March 2019

Skadden

Privacy & Cybersecurity Update

California Enacts Consumer Privacy Act

California recently enacted the Consumer Privacy Act, the most stringent privacy law in the United States. Although it does not go into effect until January 1, 2020, most companies will need a number of months to prepare. We recently authored "California Consumer Privacy Act: A Compliance Guide" in order to help clients plan for these new requirements. Note that the law applies to any company that has California customers or employees, not just those based in the state.

Massachusetts Adds New Requirements to Breach Notification Law and Credit Reporting Law

A new Massachusetts law expands a company's notification requirements after a data breach and imposes new obligations on credit reporting companies.

A new Massachusetts law goes into effect on April 11, 2019, that will expand data breach notification requirements and extend state consumer protections in the areas of credit reporting.[1] The new data breach requirement extends well beyond the standard notification requirements now found in all 50 states.

New Data Breach Notice Requirements

- **Additional State Notification Requirements.** This amendment adds new types of information a breached entity must report to the state attorney general and director of consumer affairs and business regulation in the event of a breach. Currently, entities must disclose: (1) the name and address of the party experiencing the breach; (2) the name and title of the reporting person, as well as their relationship to the entity; (3) the type of person or agency reporting the breach; (4) the nature of the incident; (5) the number of Massachusetts residents affected (at the time of notice); (6) any steps the breached entity has taken or plans to take related to the incident; and (7) a sample of the notification letter sent to impacted Massachusetts residents. Under the new law, the notification letter also must now specify:
  - if available, the identity of the person responsible for breach;

[1] Mass., HB 4806. House Bill 4806

- the type of personal information compromised; and
- whether the breached entity maintains a written information security program.

Additionally, where a notification to consumers is required, the entity must include the name of any individual or corporate owners.

The requirement that an entity must disclose whether it maintains a written information security program effectively provides a check on whether entities are complying with the Massachusetts written information security program (WISP) requirement.[2]

- **Prompt Consumer Notice.** The new data breach requirement does not permit a notification delay simply because the total number of residents impacted has not been determined. Breached entities are required to provide prompt notice and update as necessary with after-acquired details. This requirement is a response to entities that waited until having the complete picture of a breach before providing notification, and may increase compliance costs in cases where information regarding the data breach is evolving, as is often the case.
- **Free Credit Monitoring Services.** In the event of a security breach involving consumers' social security numbers, businesses must offer free credit monitoring services for at least 18 months to impacted Massachusetts residents. If the entity is a consumer reporting agency, this period is extended to 42 months. The breached business must provide consumers with all information necessary to enroll in credit monitoring services and instructions for placing a security freeze on their credit reports. In its notice to the state, the entity also must certify that the credit monitoring services comply with state law.
- **Conditions to Credit Monitoring.** The law bans entities from requiring consumers to waive their legal rights to bring a private right of action in order to obtain the credit monitoring services.

New Consumer Credit Report Requirements

- **Consumer Consent Requirement.** Subject to limited exceptions, a third party seeking access to a consumer's credit report must (1) inform the consumer of the proposed reason for requesting the credit report, and (2) obtain written, verbal or electronic consent (as appropriate) after informing the consumer of the intended use, but before requesting the report. Purported waivers of this requirement by consumers are void.
- **Free Credit Report Freeze.** Consumer reporting agencies may not charge a fee to a consumer who places, lifts or removes a security freeze from a consumer report.

Key Takeaways

Despite already having among the strongest consumer privacy protections in the United States, this latest law enhances Massachusetts' status as an influential force for new consumer privacy protections. Recent action in the consumer privacy protection arena by many states, including legislation such as the California Consumer Privacy Act, underscores the willingness of states to act in the absence of comprehensive federal legislation. As a result, the patchwork of state laws continues to increase the compliance burden on companies faced with implementing different solutions for different states rather than being able to take advantage of a single approach to breach notification and consumer rights.

Return to Table of Contents

UK Government Updates its Cybersecurity and Data Protection Legislation to Prepare for Brexit

Amidst the backdrop of the most comprehensive cybersecurity and data protection reforms in the European Union, the United Kingdom's withdrawal from the EU will complicate the future of this ever-changing regime. In March 2019, the U.K. government introduced its latest legislation to amend its existing cybersecurity and data protection laws in preparation for Brexit.

During the week of March 11, 2019, the U.K. Parliament voted for an extension of Article 50, prolonging the U.K.'s withdrawal from the EU to either April 12 or May 22, 2019 (Exit Day).[3] In this context, there remains legal uncertainty surrounding the U.K.'s compliance with the EU's recent sweeping changes to its cybersecurity and data protection legal regime. In anticipation of Brexit, the U.K. government has introduced its latest legislation

[2] Massachusetts 201 CMR § 17.03.

[3] Currently, there are three extended timeline proposals unanimously approved by the other 27 EU member states. If the U.K. leaves the EU with a deal approved by the U.K. Parliament by April 12, 2019, then the Exit Day will be set for May 22, 2019. However, if the U.K. Parliament rejects the agreement on or before April 12, then the U.K. will have two options: (1) leave the EU with no deal on April 12 or (2) seek a longer extension (with a yet-to-be confirmed Exit Day) to renegotiate the deal and participate in the EU Parliament elections scheduled on May 23-26, 2019.

with regard to two key EU cybersecurity and data protection laws: the Network and Information Systems Directive (EU) 2016/1148 (NIS Directive); and the European e-Privacy Directive (Directive 2002/58/EC as amended by Directive 2009/136/EC) (e-Privacy Directive).

Background

Adopted on July 6, 2016, the NIS Directive became the first EU-wide legislation on cybersecurity and regulates (1) operators of essential services (OES) (*i.e.* transportation, energy, health, water and digital infrastructure services) and (2) digital service providers (DSP) (*i.e.* cloud services, online marketplaces and search engines). The NIS Directive addressed potential cybersecurity threats against network and information systems in these two groups of services. In May 2018, the U.K. passed the Network and Information Systems Regulations 2018 (U.K. NIS), implementing the NIS Directive into national law and requiring OES and DSP to take appropriate technical and organizational measures to manage cybersecurity risks and to notify the relevant authorities of any significant security incidents without delay. The Information Commissioner's Office (ICO) is the main supervisory authority and may impose administrative penalties up to £17 million for serious violations of the U.K. NIS.

In effect since July 31, 2002, the e-Privacy Directive complements broader data protection laws and specifically regulated companies in the electronic communications sector regarding their use of electronic marketing materials, cookies and similar technologies. In 2003, the U.K. passed the Privacy and Electronic Communications (EC Directive) Regulations 2003 ("PECR") to implement the e-Privacy Directive into national law. PECR has been amended seven times, most recently on January 9, 2019, in light of the EU's General Data Protection Regulation (GDPR). The ICO also is the supervisory authority for PECR and may impose administrative penalties up to £500,000.

The Network and Information Systems (Amendment etc.) (EU Exit) Regulations 2019

The U.K. government introduced the Network and Information Systems (Amendment etc.) (EU Exit) Regulations 2019 ("NIS Amendment") to modify provisions of the NIS Directive and e-Privacy Directive that are inappropriate or redundant following Brexit.

Broadly speaking, the NIS Amendment:

- removes the obligations imposed under the NIS Directive on U.K. supervisory authorities and the National Cyber Security Centre (NCSC), the U.K.'s cybersecurity incident response team, to liaise, cooperate and share information with the European Commission and authorities in other member states; and
- revokes EU Regulation 526/2013, which establishes the European Union Agency for Network and Information Security (ENISA), the EU agency that improves network and information security in the union.[4]

However, the NIS Amendment provides that U.K. supervisory authorities may liaise, cooperate and share information on cybersecurity threats and incidents with the EU, as necessary. Additionally, the U.K. may continue to work with ENISA, albeit in a more limited fashion and in line with existing third-country agreements. Even so, post-Brexit, such cooperation and information sharing likely will be based on voluntary arrangements with individual member states, complicating the U.K.'s ability to address large-scale, cross-border cybersecurity threats.

The Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2019

The Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2019 ("Data Protection Amendment") not only addresses major data protection laws post-Brexit, including the GDPR and the Data Protection Act 2018 (the U.K.'s national law that supplements the GDPR), but also includes another update to PECR.

Under the Data Protection Amendment:

- the European Commission will no longer have jurisdiction to make "adequacy decisions"[5] within the U.K.; instead, the U.K.'s secretary of state for digital, culture, media, and sport will have the power to make such decisions post-Brexit;

[4] EU Regulation 526/2013 would have no operative effect in the U.K. after Brexit, so the government views ENISA, as an EU entity, to be redundant.

[5] Under Article 45(2) of the GDPR, the European Commission has the authority to find that a third country, territory, specific sector in a third country or an international organization offers levels of data protection that essentially are equivalent to those within the EU. An adequacy decision allows for international transfer of data outside the EEA.

- companies that transfer data from the U.K. to the U.S. under the EU-U.S. Privacy Shield are required to update their privacy policies in order to continue receiving personal data from the U.K. in reliance on the Privacy Shield. Note that although the U.K. will no longer be part of the EU and will therefore not be a party to the EU-U.S. Privacy Shield, the U.S. Department of Commerce has stated that in the event of a no-deal Brexit, U.S. organizations participating in the Privacy Shield must implement two additional measures by Exit Day: (1) they must update their public commitment to comply with the Privacy Shield to include the U.K. (specifically, that the commitment extends to personal data received from the U.K. in reliance on the Privacy Shield) and (2) a current Privacy Shield certification must be maintained and recertified annually. A participant that does not implement these guidelines will no longer be able to rely on the Privacy Shield to transfer personal information from the U.K. after Exit Day in a no-deal scenario and at the end of the transition period in the context of a deal; and
- the definition of "consent" in PECR now reflects the GDPR's definition.[6]

The current national laws that implement the e-Privacy Directive soon will be replaced by an EU regulation known as the "e-Privacy Regulation." It is worth noting that only if the e-Privacy Regulation passes prior to the Exit Day (in a no-deal scenario) or before the end of a transition period (in a deal scenario) would the e-Privacy Regulation become part of U.K. law.

Key Takeaways

The legal uncertainties introduced by Brexit complicate EU and U.K. cybersecurity and data protection laws. In light of the impending Exit Day, the U.K. government outlined its position to mitigate these uncertainties with regard to the NIS Directive and the e-Privacy Directive, as well as other data protection legislation, keeping much of the U.K.'s national cybersecurity and data protection laws intact post-Brexit. Nevertheless, Brexit will continue to obscure the future of the U.K.'s cybersecurity and data protection regime.

Return to Table of Contents

[6] Under Article 4(11) of the GDPR (and now PECR), "consent" is defined as "any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her."

Data Protection Experts Discuss New Frontiers in Cybersecurity

At a recent U.K. Data Protection Conference, regulatory officials and representatives of the private sector and academia discussed key issues in data protection and cybersecurity.

On March 13 and 14, 2019, the International Association of Privacy Professionals (IAPP) held its U.K. Data Protection Conference (the conference) in London, bringing together national regulatory officials, private and public sector professionals, academics and representatives from nonprofits to discuss 2019's most important issues regarding data protection and cybersecurity. While GDPR compliance was, of course, a main focus, the conference also looked beyond the GDPR, focussing on: (1) compliance with data protection laws in an ever-growing number of jurisdictions, including India, Brazil, Singapore and California; (2) looking past the basics of data protection regulation and on to new areas, including data ethics, artificial intelligence, blockchain technology, fintech and children's rights over their personal data; and (3) the underlying themes of data protection, including transparency, integrity and trust.

We have summarized a few of the conference's key discussions below.

Data Protection and the Impact of Brexit

The opening panel of the conference discussed the impact of Brexit on data protection with the most pressing issue — particularly in the case of a no-deal scenario[7] — being personal data transfers when the U.K. is a data importer.

When the U.K. is a data exporter, the scenario is straightforward. The British government officially has stated that data transfers from the U.K. to the EU and to any of the 12 "adequate countries"

[7] In a deal scenario, the status quo will remain until the end of the transition period, which is currently set to end on December 31, 2020. However, in a no-deal scenario, the U.K. will become a third party at the end of the extended timeframe that EU leaders will have agreed upon unanimously (currently scheduled for April 12, 2019, subject to the U.K. Parliament's final approval of the extended timeline).

as designated by the European Commission (EC)[8] would remain unchanged and regulated by the provisions of the U.K. Data Protection Act 2018 (or the U.K. law supplementing the GDPR).

When the U.K. is a data importer, data flows will require the implementation of appropriate safeguards. When the data import is from the EU to the U.K., in the absence of an adequacy decision from the EC, data transfers will need to be protected on the terms of a valid data transfer mechanism, such as the EC Standard Contractual Clauses, the binding corporate rules for intragroup transfers only or the use of any appropriate derogations (*i.e.* consent). Where the data import is from any of the 12 adequate countries to the U.K., most of these countries have already officially stated that the status quo would continue to apply to such transfers and only a few of these countries still need to confirm this position.

For data transfers between the U.S. and the U.K., the EU-U.S. Privacy Shield will continue to apply to the U.K. post-Brexit as long as certified U.S. companies update their external-facing privacy notices to specifically mention the U.K. and state that their self-certification extends to data received from the U.K.

Whether in a deal or a no-deal scenario, companies with international operations and cross-border transfers will need to revisit their data transfer mechanisms depending on the nature of the data flows, and rethink elements of their corporate data protection governance structure (*i.e.* where the U.K. ICO has been appointed as the lead authority based on the company's central establishment in relation to its data protection decision-making process) to ensure ongoing compliance with applicable data protection laws and regulations.

Processors, Controllers or Joint Controllers?

A difficult area in GDPR implementation has been defining the roles played in data processing, such as those of the data controller and data processor. Diarmuid Goulding, senior legal advisor at the Irish Data Protection Commission, and a number of other experts addressed case studies, ranging from parent and subsidiary roles with respect to enterprise-wide platforms to health technology, illustrating the gray areas between processors, controllers, joint controllerships and co-controllerships. To underscore the speed at which the law is changing, they also reviewed recent case law determining roles in data processing.

The GDPR speaks directly to relationships between controllers and processors, and relationships between joint controllers, but it does not mention co-controller relationships. But even in instances covered by the GDPR, identifying the exact roles played by each entity is determined by a fact-based analysis. Case studies, such as the ones presented at the conference and others presented by the ICO,[9] can help business people understand what their processing activities imply about their legal relationships and obligations.

When there are no directly applicable case studies available (either presented by data protection authorities or in case law) it is possible for entities to strategically define roles, including by establishing contractual arrangements specifying roles. An agreement about roles may help avoid ambiguity and doubt, although this contractual determination would not be binding on a data protection authority or EU court.

Case law in this area is nascent, but some patterns already are arising in opinions coming from data protection authorities and the Court of Justice of the European Union (CJEU). Particularly, joint controllership findings are becoming increasingly common. The next instructive case is awaiting resolution at the CJEU. In a CJEU case against German e-retailer Fashion ID, the advocate general delivered an opinion on December 29, 2018, in which he emphasized a granular approach to the determination of roles, which includes determining who bears responsibility and specifying their responsibilities.

Reduce Reputational and Regulatory Risk With an Effective Incident Response Plan

In light of the increasingly complex and numerous cyber threats, presenters at the conference pointed out that it is time for companies to define an approach at the board level, involving the key cross-functional heads of the business and setting a level of appetite for risk before embarking on new projects. Companies should focus their efforts on building a pre-narrative that may be used in the context of a personal data breach or in cybersecurity incident reports to demonstrate that regular audits (conducted internally and also vetted by third-party experts to effectively address any weak spots or omissions), external certifications and internal coordination are in place.

The presenters noted that the stages preceding a breach or incident also will be scrutinized by cyber insurance providers who will offer coverage to companies based on their overall preparedness. Companies should carefully audit how long they keep

[8] The European Commission has thus far deemed adequate the following countries: Andorra, Argentina, Canada (commercial organizations), Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, Switzerland and Uruguay.

[9] See here for how the ICO defines data processors and controllers.

their logged information and check that their retention periods are aligned with those of the third-party vendors to which they may have outsourced part of their information technology systems. This is to ensure that the company will not be prevented from or at a loss when, carrying out root-cause analysis of a particular incident. To reduce the reputational and regulatory risk, companies should not neglect rehearsing and testing their incident response plan on a regular basis and recalibrating it where necessary.

Companies need to ensure that they are prepared to respond to and mitigate any cyberattack. This preparation includes having a good grasp on the required timing for mandatory breach notifications and communication. Companies may have to focus and potentially revisit their internal governance structure and, at the very least, the means of communication and direct access to the board when faced with a cyberattack. The inefficiency created by the lack of internal coordination — one of the number one mistakes discussed at the conference — may undermine a company's response plan and communication strategy.

The litigation risk grows in the aftermath of an incident, especially in light of the GDPR creating a right for any person who has suffered a financial or non-financial loss to seek compensation from the company. Companies should get ahead of such risk by rolling out their staged incident response plan efficiently and getting their cyber insurance on board from the earliest stages.

The 'Weaponization' of Data Subject Access Requests

Data subject requests (DSR) allow individuals to ask entities certain questions about their personal data, or to have certain actions taken (*i.e.* the right to be forgotten). But, recent developments have shed light on a new trend: the "weaponization" of DSR, such as the use of DSR as discovery tools by ex-employees to extract information for potential legal claims.

Many organizations now use a "scalable approach" (*i.e.* scoping exercises) to verify the identity of the requester to ensure that the request is not fraudulent (in order to avoid a personal data breach) and to confirm the scope of the request to then limit the disclosure of data to what is strictly required to satisfy the scope. Article 12 of the GDPR provides some potential protection against abusive requests, stating that if there are requests that are "manifestly unfounded or excessive," the company (acting as controller) may either (1) charge a reasonable fee or (2) refuse to act on the request. However, the standard of "manifestly unfounded or excessive" sets a high threshold, and the company bears the burden of proof. Furthermore, this phrase is not clearly defined in the GDPR. As such, companies walk a fine line between complying with data subject access requests and carefully defining the scope of personal data to be disclosed.

Interplay Between Data Protection and Competition Laws

The use and processing of data is receiving increased attention from competition authorities to ensure fair and competitive markets and to decide market abuse cases. The conference presenters noted a February 2019 ruling by the German competition authority relating to Facebook's use of data.

Such competition cases apply and reinforce core data protection law principles centered on the notions of (1) transparency, (2) proportionality and purpose limitation, and (3) consent as defined under the GDPR, which must be specific, informed and clearly distinguishable from other matters (*i.e.*, not bundled), to assess whether the terms reviewed would amount to an unfair contract term. From a competition law standpoint, sharing and combining data with third parties can lead to a competitive advantage that could catch the attention of EU competition authorities, the outcome of which may be exacerbated in the absence of due consideration of applicable data protection law requirements.

Conference presenters noted that in the context of open data and data sharing initiatives, such as open banking, data is no longer used as a resource but rather as infrastructure that fosters both individual empowerment and provides a competitive boost.[10] Open banking, a technology designed for consumers to allow financial institutions to share their data with other businesses, applications and online services, is subject to a specific legal framework at the EU level (the second Payment Services Directive, or PSD2) as implemented by EU member states, such as in the U.K. with the Payment Services Regulations 2017. It remains to be seen whether new regulations on open banking promote or stifle innovation. Further complexities arise as the PSD2 empowers individual consumers to become gatekeepers of their own personal data, which may require them to educate themselves on the challenges and implications of data sharing and data protection. These questions may only be answered as open data and dating sharing initiatives become more widespread in the distant future.

Return to Table of Contents

[10] This analysis was outlined by the European Commission in its April 25, 2018, communication titled "Towards a Common European Data Space."

Nationwide Class Certification Denied in Data Breach Litigation Against Discount Store Chain

The U.S. District Court for the Middle District of Alabama denied certification of a nationwide class of approximately 2,500 banks whose cardholders had their credit and debit card numbers stolen during a 2015 data breach involving Fred's discount stores. Fatal to the certification claim were variances among state laws regarding whether a plaintiff may bring a negligence claim for purely economic loss, as well as individualized damages questions, such as whether fraud on a compromised card resulted from a different data breach.

Background

In 2015, hackers used malware installed on Fred's Inc. servers to gain access for approximately one month to the payment card information of Fred's customers. The malware only captured card numbers, not the cardholder's name, expiration date or security code. The banks who issued the cards, rather than the cardholders of the compromised cards, brought suit against Fred's. On behalf of a putative class of roughly 2,500 banks, Southern Independent Bank (SIB) alleged claims for (1) negligence for maintaining inadequate data security and (2) negligent misrepresentation based on Fred's saying it had adequate data security when it did not. The putative class claimed actual fraud losses on the compromised cards, card reissuance costs, lost revenue and ancillary costs. SIB sought certification of a damages class under Rule 23(b)(3), which requires a finding that common questions would predominate over individualized questions at trial.

The District Court Decision

Sitting in diversity jurisdiction in Alabama, the court applied Alabama's choice-of-law rules and determined that the "home-state law of each putative class member applies to the negligence claim," thus implicating all 51 U.S. jurisdictions. In analyzing the laws of those jurisdictions, the court found "significant variations in negligence law," with the main variation being the "economic loss rule," which generally precludes a plaintiff from bringing a tort claim, such as negligence, for purely economic loss.

The court explained that the economic loss rule could present a "formidable barrier to credit card data security breach cases" and that states vary in how they apply the rule and its exceptions. Certain states apply the rule regardless of contractual privity, with a minority of those states applying the rule in an absolute fashion and a majority qualifying it with exceptions. For example, Massachusetts and Pennsylvania have the absolute version of the rule, and federal circuit courts applying the laws of those states have barred classes of card-issuing banks from asserting negligence claims against a retailer arising from a data breach. States applying the qualified rule hold that tort liability may exist for purely economic loss when an "independent duty" or "special relationship" exists. Alaska, for example, recognizes the independent duty exception, but only if the breach of duty created a risk of personal injury or property damage. California recognizes a special relationship exception, which requires a court to analyze several factors to determine if that relationship exists. Both Alaska's and California's exceptions have been found inapplicable in data breach cases, the court explained, resulting in dismissal of consumers' negligence claims.

The court also explained that certain other states apply the economic loss rule only when contractual privity exists. For those states, no tort liability exists for economic loss caused by negligence in the performance or negotiation of a contract between the parties. Because of how payment card networks operate, however, no direct privity of contract exists between the card-issuing banks and merchants such as Fred's. Nonetheless, certain states would still conclude that privity exists because merchants and card-issuing banks are "integrated in the payment industry's network of contracts." Due to that web of contracts, a Colorado court dismissed an issuing bank's negligence claim against a restaurant in a data breach case — notwithstanding a lack of direct privity.

Given that a state-by-state analysis of the economic loss rule was needed, the court concluded that SIB had not "carried its burden to show, by an extensive analysis," that the variations in the economic loss rule do not pose "insuperable obstacles to certification." Rather, what SIB had presented was "merely a checklist of the elements of negligence showing that each jurisdiction recognizes the tort and its elements of duty, breach, causation, and damages." Under that cursory analysis, the court explained, all the jurisdictions would allow the negligence claim at issue. But that was not true.

The court also found predominance lacking because of individualized damages questions. Although courts often state that individualized damages questions, as opposed to individualized liability questions, will not defeat a finding of predominance, the court explained that it "may not brush aside individualized damages questions in deciding predominance simply because they do not go to liability." The court then concluded that

damages, and SIB's damages-related defenses of contributory negligence and failure to mitigate, would involve individualized inquiries into the circumstances of each card reissuance and reimbursement, including inquiries into how each issuing bank responded to the breach and the amount of fraud and lost revenue on each card. In addition, individualized inquiries would be needed to determine whether the damages occurred because of some other event or data breach. For example, of the 720,299 Visa-affiliated accounts identified as having been compromised in the Fred's breach, 74,386 of those cards also were identified as having been compromised in other breaches, thereby raising the question of whether the fraud loss on those cards was in fact caused by the Fred's breach. Accordingly, damages could not be easily determined by some common formula, statistical analysis or easy-to-apply mechanical method.

In sum, managing a class action involving 2,500 banks, 1 million payment cards and 51 different sets of law would be "highly impractical, if not impossible," the court said.

Key Takeaways

The economic loss rule presents a formidable challenge to bringing negligence claims to recover damages arising from a data breach. Depending on the jurisdiction, the doctrine may preclude such claims at the motion-to dismiss-stage, and the variations in the rule across states present a difficult obstacle to certifying a nationwide class. Furthermore, data breach cases are likely to have more individualized damages questions than other cases, which gives damages analyses a more important role than usual in the predominance inquiry under Rule 23(b)(3).

Return to Table of Contents

FTC Seeks Public Comment on Amendments to Safeguards and Privacy Rules Under Gramm Leach Bliley Act

The Federal Trade Commission (FTC) is seeking comments on amendments to the Gramm Leach Bliley Act to enhance consumer privacy and security.

In March 2019, the FTC announced that it is seeking comments on proposed changes to rules under the Gramm Leach Bliley Act that would further protect the privacy and security of personal information held by financial institutions. Specifically, the FTC is seeking to amend the Safeguards Rule, which requires that a financial institution develop, implement and maintain a comprehensive information security program, and the Privacy Rule, which requires that a financial institution inform customers about its information-sharing practices and allow customers to prevent the sharing of their information with certain third parties.

Among other proposals, the FTC seeks to expand the definition of "financial institution" to include people and entities that charge a fee to connect consumers who are looking for a loan to a lender (also known as "finders"). This change would align the FTC's rule with other agencies' interpretations of the Gramm Leach Bliley Act.

Safeguards Rule

The Safeguards Rule went into effect in 2003, and, as part of its periodic review, the FTC sought comment on the rule in 2016. In response to that review, the FTC now proposes to amend the rule to add detailed obligations with respect to the comprehensive information security program that the rule currently requires. For example, the proposed amendment would require financial institutions to encrypt customer data, implement access controls to prevent unauthorized access to customer information and use multifactor authentication to access customer data. In addition, the FTC is considering whether to require companies to submit periodic reports to their boards of directors to improve compliance with the rule.

Privacy Rule

The enactment of the Dodd-Frank Act in 2010 narrowed the scope of the Privacy Rule. Specifically, the act transferred the majority of the rulemaking authority for the Privacy Rule to the Consumer Financial Protection Bureau, leaving the FTC with rulemaking authority over only certain motor vehicle dealers. To address this change, the FTC has proposed certain changes, such as removing examples of financial institutions unrelated to motor vehicle dealers from the Privacy Rule.

Practical Considerations

The Federal Register will publish the FTC notice seeking comment on the proposed changes soon. The FTC must receive comments within 60 days after that publication. If the proposed amendments take effect, financial institutions will need to make sure their information security programs comply with the specific obligations set forth in the updated Safeguards Rule.

Return to Table of Contents

Thailand Passes New Cybersecurity Law Creating Unilateral Authority to Obtain Private Data

The National Assembly of Thailand recently passed a new cybersecurity measure substantially expanding the government's power when responding to perceived cyber threats. While proponents assert the measure is necessary to address exigent national security issues, critics claim the law is yet another attempt by the military-led government to silence dissent and maintain societal control.

On February 28, 2019, Thailand's military-appointed National Assembly passed the Cybersecurity Act, which expands the ability of the government to bypass typical legal procedures in instances of "serious cyber threats." The new law permits the country's National Cybersecurity Committee to physically and electronically seize private property in response to a perceived cyber threat, bypassing the typical judicial review process. Proponents claim the law is necessary to protect the country's emerging digital economy and is commensurate with other countries in the region. Though the law addresses national security threats on its face, opponents claim the act represents "cyber martial law," removing the few legal safeguards in the country impeding unchecked government access to data. Beyond the seemingly vague, broad scope of the law, some observers worry there are insufficient requirements the government must satisfy before proactively responding to identified threats (even if a threat has not yet materialized).[11] Some have criticized Thailand's government for passing and enforcing laws in the name of cybersecurity with an underlying motivation to centralize and enhance government power. The government already censors internet access and tends to broadly interpret criticism as a national security threat, with Thailand's 2017 Computer Crime Act already considered a key tool for exerting online control to promote "security." For example, in 2017, a man received a 35-year jail sentence for a Facebook post criticizing the country's monarchy.[12]

Separately, the National Assembly also passed the Personal Data Protection Act (PDPA), which over time will apply to all companies collecting, using or sharing personal data of subjects within Thailand. The PDPA has many parallels to the EU's GDPR and codifies several consumer rights and business obligations, all of which have extraterritorial application. Specific rights granted to data subjects include rights to access their personal data held by an entity; and direct such entity to destroy, suspend use of or anonymize their personal data. Specific obligations on businesses under the PDPA include duties to: (1) obtain explicit data subject consent prior to usage for a given purpose; (2) secure personal information; (3) restrict transfer to other countries; and (4) upon government or consumer request, disclose the type of personal data collected, purpose of such data, period of storage of the information and internal conditions required for access to personal data. Notably, unique regional concerns engrained in the law means GDPR compliance does not necessarily mean PDPA compliance.

Though there is currently less concern over the reach of the PDPA, critics are nonetheless worried about its impact over time. The measure does not mandate data localization within Thailand, as required in many regions with similar laws; however, over time it could represent yet another avenue to maintain government control in the era of cloud computing.

Return to Table of Contents

[11] The Asia Internet Coalition's statement denouncing the law can be found here.

[12] See "Man jailed for 35 years in Thailand for insulting monarchy on Facebook," *The Guardian*, June 9, 2017.

Privacy & Cybersecurity Update

Contacts

Stuart D. Levi
Partner / New York
212.735.2750
stuart.levi@skadden.com

James Carroll
Partner / Boston
617.573.4801
james.carroll@skadden.com

Brian Duwe
Partner / Chicago
312.407.0816
brian.duwe@skadden.com

David Eisman
Partner / Los Angeles
213.687.5010
david.eisman@skadden.com

Patrick Fitzgerald
Partner / Chicago
312.407.0508
patrick.fitzgerald@skadden.com

Todd E. Freed
Partner / New York
212.735.3714
todd.freed@skadden.com

Marc S. Gerber
Partner / Washington, D.C.
202.371.7233
marc.gerber@skadden.com

Rich Grossman
Partner / New York
212.735.2116
richard.grossman@skadden.com

Michael E. Leiter
Partner / Washington, D.C.
202.371.7540
michael.leiter@skadden.com

Amy Park
Partner / Palo Alto
650.470.4511
amy.park@skadden.com

William Ridgway
Partner / Chicago
312.407.0449
william.ridgway@skadden.com

Jason D. Russell
Partner / Los Angeles
213.687.5328
jason.russell@skadden.com

Ivan Schlager
Partner / Washington, D.C.
202.371.7810
ivan.schlager@skadden.com

David Schwartz
Partner / New York
212.735.2473
david.schwartz@skadden.com

Jen Spaziano
Partner / Washington, D.C.
202.371.7872
jen.spaziano@skadden.com

Ingrid Vandenborre
Partner / Brussels
32.2.639.0336
ingrid.vandenborre@skadden.com

Donald L. Vieira
Partner / Washington, D.C.
202.371.7124
donald.vieira@skadden.com

Helena Derbyshire
Of Counsel / London
44.20.7519.7086
helena.derbyshire@skadden.com

Jessica N. Cohen
Counsel / New York
212.735.2793
jessica.cohen@skadden.com

Peter Luneau
Counsel / New York
212.735.2917
peter.luneau@skadden.com

James S. Talbot
Counsel / New York
212.735.4133
james.talbot@skadden.com

Eve-Christie Vermynck
Counsel / London
44.20.7519.7097
eve-christie.vermynck@skadden.com

Skadden, Arps, Slate, Meagher & Flom LLP
Four Times Square
New York, NY 10036
212.735.3000