TEN YEARS STRONG

A Decade of Privacy and Cybersecurity Insights

HUNTON
ANDREWS KURTH

huntonprivacyblog.com

DEAR CLIENTS AND FRIENDS,

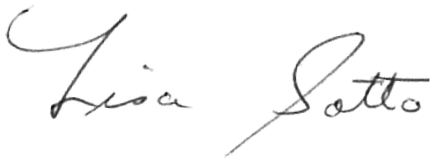
In January 2019, Hunton Andrews Kurth celebrated the 10-year anniversary of our award-winning Privacy and Information Security Law Blog. Over the past decade, we have worked hard to provide timely, cutting-edge insights into the ever-evolving global privacy and cybersecurity legal landscape.

Legal considerations surrounding privacy and information security remain a hot topic across the globe. The patchwork of laws presents unique challenges to businesses operating in multiple jurisdictions. Over the past 10 years, our Privacy and Information Security Law Blog has been a go-to resource for readers seeking to understand emerging legal developments and obtain breaking news in privacy, data protection and cybersecurity.

The following is a compilation of our blog's top ten most read posts over the decade. They address some of the most transformative changes in the privacy and cybersecurity field, serve as a reminder of how far we have come, and give us a sense of what challenges might lie ahead.

We are proud of the work we have done throughout the years, and invite you to continue to visit and share our blog with the privacy community.

Thank you for your continued support, and happy reading!



Lisa J. Sotto

Partner and Chair of the Privacy and Cybersecurity Practice

TABLE OF CONTENTS

Massachusetts Information Security Regulations Take Effect on March 1, 2010

Posted on February 23, 2010

After several delays and revisions, the Massachusetts information security regulations, entitled "Standards for the Protection of Personal Information of Residents of the Commonwealth," will take effect on March 1, 2010. The regulations apply to entities that own or license personal information about Massachusetts residents. "Personal information" is defined as a combination of a resident's first and last name and Social Security number, driver's license or state ID number, or financial account number or payment card number that permits access to the individual's financial account.

The regulations require entities to develop, implement and maintain a written, risk-based information security program that takes into account the entity's size, the nature of its business, the types of records it maintains and the risk of identity theft posed by the entity's operations. Also set out in the regulations are numerous administrative, technical and physical safeguards that the required information security program must include.

Finally, the regulations require covered entities to take steps to select and retain service providers that are capable of appropriately safeguarding personal information. Covered entities must contractually require their service providers to safeguard personal information in accordance with the Massachusetts regulations and applicable federal requirements, provided, however, that service provider contracts entered into no later than March 1, 2010, are exempt from complying with this requirement until March 1, 2012.

In previous blog posts, we had reported that the Standards for the Protection of Personal Information of Residents of the Commonwealth have been the subject of much commentary and a series of amendments as regulators seek to address concerns expressed by businesses over the stringent and specific nature of the regulations. The most recent round of amendments was announced August 17, 2009.

View the Massachusetts regulations.

FTC Privacy Report Emphasizes Privacy by Design, Individual Control and Transparency

Posted on March 27, 2012

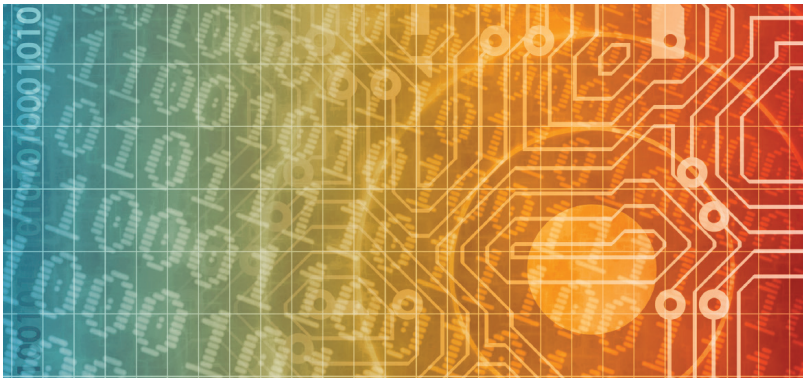
On March 26, 2012, the Federal Trade Commission issued a new privacy report entitled "Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers." The report charts a path forward for companies to act in the interest of protecting consumer privacy.

In his introductory remarks, FTC Chairman Jon Leibowitz indicated his support for Do Not Track stating, "Simply put, your computer is your property; no one has the right to put anything on it that you don't want." In later comments he predicted that if effective Do Not Track mechanisms are not available by the end of 2012, the new Congress likely would introduce a legislative solution.

The FTC's privacy framework focuses on three principles (privacy by design, simplified consumer choice and transparency), and provides steps companies can take to implement them. These principles are reflected in recent FTC consent orders entered into with Google and Facebook, and they mirror similar requirements in the European Commission's proposed privacy regulation.

The simplified choice principle builds on the preliminary 2010 report which excluded five categories of "commonly accepted" information collection and use practices. Instead, the final report took a modified approach that relies on the context of the transaction. This gives companies greater flexibility but requires them to assess the context of the interaction. This furthers the need for a company to have a comprehensive program.

The FTC has indicated that its principles should facilitate global interoperability: they are consistent with both the APEC Privacy Framework and the OECD guidelines, and the privacy by design principle specifically is reflected in forthcoming guidance from Canadian privacy authorities. Privacy by design requires implementation of privacy protections in all aspects of a company's business operations, which has been a key element of the Centre for Information Policy Leadership's work on accountability. Commonly accepted information collection and use practices were first articulated by the Business Forum on Consumer Privacy.



> #1 global leader for privacy and data security in all of its four surveys – *Computerworld*

The FTC's report recommends that Congress act in three areas, calling for baseline privacy legislation and renewing the call for legislation to address issues surrounding data security and the activities of data brokers. The report also identifies five ways in which the FTC intends to promote the framework's implementation through policymaking in 2012, calling on the business community to join the Commission in its efforts to:

- Work with browser makers, the Digital Advertising Alliance and the World Wide Web Consortium to complete work started on a Do Not Track solution.
- On May 30, 2012, convene a workshop to explore how to make privacy disclosures for mobile applications short, effective and accessible.
- Encourage data brokers to create a centralized website that identifies data brokers and describes the access rights and other choices they offer consumers.

- In late 2012, host a workshop to consider issues surrounding large platform providers that track consumers' online activities (e.g., ISPs, operating systems, browsers, social media). A senior FTC staffer indicated that these providers' ubiquitous information collection practices create privacy concerns that cannot effectively be managed by consumer choice alone.
- Participate in the Department of Commerce's multi-stakeholder process to develop binding codes of conduct, and use the FTC's authority to prosecute unfair and deceptive practices to enforce such codes when companies assert they will abide by them.

The report issued today was adopted by a 3-1 vote of the Commissioners. Commissioner J. Thomas Rosch issued a dissenting statement citing his concerns that the FTC is emphasizing unfairness rather than deceptiveness in promoting the principles, and that support for the report's findings by large businesses might stifle innovation.

The FTC's report is being released just over a month after the Obama Administration issued its Consumer Privacy Bill of Rights, which also calls for increased transparency in privacy and data security practices.

> Recognized as one of the leading Data Protection practices globally
> – *Chambers and Partners Global*, 2018

White House Announces Its Highly Anticipated Consumer Privacy Bill of Rights

Posted on February 23, 2012

The White House today released its long-awaited report outlining a framework for US data protection and privacy policy. As expected, "Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Global Innovation in the Global Digital Economy" articulates a Consumer Privacy Bill of Rights based on the individual's right to exercise control over what personal data companies collect from the individual and how companies use the data. The Consumer Privacy Bill of Rights, which reflects principles of fair information practices and applies to personal data, sets forth individual rights for consumers and corresponding obligations of companies in connection with personal data. It also provides for the consumer's right to:

- transparent privacy and data security practices;
- expect that companies will collect, use and disclose data in a manner consistent with the context in which it was collected;
- have their data handled in a secure manner;
- access and correct personal data;
- set reasonable limits on the personal data that companies collect and retain; and
- have personal data handled by companies with appropriate measures in place to assure they adhere to the Consumer Privacy Bill of Rights.

In a press release, the Administration stated its intention to work with Congress to draft legislation based on the Consumer Privacy Bill of Rights. According to the report, "enacting the Consumer Privacy Bill of Rights through Federal legislation would increase legal certainty for companies, strengthen consumer trust, and bolster the United States' ability to lead consumer data privacy engagements with our international partners."

As reported in *BNA's Privacy Law Watch*, Lisa J. Sotto, partner and head of Hunton's Global Privacy and Data Security practice, said, "Members of Congress will certainly see this as an influential document when considering new legislation. Privacy is a bipartisan issue that everyone can agree on, but of course the devil is in the details, and where it goes from here remains to be seen."

The report also describes an open forum in which stakeholders will work toward consensus on codes of conduct that would implement the provisions of the Consumer Privacy Bill of Rights. Although their adoption by organizations is voluntary, the codes will be enforceable. The report emphasizes the critical role of the FTC in privacy enforcement and encourages Congress to provide the FTC and state attorneys general with specific authority to enforce the Consumer Privacy Bill of Rights.

Finally, the report underscores the Administration's goal of global interoperability of privacy protections facilitated by effective enforcement and accountability mechanisms.

The report builds on the recommendations of the Department of Commerce Internet Policy Task Force's "Green Paper" on privacy, entitled "Commercial Data Privacy and Innovation in the Internet Economy: A Dynamic Policy Framework."

NIST Releases Final Cybersecurity Framework

Posted on February 12, 2014

On February 12, 2014, the National Institute of Standards and Technology ("NIST") issued the final Cybersecurity Framework, as required under Section 7 of the Obama Administration's February 2013 executive order, Improving Critical Infrastructure Cybersecurity (the "Executive Order"). The Framework, which includes standards, procedures and processes for reducing cyber risks to critical infrastructure, reflects changes based on input received during a widely attended public workshop held last November in North Carolina and comments submitted with respect to a preliminary version of the Framework that was issued in October 2013.

Differences between the Framework and its preliminary version are generally editorial, and the Framework's basic structure has remained substantially the same. However, in one notable change, the Framework no longer includes Appendix B, the "Methodology to Protect Privacy and Civil Liberties for a Cybersecurity Program." Appendix B of the Preliminary Framework attracted significant opposition from industry because, among other things, of its breadth, prescriptive nature, and failure to reflect the standards contained in a wide range of successful privacy and data protection programs implemented by industry, in partnership with various government agencies. The Framework issued today removes Appendix B and replaces it with a general description of privacy issues that entities should consider in the section on "How to Use the Framework."

Like the preliminary version, the Framework is broadly broken down into three components: (1) Framework Core, (2) Framework Implementation Tiers and (3) Framework Profile.

The Framework Core is organized into five overarching cybersecurity functions: (1) identify, (2) protect, (3) detect, (4) respond and (5) recover. Each function has multiple categories, which are more closely tied to programmatic activities. They include activities such as "Asset Management," "Access Control" and "Detection Processes." The categories, in turn, have subcategories, which are tactical activities that support technical implementation. Examples of subcategories include "[a]sset vulnerabilities are identified and documented" and "[o]rganizational information security policy is established." The Framework Core includes informative references, which are specific sections of existing standards and practices that are common among various critical infrastructure sectors and illustrate methods to accomplish the activities described in each subcategory.

The Framework Implementation Tiers describe how an organization views cybersecurity risk and the processes in place to manage that risk. The tiers range from Partial (Tier 1) to Adaptive (Tier 4) and describe an increasing degree of rigor and sophistication in cybersecurity risk management practice. Progression to higher tiers is encouraged when such a change would reduce cybersecurity risk and be cost effective.

The Framework Profile is the alignment of the functions, categories and subcategories with the organization's business requirements, risk tolerance and resources. An organization may develop a current profile based on existing practices and a target profile that reflects a desired set of cybersecurity activities. A comparison of the two profiles may reveal gaps that establish a roadmap for reducing cybersecurity risk that is aligned with organizational and sector goals, considers legal and regulatory requirements and industry best practices, and reflects risk management priorities.

The Framework is a flexible document that gives users the discretion to decide which aspects of network security to prioritize, what level of security to adopt, and which standards, if any, to apply. This flexibility reflects vocal opposition by critical infrastructure owners and operators to new cybersecurity regulations.

The White House has emphasized repeatedly that the Framework itself does not include any mandates to adopt a particular standard or practice. However, Section 10 of the Executive Order directs sector-specific agencies to engage in a consultative process with the Department of Homeland Security, the Office of Management and Budget, and the National Security Staff to review the Framework and determine if current cybersecurity regulatory requirements are sufficient given current and projected risks. If such agencies deem the current regulatory requirements to be insufficient, then they "shall propose prioritized, risk-based, efficient, and coordinated actions…" This process could lead to new cybersecurity regulations in various sectors.

This regulatory review, in conjunction with the Framework being used by insurance underwriters and incentives the Administration is developing to encourage adoption of the Framework, likely will result in the Framework's affecting standards of reasonableness in litigation relating to cybersecurity incidents.

> Clients praise Hunton Andrews Kurth as "the only firm to use for data privacy matters" with "consistently reliable advice and unmatched service levels across the board." – *The Legal 500 USA*, 2018

Russian Parliament Adopts Internet Privacy Bill Requiring Data Localization

Posted on July 7, 2014

Last week, the Russian Parliament adopted a bill amending portions of Russia's existing legislation on privacy, information technology and data protection. Among other provisions, the law would create a "data localization" obligation for companies engaged in the transmission or recording of electronic communications over the Internet. Such companies would be required to store copies of the data for a minimum of six months in databases that must be located within the Russian Federation. The new bill also would empower the Russian data protection authority to block public Internet access to any service that does not comply with this requirement.

It appears the amendments are aimed at preventing foreign intelligence services from accessing Russian citizens' data, as well as facilitating such access by Russia's own law enforcement agencies. Some commentators have suggested that the new bill also is intended to encourage the development of homegrown online services in Russia.

Earlier in 2014, the European Union's highest court struck down a broadly comparable data retention requirement, and Brazilian lawmakers withdrew the data localization provision from a legislative proposal in the face of opposition from Internet companies.

Update

We later reported that, on December 31, 2014, Russian President Vladimir Putin signed legislation to move the deadline for compliance to September 1, 2015, for Federal Law No. 242-FZ (the "Localization Law"). The bill originally had a compliance deadline of September 1, 2016, and then the compliance deadline was moved to January 1, 2015, before being changed to September 1, 2015, in the legislation signed by President Putin.

The Russian law firm ALRUD reported that the Localization Law creates a new obligation to store personal data of Russian citizens in Russia, meaning that companies located outside Russia "will be forced to place their servers within Russia if they plan to continue making business in the market." The exact purview of the Localization Law is somewhat ambiguous, but the law requires data operators to ensure that the recording, systemization, accumulation, storage, revision (updating and amending), and extraction of personal data of Russian citizens occur in databases located in Russia. As an example of the ambiguity regarding the scope of the Localization Law, it is unclear whether the law applies to companies that collect personal data from Russian customers but have no physical presence in Russia. In addition, it is unclear whether the law will affect the cross-border transfers of personal data from Russia to foreign jurisdictions.

> Subscribe now to our Privacy & Information Security Law Blog for the latest legal updates, developments and news in privacy, data protection and cybersecurity.

EU General Data Protection Regulation Finally Adopted

Posted on April 14, 2016

On April 14, 2016, after four years of drafting and negotiations, the long-awaited EU General Data Protection Regulation ("GDPR") has been adopted at the EU level. Following the EU Parliament's Committee on Civil Liberties, Justice and Home Affairs' vote earlier this week and the EU Parliament in plenary session, the GDPR is now officially EU law and will directly apply in all EU countries, replacing EU and national data protection legislation.

The New Data Protection Landscape in Europe

The GDPR replaces the EU Data Protection Directive 95/46/EC (the "Directive"), which was enacted in 1995, and significantly changes the EU data protection landscape. The following is a summary of the key aspects of the GDPR:

- ***Broader scope:*** The GDPR will apply to data processing activities of a data controller or a data processor established in the EU. In addition, it will apply to data controllers and data processors established outside the EU where their processing activities relate to the offering of goods and services to individuals in the EU or to the monitoring of EU individuals' behavior.
- ***Concept of personal data:*** Under the GDPR, location data, IP addresses and online identifiers would constitute personal data in most cases as this data could be used to identify individuals, in particular when combined with unique identifiers. Pseudonymization of personal data is considered a security measure used to limit the risk of singling out an individual during the processing. In addition, genetic data and biometric data are recognized as sensitive data requiring extra protection.
- ***Data controllers, processors, joint controllers:*** The GDPR will introduce additional obligations for data controllers, data processors and joint controllers. Direct obligations will be imposed on data processors for the security of personal data.
- ***Accountability obligations:*** Companies will have to implement appropriate privacy policies and robust security measures, perform data protection impact assessments in certain cases, and appoint a data protection officer under specific conditions. In addition, both data controllers and data processors will have to maintain records of data processing activities, replacing the existing registration and authorization obligations with the supervisory authorities.
- ***Data breach notification:*** The GDPR introduces a general data breach notification requirement that will apply across all industry sectors and will require data controllers to notify the competent supervisory authority within 72 hours after becoming aware of a data breach, unless they can provide a reasoned justification for the delay. If the breach is likely to result in a high risk for the individuals' rights and freedoms, data controllers will also have the obligation to notify individuals of the breach without undue delay.
- ***One-stop shop:*** For companies active in multiple EU countries, the GDPR will allow them to have a central point of enforcement through the one-stop shop

mechanism. The supervisory authority of the main establishment or of the single establishment of the data controller or data processor in the EU will act as the lead supervisory authority, supervising all their processing activities throughout the EU. This new mechanism will allow data controllers and data processors to interact with a single lead data protection authority ("DPA"); however, other DPAs may have a say for cross-border operations as the GDPR includes significant consistency and cooperation procedures. In addition, each individual supervisory authority will be competent to handle purely local complaints or deal with purely local infringements of the GDPR.

- ***Consent:*** Consent should be a freely given, specific, informed and unambiguous indication of the individual's wish to, either by a statement or by a clear affirmative action, agree to the processing of his or her personal data. The GDPR also provides specific protection in the context of children's personal data by strengthening the validity conditions of children's consent. When offering information society services directly to children under the age of 16—or a lower age provided by EU Member State law which may not be below 13 years—consent should be given or authorized by the holder of parental responsibility.
- ***Profiling:*** The GDPR will strengthen the protection of individuals against possible negative effects of profiling by providing them with the right not to be subject to automated decision making (including profiling), which produces legal effects concerning the individual or significantly affects the individual.
- ***Privacy notices:*** Under the GDPR, data controllers must take appropriate measures to provide individuals with information regarding the processing of their personal data. Information will have to be provided in a concise, transparent, intelligible and easily accessible form. The GDPR also introduces the use of standardized icons as a valid way to inform individuals.
- ***Data transfers:*** The GDPR maintains the general prohibition of data transfers to countries outside the EU that do not provide an adequate level of data protection. Consistent with the Schrems decision of the Court of Justice of the European Union, stricter conditions will apply for obtaining an "adequate" status. EU Model Clauses will remain a valid mechanism to transfer personal data outside the EU. Further, the GDPR explicitly recognizes and promotes the use of Binding Corporate Rules as a valid data transfer mechanism. Approved codes of conduct also can be used for data transfers.
- ***Rights of individuals:*** The GDPR will expand the rights of individuals. The GDPR reinforces the existing right to request the erasure of personal data that is no longer necessary by including a "right to be forgotten." It also introduces a right to data portability allowing individuals to transit and move personal data concerning them between providers.
- ***Administrative fines:*** Supervisory authorities will be given significantly more powers to enforce compliance with the GDPR, including investigative, corrective, advisory and authorization powers. In addition, supervisory authorities will have the power to impose administrative fines of up to a maximum of €20 million or 4 percent of the data controller's or data processor's total worldwide global turnover of the preceding financial year, whichever is higher.

Next Steps

The GDPR will apply to all businesses in and outside Europe that deal with personal data of EU individuals. The GDPR will enter into force 20 days after its publication in the EU Official Journal. Its provisions will be directly applicable in all Member States two years after this date, in spring 2018.

View the EU Parliament's press release.

View the European Commission's Joint Statement on the final adoption of the new EU rules for personal data protection.

For additional topics and resources on the GDPR, please visit our privacy blog here.

European Commission Adopts Privacy Shield

Posted on July 12, 2016

On July 12, 2016, the EU Commissioner for Justice, Consumers and Gender Equality, Věra Jourová, and US Secretary of Commerce Penny Pritzker announced the formal adoption of the EU-US Privacy Shield (the "Privacy Shield") framework, composed of an Adequacy Decision and accompanying Annexes.

The Privacy Shield is designed to protect the fundamental rights of individuals whose personal data is transferred to the US and ensure legal certainty for businesses with respect to transatlantic transfers of personal data.

The European Commission outlines the following principles of the new framework:

- ***Strong obligations on companies handling personal data.*** The Privacy Shield includes stricter oversight mechanisms to help ensure companies abide by their commitments, including regular monitoring by the US Department of Commerce. The Privacy Shield also includes stricter conditions for onward transfers of personal data to third parties by participating companies.
- ***Clear safeguards and transparency obligations on US government access.*** The European Commission has obtained strong written commitments and assurance from the US government that access to personal data by government authorities for law enforcement, national security and other public interest purposes will be subject to clear conditions, limitations and oversight mechanisms, preventing generalized access and bulk collection of personal data. In addition, a new redress mechanism has been established for EU individuals in the area of national security, through an Ombudsperson within the Department of State. The Ombudsperson will act independently from the US Intelligence Services.
- ***Effective protection of individual rights.*** Individuals who consider that their personal data has been misused under the Privacy Shield framework will benefit from several accessible and affordable dispute resolution mechanisms. These mechanisms include (1) the right for individuals to lodge a complaint directly with the company, (2) free-of-charge alternative dispute resolution solutions, (3) the right to lodge a complaint with national data protection authorities (the "DPAs"), working in collaboration with the US Federal Trade Commission, and (4) an arbitration mechanism as a last resort.
- ***Annual joint review mechanism.*** The European Commission and the US Department of Commerce will annually monitor the functioning of the Privacy Shield, together with national security experts from the US and European DPAs. The review also will cover the commitments and assurance regarding access to data for law enforcement and national security purposes.

Next Steps

The Adequacy Decision on the protection provided by the Privacy Shield will be notified to the EU Member States today, on July 12, 2016, and will immediately enter into force. In the US, the Privacy Shield framework will be published in the Federal Register. Companies will be able to certify with the US Department of Commerce starting August 1, 2016.

The European Commission also will publish a short guide for individuals explaining the available remedies in case an individual thinks that his or her personal data has been misused.

The Article 29 Working Party is currently analyzing the Adequacy Decision in view of its previous Opinion on the Privacy Shield. It will meet on July 25, 2016, to finalize its position on that decision.

Read the European Commission's Q&A, Factsheet and Press Release.

Read the US Department of Commerce's FAQs and Guide on how to join the Privacy Shield.

New York Announces Proposed Cybersecurity Regulation to Protect Consumers and Financial Institutions

Posted on September 15, 2016

On September 13, 2016, New York Governor Andrew Cuomo announced a proposed regulation that would require banks, insurance companies and other financial services institutions to establish and maintain a cybersecurity program designed to ensure the safety of New York's financial services industry and to protect New York State from the threat of cyber attacks.

The proposed regulation requires regulated financial institutions to take various actions, including:

- adopting a written cybersecurity policy;
- establishing a cybersecurity program;
- designating a Chief Information Security Officer to oversee and enforce its new program and policy; and
- implementing policies and procedures designed to ensure the security of information systems and nonpublic information accessible to, or held by, third parties, along with a variety of other requirements to protect the confidentiality, integrity and availability of information systems.

The proposed regulation is subject to a 45-day notice and public comment period. If adopted, this will be the first regulation of its kind in the United States.

Update

We later reported in January 2017 that on December 28, 2016, the New York State Department of Financial Services ("DFS") announced an updated version of its cybersecurity regulation for financial institutions (the "Updated Regulation"). The Updated Regulation will become effective on March 1, 2017.

Key changes from the September 2016 proposed regulation include:

- providing a definition of a "Third-Party Service Provider";
- modifying the definition of "Nonpublic Information" to make it consistent with the definition of private information under New York's state breach notification law;
- adding "asset inventory and device management" to the list of required components of a covered entity's cybersecurity policy;
- permitting a covered entity's Chief Information Security Officer to be employed by an affiliate of the covered entity or by a service provider;
- limiting the requirement for a covered entity to maintain audit trails to cover only cybersecurity events "that have a reasonable likelihood of materially harming any material part of the normal operations of the Covered Entity";
- eliminating the obligation for covered entities to require multi-factor authentication for employees accessing internal databases; and
- adding a notice of exemption form that covered entities may complete and file with DFS if they believe they are exempt from specific sections of the regulations.

In announcing the Updated Regulation, DFS Superintendent Maria T. Vullo stated that the Updated Regulation "allows an appropriate period of time for regulated entities to review the rule before it becomes final and make certain that their systems can effectively and efficiently meet the risks associated with cyber threats."

The Updated Regulation will be finalized in January 2017 following a 30-day notice and public comment period and will become effective on March 1, 2017.

Cybersecurity Law Goes into Effect in China

Posted on June 1, 2017

On June 1, 2017, the new Cybersecurity Law went into effect in China. This post takes stock of (1) which measures have been passed so far, (2) which ones go into effect on June 1 and (3) which ones are in progress but have yet to be promulgated.

A draft implementing regulation and a draft technical guidance document on the treatment of cross-border transfers of personal information have been circulated, but at this time only the Cybersecurity Law itself and a relatively specific regulation (applicable to certain products and services used in network and information systems in relation to national security) have been finalized. As such, only the provisions of the Cybersecurity Law itself and this relatively specific regulation went into effect on June 1.

On June 1, 2017, the following obligations (among others) become legally mandatory for "network operators" and "providers of network products and services":

- personal information protection obligations, including notice and consent requirements;
- for "network operators," obligations to implement cybersecurity practices, such as designating personnel to be responsible for cybersecurity, and adopting contingency plans for cybersecurity incidents; and
- for "providers of network products and services," obligations to provide security maintenance for their products or services and to adopt remedial measures in case of safety defects in their products or services.

Penalties for violating the Cybersecurity Law can vary according to the specific violation, but typically include (1) a warning, an order to correct the violation, confiscation of illegal proceeds and/or a fine (typically ranging up to RMB 1 million); (2) personal fines for directly responsible persons (typically ranging up to RMB 100,000); and (3) in particularly serious circumstances, suspensions or shutdowns of offending websites and businesses, including revocations of operating permits and business licenses.

A final version of the draft implementing regulation and a draft technical guidance document on the treatment of cross-border transfers of personal information are forthcoming. When issued, they are expected to finalize and clarify the following prospective obligations:

- restrictions on cross-border transfers of personal information (and "important information"), including a notice and consent obligation specific to cross-border transfers; and
- procedures and standards for "security assessments," which validate the continuation of cross-border transfers of personal information and "important information."

The draft version of the implementing regulation on the treatment of cross-border transfers of personal information contains a grace period, under which "network operators" would not be required to comply with the cross-border transfer requirements until December 31, 2018. The final draft likely will contain a similar grace period.

California Consumer Privacy Act Signed, Introduces Key Privacy Requirements for Businesses

Posted on June 29, 2018

On June 28, 2018, the Governor of California signed AB 375, the California Consumer Privacy Act of 2018 (the "Act"). The Act introduces key privacy requirements for businesses, and was passed quickly by California lawmakers in an effort to remove a ballot initiative of the same name from the November 6, 2018, statewide ballot. We previously reported on the relevant ballot initiative. The Act will take effect January 1, 2020.

Key provisions of the Act include:

- ***Applicability.*** The Act will apply to any for-profit business that (1) "does business in the state of California"; (2) collects consumers' personal information (or on the behalf of which such information is collected) and that alone, or jointly with others, determines the purposes and means of the processing of consumers' personal information; and (3) satisfies one or more of the following thresholds: (a) has annual gross revenues in excess of $25 million, (b) alone or in combination annually buys, receives for the business's commercial purposes, sells, or shares for commercial purposes the personal information of 50,000 or more consumers, households or devices, or (c) derives 50 percent or more of its annual revenue from selling consumers' personal information (collectively, "Covered Businesses").
- ***Definition of Personal Information.*** Personal information is defined broadly as "information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household." This definition of personal information aligns more closely with the EU General Data Protection Regulation's definition of personal data. The Act includes a list of enumerated examples of personal information, which includes, among other data elements, name, postal or email address, Social Security number, government-issued identification number, biometric data, Internet activity information and geolocation data, as well as "inferences drawn from any of the information identified" in this definition.
- ***Right to Know***
  - Upon a verifiable request from a California consumer, a Covered Business must disclose (1) the categories and specific pieces of personal information the business has collected about the consumer; (2) the categories of sources from which the personal information is collected; (3) the business or commercial purposes for collecting or selling personal information; and (4) the categories of third parties with whom the business shares personal information.
  - In addition, upon verifiable request, a business that sells personal information about a California

consumer, or that discloses a consumer's personal information for a business purpose, must disclose (1) the categories of personal information that the business sold about the consumer; (2) the categories of third parties to whom the personal information was sold (by category of personal information for each third party to whom the personal information was sold); and (3) the categories of personal information that the business disclosed about the consumer for a business purpose.

  - The above disclosures must be made within 45 days of receipt of the request using one of the prescribed methods specified in the Act. The disclosure must cover the 12-month period preceding the business's receipt of the verifiable request. The 45-day time period may be extended when reasonably necessary, provided the consumer is provided notice of the extension within the first 45-day period. Importantly, the disclosures must be made in a "readily useable format that allows the consumer to transmit this information from one entity to another entity without hindrance."

- ***Exemption.*** Covered Businesses will not be required to make the disclosures described above to the extent the Covered Business discloses personal information to another entity pursuant to a written contract with such entity, provided the contract prohibits the recipient from selling the personal information, or retaining, using or disclosing the personal information for any purpose other than performance of services under the contract. In addition, the Act provides that a business is not liable for a service provider's violation of the Act, provided that, at the time the business disclosed personal information to the service provider, the business had neither actual knowledge nor reason to believe that the service provider intended to commit such a violation.
- ***Disclosures and Opt-Out.*** The Act will require Covered Businesses to provide notice to consumers of their rights under the Act (e.g., their right to opt out of the sale of their personal information), a list of the categories of personal information collected about consumers in the preceding 12 months, and, where applicable, that the Covered Business sells or discloses their personal information. If the Covered Business sells consumers' personal information or discloses it to third parties for a business purpose, the notice must also include lists of the categories of personal information sold and disclosed about consumers, respectively. Covered Businesses will be required to make this disclosure in their online privacy notice. Covered Businesses must separately provide a clear and conspicuous link on their website that says, "Do Not Sell My Personal Information," and provide consumers a mechanism to opt out of the sale of their personal information, a decision which the Covered Business must respect. Businesses also cannot discriminate against consumers who opt out of the sale of their personal information, but can offer financial incentives for the collection of personal information.
- ***Specific Rules for Minors.*** If a business has actual knowledge that a consumer is less than 16 years of age, the Act prohibits a business from selling that consumer's personal information unless (1) the consumer is between 13 and 16 years of age and has affirmatively authorized the sale (i.e., they opt in); or (2) the consumer is less than 13 years of age and the consumer's parent or guardian has affirmatively authorized the sale.
- ***Right to Deletion.*** The Act will require a business, upon verifiable request from a California consumer, to delete specified personal information that the business has collected about the consumer and direct any service providers to delete the consumer's personal information. However, there are several enumerated exceptions to this deletion requirement. Specifically, a business or service provider is not required to comply with the consumer's deletion request if it is necessary to maintain the consumer's personal information to:
  - Complete the transaction for which the personal information was collected, provide a good or service requested by the consumer, or reasonably anticipated, within the context of a business's ongoing business relationship with the consumer, or otherwise perform a contract with the consumer.

- Detect security incidents; protect against malicious, deceptive, fraudulent or illegal activity; or prosecute those responsible for that activity.
- Debug to identify and repair errors that impair existing intended functionality.
- Exercise free speech, ensure the right of another consumer to exercise his or her right of free speech, or exercise another right provided for by law.
- Comply with the California Electronic Communications Privacy Act.
- Engage in public or peer-reviewed scientific, historical or statistical research in the public interest (when deletion of the information is likely to render impossible or seriously impair the achievement of such research) if the consumer has provided informed consent.
- Enable solely internal uses that are reasonably aligned with the consumer's expectations based on the consumer's relationship with the business.
- Comply with a legal obligation.
- Otherwise use the consumer's personal information, internally, in a lawful manner that is compatible with the context in which the consumer provided the information.

- ***Enforcement***
  - The Act is enforceable by the California Attorney General and authorizes a civil penalty up to $7,500 per violation.
  - The Act provides a private right of action only in connection with "certain unauthorized access and exfiltration, theft, or disclosure of a consumer's nonencrypted or nonredacted personal information," as defined in the state's breach notification law, if the business failed "to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information."
    - In this case, the consumer may bring an action to recover damages up to $750 per incident or actual damages, whichever is greater.
    - The statute also directs the court to consider certain factors when assessing the amount of statutory damages, including the nature, seriousness, persistence and willfulness of the defendant's misconduct, the number of violations, the length of time over which the misconduct occurred, and the defendant's assets, liabilities and net worth.

Prior to initiating any action against a business for statutory damages, a consumer must provide the business with 30 days' written notice of the consumer's allegations and, if within the 30 days the business cures the alleged violation and provides an express written statement that the violations have been cured, the consumer may not initiate an action for individual statutory damages or class-wide statutory damages. These limitations do not apply to actions initiated solely for actual pecuniary damages suffered as a result of the alleged violation.

For more information on the Act, visit our privacy blog.

Our Team

Lisa J. Sotto
Partner, New York

lsotto@HuntonAK.com
+ 1 212 309 1223

Brittany M. Bacon
Partner, New York

bbacon@HuntonAK.com
+ 1 212 309 1361

Aaron P. Simpson
Partner, New York and London

asimpson@HuntonAK.com
+ 1 212 309 1126
+44 (0) 20 7220 5612

Paul M. Tiao
Partner, Washington, DC

ptiao@HuntonAK.com
+ 1 202 955 1618

Bridget Treacy
Partner, London

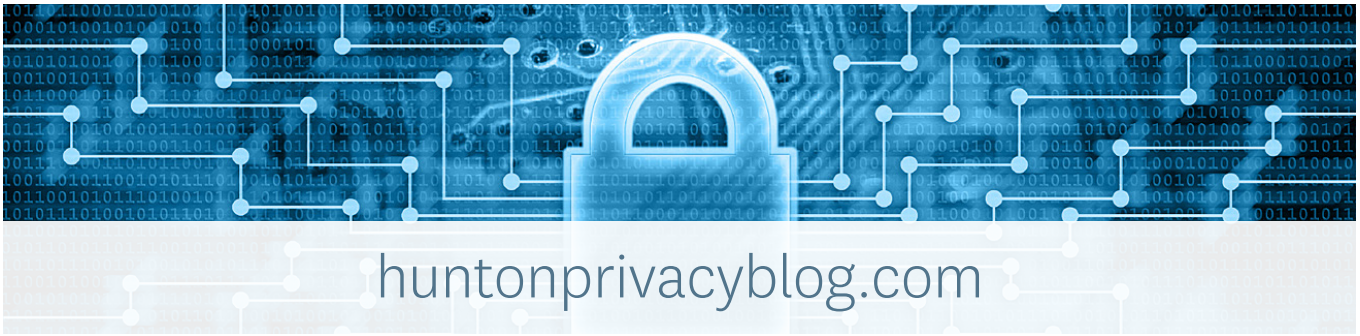
btreacy@HuntonAK.com
+44 (0) 20 7220 5731

Bojana Bellamy
President, Centre for Information Policy Leadership, London

bbellamy@HuntonAK.com
+44 (0) 02 0722 0570

Our Privacy and Cybersecurity Practice

Hunton Andrews Kurth's privacy and cybersecurity practice is known throughout the world for its deep experience, breadth of knowledge and outstanding client service. *Chambers and Partners*, *The Legal 500* and *Computerworld* magazine, all have named Hunton Andrews Kurth as a top firm for privacy, data protection and cybersecurity. In addition to our legal practice, we distinguish ourselves through our Centre for Information Policy Leadership, which boasts the active participation of more than 60 leading multinational corporations. Visit us on HuntonAK.com, Twitter and YouTube.



HUNTON
ANDREWS KURTH