding the appropriateness of model clauses and binding corporate rules for transfers to the U.S., and will be reassessing those mechanisms in light of the new Privacy Shield framework once it is released. Thus, while they made clear that business may rely on model clauses and binding corporate rules in the interim, that issue will be subject to review expected to be completed by the end of April. Indeed, it is fair to say that the Privacy Shield itself, as well as the model clauses and binding corporate rules, are susceptible to a legal challenge to their ability to afford an adequate level of protection for the transfer of personal data outside of the EEA (in much the same way that Maximilian Schrems challenged the adequacy of the first Safe Harbor framework). Thus, as we indicated earlier, businesses should reevaluate their current EU data collection processes and consider other steps. The new EU General Data Protection Regulation (GDPR) due to be finalized this spring may have some effect on this also.

Here are some suggested steps for the near term:

- Identify personal data flows of the company from the EU to U.S., including employee, customer and lead data. Identify the path that the personal data follows, from its collection

by the EU company, to its transfer to the entity in the U.S., and any onward transfers; identify the purposes for which the personal data is collected and used; and identify the systems, software and hardware used by or on behalf of the company to store and process the personal data. Determine which EU countries the data is being transferred from, as the oversight and positions of EU national DPAs may be different.

- Identify all instances of where the company relies (or relied) on Safe Harbor (or on other cross-border data transfer mechanisms), including, for example, in intra-group transfers, and transfers to U.S. vendors, partners, sub-processors and sub-contractors. Review the data protection due diligence on these EU and U.S. entities.
- Check if other derogations or exclusions apply, such as consent or transfers that are necessary for the performance of a contract with the individual in respect to whom the personal data relates or for compliance with a legal obligation. If the company relies on consent, ensure that the company's privacy policies, notices and consents are adequate and effective (do they explicitly allow transfers of the personal data to the U.S.) and that the company does not process (at least going forward) the personal data of anyone who has withdrawn their consent.
- Review the company's public or consumer-facing statements (such as terms and conditions, promotional content, current contracts with customers) and make sure that nothing misstates the data protections or privacy practices which the company has in place. This may need to include disclaimers as to current Safe Harbor invalidity in the company's posted Safe Harbor privacy policy, according to the FTC.

- Review indemnity provisions in the company's agreements with relevant service providers, third parties and other entities in the data processing and transfer chain so as to ensure that any privacy related risks are addressed.
- Identify the implementation mechanisms, means and back-off steps whereby Safe Harbor, EC Model Contract Clauses and/or consents are actually put into effect or accomplished.
- Identify relevant stakeholders in the process and inform them, where appropriate, of their obligations. These may include company or third party sales representatives, distributors, data gathering entities, customers, and other employees.
- Consider the impact on current and upcoming projects of the company, including technology resets or re-configurations.
- Review your exit, break, force majeure and compensation clauses in existing contracts that may have exposure and initiate strategic discussions regarding privacy and data protection amendments to these contracts.



Practical Wisdom, Trusted Advice.

www.lockelord.com

Atlanta | Austin | Boston | Chicago | Dallas | Hartford | Hong Kong | Houston | Istanbul | London | Los Angeles | Miami | Morristown
New Orleans | New York | 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 piece 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 or Locke Lord LLP, 111 South Wacker Drive, Chicago, Illinois 60606, Attention: Marketing. If we are not so advised, you will continue to receive similar mailings. (022316)

Attorney Advertising © 2016 Locke Lord LLP