2020

SheppardMullin

Eye On Privacy:
2020 Year in Review

These articles appeared in the "Eye On Privacy" Blog in 2020 (www.eyeonprivacy.com)

Sheppard Mullin's 2020 Eye on Privacy Year in Review

As we begin to get some distance from 2020 (no doubt much to everyone's relief), we wanted to take time as we do each year to reflect on some of the privacy and cyber security trends from last year that may impact 2021. The following pages contain all the articles from our Eye on Privacy blog (www.eyeonprivacy.com) posted in 2020. From artificial intelligence, to CCPA regulations and CPRA, to significant developments with cross-border data transfers, 2020 was another busy year in privacy.

With the "Schrems II" decision, the EU invalidated Privacy Shield as a mechanism for transferring personal data between the EU and the US. Brazil enacted a comprehensive data protection law, with enforcement set to begin sometime in 2021 (as of now). In California, the CCPA went into effect, regulations were issued, modified, modified again, and finalized. As our world moved online, we saw an uptick in children's privacy enforcement, something we anticipate will continue in 2021. Things were similarly busy on the data security front, with NIST, CIS, and the FTC issuing guidelines and New York's SHIELD Act coming into effect.

We anticipate 2021 will be another busy year for privacy and data security. With renewed focus on children online, concerns around use of artificial intelligence, and ongoing changes to the California privacy scheme, we expect many privacy developments over the coming months, including at the Supreme Court. We expect similar activity in the data security space, with ongoing ransomware and other cyber-attacks, as well as ongoing focus by regulators and class action lawyers on companies security measures.

We will continue to track these developments in www.eyeonprivacy.com. In the meantime, we hope that you find this compilation of 2020 actions helpful as you move forward in planning your privacy efforts for 2021 and beyond.

Sheppard Mullin Privacy & Cybersecurity Team

Our group includes some of the most respected lawyers in the privacy space, including a former U.S. Department of Homeland Security deputy general counsel, a lawyer who literally "wrote the book" on data breach, award-winning privacy class action litigation practitioners, and leading EU-based data protection experts. Our accolades include being highly ranked by Legal 500 USA (Cyber Law) and Legal 500 Europe (EU Data Protection), and we were one of only 25 firms ranked in the inaugural ATL Top Law Firm Privacy Practice Index.

Nearly every facet of a company's operations—from internal employment practices to online operations, data collection, and customer contact—is subject to a complex array of legal and business challenges related to privacy. Our team recognizes that companies need practical advice from experienced counsel who thoroughly understand privacy law. We partner with clients to help them extract value from the data they collect, while identifying and addressing regulatory compliance requirements, and ensuring that data is appropriately protected.

Our lawyers have experience responding to high-profile data breaches and the regulatory investigations, Congressional oversight, and litigation that often follow such incidents. In addition, as data becomes more entwined with the enterprise value of businesses, we conduct data and privacy compliance due diligence in connection with mergers and acquisitions and other corporate and strategic transactions.

CONTENTS

CONTENTS

BIOMETRICS

2020 In Review: An AI Roundup

Posted December 28, 2020

There has been much scrutiny of artificial intelligence tools this year. From NIST to the FTC to the EU Parliament, many have recommendations and requirements for companies that want to use AI tools. Key concerns including being transparent about the use of the tools, ensuring accuracy, and not discriminating against individuals when using AI technologies, and not using the technologies in situations where it may not give reliable results (i.e., for things for which the was not designed). Additional requirements for use of these tools exist under GDPR as well.

Legal counsel may feel uncomfortable with business teams who are moving forward in deploying AI tools. It's not likely, however, that lawyers will be able to slow down the inevitable and widespread use of AI. We anticipate more developments in this area into 2021.

PUTTING IT INTO PRACTICE: Companies can use "privacy by design" principles to help them get a handle on business team's AI efforts. Taking time to fully understand the ways in which the AI tool will be used (both immediately in any future phases of a project) can be critical to ensuring that regulator concerns and legal requirements are addressed.

Seventh Circuit Issues Landmark BIPA Decision

Posted May 20, 2020

The Seventh Circuit has recently ruled that plaintiffs have standing to enforce the Illinois Biometric Information Privacy Act's informed consent requirements in federal court. As we have written before, BIPA regulates the collection, use, and retention of a person's biometric information, e.g., fingerprints, face scans, etc. For years, federal trial courts have been split on whether a violation of BIPA's informed consent provision is alone sufficient to confer Article III standing. The decision in Bryant v. Compass Group USA, Inc., — F.3d — 2020 WL 2121463 (7th Cir. May 5, 2020) removes that uncertainty and will drastically change the landscape of BIPA litigation going forward.

In allowing the case to proceed in federal court, the Bryant Court found the defendant, Compass Group USA, Inc., had "inflicted the concrete injury BIPA intended to protect against, i.e., a consumer's loss of the power and ability to make informed decisions about the collection, storage, and use of her biometric information." The plaintiff, Christine Bryant, had worked for a call center in Illinois and voluntarily provided her fingerprint information to her employer so she could access workplace vending machines. Her employer, however, did not obtain plaintiff's written consent to collect, store, and use her fingerprint. Bryant sued Compass Group USA, Inc. on a class action basis in Illinois state court, and Compass removed the case to federal court.

Significantly, the Bryant Court's ruling on standing only applies to Section 15(b) of BIPA—the provision that requires collectors of biometric information to obtain written informed consent. Although the plaintiff also alleged a violation of Section 15(a), which requires private entities to make a data retention schedule publicly available, the Court held that Section 15(a) violations do not cause particularized harm and thus, are not sufficient for federal standing.

PUTTING IT INTO PRACTICE: We anticipate an increase in BIPA cases filed in Illinois federal courts. The previous uncertainty over federal standing led to the vast majority of BIPA claims being filed in Illinois state court. But Bryant opens the federal courts to Section 15(b) BIPA claims so long as the court also has diversity or federal question jurisdiction. With this new avenue of recourse open in federal courts, we also anticipate increased scrutiny on company practices surrounding the collection, use, and retention of biometric information; and, therefore, now more than ever companies should review their current practices under BIPA to ensure the statutory mandates are addressed.

Taking Temperatures During COVID-19: A Practical Toolkit

Posted April 29, 2020

As we move into the second quarter of 2020, governments around the country are analyzing how to best open up their economies. Part of this will include people returning to work, restaurants, retail establishments, and other places of public accommodation. Landlords, business owners, and others want to know how to take steps to reopen safely while government mitigation efforts are being developed to help slow the spread of COVID-19 until a vaccine is developed. And where authorities don't have specific mitigation efforts, instituting protocols will fall squarely on landlords, business owners, and those who operate places of public accommodation.

Part of the government directives regarding opening include taking the temperatures of those who come into your establishment. Instructions from city, county, state, and federal governments on temperature checks are often included within Social Distancing Protocol requirements. Other issues arise under ADA considerations, as well as under general privacy and data security law principles. (See, for example, information we posted on our sister labor and employment blog about EEOC testing approval.)

Drawing from these requirements, how can an organization put together an appropriate policy, especially if it has operations around the country? To help employees, landlords and others address these issues we have put together a toolkit consisting of a checklist and FAQs for employers.

California Privacy

The Button is Back! Fourth Set of Modifications to CCPA Regulations Released

Posted December 16, 2020

As 2020 draws to a close and we approach CCPA's first birthday, the regulations continue to remain very much in "infant" mode. On December 10, 2020, the California Attorney General released a fourth set of proposed regulations. This is the second set of proposed changes released since the regulations went into effect in August 2020. Companies have until December 28, 2020 to submit comments to the AG on the modifications.

These proposed modifications present two changes to the "do not sell" rules.

Clarifies that only businesses that "sell" personal information collected in the course of interacting with consumers offline need to provide consumers with an offline notice of their right to opt-out. This should include instructions about how consumers can opt-out.

Adds a "Do Not Sell My Personal Information" button that businesses may use in addition to having the link on the bottom of their website. If businesses choose to use the button, it must be located to the left of the link and must be the same size as other buttons used by businesses on the website.

PUTTING IT INTO PRACTICE: Businesses are reminded that the CCPA statute and regulations are currently in effect. This latest proposal just contains further modifications. Further, the CPRA contemplates that additional regulations will be issued. The rulemaking process for CPRA is anticipated to start sometime in 2021.

The CCPA Wheels Keep Turning: The Addition of CPRA

Posted November 5, 2020

By ballot initiative, California residents recently approved Proposition 24, or the California Privacy Rights Act (CPRA), with approximately 56 percent voting in favor. CPRA significantly amends the CCPA by expanding individual rights, introducing new GDPR-style governance measures, and establishing a new enforcement agency (among other things). Importantly, CPRA does not replace or repeal CCPA, but rather augments it. Further, no new private right of action will be added by CPRA. The substantive provisions of CPRA do not take effect until January 1, 2023.

How did we get here?

The CPRA was backed by the non-profit "Californians for Consumer Privacy." This is the same organization that was behind the 2018 ballot initiative. Last-minute, the 2018 initiative was pulled from the ballot in exchange for enactment of the CCPA. CPRA was introduced in late 2019 given concerns that amendments to the CCPA had gutted the key provisions. The final text of the CPRA was published November 13, 2019. In late June 2020, the Secretary of State confirmed that the initiative had received enough valid signatures to appear on the November ballot.

What are some of the key provisions?

- **Scope**. The thresholds to qualify as a "business" under CCPA has been revised to: (i) clarify the revenue threshold is based on previous year's activities, (ii) increase the processing to 100,000 consumers or households (from 50,000 currently under CCPA), and (iii) require that entities sharing common control and common branding must also share personal information.

- **Employee / B2B Exemption**. CPRA retains the CCPA's exceptions for personal information collected in the employment and business-to-business contexts and extends their sunset provisions to January 1, 2023.

- **Governance concepts**. CPRA introduces a new storage limitation requirement. Personal information is not to be retained for longer than is "reasonably necessary" for the specific, disclosed purposes. A data minimization principle is also included. Collection, use, retention, and sharing of personal information should be limited to what is "reasonably necessary" to achieve the specified purposes.

- **Individual Rights**. Among some modifications to the right to know, deletion, and do-not-sell rights, CRPA includes a new right to "correction." There are also certain rights for "sensitive personal information" (a new category of information introduced).

- **Enforcement**. A new California Privacy Protection Agency would replace the attorney general's office as the regulator implementing CPRA rules and enforcing its requirements against violators. Enforcement will begin on July 1, 2023 and applies to violations occurring on or after that date.

PUTTING IT INTO PRACTICE: While 2023 may seem far away, the passage of CPRA serves as another reminder of the benefit of establishing overarching principles-based privacy programs – that can expand and grow as laws change. We will be monitoring developments of CPRA; we expect that additional regulations may also be promulgated.

California Governor Pulls the Plug on Genetic Information Privacy Act

Posted October 20, 2020

Governor Gavin Newsom of California vetoed a bill that would have created new limitations on data sharing for direct-to-consumer genetic testing companies.

The Genetic Information Privacy Act (GIPA) asked testing companies to get informed consent from customers before disclosing their data to third parties. GIPA was aimed as a stop-gap to cover data sharing that is not already regulated by the California Consumer Privacy Act (CCPA) and the federal Health Insurance Portability and Accountability Act (HIPAA).

The final bill gained significant traction in the legislature. It passed both houses without a single vote against it.

In his veto message, the Governor expressed concern about the "unintended consequences" of the bill. Governor Newsom fears the bill would constrain mandatory reporting of COVID-19 test results to local public health departments and the California Department of Public Health.

California has been exceedingly active in the past few years putting forward innovative regulation of personal information. This veto is an example of the state taking a measured approach to the regulation of health data in the midst of the COVID-19 pandemic.

The Governor signaled that he supports the overall goals of the bill. He directed California state agencies to work with the Legislature on a revised version that takes into account the need to share COVID-19 testing data with authorities.

PUTTING IT INTO PRACTICE: This version of the GIPA is put to rest. However, California has signaled it plans to pass a law regulating data sharing for genetic testing companies in the near future. Companies innovating in this area can begin reviewing their existing disclosures and consents with an eye toward getting opt-in consent in the future.

Will CCPA Regulation Change Again?: Comment Deadline Looming

Posted October 19, 2020

The California Attorney General recently released a third set of proposed modifications to the CCPA regulations. As we previously covered, the CCPA regulations were approved and went into effect on August 14, 2020. Many companies will likely be frustrated by the fact that new changes have been proposed again, just two months after the final version was approved. Companies have until October 28, 2020 to submit comments to the AG on the modifications.

Generally, the proposed modifications provide additional detail to the requirements for those companies selling information. They also address requirements related to the use of authorized agents for identity verification. The proposed modifications are summarized here, and seem to center on areas of confusion for many companies:

- **999.306(b)(3) (Notice of Right to Opt-Out)**. Provides examples of how businesses that collect personal information from consumers offline can provide the notice of right to opt-out of the sale of personal information through an offline method. Specifically, brick-and-mortar stores may choose to print the notice on the paper forms that collect the personal information. They could also post signage in the area where the personal information is collected, directing consumers to where the notice can be found online.

- **999.315(h) (Requests to Opt-Out)**. Provides guidance on how a company's methods for submitting requests to opt-out should be easy and require minimal steps. It includes some examples of methods that would have a "substantial effect of subverting or impairing a consumer's choice to opt-out." For example, a process that requires consumers to click through or listen to reasons why they should not submit a request to opt-out before confirming their choice. Or, if clicking on the "Do Not Sell My Personal Information" leads consumers to a page that requires them to scroll through a privacy policy or other webpage to find the mechanism for opting out.

- **999.326(a) (Authorized Agents)**. Clarifies the proof a business may require from an authorized agent to verify a request, as well from a consumer.

- **999.332(a) (Notice to Consumers Under 16)**. Clarifies that businesses subject to *either* section 999.330 (those selling information of consumers under 13), section 999.331 (those selling information of consumers 13 through 15) or both of these sections, must include a description of the processes in those sections in their privacy policies.

PUTTING IT INTO PRACTICE: The timing of these proposed changes could suggest areas where the AG is focusing from an enforcement perspective. Companies have until October 28 to submit comments, which the AG has asked be confined only to these proposed changes.

CCPA Bill Extending Exemptions Passes Through California Legislature

Posted September 1, 2020

As the California legislature session concluded at the end of August, a significant amendment to the CCPA finally passed both houses. California bill AB-1281 passed the Senate in the last days of the month, extending the business-to-business and employee/applicant carve-outs through January 1, 2022 (as we wrote about previously). The bill now sits with Governor Newsom to sign before the end of September.

The passage of this bill likely brings some welcomed relief to companies subject to CCPA, as the existing exemptions were set to expire at the end of 2020. While the requirements under CCPA will not fully apply to B2B communications and employee/applicant information, a reminder that in its current form, CCPA still imposes certain obligations for this type of information. Namely, that businesses must provide a notice at collection for employee/applicant information. And, all personal information, regardless of from whom it is collected, is subject to the data breach provisions.

Once signed by the Governor, AB-1281 is set to go into effect *only* to the extent the California Privacy Rights Act (CPRA or Prop 24) fails the November ballot. However, if CPRA is enacted, then the exemptions will be extended until January 1, 2023.

PUTTING IT INTO PRACTICE: Organizations can let out a sigh of relief knowing that will in all likelihood not need to expand their CCPA compliance programs by January 1, 2021 to address the expiration of the business-to-business and employee/applicant carve-outs. Want a current version of the law? For easy reference to keep track of the most current version of the CCPA statute (i.e., without this proposed amendment) we have compiled both the CCPA statute and the regulation (as well as GDPR) here. We will update this link should AB-1281 be signed into law.

CCPA Regulations Finally Approved, Effective Immediately

Posted August 18, 2020

The California AG has now released the final CCPA regulations, as approved by the Office of Administrative Law (OAL). The final draft (issued August 14, 2020) incorporates some relatively minor changes that the OAG submitted as part of its final rulemaking package, as summarized in its addendum to the final statement of reasons. In addition to generally "non-substantive" edits for consistency, etc. the OAG withdrew four sections (999.305(a)(5), 999.306(b)(2), 999.315(c), and 999.326(c)) from OAL review.

For those organizations that have concluded that they are "selling" information as that term is defined under CCPA, there are two changes of consequence to note. First, is the removal of the short-form option (e.g., "Do Not Sell My Info") that the regulations had previously permitted. Now, the regulations align with the statute (1798.135(a)(1)), which requires that any "do not sell" link be entitled "Do Not Sell My Personal Information." (999.306(b)(1) and 999.315(a)). Second, the OAL removed 999.306(b)(2), which previously required that those businesses substantially interacting with consumers offline provide notice of right to opt-out via an offline method.

PUTTING IT INTO PRACTICE: Organizations are reminded that in addition to the statute (effective January 1), the regulations are now also effective. The regulations added substantial color to how to process and handle individual rights; and we expect to see additional AG enforcement in this area.

What Will Come First: Pending CCPA Amendment Could Clarify Key Exemptions

Posted August 7, 2020

With the current limited exemptions under CCPA for employment and business-to-business related information set to expire January 1, 2021, there is uncertainty over when businesses should prepare to extend CCPA compliance efforts to this type of information. However, a pending amendment in the California senate, and/or the impending CPRA ballot initiative in November may bring clarity to the issue.

Assembly Bill 1281 (AB 1281), a bill amended in late June, would extend the CCPA exemptions until January 1, 2022. However, this bill would take effect only if it is enacted **and** the California Privacy Rights Act of 2020 (CPRA) is not approved in the statewide general election on November 3. CPRA would extend the exemptions to January 1, 2023. In sum, companies have three different potential outcomes to prepare for with respect to the employment and business-to-business related information exemptions:

- If neither AB 1281 and the CPRA is approved, then the exemptions will expire on January 1, 2021.
- If AB 1281 is passed and the CPRA is not approved, the exemptions will expire on January 1, 2022.
- Notwithstanding AB 1281, if the CPRA is approved, then the exemptions will expire on January 1, 2023.

AB 1281 is scheduled to be heard before the Judiciary Committee on August 12. In California, both houses have until August 31 to pass bills. September 30 is the last day for Governor Newsom to sign or veto bills.

PUTTING IT INTO PRACTICE: If AB 1281 is enacted, businesses will at least know they have until January 1, 2022 for the exemption to apply. We will continue to monitor the status of AB 1281 because if it is *not* enacted, the CPRA will become even more important to businesses deciding when they must extend their CCPA compliance program to other types of information.

Final Draft CCPA Regulations Submitted, Effective Date Unclear

Posted June 4, 2020

On June 1, 2020, the California AG submitted the final text of the proposed CCPA regulations to the Office of Administrative Law (OAL). There were no changes to the final text from the last version released in March, which we previously summarized here.

The OAL typically has 30 working days to review and approved submitted regulations. An executive order related to COVID-19 extends that review period an additional 60 days. Once approved by OAL, the final text is filed with the Secretary of State and becomes law. While that timeline would suggest that the regulations might not be effective until an October timeframe, the AG requested an expedited review to allow the regulations to become effective July 1. The AG has publicly said that it intends to enforce the law beginning July 1.

The final text also is accompanied by a revised Statement of Reasons that explains the basis for the regulations and outlines textual changes from the initial draft regulations published on October 11, 2019.

PUTTING IT INTO PRACTICE: While it may be unclear the exact effective date of the CCPA regulations, companies are reminded that the statute already went into effect on January 1. The AG has the authority to begin enforcing violations beginning July 1, 2020 and said "[b]usinesses have had since January 1 to comply with the law, and we are committed to enforcing it starting July 1." Companies should keep in mind the laws' requirements regarding notice and access, as well as the implications on data that might be viewed as being "sold" (as that term is expansively defined).

Can you Zigzag? California AG Releases Latest Draft of CCPA Regulations

Posted March 17, 2020

On March 11, 2020, the second set of modifications (or the third version) of the CCPA draft regulations were released. While the number of substantive changes dwindled in this version, there are a number of drafting corrections and a few modifications of note. Namely:

- Removal of the suggested UX for the "do not sell" opt-out button, with no alternative proposed. The statute still contemplates that a "recognizable and uniform" opt-out logo or button will be made available on or before July 1, 2020, so stay tuned for something in the final draft! (§1798.185(a)(4)(C); 999.306(f));
- Removal of the addition that was made to the last draft attempting to clarify when IP addresses constitute "personal information" or not (999.302);
- Reinsertion of the requirement for businesses to identify the categories of sources from which personal information is collected and the business/commercial purpose for collecting or selling the information in its privacy policy. Unlike the first draft, this language does not require such disclosures "for each" category of personal information (999.308(c)(1)(e)-(f));
- Addition to clarify that even if a business withholds sensitive data in a request to know, the business should provide a description of that information withheld (999.313(c)(4)); and
- Clarification that permitted service provider purposes includes internal use to build or improve the quality of its services, *provided however* that such use does not include building or modifying household or consumer profiles to use in providing services to another business (999.314(c)(3)).

As with the last set of modifications, which we discussed here, the public has another 15 days (March 27, 2020) to submit written comments. If no additional changes are made, a final rulemaking record will be submitted to the Office of Administrative Law. The OAL has 30 working days to review the record for approval.

PUTTING IT INTO PRACTICE: With just 106 days to go until enforcement, now is the time for companies to take a hard look at the state of their CCPA compliance and prepare for some potential last minute updates once the AG releases the final regulations. The limited number of changes in this last draft signals that the next draft may (finally) be final!

And the Modified Proposed CCPA Regulations are Here!

Posted February 13, 2020

On February 10, the California Attorney General's office released a highly anticipated updated draft of the proposed CCPA regulations. This draft corrected a version first issued on February 7, 2020. These latest updates follow the four public hearings held in December 2019 and nearly 1,700 pages of comments submitted after the AG first released the initial proposal in October 2019. While these modified regulations are still not final, some of the notable changes include:

- Clarifying that businesses do not collect "personal information" when it collects IP addresses but does not link the IP address to any particular consumer or household, and could not reasonably link the IP address (999.302);
- Removing the 90-day claw back period on businesses to pass on an individual's opt-out of the sale of information (instead requiring the lookback only for sales between the submission of a request and the honoring of that request) (999.315(f));
- Deleting the prior requirement to treat unverifiable deletion requests as opt-out requests, but requiring the business to ask the consumer if they would like to opt out of the sale of their personal information (999.313(d)(1));
- Introducing the opt-out button that can be used in addition to (but not in place of) the notice of the right to opt-out (999.306(f));
- Explaining that the requirement to have a two-step process for online requests to delete is allowed but not required (999.312(d)); and
- Increasing the threshold for the number of consumers from 4 million to 10 million for the metrics and transparency reporting requirement (999.317(g))

The deadline to submit written comments is Tuesday, February 25, 2020 at 5pm PST. If no additional changes are made, a final rulemaking record will be submitted to the Office of Administrative Law. The OAL has 30 working days to review the record for approval.

PUTTING IT INTO PRACTICE: As companies are beginning to see how CCPA compliance is playing out in practice, now is the time to conduct an initial evaluation of successes and challenges and use the opportunity to submit additional comments to the Attorney General. Organizations should continue to be mindful that additional changes may be forthcoming – with potentially not a lot of time to review before the July enforcement date.

CHILDREN'S PRIVACY

Back to School Special: But I'm Just an Ad Network! Am I Subject to Children's Privacy Laws?

Posted August 28, 2020

As we wrote previously, kids are spending more of their days online and are using online platforms for virtual learning and entertainment. Much of this environment is funded through online advertising. All companies thus need to think about the impact that children's privacy laws, like COPPA, have on the online environment, as they will see the outcomes of this applicability in their contracts.

First, what obligations do third parties, such as ad networks and ones that provide third-party plug-ins have? As highlighted by the FTC in its FAQs, ad networks and providers of third-party plugins are subject to COPPA when they have "actual knowledge" that they collect personal information from children under 13. Such third parties have "actual knowledge" of collecting information from children where a child-directed content provider directly communicates the child-directed nature of its content to the third party or where the third party otherwise gains knowledge of the child-directed nature of the content. (FAQ E(1)).

Companies engaging with third party services like ad networks and providers of third-party plugins can thus expect to see COPPA-related elements built into their contracts. These might include reps and warranties that the company's website is not directed to children, the company does not have actual knowledge of children on its site, or the like. They should also expect to see the FTC paying attention to their use of these third-party tools on their websites. For example, this summer, the FTC settled with an app that had third-party ad networks collecting personal information from children through persistent identifiers used to target ads to children.

PUTTING IT INTO PRACTICE: We anticipate that the FTC will continue its scrutiny of the targeted ad environment. It is thus timely, if engaging in online advertising, to both review the FTC FAQs and contracts with ad networks and other similar third parties.

Back to School Special: Is My Multi-Age Platform Subject to Child Protection Requirements?

Posted August 27, 2020

In our online world, one of the challenges (and opportunities) for companies is the increased use of their websites, apps, and connected devices. For platforms directed to both adults and children, or platforms previously directed to adults which would like to now also direct their services to children, the FTC's recently streamlined FAQs, and ICPEN's guide (both of which we introduced earlier this week) can help companies in this space. The information is particularly helpful for those that were aimed mostly toward adults, and are now shifting their business plans to direct products or services to children as well.

First, an important reminder from both the FTC and ICPEN is that "online" privacy considerations for children do not just apply to websites, but apply to all connected services, including smart toys and applications. Second, we turn to examining if the platform is subject to COPPA or other child protection considerations. Platforms are subject to COPPA if they are "directed to children." The FTC's FAQs lay out factors from the COPPA Rule that the FTC will examine, including the age of people who appear on the site, the language used on the site, music or other content, and more. (FAQ D(1)). ICPEN uses similar factors, including the nature of the marketing content, the placement of the marketing and the audience and the use and appeal of the product or service.

For platforms that have both adults and children visitors, the question is thus whether or not it is directed to children. It is not, according to the FTC, just because some children happen to visit. That is a general audience platform, and the FTC's perspective is that COPPA would not apply unless the company has actual knowledge of the child's age. (FAQ H(1)). On the other hand, "mixed audience" sites are those that, for example, have both adults and children and one of the "intended audiences" are children. (FAQ D(3)). These mixed audience websites, the FTC makes clear, are still subject to COPPA. As such, requirements like obtaining prior parental consent (unless an exception exists), having appropriate notices, and the like, will apply.

PUTTING IT INTO PRACTICE: Looking to expand your website, app, or connected service into the youth market? Hosting a general audience platform where children might visit? The recently streamlined FTC FAQs as well as the ICPEN guides can help.

Back to School Special: Recordings, Photos, Kids, and Parental Consent

Posted August 26, 2020

In this remote era, companies are increasingly being approached by their business teams with ideas about products and services that involve video or audio recordings of their consumers. It may also involve letting people manipulate photos of themselves. Sometimes, those recordings and pictures are of children. Content that contain images or audio of individuals are considered personal information under many laws, including the Children's Online Privacy Protection Act (COPPA). What does this mean for companies? As we discussed in our previous blog post, COPPA requires obtaining parental consent if the personal information collected is being collected by the company online, and being collected *from* the child. The FTC's recently streamlined FAQs help companies find and understand obligations if collecting photos or recordings from children. Namely, a reminder that this content is personal, and does require verifiable parental consent before being collected.

The FAQs give some examples of when a company's activities might fall outside the consent obligations. One is if the company blurs the images of children's photos. (FAQ F(3)). Another is if the photo is uploaded by someone else (a parent, grandparent, etc.). The Rule, the FTC reminds companies, applies only when information is supplied *by the child*. (FAQ F(4)). Consent is also not required if photos are pre-screened to delete images of the child as well as any other personal information (geolocation metadata for example) and persistent identifiers that are collected are used only for internal app operations. (FAQ F(2)). Another exception is if the photo or video is stored on the user's device, and is not transmitted to the company. (FAQ F(5)). Finally, consent is not needed if the child's voice is collected to "replace the written word," i.e., in situations where a child can do a voice command). This exception applies only if the business maintains the file only for the brief time necessary for that purpose.

PUTTING IT INTO PRACTICE: While exceptions to obtaining parental consent exist under COPPA when collecting audio, video and photographs from children, companies should proceed with caution. The revamp of the FTC COPPA guidelines suggests that the FTC will be looking carefully at companies' activities in this area to ensure that they are properly collecting consent unless an exception applies.

Back to School Special: COPPA Consent in the COVID Era

Posted August 25, 2020

In the current pandemic era, kids are spending more time online, be it for school or entertainment. Companies are therefore gearing up for increased interaction with children online or through connected devices. As children around the globe return to school, whatever that return looks like, the FTC and the International Consumer Protection Enforcement Network (ICPEN) remind us that certain rules apply when dealing with kids online.

In the U.S., the Children's Online Privacy Protection Act (COPPA) requires parental consent to collect personal information from kids under the age of 13. There are exceptions, like getting the parent's information in order to seek consent, or responding one time to an inquiry from a child. There are also requirements under CCPA. Countries in the EU and countries with comprehensive privacy regimes also have laws that impact collecting information from children online. Most are not as specific as COPPA, which is where ICPEN's guidelines can be of help. Of the myriad requirements (notice, choice, etc.), we focus our first article in this series on one that is often forgotten: the need to get parental consent.

To help companies in this virtual world, the FTC recently published a "decluttered" version of its COPPA FAQs. ICPEN similarly recently released a set of online marketing best practices. While the FTC FAQs remain the same in substance, they are now more user-friendly and streamlined. This is timely as companies gear up for increased interaction with children in an online environment. As noted, one thing that companies often forget is that if collecting information online *from a child*, COPPA requires prior parental consent. ICPEN similarly recommends obtaining parental consent. (Principle 3, no. 38). In this back to school series, we will look at situations where consent might not be required including potential exceptions of situations where the law does not apply.

But first, what does parental consent look like? It will require specific disclosures (COPPA has several, including explaining how the child's information will be used, and ICPEN mirrors this). Consent can take many forms, including:

- Asking the parent to sign and return a consent form via mail, fax or electronic scan;
- Requiring payment for services by credit card, debit card, or other online payment system that provides notification of each discrete transaction to the primary account holder; and
- Asking the parent to call a toll-free number or connect to trained personnel via video conference.

PUTTING IT INTO PRACTICE: Businesses that collect personal information from a child online are required to obtain verifiable parental consent, and the FTC has tried to give some flexibility so that they can do so in ways that works for their product. When designing the approach, a good rule of thumb is that the chosen method must be reasonably calculated to ensure that the person providing consent is the child's parent.

KleptoCats Maker Settles with FTC Over Failure to Get Parental Consent

Posted June 29, 2020

HyperBeard, the makers of several children's mobile apps (including KleptoCats), recently settled with the FTC over failure to obtain verifiable parental consent before collecting children's personal information online, in violation of COPPA. In its complaint, the FTC argued that the HyperBeard apps were clearly directed to children. The apps contained brightly-colored animated characters, kid-friendly language, games that were easy to play, and were promoted on kids' websites and publications.

In the settlement, the company agreed to pay $150,000 in civil penalties and to delete the information it collected without obtaining appropriate parental consent. The $150,000 payment was in lieu of the $4,000,000 judgment entered against both the company and its CEO. Even still, in an unusual move, one of the commissioners dissented, stating that the penalty was too high in view of the (little) harm that resulted from the violation. The company and its officers also agreed to provide appropriate notice (as required by COPPA), as well as to get parental consent in the future.

PUTTING IT INTO PRACTICE: This settlement is a reminder that the FTC continues to scrutinize mobile apps for compliance with COPPA. Those that are "directed to children," as defined by the law, should think through the statute's notice and parental consent requirements.

COMMUNICATION PRIVACY

TCPA's 2015 Government Debt Collection Exception Struck Down – Now What?

Posted August 3, 2020

The Supreme Court's recent decision in *Barr v. American Association of Political Consultants* held the government-debt exception of the TCPA unconstitutional under the First Amendment's Free Speech Clause. This means that going forward, companies that make "debt-collection" calls on behalf of the federal government can only do so with the prior express written consent of the called individuals.

The plaintiffs in this case had argued that the TCPA violated the First Amendment because it was a content-based restriction on speech that did not serve a compelling governmental interest. Their concern related to the TCPA prohibition (in many situations) of unsolicited, automated calls to cell phones. In particular, the 2015 amendment to add a new exception only for unsolicited automated calls related to the collection of debts on behalf of the federal government. The American Association of Political Consultants and other political nonprofit organizations challenged this "government debt" exception on First Amendment grounds, arguing that the 2015 amendment favored speech made for collecting government debt over political and other speech.

By a 6 to 3 vote, the Supreme Court agreed and struck down the government-debt exception and affirmed the ruling of the Fourth Circuit. The Supreme Court concluded that the government could not exempt calls attempting to collect *government* debts while unsolicited calls to collect *private* debts remained illegal. Instead of striking down the entire statute, however, the court held the exception was severable from the rest of the TCPA. Therefore, only the government debt collection exception was thrown out. The rest of the TCPA still stands.

PUTTING IT INTO PRACTICE: The most significant outcome of this decision to leave the bulk of the TCPA intact. Although the government debt-collection exception was scrapped, the TCPA's prohibition on unsolicited automated calls to cell phones still applies to all calls except those made for an "emergency purpose." Government-debt calls are now treated the same as all other automated calls to cell phones—as they were before the 2015 amendment.

Maine Internet Privacy Law Survives Challenge

Posted July 21, 2020

Maine's internet privacy law has survived its first challenge from internet service providers earlier this month. As we previously discussed, here, this law prohibits the sale of certain information about customers' internet use by internet service providers and went into effect on July 1, 2020.

The Plaintiffs, made up of several trade associations that represent internet service providers who provide service in Maine, filed a Motion for Judgment on the Pleadings alleging that the statute is unconstitutional on the grounds that it violates the First and Fourteenth Amendments, is unconstitutionally void for vagueness, and is preempted by federal law. Defendant, Maine's Attorney General, Aaron Frey, filed a Cross Motion for Judgment on the Pleadings seeking judgment on the Plaintiffs' preemption claim.

The court denied the Plaintiffs' motion and granted the Defendant's motion to dismiss the preemption claims, finding, in part, that Maine's internet privacy law is an exercise of state regulatory authority that is anticipated by federal law.

PUTTING IT INTO PRACTICE: The Maine internet privacy law is in effect and has survived its first challenge. This case is a reminder that internet service providers should review their consumer information sharing practices if they have not done so already.

CONSUMER PRIVACY

2020 In Review: Ongoing Enforcement Actions and a Patchwork of Privacy Laws

Posted December 23, 2020

Throughout 2020 we saw many enforcement actions brought by EU and U.S. regulators. Whether for allegations of deception (misleading privacy representations) or unfairness (failure to protect information), COVID did not appear to slow down regulatory action. Laws that many companies forget about -or don't know as well- were enforced by regulators, as well as through class action lawsuits. This included the Children's Online Privacy Protection Act, Illinois's Biometric Information Privacy Act, and the Telephone Consumer Protection Act.

There are other laws that create a patchwork of requirements for organizations. They range from laws based on the type of entity (HIPAA, GLBA), to those that regulate the activities in which the entity engages (CAN-SPAM, TCPA), and laws designed to protect individuals from whom the company is collecting information (COPPA, FERPA).

PUTTING IT INTO PRACTICE: That enforcement did not slow down during 2020 signals that it likely will continue into 2021, and companies developing internal compliance programs will want to keep these actions –and the wide variety of laws that govern them– in mind (an upcoming publication we anticipate publishing with Thomson Reuters next year should help on this front).

2020 In Review: Exchanging Data with Business Partners

Posted December 22, 2020

Throughout 2020, companies have been negotiating with their business partners the issue of "selling" under CCPA. Is the partner a service provider? A third party? Is there an exchange of consideration? These issues will not likely go away in 2021, especially as we turn to addressing the CCPA modification, CPRA.

The final CCPA regulations passed in August did not provide the type of clarity that companies were hoping to receive, and that confusion may not disappear in 2021. Indeed, how companies can address disclosures about their possible sale of information is back on the regulatory table, with new proposed modifications to the CCPA regulation. As we wrote, the new proposed change (to the regulations, not CCPA itself), brings back the concept of a website "button." Companies that have business relationships internationally have needed to think not just about CCPA, but GDPR as well, which requires specific language when sharing personal information with third parties. The EU sought comments this year on standard language for sharing between controllers and processors of information, signaling that new language will be on the horizon in 2021.

PUTTING IT INTO PRACTICE: Companies sharing information with third parties will have much on their plates in 2021, as they think about requirements under laws like CCPA and GDPR. This is a good time to evaluate which relationships are priorities for contractual review, such as those entities with whom significant amounts of information, or sensitive information, is being exchanged.

Brazil's Comprehensive Privacy Law Now in Effect

Posted September 29, 2020

Following lots of legislative uncertainty, Brazil has now formally enacted the country's first general data protection law, *Lei Geral de Proteção de Dados*, or "LGPD." While administrative sanctions do not go into effect until August 1, 2021, individuals and public prosecutors can now bring claims for losses and damages. Indeed, at least one public civil action has already been filed. LGPD is the first comprehensive general data protection law in Latin America. It was modeled after the EU's GDPR. While there are many similarities, LGPD does introduce new concepts. Below are some of the key elements to keep in mind.

- **When does LGPD apply?** Like GDPR, LGPD has extraterritorial effect. A company does not need to be based in Brazil or otherwise have any physical presence for the law to apply. Generally, LGPD applies when an organization does any of the following: (i) processes personal data in Brazil; (ii) processes personal data that was collected in Brazil; or (iii) processes personal data to offer goods or services in Brazil.

- **Does LGPD provide rights to individuals?** Yes. While many of the rights are similar to those in GDPR, LGPD also introduces additional rights. In addition to GDPR-like rights of access, deletion, portability, LGPD also gives people a right to access information about those with whom an organization has shared the individual's data. It also calls for individual access to information on whether an organization holds particular data.

- **What are the requirements for transferring data?** Organizations may transfer personal data to other countries that provide an "adequate level of data protection." Brazil has not yet identified which countries it considers as providing an adequate level of protection. All other transfers require a valid legal transfer mechanism. While there are several available transfer methods, the two main ways organizations can transfer data include: (1) with the specific and express consent of the individual, which must be prior and separated from the other purposes and requisitions of consent; and (2) through contractual instruments such as binding corporate rules and standard clauses, committing the organization to comply with the LGPD principles, individual rights, and the Brazilian data protection regime. No specific model clauses or language are available yet.

- **Are there other record keeping requirements?** LGPD calls for record of processing requirements. There are also certain requirements for "impact reports."

- **Do we have to appoint a Data Protection Officer?** It depends. Companies that qualify as "controllers" are required to appoint a data protection officer. Unlike GDPR, there are no specific requirements for the qualifications of this individual.

PUTTING IT INTO PRACTICE: Many questions remain open as to the interpretation and enforcement of this law. Brazil's National Data Protection Authority (ANPD), the administrative agency tasked with enforcing administrative sanctions and issuing regulations under the LGPD, has not yet been established. In the meantime, organizations can begin reviewing their global privacy programs to assess any gaps in compliance. They may want to focus on, among other things, the differences between current rights processes and the rights anticipated under LGPD.

NIST Seeking Comments on Draft AI Principles

Posted August 24, 2020

The National Institute of Standards and Technology has issued a set of draft principles for "explainable" artificial intelligence and is accepting comments until October 15, 2020. The authors of the draft principles outline four ways that those who develop AI systems can ensure that consumers understand the decisions reached by AI systems. The four principles are:

1. **Explanation:** Delivering evidence and reasons for the decisions, which will vary depending on the consumer and may include (a) user benefit explanations, (b) those that attempt to garner support by society, (c) those that assist with compliance with laws, regulations, and safety standards, or (d) those that explain a benefit to the system operator (recommending a list of movies to watch).

2. **Meaningful:** Having systems that provide meaningful and understandable explanations to users, which will vary by context and by user.

3. **Explanation Accuracy:** Those explanations being correct reflections of the system's process for creating its outputs, which the authors analogize to an explanation by an individual that shows the mental processes the person took to reach the decision.

5. **Knowledge Limits:** Having the AI system work only when the conditions for which it was designed exist, and thus avoids giving results that are not reliable.

These principles follow similar guidance issued earlier this year by the FTC, as well as the European Parliament. As a non-regulatory federal agency (which sits within the US Department of Commerce), NIST's goal is to promote US commerce by advancing standards such as those set out in these principles. For this draft, NIST indicates that it is seeking to improve the level of trust users have in AI so that the systems are more easily and readily adopted and used.

PUTTING IT INTO PRACTICE: Companies that are developing AI systems will find these principles a helpful preview of what may become industry standard, and may want to submit comments (by email to explainable-AI@nist.gov) prior to the October 15, 2020 deadline. In the meantime, companies should keep in mind the existing direction from the FTC and the EU, which include human oversight and transparency of how AI systems reach their decisions.

FTC Provides Direction on AI Technology

Posted May 5, 2020

The FTC recently issued comments on how companies can use artificial intelligence tools without engaging in deceptive or unfair trade practices or running afoul of the Fair Credit Reporting Act. The FTC pointed to enforcement it has brought in this area, and recommended that companies keep in mind four key principles when using AI tools. While much of their advice draws on requirements for those that are subject to the Fair Credit Reporting Act (FCRA), there are lessons that may be useful for many.

The recommendations from the FTC include:

- *Transparency*: the FTC encourages companies to tell people if they are making automated decisions using AI tools. Such disclosures may be mandated under laws like the FCRA, if the entity is automating decision-making about credit eligibility, for example. The FTC also reminds companies not to be deceptive or secretive about use of AI tools (pointing to its Ashley Madison decision, where the company was found to have deceptively used false profiles to encourage sign-ups). In order to be transparent, the FTC stressed that companies need

to know "***what*** data is used in [the company's] model and ***how*** that data is used." The FTC cautioned companies to think about how they would describe to consumers the AI decisions made about them.

- *Fairness*: Here, the FTC reminded companies not to discriminate against protected classes by, for example, making decisions about credit based on zip codes, when those decisions have a "disparate impact" on groups protected under the Civil Rights Act. The FTC in its comments also instructed companies to ensure fairness by giving people the ability to both access and correct information, something required when the FCRA applies.

- *Accuracy*: The FCRA has requirements for accuracy. The FTC reminded companies that even if they are not providing consumer reports, they should still be concerned about accuracy, as information they compile may be used for consumer reporting purposes, and as such the FCRA may apply. The FTC also pointed to the world of consumer lending when looking for "lessons" on the accuracy front, recommending that companies ensure that AI models work, are validated, and are retested to ensure that they work as the company had originally intended.

- *Accountability*: The FTC stresses that companies should think about the impact their use of AI will have on consumers. As a resource, they direct companies to the FTC's 2016 Big Data report. Questions to ask include whether or not the data set being used is appropriately representative and if the model takes into account potential biases. The FTC suggests companies consider using independent standards or outside experts to hold themselves accountable.

PUTTING IT INTO PRACTICE: As automation tools become more common, these recommendations from the FTC can be helpful for companies to keep in mind. They signal expectations from the FTC, which are often enforced by the Commission after issuing signaling commentary like this to the industry.

FTC Releases 2019 Privacy and Security Year in Review

Posted March 4, 2020

The FTC recently released its annual privacy and security report, providing a snapshot of the issues focused on in the previous year. These reports are often looked at as a signal for insights into the agency's upcoming priorities. Generally, the report contains a summary of the FTC's enforcement, advocacy, and rulemaking actions from 2019, a year where we saw several record-setting fines. The report also discusses privacy/security workshops, consumer education, and international engagement. Some of the highlights from 2019 discussed in the report include:

- The FTC brought 13 cases against companies that allegedly made false promises related to the EU-US Privacy Shield. Since the framework's inception, the FTC has brought a total of 21 cases.

- In 2019, the FTC levied a 170 million dollar fine against YouTube and Google for COPPA violations (the largest COPPA fine to date).

- The 7 data security orders issued in 2019 signaled a number of new trends we can expect to continue (as we previously wrote about).

- There were 8 cases of violations of the Telemarketing Sales Rule. This includes first enforcement action against a VoIP provider.

- The public comment period for the Red Flags Rule, COPPA Rule, and GLB Privacy and Safeguards Rule all closed in 2019.

- On the advocacy front, the FTC submitted comments to the NIST's privacy framework. The agency also held a workshop on the future of the COPPA rule.

PUTTING IT INTO PRACTICE: 2020 is already proving to be an active year for privacy legislation and commentary in the US (both at the state and federal level). We expect the FTC to continue to be busy this year with issues such as COPPA and more substantive enforcement related to EU-US Privacy Shield compliance. With many frameworks and written discussions emerging on AI both domestically and abroad, it's likely the FTC may hold workshops and other public forums on the topic. We also anticipate there to be next steps from the public comment periods that concluded in 2019 for the three rules.

Final Draft of NIST Privacy Framework Released

Posted February 25, 2020

NIST recently released a final version of its Privacy Framework to incorporate public feedback in response to the draft it issued late last year. For organizations familiar with the NIST Cybersecurity Framework first released in 2014, the privacy framework follows a similar structure and it is intended to be used together.

The document details a voluntary approach to assist organizations managing privacy risks. Like the NIST Cybersecurity Framework, the Privacy Framework calls for a risk-based approach to protecting privacy information. The Privacy Framework includes three sections – the Core, Profiles, and Implementation Tiers. The Core is a set of privacy protection activities and outcomes divided into key categories and subcategories with discrete outcomes. A Profile represents an organization's current privacy activities or desired outcomes. Implementation Tiers provide a point of reference on how an organization views privacy risk and whether it has sufficient processes and resources in place to manage that risk. Tiers reflect a progression from informal, reactive responses to approaches that are agile and risk informed.

PUTTING IT INTO PRACTICE: The NIST framework may help companies as they benchmark and work to identify potential gaps in compliance with privacy laws. It should not be viewed as a one-size fits all approach – particularly for companies in regulated industries or subject to numerous privacy laws. Although the framework doesn't necessarily introduce significantly new concepts, we anticipate that companies could begin to see some business partners asking whether they adhere to or are familiar with this framework.

Getting Prepared for a Decade of Privacy

Posted January 14, 2020

As we get settled into the reality of living with both CCPA and GDPR, companies are looking for new approaches for keeping their privacy houses in order. CCPA reminds us that there is no end to new legislation: proposals are already coming in from states as varied as Nebraska, New Hampshire and Virginia. Similar legislative trends exist around the globe. How can companies be prepared to address this ever shifting legislative landscape? There are a few essential steps privacy officers can take, including (1) aligning the privacy team's efforts with the underlying corporate mission, (2) having a clear understanding of both the company's data and its use practices, and (3) having infrastructure in place that will allow for updates to notices and rights.

Privacy teams that have aligned their efforts with the company's underlying mission will have an easier time getting buy-in from fellow employees. They will likely also find leadership support much easier. Those who have a clear understanding of their data assets and use practices will find making updates to notices - to the extent legal notice requirements change - a much more achievable exercise. Finally, given all the changes to privacy laws that are being contemplated by states and around the globe, having mechanisms in place to implement new practices will prove crucial.

Putting it Into Practice: If past history is any indication, privacy laws and enforcement priorities will be shifting over the coming decade. Privacy teams may want to take a different approach to prepare for change. Learn more about privacy trends for 2020 and beyond in this *Law360* article.

CROSS-BORDER DATA TRANSFERS

New Year, Same Transfer (for now): Temporary Brexit Deal Keeps EEA-UK Data Flowing

Posted December 29, 2020

Many in the world have been watching the Brexit deal closely, including privacy lawyers and others who deal with global data transfers. Under the recently-announced deal, a temporary solution will allow companies to continue to transfer data between the UK and European Economic Area (EEA) as normal during a short post-Brexit transition period. As many know, transfers of personal data are restricted out of the EEA to third countries unless certain steps are taken or exceptions apply. One of those mechanisms being an EU determination that the country to which data is being transferred is "adequate." With the current transition period set to expire December 31, 2020, and no adequacy decision for the UK issued yet from the Commission, companies have been worrying about how to receive data from the EEA into the UK given its impending status as a "third country."

The Trade and Cooperation Agreement announced in these last days of December 2020 calls for data flows to continue unchanged to the UK for four months, extendable to six months. This agreement means that even though the UK is leaving the EU without an adequacy decision, the need for parties who are engaging in such transfers to take extra steps, including use of appropriate safeguards (as we have written about this year) or reliance on transfer derogations for the data transfers will not be triggered. This temporary period (lasting up to six months) will apply so long as the UK does not modify its existing data protection law and does not exercise certain provisions provided for in that law without EU agreement.

PUTTING IT INTO PRACTICE: While this transition period offers a reprieve for companies while we await the EU Commission's decision on adequacy, companies are reminded of the other obligations under GDPR that are also impacted by Brexit. This includes the possible need to appoint a representative in the EEA and to re-evaluate the impact to your lead supervisory authority.

2020 In Review: Dealing with Schrems II Fallout

Posted December 21, 2020

As 2020 comes to a close, we take this opportunity to look back at some of the more significant developments that we discussed in the blog this year. The first is the EU Court of Justice's Schrems II decision, finding that the EU-U.S. Privacy Shield was not a valid mechanism for transferring personal data from the EU to the U.S. Related decisions came out of Switzerland and Israel.

As a result of that decision, companies transferring data between the EU and the U.S. have had to rely on Standard Contractual Clauses, along with "additional steps" to make sure there are sufficient safeguards in place to protect the transferred data. The European Data Protection Board has, as we wrote, provided input on what might constitute such additional measures. Companies are working through this now, and anticipating changes that will be made to the SCCs themselves next year.

PUTTING IT INTO PRACTICE: The issue of data transfers from the EU to the U.S. was one of many developments from 2020 that we anticipate reverberating well into next year.

EU Seeking Comment on Revisions to Standard Contractual Clauses

Posted November 30, 2020

One of the methods US and EU companies rely on most frequently for the transfer of personal data from the EU to the US are standard contractual clauses. For the method to be acceptable as a valid basis for transfer of personal information, one critical step is for companies to use the version of the clauses as approved by the EU Commission. This has causes some confusion and concern, as the clauses predate GDPR and thus do not include provisions related to that 2018 law. Another area of confusion has been the recent criticism of the clauses as a valid method -alone- for transferring personal data to certain jurisdictions, including the US. (See proposed supplemental protection measures proposed by the European Data Protection Board to address this latter issue, which we discussed recently.)

Given these concerns, it has long been anticipated that the EU Commission would revisit and revise the clauses. It has done so, and is seeking comment on modifications to the clauses. Unlike the current SCCs, of which there are a few (including for transfers between two controllers, and transfers from controllers to processors), the new version has a variety of different provisions that the parties can select based on their respective roles (controller, processor). The updated clauses also take into account GDPR-required content, like data minimization and security. They also contemplate more thoroughly "onward transfers" of information, and allow for more parties to be signatories than under the current scheme.

Interested parties have until 10 December 2020 to comment on the draft. It is anticipated that a vote will be made on the clauses by the EU early next year, and they will be adopted shortly thereafter. There would then be a one-year grace period to allow companies to switch over from the current set of clauses to the new ones. The caveat, though, is that companies must use "necessary supplemental measures" to ensure that data is adequately protected. The EU is also seeking comment on controller-processor standard clauses to address general GDPR requirements (in Data Protection Agreements) when data is not being transferred out of the EU.

Putting it Into Practice: Until the new clauses are implemented, companies transferring data between the EU and the US will need to rely on current measures, which include the current set of SCCs, and keep in mind the EDPB's cautions around "supplementary measures" needed for protecting outbound data. While there is time before any new clauses come into effect, in anticipation of the new clauses, we expect EU companies transferring data will likely be auditing and mapping the data they transfer.

EDPB Sheds Post-Schrems II Light on Supplementary Measures for Data Transfers

Posted November 17, 2020

The EDPB recently published recommendations on additional security steps to take when transferring personal data out of the EU. As outlined in our previous series of posts, the EU found this summer that the EU-US Privacy Shield was an invalid mechanism for transferring personal information from the EU to the US. As an alternative for companies wishing to transfer personal information to the US from the EU, the EU pointed to standard contractual clauses. At the time, though, they caveated that controllers relying on the SCCs may have to use supplementary measures to protect outbound personal data. There was confusion, however, around what such additional measures should be. In this recent guidance, the EDPB recommends that companies exporting data out of the EU in reliance on SCCs take six steps. These are useful for review by exporting companies in the EU, as well as entities in the US. The latter can expect to be asked questions by their EU counterparties that relate to these steps:

- **Map out all transfers** out of the EU. While difficult, the EDPB noted, it stated in the guidance that knowing the destination of data is an important step to understanding the levels of data it is provided. A related step is limiting the amount of information transferred to that which is actually needed.

- Understand the **basis for the transfer** (SCCs, etc.). This, too, is an important fundamental step according to the EDPB.

- Determine if the **recipient's country has laws that would negatively impact safeguard measures**. These might include "the likelihood of public authorities' access to your data in a manner not in line with EU standards." When thinking about the legal context in the recipient country, the EDPB recommends that companies look to the context of the transfer, such as the reason for the transfer, industry sector, and format of the data being transferred (is it encrypted, for example?).

- Put **additional security measures** in place that will ensure the same level of protection as afforded in the EU. This is relevant to the extent that the exporter concludes that the recipient's country's laws would negatively impact security measures. An example of supplementary measures is using encryption and keeping the keys under the EU exporter's control. Or, adding provisions to the contract like transparency obligations, restrictions on onward sharing, requirements for internal policies, or data minimization requirements. The EDPB points out, though, that there may be times when there are no appropriate supplementary measures.

- Take **appropriate formal steps**, if needed, depending on the basis of the transfer. For example, if a company decides to modify the SCCs in a way that "contradicts" (i.e., substantively modifies the provisions of) the clauses, then supervisory authority authorization would be needed.

- **Regularly evaluate and monitor the security afforded** to the data that is exported. This includes staying current on the legal developments in the recipients' countries for things that might negatively impact the security of the data being exported.

The guidance is open to public comment until November 30, 2020. Companies interested in comment may want to consider this EDPB document in conjunction with the proposed modification to the Standard Contractual Clauses, issued by the European Commission and open for comment until December 10, 2020.

PUTTING IT INTO PRACTICE: Businesses relying on Standard Contractual Clauses for exporting data from the EU (including import into the US) may find these steps useful to better understand what the EDPB views as appropriate supplementary measures. US companies can expect more questions from their EU partners about the status of US laws, and may find EU companies asking for additional provisions above the SCCs.

Israel Follows Europe's Lead on Privacy Shield

Posted October 12, 2020

Israel's Privacy Protection Authority recently announced that Privacy Shield can no longer be relied on for data transfers between Israel and the United States. Israel did not have a direct Privacy Shield arrangement with the U.S., instead permitting the many Israeli companies that exchange data with their American counterparts to rely on a provision of its Privacy Protection Regulations that allows for transfers of data to any country that receives data from the EU under the same terms of such transfer.

In light of Israel's reliance on the EU's use of Privacy Shield, it is not surprising that Israel has followed suit in stating that Privacy Shield could no longer be relied upon for data transfers. The announcement does mention that standard contractual clauses that are approved by the EU are acceptable under the Israeli Privacy Protection Regulations.

This builds on the fallout from the Schrems II decision, which we have previously discussed. Companies relying on Privacy Shield will need to look to alternative methods for these data transfers, which could include consent or contractual clauses.

PUTTING IT INTO PRACTICE: Israel joins the EU in forcing to continue to adapt to the fallout from the Schrems II decision. Alternative mechanisms for data transfers from Israel to the US will need to meet Israel's Privacy Protection Regulations.

Impact of Swiss Privacy Shield Inadequacy Decision

Posted September 22, 2020

In a much anticipated ruling, this month the Swiss Data Protection Authority concluded that the EU-US Swiss Privacy Shield was no longer an adequate method for transferring personal information from Switzerland to the US. In reaching this decision, the Swiss data protection authority agreed with the recent, similar, EU decision of inadequacy. Like the EU, Switzerland anticipates those transferring personal information from Switzerland to the US to rely on standard contractual clauses. However like the EU, Switzerland cautions that companies should assess "on a case-by-case basis" whether the recipient provides sufficient protection.

The policy paper from the Swiss authority provides not only a list of factors that Swiss companies can take when determining whether to transfer data to the US, but also outlines the interplay between Swiss and EU laws (keeping in mind, of course, that Switzerland is not a member of the EU). Noting that Switzerland is not bound to the recent Schrems II decision that resulted in the downfall of the EU-US Privacy Shield adequacy, it did indicate times where EU courts would expect Swiss companies to observe EU law. With this in mind, the Swiss data protection authority felt it necessary to reassess the US-Swiss Privacy Shield, and in doing so, reached the same conclusion as the EU (i.e., that it was not adequate).

PUTTING IT INTO PRACTICE: This decision places transfers from Switzerland to the US on the same footing as those from the EU. Companies engaging in these activities will likely turn to Standard Contractual Clauses, but should keep in mind the suggestions raised by both the EU (which we covered here) and Switzerland when implementing them.

Schrems II Fallout Continued: Can Companies Rely on Consent?

Posted July 30, 2020

The EDPB has provided input about consent in its recent FAQs responding to the Schrems II invalidation of Privacy Shield. As we wrote about previously in this series, Schrems II impacted how companies transfer data from the EU to the U.S.. As background, under GDPR, consent from the individual can be relied on to transfer information from the EU to an entity outside of the EU's borders if three conditions exist. The EDPB reminded companies of these three conditions in its FAQs, drawing on prior guidance about consent:

1. The consent is explicit.

2. The consent is specific to a specific data transfer or set of transfers.

3. The consent is informed, including informing the individual about the risks to their information if it is sent outside of the EU's borders.

What does this mean for companies in practice? This decision is a reminder of takeaways from EDPB's prior guidance: consents are difficult to rely on when addressing large volumes of data transfers. As a result, companies will likely need to continue to use Standard Contractual Clauses, albeit with the additional review that we discussed in our prior article in this series.

Why the difficulty with consent? For transfers made because they are necessary for a contract between the company and the individual, the EDPB's original guidance explained that consent works if the transfer is "occasional," something the EDPB acknowledges is a case-by-case issue. A transfer made by a travel agency to a hotel was an example of an acceptable necessary transfer made based on consent given in the prior guidance. With respect to occasional transfers, two examples were given in the prior guidance. First, transferring the personal details of a sales manager who travels to third countries to his or her clients in those third countries in order to arrange meetings with the sales

manager and clients. Second, transferring personal information to a bank in a country outside of the EU in order to make a payment that the bank client requests be made. In sum, the EDPB guidance makes clear that consent cannot always be used.

PUTTING IT INTO PRACTICE: Since the advent of GDPR, it has become harder to rely on consent as a basis for mass transfers of data out of the EU. While in some circumstances consent may be viable, it will likely not be the "magic bullet" to solving Schrems II, and instead companies will likely need to rely on an "SCC plus" model.

EU Reaction to the Fall of Privacy Shied: The Rise of SCCs?

Posted July 29, 2020

Companies who transfer data from the EU to the U.S. are struggling to determine the appropriate basis under which they can make these transfers. Continuing our examination of the outcome of this decision, we think now about what companies can do for transfers of information from the EU to the U.S.

As we previously wrote at the time of the Schrems II decision, one of the alternate mechanisms for data transfers are Standard Contractual Clauses. While the court concluded that SCCs remained valid, it outlined restrictions that have been giving companies pause. Of note was the comment that companies relying on SCCs would need to take proactive roles in making sure that there was an "adequate level of protection" of data in the importing jurisdiction. In sum, companies can continue to rely on SCCs as a mechanism, but would need an "SCC plus" approach to address the need for adequate levels of protection, including the European Data Protection Board's concerns (described below).

To better understand how SCCs would be received in the wake of the Schrems II decision and what might constitute how to assess levels of protection, many have been watching the various EU countries' privacy authorities for guidance. Some, like the DPA for Hamburg, have called for revisions to and/or more scrutiny of the SCCs. Others, like France and Norway, indicated that they are "analyzing" the impact. Germany's conference of data protection authorities, the DSK, reiterated the need to assess adequate security if relying on SCCs (without indicating how specifically to do this). The European Data Protection Board for its part, confirmed that the SCCs "remain valid," but emphasized that in practice both the data importer and exporter should take context into account to make sure that protection is adequate.

To assist businesses, the EDPB recently issued a set of FAQs, where it reiterated the need for an assessment that "takes into account the circumstances of the transfers and supplementary measures you could put in place." These include "making sure that U.S. law does not impinge on the adequate level of protection." How, specifically, a company would go about making this determination was not covered in the FAQs.

PUTTING IT INTO PRACTICE: Companies who rely on SCCs for their data transfers from the EU to the U.S. will want to think about the context of the transfer in light of this recent EDPB direction. Many also anticipate that the wording of the SCCs may change in the future. Stay tuned to our next article discussing the limits of consent for data transfers from the EU to the US.

How to Rise from the Privacy Shield Ashes: A View from the U.S.

Posted July 28, 2020

U.S. companies are in a bind in the wake of the recent EU decision rejecting the validity of the Privacy Shield. While it is clear that the EU will not accept Privacy Shield participation as a basis for transferring data from the EU to the U.S., next steps for participants are unfortunately not clear cut. U.S. companies who participate in the Shield program face two decisions: (1) whether to continue participation in the Privacy Shield program and (2) what mechanism to rely on for data transfers from the EU to the U.S.

For the first, companies should keep in mind that the Department of Commerce and the FTC have both issued statements that -notwithstanding the EU decision- the Privacy Shield program *has not* been discontinued. Thus participants still need to follow the program's requirements, which include "inform[ing] individuals about . . . [their] participation in the Privacy Shield" and providing a link to the Shield list. (*See* Privacy Shield Framework, 1(a)(i)). This of course would need to be balanced with the need, under GDPR, to disclose the basis under which information is transferred from the EU to the U.S. (GDPR Art. 13(1)(f)). Both of these requirements are usually addressed in the privacy policy. One of the questions that has arisen since the decision because of GDPR's requirement has been: should we remove reference to the Shield in the policy since the EU doesn't view it as a valid mechanism? However removing this would, given the requirements of the Shield program, mean a company would first have to withdraw from the Shield program.

Companies may thus For those companies who have considered removing references to the Privacy Shield from their website privacy policies, they may find that they need to reference *both* their Privacy Shield participation *and* another data transfer mechanism in their privacy policies to address the U.S. issues. To the extent that a company wants to consider withdrawing from the Privacy Shield, they may want to wait to see if the Department of Commerce issues any direction. Currently, under the terms of the program, withdrawing companies must complete a questionnaire at the time of withdrawal and then annually, to verify that information collected while in the Shield program continues to be treated under the terms of the program.

PUTTING IT INTO PRACTICE: U.S. companies who are current participants in the Privacy Shield program may want to wait before making a decision about whether or not to withdraw. In the meantime, keep in mind the disclosure obligations that exist under the terms of the program when assessing your EU-U.S. data transfer mechanisms. Stay tuned for our next article, discussing the view of the Shield's demise from the EU perspective and the status of potential alternate data transfer mechanisms.

CJEU Invalidates Privacy Shield, But Upholds SCCs with Conditions

Posted July 16, 2020

On July 16, 2020, in the case colloquially known as "Schrems II," the Court of Justice of the European Union (CJEU) struck down the EU-US Privacy Shield, finding it an invalid mechanism for transferring data from the EU to the US. The CJEU concluded that the Standard Contractual Clauses (SCCs) are valid for the transfer of personal data outside the EU (which would include transfers to the US), with certain conditions.

Brief Background

The Schrems II case followed closely on the heels of the CJEU's decision in Schrems I (October 2015), which invalidated the EU-US Safe Habor Framework. In Schrems I, a key concern was that EU personal data might be at risk of being accessed and processed by the U.S. government once transferred. Schrems II then challenged the validity of SCCs for similar reasons advanced in Schrems I. The EU-US Privacy Shield was adopted in July 2016.

CJEU Decision

With regard to the SCCs, the CJEU judgment mainly followed the CJEU's Advocate General's non-binding opinion published on December 19, 2019. The CJEU stated that the SCCs provide sufficient protection for EU personal data, but emphasized the fact that EU organizations relying on them have an obligation to take a proactive role in evaluating, *prior* to any transfer, whether there is in fact an "adequate level of protection" for personal data in the importing jurisdiction. The CJEU noted that organizations may implement additional safeguards, over and above those contained in the SCCs – although it is unclear what those safeguards might include. The ruling also highlights the role that supervisory authorities should take in assessing and, where necessary, suspending and prohibiting transfers of personal data to an importing jurisdiction. Many anticipate that this decision will result in modifications to the standard contractual clauses, something that had been under discussion prior to the decision (as the SCCs predate GDPR).

While the CJEU AG's view was that the CJEU is not required to rule on the validity of the EU-US Privacy Shield in the context of Schrems II, as it was not specifically requested to consider this question, the CJEU decided to examine and rule on the validity of the framework. In finding the Privacy Shield invalid, the CJEU took the view that "the limitations on the protection of personal data arising from [U.S. domestic law] on the access and use by U.S. public authorities [...] are not circumscribed in a way that satisfies requirements that are essentially equivalent to those required under EU law, by the principle of proportionality, in so far as the surveillance programmes based on those provisions are not limited to what is strictly necessary." The CJEU also found that the EU-U.S. Privacy Shield framework does not grant EU individuals actionable rights before the courts against the US authorities.

PUTTING IT INTO PRACTICE: Companies who engage in transfers of personal information from the EU to the US will want to look at the basis on which they engage in that transfer. For those US companies who are Privacy Shield participants, keep in mind that although the EU has "invalidated" the program from the EU perspective, the program is a US-run one and still exists. We thus anticipate direction coming soon from the Department of Commerce regarding how to address participation and reference current Shield participation. In the meantime, changes in the basis for transfer will need to be made (such as standard contractual clauses). We also anticipate, however, modifications to the standard contractual clause regime, and will be watching those developments closely. Given the EU's concern around disclosures to the US government, companies may also want to review this aspect of their policies, procedures and data protection agreements. As solutions are fact specific, feel free to contact any one of the authors or your regular Sheppard Mullin contact for more information.

FTC Finalizes Five Settlements Regarding Privacy Shield Claims

Posted January 22, 2020

The FTC recently finalized settlements with five companies over allegations that they falsely claimed certification under the EU-U.S. Privacy Shield framework. In each complaint, the FTC alleged that DCR Workforce, Inc., Thru, Inc., LotaData, Inc., and 214 Technologies, Inc. made false and misleading representations when they stated that they participated under the Privacy Shield framework on their website when they were not participants under the framework. Additionally, in the complaint against EmpiriStat, Inc., the FTC alleged that EmpiriStat, Inc. made a false and misleading representations when it stated that it was a current participant under the Privacy Shield framework on its website after it had allowed its certification to lapse and had been warned by the U.S. Department of Commerce to take down its claim of participation.

As a part of the settlements, each company is prohibited from misrepresenting participation in the EU-U.S. Privacy Shield framework or any other privacy or security program sponsored by a government or self-regulatory or standard setting organization. Additionally, EmpiriStat, Inc. must continue to apply the Privacy Shield framework to any personal information it collected while participating in Privacy Shield.

These settlements appear to address a concern by the EU Commission, as we previously have discussed, that more companies should be examined for Privacy Shield compliance.

PUTTING IT INTO PRACTICE: The FTC continues to focus on Privacy Shield enforcement. It is a good reminder for those companies whose policies state they are participating in this framework to review their practices and ensure their certification is up to date.

DATA BREACH

Vermont Updates Data Breach Notification Law

Posted June 24, 2020

Vermont recently amended its data breach notification law. The changes will go into effect July 1, 2020. As amended, the definition of "personal information" now includes the following when combined with a consumer's first name or first initial and last name:

- Individual taxpayer identification number, passport number, military identification card number, or other identification number that originates from a government identification document that is commonly used to verify identity for a commercial transaction;
- Unique biometric data generated from measurements or technical analysis of human body characteristics used by the owner or licensee of the data to identify or authenticate the consumer, such as a fingerprint, retina or iris image, or other unique physical representation or digital representation of biometric data;
- Genetic information; and
- Health records or records of a wellness program or similar program of health promotion or disease prevention; a health care professional's medical diagnosis or treatment of the consumer; or a health insurance policy number.

The amended law also includes notification requirements for breaches of "login credentials" (a user name or e-mail address, in combination with a password or an answer to a security question, that together permit access to an online account). If a breach is limited to "login credentials" (and no other PII), the data collector is only required to notify the Attorney General or Department of Finance, as applicable, if the login credentials were acquired directly from the data collector or its agent.

PUTTING IT INTO PRACTICE: Beginning July 1, companies who suffer a breach that impacts login credentials will need to keep in mind the requirements under Vermont's law. Companies should also keep in mind the expanded definition of personal information.

SCOTUS Review of CFAA May Impact Analysis in Data Breach Notification Obligations

Posted May 18, 2020

For the first time, the U.S. Supreme Court has agreed to review the Computer Fraud and Abuse Act (CFAA) in *Van Buren v. United States*, No. 19-783. A federal circuit split exists on the issue of whether the statute can only be used against hackers and unauthorized users of electronic systems, or also against authorized users who use the information for unauthorized purposes. In the context of data breaches, companies sometimes look to interpretations of the meaning of "authorization" in CFAA cases to analyze whether notification obligations may exist.

Enacted in 1986 to combat the perceived growing threat of hackers, the CFAA makes it a federal crime to "access[] a computer without authorization or exceed[] authorized access, and thereby obtain[] information from any protected computer." In addition to criminal penalties, the CFAA contains a private right of action allowing any person who sustains damages or loss because of a CFAA violation to sue for damages or equitable relief. Our sister blog discusses the existing case law involving CFAA claims in more depth.

While a state-by-state inquiry, data breach notification obligations are generally triggered when there has been *unauthorized* acquisition or access of personal information. Data breach notification statutes do not define what constitutes authorization, and there is a lack of case law in the data breach notification laws analyzing what "authorization" means. However, case law interpreting CFAA has historically helped provide some guidance to organizations on this point.

For example, if an employee sends files to a personal email containing personal information that she uses in the normal course of her responsibilities, but those files are not otherwise acquired or accessed by anyone else, does that company have data breach notification obligations? Under the narrow view (held by the Second, Fourth, and Ninth Circuits), many would argue no. Under the narrow interpretation, if a person is given access to a computer or network (i.e., an employee) then he or she is authorized to access that computer regardless of his or her intent to misuse information or violate any policies that regulate use of the information. In contrast, the First, Fifth, Seventh, and Eleventh Circuits have held that accessing a computer for an improper purpose violates the CFAA, even if the person was otherwise authorized to access the information.

PUTTING IT INTO PRACTICE: How the Supreme Court decides *Van Buren* will transform the landscape for CFAA claims in trade secrets and employment litigation. Simultaneously, the decision should also bring much needed clarity to the definition of "authorization" in the context of data breach statutes, notification obligations, and ensuing data breach litigation.

D.C. Amends Data Breach Notification Law, Adds Security Requirements

Posted May 14, 2020

At the end of March, Washington, D.C. signed the Security Breach Protection Amendment Act of 2019, which adds some significant changes to D.C.'s existing data breach law, first enacted in 2007. The law is projected to take effect by June 13, 2020. Some of the major changes are summarized below.

Definition of "Personal Information" Expanded

The law adopts a broader definition, adding the following new data elements:

- individual taxpayer identification number, passport number, military identification number, or other unique identification number issued on a government document;
- financial account number or any other combination of numbers or codes that may allow access to an individual's financial or credit accounts;

- medical information, biometric data, genetic information, health insurance information, and DNA profile; and
- username or email address in combination with any authenticators necessary to access a person's account.

The law also includes a catch-all for any combination of enumerated data elements that would enable a person to commit identity theft.

Content Requirements for Individual Breach Notifications

The law creates new content requirements for individual notices. Namely, the notice must describe the types of data elements compromised, the contact information for the entity reporting the breach, the toll-free numbers for credit reporting agencies, the FTC, and the D.C. Attorney General. The notice must also include information on the right to obtain a security freeze free of charge and information about how to much such request.

Mandatory Breach Notification to the D.C. Attorney General

There is also a new requirement to report data breaches to the D.C. Attorney General if 50 or more D.C. residents have been affected. Notice must be made no event later than when notice is provided to affected D.C. residents. The law also includes specific content requirements for Attorney General notices, some of which include:

- the nature of the data breach;
- types of personal information compromised;
- the number of D.C. residents affected;
- the cause of the data breach;
- remedial steps taken; and
- a sample of the notice sent to affected D.C. residents.

Security Requirements

The law creates new security requirements for entities handing personal information of D.C. residents to implement and maintain "reasonable security safeguards" to protect personal information. Entities using third-party service providers must also have a written agreement in place requiring the service provider to implement appropriate security safeguards.

Credit Monitoring

The law now requires entities that experience a data breach of social security numbers or taxpayer identification numbers to offer free identity theft protection services to affected individuals for a period of at least 18 months. With this addition, D.C. joins just a small handful of other states with potential mandatory credit monitoring requirements.

PUTTING IT INTO PRACTICE: For companies with nationwide incident response plans, D.C.'s modified law will require some changes. Among these are the definition of personal information, the mandatory Attorney General notification, content requirements for individual notice, and potential mandatory credit monitoring.

DATA SECURITY

FTC Finalizes Guidance on Security and Privacy Control Baselines – SP 800-53B

Posted December 28, 2020

Alleging unfair and deceptive practices in violation of the FTC Act, the FTC recently entered into a settlement agreement with SkyMed International, Inc. The company sells travel emergency plans to individuals who sustain medical emergencies or injuries while traveling internationally, and has signed up -according to the FTC- thousands of consumers. During the sign-up process individuals provided the company with sensitive health information.

The FTC found that SkyMed mislead consumers into thinking that a government agency or other third party had reviewed SkyMed's services through placement on the SkyMed site of a "HIPAA compliance seal" when in fact no third party had reviewed the company's practices, much less determine that SkyMed's practices met the requirements of HIPAA. The FTC also found that the company had engaged in unfair practices by failing to properly secure customer information, which led to the exposure of a cloud database containing 130,000 consumers' health information. Upon learning of the exposure, SkyMed did notify impacted individuals. According to the FTC, the notice falsely stated that no medical information was impacted and that no information had been accessed by an unauthorized third party, when in fact the company's investigations did not substantiate either of these claims.

The FTC alleged that the reason for the exposure was because SkyMed had failed to implement reasonable security controls to protect personal information. Of concern for the FTC was the fact that SkyMed had no written information security policies; it stored consumer PII in plain text without adequate access controls; it failed to perform periodic risk assessments; and it did not adequately train employees or third party contractors. While SkyMed did not agree to the allegations in the FTC's complaint, it did agree as part of the recent settlement to:

- Not further misrepresent its privacy or security program.
- Provide an update notice to affected consumers regarding the unsecured cloud database.
- Implement a comprehensive information security program.
- Obtain an initial and biennial assessments of its information security program for 20 years.
- Annual certification to the FTC regarding its information security program.
- Report any future breach of personal information to FTC within 30 days of discovery.

PUTTING IT INTO PRACTICE: This settlement is a caution for companies to take care when putting together breach notification letters as the statements made in those notices will be scrutinized closely. This settlement also serves as a reminder for companies to examine their data security practices and to keep in mind the elements that the FTC views as reasonable, as well as to avoid making statements -or using "seals"- that might be viewed as misleading and deceptive.

NIST Finalizes Guidance on Security and Privacy Control Baselines – SP 800-53B

Posted November 6, 2020

NIST has now finalized its guidance providing important information on selecting both security and privacy control baselines for the Federal Government. The guidance is available here: Special Publication 800-53B, Control Baselines for Information Systems and Organizations. As we previously discussed when the draft version was released, these control baselines are from NIST Special Publication 800-53, and have been moved to this separate publication as a consolidated catalog of privacy and security controls. While the implementation of a minimum set of controls is required for protecting federal information systems, NIST envisions that these control baselines can be implemented by any organization that processes, stores, or transmits information.

The overall purpose and intent of the guidance has not changed since we last reviewed the draft guidance, which you can review here. However, edits were made in the finalization process and this final version should be thoughtfully reviewed when implementing the control baselines.

PUTTING IT INTO PRACTICE: Now that this guidance is final, federal contractors should review carefully as these new security and privacy baselines will be applied to any federal information system used or operated by a contractor on behalf of an agency, or another organization on behalf of an agency. Companies in the private sector should pay attention as well, as NIST guidance is often used as a basis for industry standards in security and privacy.

Interim Rule Solidifies Cybersecurity Requirements for Defense Industrial Base

Posted October 9, 2020

The Department of Defense (DoD) recently published an interim rule that sets forth its Cybersecurity Maturity Model Certification (CMMC) program plan, as well as new requirements for a "NIST SP 800-171 DoD Assessment Methodology." NIST SP 800-171 relates to protection of sensitive, but unclassified information (within a company's system.) The interim rule will be effective November 30, 2020, and comments are due the same day. You can read our in-depth breakdown of the key provisions here.

The interim rule has an immediate effect for DoD contractors and subcontractors that are already required to comply with the security controls in NIST SP 800-171, as it institutes a new assessment and reporting system to verify compliance prior to contract award. With respect to the CMMC, the interim rule largely is consistent with what DoD previously has shared (see our articles here and here for more information). CMMC requirements may be included in solicitations and contracts through September 30, 2025 only where approved by the Office of the Under Secretary of Defense for Acquisition and Sustainment. On or after October 1, 2025, CMMC will apply to all DoD solicitations and contracts (with very limited exceptions, including procurements solely for commercially available off-the-shelf items).

PUTTING IT INTO PRACTICE: This rule has immediate implications for all companies that do business with DoD (either directly or indirectly). DoD contractors (and subcontractors) need to assess what type(s) of information they have as well as which assessment(s) will apply to them. Companies outside of the Defense Industrial Base can benefit from following closely what DoD is doing as it is expected other government agencies and regulators will adopt the same or a similar approach for cybersecurity in the near future.

NIST Issues Long-Awaited Final Guidance on Security and Privacy Controls – SP 800-53

Posted October 5, 2020

After many years of being in draft form, NIST recently released its final version of Revision 5 of Special Publication 800-53, Security and Privacy Controls for Information Systems and Organizations to address a need for a more proactive and systematic approach to cybersecurity. With the release of Revision 5, NIST hopes to provide updated security and privacy controls that will make information systems more penetration resistant, limit damages from cyber-attacks, make systems more cyber-resilient, and protect individuals' privacy. NIST intends this update to be usable by a more diverse set of consumer groups than previous iterations of the document permitted.

The following are the most significant updates provided by Revision 5:

- Removal of assignment of control responsibility to either the organization or information system to make the controls more outcome-based.

- Integration of the information security and privacy controls into a consolidated control catalogue for organizations and information systems.
- Establishment of a supply chain risk management control family.
- Separation of control selection processes from the controls to allow the controls to be used by different communities of interest.
- Removing control baselines and tailoring guidance and transferring that information to NIST SP 800-53B, Control Baselines for Information Systems and Organizations.
- Clarifying the relationship between requirements and controls and the relationship between security and privacy controls.
- Incorporating new, state-of-the-practice controls based on the latest threat intelligence and cyber-attack data.

These controls are mandatory for federal information systems, which include any information system used or operated by an agency or by a contractor on behalf of an agency. Companies will want to review these controls carefully and consider implementing where appropriate, as NIST controls are often used as a baseline for industry standards in security and privacy and are likely to be seen as "reasonable" for purposes of compliance with broader data security laws.

NIST is also releasing supplemental materials that will be available in the near future. Among these materials will be a comparison of Revision 5 with Revision 4 and control mappings to the Cybersecurity and Privacy Frameworks.

PUTTING IT INTO PRACTICE: Federal contractors should review these guidelines closely as these updated controls will be applied to any federal information system used or operated by a contractor on behalf of an agency. Other organizations in the private sector should pay attention as NIST guidance often influences industry standards in security and privacy.

What the First Enforcement Action under NYDFS Cybersecurity Reg Means to Companies

Posted September 23, 2020

Late this summer the New York Department of Financial Services (NYDFS) announced its first enforcement action since the cybersecurity rules went into effect in March 2017. The action was brought against First American Title Insurance Co. as a result of a 2018 data breach exposing 850 million customer records containing sensitive personal information.

NYDFS charged First American with violating six provisions of the Cybersecurity Regulation, arguing that, among other violations, First American:

- failed to utilize risk assessments, security reviews, and its own cybersecurity policies when investigating the vulnerability and sensitive data associated with the vulnerability;
- misclassified the vulnerability as a "low" severity, and subsequently failed to investigate under the criteria set forth in its cybersecurity policies;
- did not conduct a reasonable investigation into the vulnerability even after its detection in December 2018, and instead only reviewed 10 of the millions of exposed documents; and
- failed to follow the advice of its own in-house cybersecurity team to further investigate and remedy the vulnerability.

The statement of charges highlight the NYDFS's cybersecurity concerns. Namely that a company: (i) encrypt documents containing non-public information (NPI); (ii) limit user access to NPI through access controls, and (iii) provide regular cybersecurity awareness training, as required by the regulations. The NYDFS is seeking civil monetary penalties and an order to remedy the alleged violations, and a hearing is set for October 26.

The NYDFS is not alone in its pursuit to hold companies accountable for what it perceives are failures to implement adequate cybersecurity measures and adequately respond to data incidents. The New York Attorney General's office has similarly recently pursued enforcement actions against companies the AG's office believes have failed to adequately respond to data incidents and address cybersecurity, with the settlement of at least one such enforcement action requiring augmentation of cybersecurity practices, detailed incident response procedures, and the payment of fines.

PUTTING IT INTO PRACTICE: The enforcement action highlights the importance that should be placed on properly assessing and categorizing the severity of risks associated with cybersecurity vulnerabilities and taking swift and necessary action to respond to such risks. It also serves as a reminder of the expectation that companies have, test, and internal policies and procedures for incident response. Lastly, employees responsible for addressing remediation items identified in the aftermath of a security incident should be armed with appropriate resources and background to effectuate change. Without measured, proactive attention to cybersecurity and incident response, companies could face enforcement actions and fines and penalties following the disclosure of a data breach.

NIST Issues Draft Guidance on Security and Privacy Control Baselines – SP 800-53B

Posted August 6, 2020

NIST's new draft guidance, Special Publication 800-53B, Control Baselines for Information Systems and Organizations, provides important information on selecting both security and privacy control baselines for the Federal Government. These control baselines are from NIST Special Publication 800-53 and have been moved to this separate publication "so the SP 800-53 [can] serve as a consolidated catalog of security and privacy controls regardless of how those controls [are] used by different communities of interest." The new guidance addresses federal information systems and is applicable to information systems used or operated by an agency, a contractor on behalf of an agency, or another organization on behalf of an agency.

This guidance provides security control baselines for low, moderate, and high-impact systems and an initial privacy baseline for meeting and managing privacy risks that arise from processing personally identifiable information. These control baselines are organized and mapped out to 20 control families from SP 800-53 (Revision 5), including Personally Identifiable Information Processing and Transparency and Supply Chain Risk Management. It also outlines a tailoring process in which companies can align their controls to more closely address the specific security and privacy requirements required by their specific circumstances. The goal of this process is to provide cost-effective solutions to support organizational missions and business needs along with adequate security and privacy protections commensurate with risk.

Companies can tailor the control baselines through use of common controls, applying scoping considerations, selecting compensating controls, assigning control parameter values, supplementing control baselines, or providing specification information for control implementation.

When making tailoring decisions, companies need to address every control in the selected baseline and document the rationale of the tailoring decisions. In particular, if a control is determined not to be needed, the rationale must be recorded in the system and in the security plans, which must be subsequently approved by responsible individuals within the company.

NIST is soliciting comments on this draft guidance through the end of the public comment period on September 11, 2020.

PUTTING IT INTO PRACTICE: Federal contractors should pay close attention to these guidelines as these new security and privacy baselines will be applied to any federal information system used or operated by a contractor on behalf of an agency, or another organization on behalf of an agency. Companies in the private sector should pay attention as well, as NIST guidance is often used as a basis for industry standards in security and privacy.

NIST Proposes Draft Enhanced Security Requirements for Protecting CUI

Posted July 28, 2020

NIST recently released the final public draft of SP 800-172, Enhanced Security Requirements for Protecting Controlled Unclassified Information: A Supplement to NIST Special Publication 800-171 (formerly Draft NIST SP 800-171B). NIST is proposing additional security requirements for certain CUI in non-federal systems that is associated with critical programs or high value assets and is soliciting public comments through August 21, 2020.

The enhanced security requirements focus on promoting (1) penetration-resistant architecture, (2) damage-limiting operations, and (3) designs to achieve cyber resiliency and survivability. While these requirements apply to critical programs and high value assets, NIST did not include guidance on determining which organizational programs or assets fall under these categories. Such determinations will be left to organizations/agencies mandating the use of the enhanced security requirements and such organizations should look to applicable laws, executive orders, directives, regulations or policies.

NIST envisions that federal agencies can implement these enhanced security requirements comprehensively or they may select a subset of requirements as a part of their risk management strategy. Federal contractors can expect that agencies may contractually require certain enhanced security requirements contained in the publication regarding the handling of CUI.

The enhanced security requirements themselves are derived from the security controls in SP 800-53, which focuses on the security of government systems, and are particularly focused on the following elements, which are essential for addressing advanced persistent threats:

- Applying a threat-centric approach to security requirements specification;
- Employing alternative system and security architectures that support logical and physical isolation using system and network segmentation techniques, virtual machines, and containers
- Implementing dual authorization controls for the most critical or sensitive operations;
- Limiting persistent storage to isolated enclaves or domains;
- Implementing a comply-to-connect approach for systems and networks;
- Extending configuration management requirements by establishing authoritative sources for addressing changes to systems and system components;
- Periodically refreshing or upgrading organizational systems and system components to a known state or developing new systems or components;
- Employing a security operations center with advanced analytics to support continuous monitoring and protection of organizational systems; and

- Using deception to confuse and mislead adversaries regarding the information they use for decision-making, the value and authenticity of the information they attempt to exfiltrate, or the environment in which they are operating.

PUTTING IT INTO PRACTICE: While not finalized yet, companies that contract with the federal government and have access to CUI associated with critical programs or high value assets should consider how these enhanced security requirements may affect their operations. NIST is accepting comments from the public on SP 800-172 until August 21, 2020.

NIST Releases Cybersecurity Guidance for Manufacturers of IoT Devices

Posted June 18, 2020

As a part of its Cybersecurity for IoT Program, NIST recently released two publications with the goal of providing cybersecurity guidance and best practices specific for companies manufacturing IoT devices. These publications were developed as a part of NIST's implementation of the 2017 Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure. With these publications, NIST provides a set of recommended activities that manufacturers should consider to improve the securability of IoT devices, as well as a baseline level of security requirements for these devices.

The first, NISTIR 8259, provides device manufacturers of new IoT devices with a map of recommended activities to help address cybersecurity in the product development process. There are six recommended activities, four of which address identifying and implementing appropriate security controls in the pre-market phase and two that focus on meeting customers' cybersecurity needs once the device is on the market. These activities focus on identifying a device's customers and their cybersecurity needs, meeting those cybersecurity needs and planning for how cybersecurity will be addressed once the device is out on the market.

NISTIR 8259A sets out a core baseline of security requirements generally needed to support commonly used cybersecurity controls. At a high level, this core baseline requires the following:

- *Device identification:* The individual device can be identified both logically and physically.
- *Device configuration:* An IoT device's software configuration can be changed and such changes can only be performed by authorized entities.
- *Device protection:* The data from an IoT device is protected from unauthorized access or modification, both in storage and transit.
- *Logical access interfaces:* Only authorized entities should have logical access to local and network interfaces, and the protocols and services used by those interfaces.
- *Software update:* The IoT device's software can be updated by authorized entities.
- *Cybersecurity state awareness:* An IoT device can report on its cybersecurity state to authorized entities only.

As we have noted before, the security of IoT devices is increasingly regulated at both the federal and state level. NIST has indicated that it is adapting NISTIRs 8259 and 8259A to enable federal government agency adoption of more secure IoT devices. We also expect legislative activity around IoT security to continue and will be keeping a close eye on any developments in this area.

PUTTING IT INTO PRACTICE: While implementation of the security controls included in these two publications is not required by law, this guidance likely will be referenced when determining the reasonableness of IoT device security. Device manufacturers, particularly those that sell or seek to sell to the government, should assume security requirements similar to those in the recent NIST publications will become the standard and should take these two guidance documents into consideration when designing and implementing cybersecurity controls in new IoT devices.

CISA Issues First Installment of Cyber Essentials

Posted June 2, 2020

On Friday, May 29, the Cybersecurity and Infrastructure Security Agency (CISA) issued the first in a series of six Cyber Essentials Toolkits. These toolkits are described as "bite-sized actions for IT and C-suite leadership to work toward full implementation of each Cyber Essential," focused on building a company's cyber readiness.

The first of these elements, entitled "Essential Element: Yourself, the Leader," is a short, two-page document packed with advice and links to additional resources. It lists four essential actions for leaders of organizations:

- Approach cyber as a business risk;
- Determine how much of your organization's operations are dependent on IT;
- Lead investment in basic cybersecurity; and
- Build a network of trusted relationships for access to timely cyber threat information.
- Added to these is a fifth essential action that leaders should discuss with IT Staff or Service Providers:
- Lead development of cybersecurity policies.
- Each of these five essentials is accompanied by discussion, as well as descriptions of additional resources available on the topic and links to those resources. These include resources such as a document on "Questions Every CEO Should Ask About Cyber Risks," the Cyber Readiness Institute and the National Cyber Security Alliance, and of course NIST, the National Institute of Standards and Technology.

PUTTING IT INTO PRACTICE: For a two-page document, the first Cyber Essentials Toolkit is packed with useful information. Corporate leadership that fears they are not on top of their organization's cybersecurity should review the document and its resources to launch an initiative to catch up. Those leaders who believe their cyber readiness is on par should review it to confirm they are doing things right and have not missed a key element for their program.

Privacy and Data Protection Enactment and Enforcement Timelines During COVID-19

Posted April 24, 2020

During COVID-19, in certain areas of the law, we have seen significant flexibility from regulators and government agencies in how they are addressing typical approval processes and/or compliance requirements. In the context of privacy and cybersecurity regulations, largely, regulators are emphasizing that personal privacy and data security are important now more than ever. New information is being collected and used in new ways. Certain data security vulnerabilities may be more prevalent in this work-from-home environment.

The below summarizes the status of enactments, deadlines, and other public comments from regulators surrounding privacy and data security laws globally.

- **California Consumer Privacy Act (CCPA)**. CCPA became effective January 1, 2020. While the regulations are still not yet final, the Attorney General is permitted to begin bringing enforcement actions on July 1, 2020. Despite urging from various coalitions and trade associations to delay enforcement, a statement from the AG's office said that CCPA has been effect since January 1, 2020 and that the agency is committed to enforcing the law starting July 1. The office also "encourage[s] businesses to be particularly mindful of data security in this time of emergency."

- **23 NYCRR Part 500**. Financial services companies subject to New York's cybersecurity law typically must file a Certification of Compliance annually by April 15. DFS announced that it has extended its original deadline to June 1, 2020.

- **HIPAA**. As we reported on in more detail here, HHS has released a limited waiver allowing for certain PHI disclosures, provided other requirements under the business associate agreement are still met, and the BA informs the covered entity within 10 days after the use or disclosure occurs.

- **Brazil's Data Protection Law**. Brazil's first comprehensive data protection law – LGPD – was schedule to become effective August 2020. In early April, the Brazilian Senate approved a bill which would delay the effective date of the law until January 2021. In the bill, fines and sanctions for companies that fail to comply are now scheduled to become effective August 2021. The bill is now with the House of Delegates for consideration and if approved, will be sent to the President to be signed into law.

- **Global Data Protection Regulation (GDPR)**. The EDPB has stated that businesses are not exempt from complying with the GDPR and ensuring the protection of personal data "even in these exceptional times." While there has been nothing to signal that requirements of the laws themselves should be lessened, certain regulators, such as the UK's ICO, has signaled that when it comes to enforcement, they will take a pragmatic approach in the context of this crisis.

PUTTING IT INTO PRACTICE: Organizations should continue to be mindful of the laws that surround the collection, use, and sharing of information both in the US and abroad. While these are extraordinary times, regulators are continuing to signal that privacy and data protection laws still apply (even if certain deadlines may be extended in particular circumstances). For organizations subject to CCPA, a reminder that the AG can consider activity as early as January 1, 2020 when it comes to enforcement.

FTC Settles with Company Over Alleged Deceptive Security Practices

Posted April 21, 2020

The FTC recently settled with smart lock maker Tapplock, Inc., a Canadian company, over allegations that it deceived consumers with false claims about its product's security practices. These allegations arose based on vulnerabilities that a security researcher demonstrated – not in the aftermath of a data security breach where these complaints often originate.

In its complaint, the FTC cited claims Tapplock made in its product advertisements, including that the product was "secure," with an "unbreakable" design. The FTC also noted that Tapplock's privacy policy stated that the company deployed "reasonable precautions and follow[s] industry best practices to make sure [personal information] is not inappropriately lost, misused, accessed, disclosed, altered or destroyed."

However, security researchers pointed out a number of alleged physical and electronic vulnerabilities. For example, by unscrewing the back panel, a researcher was able to unlock the product within a few seconds. The lack of encryption on the Bluetooth communication between the lock and the app also allowed a researcher to discover and replicate the private keys necessary to lock and unlock the product. There were also issues with how user access was revoked, essentially allowing even revoked users an ability to later authenticate access to another user's lock.

The FTC alleged that these product vulnerabilities, combined with a lack of certain compliance measures such as: vulnerability testing, written data security policies and procedures, and privacy and security guidance and training for employees designing the software meant that the company was contrary to its security claims of "reasonable precautions" and "industry best practices."

As part of the settlement, Tapplock will be required to implement a comprehensive information security program, train employees at least once a year on safeguarding personal information, use certain data access controls, and conduct vendor management. Tapplock must also obtain independent third-party assessments of its program every two years and submit that assessment to the FTC for approval.

PUTTING IT INTO PRACTICE: This settlement highlights that even in the absence of a data breach, the FTC may look to researchers and other evidence finding security vulnerabilities in products and services that may be contrary to claims made about privacy and security. This settlement also highlights the importance and value the FTC (like other regulators) places on having written information security policies and procedures, regular data security training for employees, and periodic vulnerability tests and security audits; companies will be served by acting proactively to implement or establish such compliance measures. For organizations based outside the US, this settlement also serves as a reminder of certain factors the FTC may look to when evaluating whether a non-US company is targeting US consumers. Namely, the FTC cited the fact that the product was advertised in U.S. dollars, and fulfilled by a service provider in the US and shipped to a US-based warehouse (and the website refenced this fact).

Turn on the Camera Part Two: Are You Prepared to Handle a Breach Remotely and Do You Know Your Legal Security Obligations?

Posted March 12, 2020

During their COVID-19 preparations, companies are dusting off -and deploying- their business continuity plans. Also worth revisiting are incident response plans. Teams working remotely, if faced with a data breach, will still face privilege issues. For this reason simply moving to asynchronous forms of communication (email, chat, etc.) may not suffice, or may increase legal risk and exposure. Teams will thus need to be prepared for coming together virtually. Turning on the camera to converse remotely with video can be an impactful and important way to effectively handle a breach situation. To prepare, here are three key questions companies can consider:

1. In the event of a data breach, is your incident team prepared to handle the situation remotely?

2. What steps will be taken to bring people together? Have those steps been practiced?

3. Does everyone on the team fully understand how to use virtual technologies, have cameras on their devices, and understand those cameras' benefits?

In addition to thinking about data breach response, many companies will want to bear in mind the obligations to protect personal information. There are many jurisdictions with laws that govern how companies must protect information. These laws would apply to information the company already holds, and may also apply to new personal information that might be collected during a company's COVID-19 response (see more about this in the first post in this series). For example, as we have written in the past, New York's data protection law will go into effect on

March 21, and other states already have data security laws in place with specific requirements, including notably Massachusetts and Nevada. And other states, like Ohio provide companies that suffer a breach certain safe harbors if they have security programs in place.

PUTTING IT INTO PRACTICE: As companies reflect on (and use) their business continuity plans, thought should be made to breach response plans, and how teams will handle the -hopefully unlikely event- that they must address a breach with an entirely virtual team. At the same time, thought should be given to the legal data privacy protections that exist, and what steps companies are taking to meet those obligations.

NY SHIELD Act Data Security Requirements Effective This Month

Posted March 9, 2020

Businesses collecting personal information from New York residents will soon be expected to apply enhanced data security requirements. The New York SHIELD Act, signed into law in July 2019, expanded breach notice requirements in October 2019. Now, On March 21, 2020, the remaining provisions related to data security will also come into effect. As we wrote previously, businesses subject to the law must implement data security programs that include at least the following:

- **Reasonable administrative safeguards**, including: designate one or more employees to coordinate the security program; identification of internal and external risks and safeguards to control the risks; train employees on security practices; select service providers capable of maintaining appropriate safeguards (and contractually require said safeguards);

- **Reasonable technical safeguards**, including: assess risks in network and software design; regularly test and monitor effectiveness of controls, systems, and procedures; and

- **Reasonable physical safeguards**, including: assess risks of information storage and disposal; dispose of private information within a reasonable amount of time after it's no longer needed for a business purpose; erase information so that it cannot be read or reconstructed.

There are some limited exceptions. Organizations otherwise regulated by federal law such as GLBA and HIPAA are exempt. There is also an exception for small businesses of fewer than 50 employees, less than $3 million in gross revenues in each of last three (3) fiscal years, or less than $5 million in year-end total assets. These "small businesses" may scale their data security program according to their size and complexity, the nature and scope of its business activities, and the nature and sensitivity of the information collected.

PUTTING IT INTO PRACTICE: New York joins other states (including Massachusetts, Nevada and Oregon) to require specific data security protections. Companies who have nationwide security programs in place will want to conduct a gap assessment to verify whether their existing program meets New York's requirements.

Buyers (And Sellers) Beware!: SEC Observations on Cybersecurity and Resiliency

Posted March 2, 2020

The Securities and Exchange Commission recently published a set of observations designed to assist financial market participants. While not legally binding, the observations are guideposts for investment companies, securities issuers, and others. They outline steps to improve cyber preparedness and to protect against well-known and evolving cybersecurity threats faced by companies in the United States and worldwide.

The observations come from the SEC's Office of Compliance Inspections and Examinations. The OCIE operates the SEC's National Exam Program, which is a risk-based inspection program intended to protect investors and ensure market integrity. OCIE collects and analyzes information on various measures that have been taken by market participants. Information gathered includes information about governance and risk management, access rights, and data loss prevention. OCIE also looks at mobile security, incident response resiliency and vendor management. Finally, OCIE looks at training and awareness as well.

The recently-issued observations provide specific examples of policies and practices that U.S. market participants have undertaken to protect sensitive data. Effective cybersecurity programs, the SEC noted, include those that look comprehensively at their risks. They also implement vulnerability scanning and monitor network traffic and detect security threats. The SEC also found effective programs are ones that had mobile device management and risk-assessed incident response plans for data breaches. The OCIE did recognize, though, that there is no "one-size fits all" approach for cybersecurity.

PUTTING IT INTO PRACTICE: These observations give companies ideas about steps the SEC expects they will have taken to evaluate current cyber-risk infrastructure and make potentially-needed upgrades. While aimed at the financial markets, these recommendations may be helpful benchmarks for others as well.

CMMC Version 1.0: Enhancing DOD's Supply Chain Cybersecurity

Posted February 12, 2020

Cybersecurity Maturity Model Certification ("CMMC") v.1.0, after releasing several draft versions of the document over the past year. In an effort to enhance supply chain security, the CMMC sets forth unified cybersecurity standards that DOD contractors and suppliers (at all tiers, regardless of size or function) must meet to participate in future DOD acquisitions. Through the CMMC, DOD adds cybersecurity as a foundational element to the current DOD acquisition criteria of cost, schedule, and performance. We have previously discussed CMMC on our Government Contracts & Investigations Blog.

CMMC Maturity Levels

The CMMC includes five levels of certification, with five being the highest or most secure. This table provides a snapshot of the focus areas, number of practices, and requirements at each level:

CMMC Level	Primary Focus Area	Total Practices	Underlying Requirements
Level 1: Basic Cyber Hygiene	Basic safeguarding of Federal Contract Information (FCI).	17	17 practices that comply with FAR 48 CFR 52.204-21.
Level 2: Intermediate Cyber Hygiene	Transition step to protecting Controlled Unclassified Information (CUI).	72	Level 1, plus 48 selected practices from NIST SP 800-171 r1, and an additional 7 practices.
Level 3: Good Cyber Hygiene	Protecting CUI.	130	Level 1 and Level 2, plus 58 additional practices (all NIST SP 800-171 r1, and others).
Level 4: Proactive	Protecting CUI and reducing the risk of Advanced Persistent Threats (APTs).	156	Levels 1-3, plus an additional 26 (from Draft NIST SP 800-171B and others).
Level 5: Advanced/Progressive	Protecting CUI and reducing the risk of APTs.	171	Levels 1-4, plus an additional 15 practices (from Draft NIST SP 800-171B and others).

Source of information: CMMC v.1, Sec. 2.7.1, available here.

Timeline
The DOD has expressed its commitment to a "crawl, walk, run" approach to implementing the CMMC. So, although CMMC v.1.0 was released last month, there will be a five-year rollout period, with all new DOD contracts containing the CMMC requirement beginning in FY 2026, but some could start requiring it as soon as this summer.

PUTTING IT INTO PRACTICE: Any company that does business with the DOD will need to comply with CMMC. Companies should review current CMMC materials, track new releases, and aim to comply with the requirements in preparation for a third-party audit as soon as possible.

Iran's Imminent Cybersecurity Threat

Posted January 7, 2020

In response to the killing of Major General Qassim Suleimani, the government of Iran and its supreme leader, Ayatollah Ali Khamenei, have declared the country's intention to strike back at the United States. According to reports, their desire is to respond proportionally, but not start a war, and they are contemplating multiple options, any subset of which they may implement.

Almost certainly, these options include cyberattacks. Iran has long been an active source of Advanced Persistent Threat (APT) attacks against the U.S. Government, as well as industry. These are among the most sophisticated sets of cyberattacks that have occurred in recent years. As a result, the U.S. Government is preparing for potential Iranian cyberattacks and is alerting the public to the danger. On January 6, CISA, the cyber component of the Department of Homeland Security, issued an alert, warning of the increased threat of cyber attacks from Iran. The two-page document is worth the read.

PUTTING IT INTO PRACTICE: Companies, particularly those that do business with the U.S. Government or that handle sensitive information, should consider additional security measures in light of this imminent threat. Some options include:

- Increasing the frequency of your backups of important data, until the threat eases.
- Implementing multi-factor authentication, if you have not already done so.
- Temporarily increasing the frequency of password changes on your system.
- Moving up any plans to upgrade system security so that they are completed sooner.
- Increasing the logging functions on your system to better monitor activity.

This list is by no means exclusive. Each company will have to evaluate the state of its cybersecurity independently, but for all of them increased vigilance is now in order.

EU PRIVACY

EDPB Announces Scope of COVID-19 Guidance

Posted April 15, 2020

Following its 20th plenary session on April 7, the European Data Protection Board (EDPB) selected geolocation and health data to focus on in its upcoming COVID-19 guidance. This follows in response to the EDPB's earlier broad statement on the processing of personal data in the context of COVID-19.In its March statement, the EDPB made clear that the GDPR does not hinder measures taken in the fight against the current coronavirus pandemic, but that businesses are not exempt from complying with the GDPR and ensuring the protection of personal data "even in these exceptional times." The EDPB emphasized that the GDPR allows certain public health authorities and employers to process personal data in the context of an epidemic, provided a lawful basis is met such as necessary for reasons of substantial public interest in the area of public health. The EDPB also reminded that when processing location data, national laws implementing the ePrivacy Directive must be followed. In principle, location data can only be used by the operator when the information is made "anonymous" or with the consent of individuals. While the EDPB's statement provided some answers to questions on processing of data in the context of COVID-19, there are few concrete recommendations. The authorities of nearly all EU member states have issued supplemental guidance.

As businesses and public agencies grapple worldwide with how to better understand COVID-19 and the pattern of its outbreak and spread, organizations are looking to use and analyze certain personal data in new ways. For example, will analyzing geolocation data help to assess efficacy of social-distancing? How can medical data collected in the context of COVID-19 be re-used and shared? EDPB's impending guidance is intended to focus on these two topics: geolocation and health data.

The guidance on geolocation and other tracing tools is expected to address: (1) the use of aggregated / anonymised location data (e.g. provided by telecom or information society service providers) and the effectiveness of such techniques; (2) the application of GDPR's principles to the different ways available to gather location data or trace interactions between people; (3) a legal analysis of the use of apps and collection of personal data by apps to help contain the spread of the virus; (4) the required safeguards to protect geo-location or other tracing tools; (5) recommendations or functional requirements for contact tracing applications; and 6) a potential pre-defined timeframe for the processing of such data limited to what is strictly necessary to tackle the emergency situation.

The guidance for the processing of personal health data for research purposes will address: (1) the fundamental aspects of processing of health data, such as legal basis, data subject rights, and retention; (2) re-use of medical research data connected to the COVID-19 crisis and data sharing; and (3) exercise of data subject rights in an emergency situation. The EDPB decided to postpone the guidance work on teleworking tools and practices, instead focusing on the above topics for the time being.

PUTTING IT INTO PRACTICE: While organizations in various sectors are actively working to better understand COVID-19 and the pattern of the outbreak, regulators are signaling reminders that such efforts must be conducted within the framework of existing privacy laws. We expect the EDPB's forthcoming guidance to provide more specific recommendations.

European Parliament Weighs in on Automated Decision-Making

Posted February 24, 2020

The European Parliament recently issued a resolution directed at the European Commission on its concerns with automated decision-making processes and artificial intelligence. While the EU Parliament addresses several areas of automated decision-making, the underlying theme of this resolution is that the Commission should ensure that there is transparency and human oversight of these processes. In particular, the EU Parliament stresses that consumers should be properly informed about how the automated decision-making functions, be protected from harm, and, particularly with automated decision-making in professional services, that humans are always responsible and able to overrule decisions. Additionally, this resolution stresses the need for a risk-based approach to regulating AI and automated decision-making and for the availability of large amounts of high quality data, while at the same time protecting any personal data under GDPR.

These concerns look to provide valuable input to the European Commission, as it gathers public commentary on its recently published white paper on artificial intelligence. Through this paper, the Commission hopes to offer policy options to encourage a trustworthy and secure development of AI, while still respecting European values and rights.

PUTTING IT INTO PRACTICE: Companies using or considering the use of automated decision-making or AI should keep in mind the EU's focus on both the level of human oversight and transparency with individuals about use of AI.

HEALTHCARE PRIVACY

CCPA Amendment Adds Needed Clarity for Medical & Research Community

Posted September 14, 2020

An amendment to the CCPA recently passed through the legislature, adding some much needed clarity to HIPAA-regulated entities, research institutions and other life science and medical device companies. CCPA in its current form left open uncertainty for business associates, de-identified information, and information collected in the course of medical research. AB 713 helps clarify certain exemptions and applicability of CCPA to organizations in the health and research space.

CCPA and Business Associates: Currently, CCPA does not regulate protected health information (PHI) that is collected by either a HIPAA covered entity or business associate. CCPA also exempts covered entities to the extent that they maintain patient information in the same manner as PHI subject to HIPAA. CCPA does not, however, currently

include a similar entity-based exemption for business associates. However, AB 713 adds an exemption for business associates to the extent that they maintain, use and disclose patient information consistent with HIPAA requirements applicable to PHI.

Applicability of CCPA to De-Identified Information: There was confusion about the applicability of CCPA to information that was de-identified pursuant to HIPAA. The bill clarifies that information de-identified pursuant to HIPAA would be exempt from CCPA. By explicitly providing that CCPA does not apply to HIPAA de-identified information, this alleviates the compliance challenges posed by potential inconsistencies between the HIPAA de-identification standard and CCPA's definition of de-identified information. Further, because the exception for de-identified information under AB 713 applies to de-identified information rather than HIPAA covered entities or business associates, the exception would be available to businesses that are not HIPAA-regulated entities but create de-identified data sets in accordance with the HIPAA de-identification standard and otherwise meet certain conditions.

New Notice Obligations for De-Identified Information: The amendment adds a new requirement to privacy policies. Businesses are now required to disclose if it sells or discloses deidentified patient information derived from personal patient information. If so, the disclosure must also state whether that deidentified health patient information was deidentified in accordance with the HIPAA "expert determination" (45 CFR 164.514(b)(1)) method or the HIPAA "safe harbor" (45 CFR 164.514(b)(2)) method.

Contractual Requirements for Sale of De-Identified Information: The amendment requires applicable businesses to include contract provisions whenever there is a sale or license of deidentified information. Businesses would need to represent that the deidentified information in the transaction includes patient information. The contract must prohibit the receiving party from reidentifying the deidentified patient information. The receiving party, subject to applicable law, must also be prohibited from further disclosing the deidentified to third parties unless contractually bound by equal or stricter confidentiality measures.

Exceptions for Research Data: In its original form, CCPA excepts personal information collected during "clinical trials." Because this term was undefined, it left uncertainty about the extent of the exception. With the amendment, information will be exempt from CCPA to the extent it is:

"…collected, used, or disclosed in research, as defined in Section 164.501 of Title 45 of the Code of Federal Regulations, including, but not limited to, a clinical trial, and that is conducted in accordance with applicable ethics, confidentiality, privacy, and security rules of Part 164 of Title 45 of the Code of Federal Regulations, the Federal Policy for the Protection of Human Subjects, also known as the Common Rule, good clinical practice guidelines issued by the International Council for Harmonisation, or human subject protection requirements of the United States Food and Drug Administration."

This exception will ease the burden that CCPA presents for the research community. For example, this exempts activities such as registry studies that are conducted with IRB oversight and that are subject to federal research regulations, but that are not "clinical trials."

PUTTING IT INTO PRACTICE: Like the CCPA B2B and employee exception amendment (which we covered here) this bill is now before the Governor to sign by the end of September. This bill should hopefully streamline CCPA compliance for many organizations in the health and research space. It helps eliminate some of the conflicts between HIPAA and CCPA de-identification standards. It also clarifies and broadens certain exemptions.

Using Health Data in Europe During COVID-19

Posted April 30, 2020

The EDPB recently issued guidelines about how to use health data during the current pandemic in compliance with GDPR. Given the COVID-19 pandemic, there have been many research efforts in place to fight against the virus. The EDPB's guidelines shed light on the special rules for processing health data for scientific research, which apply in the context of the COVID-19 pandemic:

- *Legal basis for processing:* The EDPB explained that the processing of health data for purposes of scientific research must be covered by one of the legal bases set out in Article 6(1) GDPR, such as consent. If consent is the legal basis that is relied on, the consent must be freely given and the data subject must be able to freely revoke consent. Member states may enact specific laws to enable the processing for scientific research purposes, as long as they are consistent with Article 5, Article 32 and Article 89 of the GDPR. Member states must also assess if a Data Processing Impact Assessment should be carried out.

- *Protection of information:* The guidelines also remind entities that GDPR's protection principles are still imperative, even if data is being processed for scientific research purposes. There are several parts of this, as the guidelines discuss. These include collecting information only for specific purposes and not using the information beyond those specific purposes. Personal data also needs to be processed fairly and in a transparent manner in relation to data subjects. The guidelines also remind those using health information to keep it only for as long as is strictly necessary to process the data for scientific research purposes, and to use adequate protection safeguards.

- *Transferring outside of the EU:* For transfers of personal data outside the EU to countries where there is no adequacy decision or appropriate safeguards, the guidelines include reminders about the restrictions on transfers. The EDPB reminds public authorities and private entities that in those circumstances they may rely on exceptions that are set out in Article 49 of the GDPR, such as consent. These determinations should be made on a case-by-case basis.

PUTTING IT INTO PRACTICE: Those who wish to use health information during COVID-19 to foster scientific research during the COVID-19 pandemic can use these guidelines to understand GDPR requirements. As the EDPB emphasizes, these still apply when processing such data.

HHS Relaxes Restrictions on Certain PHI Disclosures During COVID-19 Public Health Emergency

Posted April 16, 2020

HHS recently announced that it will not impose penalties if business associates disclose protected health information relating to COVID-19 during the public health emergency period. This waiver, announced in a Notification of Enforcement Discretion, applies if the disclosure is for public health and health oversight activities. It will apply, the Office for Civil Rights at HHS explained, even if their business associate agreement with covered entities does not specifically allow for such disclosure if two things hold true. First, that the disclosure or use is made in "good faith" for public health activities and health oversight activities. Second, that the BA informs the covered entity within ten days after the use or disclosure occurs. Examples provided by HHS include BA notifications to public health authorities, such as the CDC, health departments and CMS.

As we reported on in more detail in our healthcare blog, it is important to note that HHS' notification is not a broad waiver of the use and disclosure requirements of HIPAA. BAs must continue to comply with other provisions of HIPAA.

This notification aligns with the general shift toward deregulation of the healthcare industry during the COVID-19 pandemic. We will continue to monitor regulations surrounding COVID-19 and the healthcare industry to evaluate whether the industry continues down a path of deregulation or if a new series of regulations are imposed following the pandemic's end.

PUTTING IT INTO PRACTICE: With this announcement, HHS has granted greater freedom for BAs to cooperate with and exchange COVID-19-related information with public health and oversight agencies. BAs, however, must still comply with the other provisions of the HIPAA Privacy and Security Rules.

MOBILE PRIVACY

Apple Privacy Nutrition Labels Effective Starting Next Month

Posted November 30, 2020

Apple has launched, in connection with other privacy changes in iOS 14, a requirement for privacy "nutrition labels." The labels are required for new and existing apps, and are in addition to the existing requirement of linking to the company's long-form privacy policy. Apple will automatically generate the label based on the company's answers to its online questionnaire. Apple is requiring companies to explain what information they -and third-party partners collect. Answers will be turned into visuals for the label (a circle "i" for example, for contact information). Companies can also include optional disclosures, like confirming that data is not being used for tracking or third-party advertising purposes (if that is accurate).

Care should be taken that the person completing the questionnaire has accurate information about the company's practices. Apple stresses that companies are responsible for the accuracy of the information provided to it. We will be watching the launch of this program to see what perspective regulators take about these labels, and potential unfair and deceptive trade practice exposure if they are inaccurate. Responses can be updated at any time.

PUTTING IT INTO PRACTICE: Companies that operate mobile apps will need to address these App Store requirements. Care should be taken that the answers submitted into the questionnaire are accurate. To address potential UDAAP exposure, companies will want to track and update their "label" for accuracy just as companies do for their privacy policies.

Using Mobile Apps and Location Data to Combat COVID-19

Posted April 20, 2020

A number of private and government entities have released apps and software development kits (SDKs) relying on location tracking data to help tackle the COVID-19 pandemic. While the use of such technologies are being hotly debated, commentary continues to emerge from the EU about developing such applications in compliance with EU data protection laws.

On April 8, the European Commission issued its recommendation for a common EU toolbox for the use of technology to combat COVID-19. The Toolbox consists of practical measures for making effective use of technologies and data, with a focus on two areas in particular:

- A pan-European approach for the use of mobile apps, coordinated at EU level, for empowering citizens to take effective and more targeted social distancing measures, and for warning, preventing and contact tracing to help limit the propagation of the COVID-19 disease.

- A common scheme for using anonymized and aggregated data on mobility of populations in order (i) to model and predict the evolution of the disease, (ii) to monitor the effectiveness of decision-making by Member States' authorities on measures such as social distancing and confinement, and (iii) to inform a coordinated strategy for exiting from the COVID-19 crisis.

On April 14, the EDPB released comments on the Commission's initiative. The EDPB highlights the need to consult with national data protection authorities when developing apps, the importance of making the source code of apps publicly available, and the need for documentation through DPIAs.

While the EDPB encourages making the adoption of apps voluntary, the EDPB stated that performance of a task in the public interest may in some cases be the appropriate legal basis for processing rather than consent. The EDPB also notes that contact tracing apps will not require the location tracking of individual users, which would violate the principle of data minimization and create security and privacy risks. Further, while the EDPB noted that storage of information about contact "events" could be valid either locally or in a centralized database, provided that adequate security measures are put in place, the decentralized solution is more compatible with the principle of data minimization. Finally, the EDPB called for the need of all applications to be under the supervision of "qualified personnel" and that once the crisis is over, the system should be disbanded and the collected data should be erased or anonymized.

PUTTING IT INTO PRACTICE: As we previously wrote on, and noted in the EDPB's latest letter, the board will be releasing guidelines on geolocation and other tracing tools in the context of COVID-10 in the "upcoming days." Organizations looking to use location tracking apps must continue to be mindful of key principles under EU data protection laws, even in this time of crisis. Such safeguards include being transparent about why information will be collected and shared; making the use of the app as voluntary as possible; deleting any data generated by using the app once it is no longer relevant; using encryption and other data security measures, and documentation of all steps in a DPIA.

As you are aware, things are changing quickly and the guidance described here may change. This article represents our best understanding and interpretation based on where things currently stand.

FCC Ruling Helps Clarify What COVID-19 Texts and Calls Are "Emergency" Under TCPA

Posted April 10, 2020

The FCC recently issued a declaratory ruling explaining what calls and text message alerts it viewed as "emergency" for purposes of the Telephone Consumer Protection Act. Under TCPA, requirements to obtain consent to make certain calls and texts to cell phone numbers do not apply when a message is an "emergency." Under the FCC's new ruling, certain calls and texts from government officials and healthcare providers about the COVID-19 pandemic will be viewed as emergency messages.

This ruling is narrow. First, the call or text must be from a hospital, health care provider, state or local official, or other government official. (Or initiated by a person acting under the express direction of such an organization.) Second, the message must provide information directly related to imminent health or safety risks arising out of the pandemic. Examples might be a government-issued "shelter in place" text, or a text from a hospital with vital information intended to slow the spread of the virus. The exception thus does not apply to general information about COVID-19, nor information about the pandemic that comes companies that do not fit into the narrow scope (hospital, health care providers, etc.).

PUTTING IT INTO PRACTICE: This ruling provides direction for hospitals, health care providers and others about what might be viewed as an exception to the need to obtain consent prior to sending the call or text.

Apple Eases Push Notification and Other Privacy Restrictions

Posted April 9, 2020

Apple recently revised its review guidelines to allow push notifications that include "advertising, promotions, or direct marketing." This changes a prior -and longstanding- prohibition on push notices that contain such content. Customers must affirmatively opt in to get promotional push notices, though ("through consent language displayed in your app's UI"). They must also be able to opt out through an in-app mechanism. Although promotional push notices were previously prohibited, many apps sent them. These modifications may be a step by Apple to acknowledge this use and put requirements in place around it.

The review guidelines also include other changes with an impact on information collection, use and sharing. These include for apps that provide services in "highly-regulated fields." Such apps must be submitted by the regulated entity (i.e., the one providing the regulated services) rather than the app developer. For example, if a bank hires an app developer to create an app for the bank, the bank should submit the app to the Apple App Store, not the developer it hired to make the app.

Another change are the provisions for apps that provide users with Mobile Device Management (MDM) tools. Previously those apps were prohibited from "disclosing to third parties" any data. Now those apps can share information but only if it is about the "performance of the developer's MDM app" and does not include user data ("data about the user, the user's device, or other apps used on that device").

PUTTING IT INTO PRACTICE: Apple's modified guidelines may help companies that send push notices, as well as those that provide MDM apps. For companies in regulated areas, keep in mind the new requirement on who should be submitting apps to the Apple App Store.

PRIVACY MANAGEMENT

Turn On the Camera Part Three: Fulfilling CCPA Training Obligations in the Face of COVID-19

Posted March 13, 2020

As many who have been tracking CCPA are aware, the law requires training employees who handle consumer inquiries, and ensuring that employees understand how to help consumers exercise their rights. Since most of those rights requests are arriving by web page, email, and phone, it is unlikely that rights requests will slow in the face of COVID-19. Indeed, it is possible that they may increase. Employees will thus still need training, something many companies had anticipated doing in-person.

In-person training is particularly useful to ensure employees adequately understand and digest CCPA requirements, and many coordinate with their law firms to put together such sessions. These trainings typically address not just CCPA-related privacy training requirements, but also training required under other privacy laws (GDPR, GLBA, HIPAA, to name but a few) and industry guidelines. Potential restrictions on group gatherings, corporations limiting travel, and employees working remotely puts in-person in jeopardy.

Rather than avoid privacy training, companies can tweak their existing training plans and make use of the myriad of virtual platforms available in this modern age. When doing so, companies do not have to sacrifice interactivity. As those who regularly use interactive tools can attest, they provide several useful features that can help gauge effectiveness of training. Chief among these is the simple video camera. For companies who have a culture of "camera off," now is the time to shift to "camera on." Training programs should still, as would have been the case with in-person training, focus on measurable success. Do employees understand how to direct consumers to exercise their rights?

Do employees who are gathering information know where to look? These issues and others should be covered in training.

PUTTING IT INTO PRACTICE: As companies map out their CCPA training plans, they can work with legal counsel to move towards -effectively implemented, interactive- virtual training in light of COVID-19. This can help prepare for rights request responses and otherwise address privacy training requirements.

Turn on the Camera Part One: Keeping Your Privacy Compliant Efforts Moving Forward in the Face of COVID-19

Posted March 11, 2020

As companies brace for the impact of COVID-19, the last thing on everyone's mind may be proactive privacy compliance obligations. Certainly, companies may be thinking about privacy obligations that relate specifically to their COVID-19 response. What types of employee information can be disclosed, for example, especially in European offices? (On this, see guidance from the French, Italian and Irish data protection authorities.) But companies can think more broadly, in particular about how they will continue the proactive operations of the privacy team during this time. Some questions companies can ask themselves now include:

- How will employees continue to fulfill CCPA and GDPR rights requests if the work force is remote?
- How are privacy functions ensuring that personal information is being used in compliant ways? For example, when companies turn to technologies to facilitate remote communications, like texts, which are governed by TCPA discussed in more detail here, are organizations sufficiently knowledgeable about those laws' requirements?
- Or, if companies move to using biometric-based, touch-free entry systems to limit the spread of germs, is there a strong understanding of the legal requirements? (The use of these technologies being regulated in many states, as we have discussed in the past.)
- What about companies considering using geographic tracking systems to help locate employees? These activities, too, are often regulated.

In addition to new activities that might impact existing laws, many jurisdictions are proposing new privacy regulations (as we have written previously), which appear to be moving forward despite COVID-19. Add to this that several existing privacy laws have private rights of action, and there may be actions brought under those laws in the coming months despite COVID-19. All of this collectively points to an increase in demand for the privacy function's time.

Typically when demand increases, teams meet to brainstorm through in-person meetings or off-site retreats. And, under normal business circumstances, companies facing these pressures (new laws, potential privacy-based law suits) include in compliance efforts data diligence exercises. These help companies get a good handle on what data they have, how they obtained it, and how it is being used. Normally -as with brainstorming- the emphasis is on in-person data gathering, allowing fulsome conversations that go beyond questionnaires. The results of these efforts help companies understand the scope of their privacy obligations, design compliance programs, and implement those programs.

In light of the new business environment under COVID-19, many may be concerned about how to conduct planning and diligence efforts if key personnel are working remotely and travel is restricted. Instead of deferring important planning and diligence exercises, companies can turn to interactive virtual platforms, and make good use of the

interactive features of those platforms – like communicating with cameras (and having cameras turned on). Using these tools, teams can use this time to not only ensure ongoing compliance in this business climate, but also to get ahead of upcoming privacy regulations.

PUTTING IT INTO PRACTICE: Privacy teams may want to take the opportunity now to get ahead of the potential uptick in individuals making rights requests, new methods of data use by business teams, and upcoming privacy laws.

For more legal insights visit our Coronavirus (COVID-19) page.

New Trends Emerge in FTC Data Security Orders, Including Emphasis on C-Suite Involvement

Posted January 15, 2020

The FTC recently summarized three major changes it made to its orders in data security cases. In a blog signaling these changes, the FTC Indicated that some of the things it has been requiring of companies in 2019 are here to stay. First, the orders have been – and will continue to be – more specific about the expectations for implementing a comprehensive data security program. Historically, orders had generally required companies to implement an information security program with reasonable safeguards to control the risks identified through a risk assessment. In more recent cases, the FTC has itemized the specific controls it expects the data security program to include. For example, training all employees at least every 12 months and encrypting certain information. Also, using access controls such as authentication and restricting connections to approved IP address.

Second, the FTC plans to hold third-party assessors that review company's security programs more accountable. Assessors may now be expected to identify the evidence supporting their conclusions. This may include employee interviews. The FTC also plans to approve and review assessors every two years.

Finally, senior officers may be expected to provide annual certifications of compliance to the FTC as part of the order. The certification will require the senior officer to confirm that the requirements of the order have been implemented and that there's no material instance of noncompliance.

PUTTING IT INTO PRACTICE: Companies should be mindful of these trends when putting together 2020 strategic priorities for cybersecurity efforts. Namely, organizations should make sure training efforts can withstand the test of interviews of employees. Also, senior officers must have a meaningful understanding of a company's information security program.

CONTRIBUTING AUTHORS

Craig Cardon
Partner, Team Leader, Privacy and Cyber Security Practice
ccardon@sheppardmullin.com
310.228.3749

Liisa Thomas
Partner, Team Leader, Privacy and Cyber Security Practice
lmthomas@sheppardmullin.com
312.499.6335

Townsend Bourne
Partner
tbourne@sheppardmullin.com
202.747.2184

Kari Rollins
Partner
krollins@sheppardmullin.com
212.634.3077

Jonathan Meyer
Partner
jmeyer@sheppardmullin.com
202.747.1920

Matthew Shatzkes
Partner
mshatzkes@sheppardmullin.com
212.634.3062

Brian Murphy
Partner
bmurphy@sheppardmullin.com
212.634.3059

Rachel Tarko Hudson
Partner
rhudson@sheppardmullin.com
415.774.2999

Hayley Grunvald
Special Counsel
hgrunvald@sheppardmullin.com
858.720.7410

Snehal Desai
Associate
sndesai@sheppardmullin.com
415.774.2960

Susan Ingargiola
Associate
singargiola@sheppardmullin.com
212.869.0624

Julia Kadish
Associate
jkadish@sheppardmullin.com
312.499.63340

Elfin Noce
Associate
enoce@sheppardmullin.com
202.747.2196

Samuel O'Brian
Associate
sobrian@sheppardmullin.com
424.288.5316

David Poell
Associate
dpoell@sheppardmullin.com
312.499.6349

Bridget Russell
Associate
brussell@sheppardmullin.com
310.228.2273

Alyssa Shauer
Associate
ashauerr@sheppardmullin.com
424.288.5305

Nikole Snyder
Associate
nsnyder@sheppardmullin.com
202.747.3218

SheppardMullin

Brussels | Century City | Chicago | Dallas | London | Los Angeles | New York | Orange County | Palo Alto
San Diego (Downtown) | San Diego (Del Mar) | San Francisco | Seoul | Shanghai | Washington, D.C.

www.sheppardmullin.com