2021

SheppardMullin

# Eye On Privacy:
## 2021 Year in Review

These articles appeared in the "Eye On Privacy" Blog in 2021 (www.eyeonprivacy.com)

# Sheppard Mullin's 2021 Eye on Privacy Year in Review

Just as we thought 2022 was going to be significantly different than 2021, December 2021 and January 2022 events have thrown us for another (pandemic) loop. We anticipate that some of the privacy and cybersecurity developments from 2021 may similarly repeat in 2022. As you and your teams put together your privacy and cybersecurity program plans for the year, we hope that this compilation of articles is helpful.

This year-in-review contains all of the 2021 blog posts from www.eyeonprivacy.com. Reviewing them highlights several themes. There was significant focus on artificial intelligence, biometrics, and tracking. We expect similar focus in this area in 2022, whether in the form of enforcement or new regulations. Data security and breach issues continued to take center stage, with more and more regulators adding security measures to the top of their priority lists. These will no doubt be top-of-mind in 2022 as well.

Given the continued focus on privacy and cybersecurity, we published several articles in 2021 with suggestions and tips for managing privacy compliance. These articles are compiled in the "privacy management" section, and include an examination of right-sized privacy programs, regulatory priorities, and managing "unknown" and unpredictable risks.

We will continue to track these developments in 2022 at www.eyeonprivacy.com. In the meantime, we hope that you find this compilation helpful as you move forward in planning your privacy efforts for 2022 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

# ARTIFICIAL INTELLIGENCE, BIOMETRICS AND TRACKING

## New York Imposes New Requirements for Employee Monitoring

*Posted November 23, 2021*

New York recently enacted a law governing employee monitoring. The law applies to New York employers who monitor employees through electronic devices. This includes monitoring of telephone, emails, and internet access or usage. The law takes effect May 7, 2022.

**Requirements**
Under the law, employers must provide notice of monitoring to current employees and to new employees upon hire. The notice must be in writing or in an electronic form and conspicuously posted, and individually distributed. This means that the notice is readily available for viewing, on the company intranet, or at the worksite. Employees must acknowledge the notice in writing or electronically. The law appears to impose specific content requirements for the notice. Namely, that telephone conversations, email, or internet usage may be monitored at any and all times and by any lawful means.

**Exceptions**
Importantly, the law does not apply to processes that manage electronic communications and internet usage or systems maintenance. To qualify for the exception, the systems management processes must also not target the activities of a particular individual. Further, the processes must be performed solely for the purpose of computer system maintenance or protection.

**Penalties**
The NYAG has the authority to enforce these requirements. Civil penalties may range from $500 for a first offense, up to $3,000 for subsequent offenses. There is no private right of action for violations of the law.

**PUTTING IT INTO PRACTICE: New York joins other states, like Connecticut and Delaware, in requiring notice of employee monitoring. Companies should review their existing practices for providing notice of monitoring, such as employee handbooks, acceptable use policies, and login banners to confirm compliance with New York's requirements. Companies should also develop a process for tracking and maintaining employee acknowledgements. While not expressly required by the statute, should the scope of the employer's monitoring change, it is recommended that updated notice be provided to employees.**

## Australia Objects to 7-Eleven's In-Store Use of Facial Recognition Technology

*Posted November 17, 2021*

The Office of the Australian Information Commissioner issued a determination earlier this fall about 7-Eleven's use of "faceprints." The OAIC found the convenience store improperly collected faceprint information without getting individuals' consent in violation of the Privacy Act.

Accordingly to the OAIC, 7-Eleven used facial recognition technology as part of in-store surveys in 700 stores across the country. Approximately 1.6 million customers (as of March 2021) complete the survey on tablets with built-in cameras. The cameras took facial images of the customer as they went through the survey. These images were uploaded by the third party providing the service to a centralized server. The third party then processed the images to make sure the same person wasn't leaving multiple responses. The images were also analyzed to understand the gender and age of survey respondents.

7-Eleven argued that the images were not "personal information" and that in any event, it had disclosed the recording in notices posted at the entrance of its stores. Some notices had only an image of a surveillance camera, other signs though did say "*by entering the store you consent to facial recognition cameras capturing and storing your image*." The OAIC disagreed with the company, stating that the images were personal information. Moreover, it found the signage (even the signs with the full statement) were insufficient for obtaining consent. The OAIC held that express consent was required, and could not be implied as a result of someone entering the store after reading the sign.

**PUTTING IT INTO PRACTICE: This case is a reminder that regulators beyond those in the US and the EU are concerned about use of facial recognition. Companies using these technologies in Australia will want to keep in mind the expectations around obtaining express consent when collecting faceprints.**

## Baltimore Blows by Brother Burghs with Big Biometrics Ban

*Posted September 14, 2021*

Baltimore recently prohibited several uses of "face surveillance" technology. Under the new law companies cannot use systems that identify or verify individuals based on their face. The law also prohibits saving information gathered from these systems. Getting an individual's consent is not a way around the prohibition. Nor is promising not to connect information gathered with other personal information.

There is an important exception that many companies will find useful. Namely, the law permits facial recognition technologies that are used to give access to specific locations or devices. Some are concerned that the law is overly restrictive. It applies to both people and companies, and does not have standard exceptions like research. Coding projects that scan and use data of the researchers' own faces would thus be a violation.

Violations of the law are misdemeanors that can result in a 12-month prison term and/or a $1,000 fine. The law went into effect on September 8, 2021 and automatically expires on December 31, 2022. The city council can extend the bill for another five years if it determines that the law remains in the public interest.

**PUTTING IT INTO PRACTICE: Organizations with operations in Baltimore will want to review their use of facial recognition technology. While using the tools for accessing locations or services is acceptable, use beyond this is prohibited.**

## New York City Biometric Ordinance Effective July 9, Are You Ready?

*Posted June 17, 2021*

New York City recently enacted a biometric ordinance that is set to come into effect July 9, 2021. With this ordinance, NYC joins other cities (like Portland) in regulating the use of biometric information. The ordinance may impact retailers, restaurants, and entertainment venues in the city that use security cameras with facial-recognition technology or otherwise collect biometric identifiers from their customers.

*Applicability*. The law applies to commercial establishments (like the type itemized above) that collect "biometric identifier information" from "customers." Biometric identifier information is defined as physiological or biological characteristics that are used by or on behalf of a commercial establishment, singly or in combination, *to identify, or assist in identifying*, an individual, including, but not limited to: (i) a retina or iris scan, (ii) a fingerprint or voiceprint, (iii) a scan of hand or face geometry, or any other identifying characteristic. Customers are purchasers, lessees, or prospective purchaser or lessees of goods or services from a commercial establishment. Thus, this ordinance does not apply to biometric information that may be collected from employees.

*Requirements and Restrictions*. The ordinance requires commercial establishments that collect, store, or share biometric information *from customers* to disclose the practice by posting a sign near all customer entrances. The sign must be in "plain, simple language" and a form to be prescribed by the City. Under the ordinance, commercial establishments are also prohibited from selling, leasing, trading, or sharing in exchange for anything of value, or otherwise profiting from the transaction of biometric identifier information.

*Enforcement -Private Right of Action*. There is a private right of action in the ordinance. For violations of the signage requirement, customers have to provide a business with written notice of the deficiency, and a 30-day opportunity to cure. If such alleged violation has been cured within that time, no action can be brought. No prior written notice is required for allegations of the "no sale" requirement. Plaintiffs can recover $500 per violation for *uncured* breaches of the notice requirement or any negligent violation of the prohibition on sale/sharing of biometric data, plus attorneys' fees. For intentional or reckless violations of the sale/sharing prohibition, plaintiffs can recover $5,000 per violation.

*Exemptions*. The ordinance exempts the collection, storage, or sharing of biometric information by government agencies, employees, and agents entirely. Financial institutions are exempt from the signage requirement, but not the prohibition on sale. Further, commercial establishments that collect biometric information through photographs or video recordings, but do not use software or applications in order to identify, or assist with identifying individuals based on physiological or biological characteristics and do not share it with third parties (other than law enforcement), are also exempt from the signage requirement (but not the prohibition on sale).

**PUTTING IT INTO PRACTICE. Companies that operate a retail store, restaurant, or entertainment venue in New York City should evaluate if they are collecting or using biometric information as contemplated by the ordinance. Depending on how such technology is used, there may be obligations to post prominent signage of these practices.**

## Wondering How to Use AI? The FTC Has Some Thoughts

*Posted April 28,2021*

The FTC recently provided guidance to companies on how to use artificial intelligence with an aim for "truth, fairness and equity." The FTC reminded companies of three laws it enforces which have lessons for those in the AI space: Section 5 of the FTC Act (which would prohibit unfair algorithms, for example); the Fair Credit Reporting Act (which would prohibit algorithms that might deny housing, as an example); and the Equal Credit Opportunity Act (which would prohibit algorithms that might result in credit discrimination on the basis of race, as an example).

These comments come almost a year after the FTC's recommendations about AI, and show that the topic remains a priority for the FTC. In these recent comments, the FTC now provides more detail for developers of AI. These include:

- **Start with the right foundation**. For example, is your data set missing information from particular populations? If so, using that data to build an AI model may yield results that are unfair or inequitable to legally protected groups.
- **Watch out for discriminatory outcomes**. Testing your algorithm before and during use is needed to make sure that it doesn't discriminate on the basis of race, gender, or another protected class.
- **Embrace transparency and independence**. Transparency frameworks and other actions such as publishing the results of independent audits or opening data or source code can help increase transparency.
- **Don't exaggerate what your algorithm can do or whether it can deliver fair or unbiased results**. Be careful not to overpromise what your algorithm can deliver, or else, risk running into FTC Act territory.

- **Tell the truth about how you use data**. Pay attention to the statements made about how data is used and the control users will have over that data.

- **Do more good than harm**. If your model causes more harm than good – i.e., if it causes or is likely to cause substantial injury to consumers that is not reasonably avoidable by consumers and not outweighed by countervailing benefits to consumers or to competition – the FTC can challenge the use of that model as unfair.

- **Hold yourself accountable – or be ready for the FTC to do it for you**. As an example, if your algorithm results in credit discrimination against a protected class, a company may face a complaint alleging violations of the FTC Act and Equal Credit Opportunity Act.

**PUTTING IT INTO PRACTICE. With these new comments, the FTC provides companies with more concrete examples of ways to meet its transparency, fairness, and accuracy guidance from last year. It also signals the focus the FTC will give to AI under the new administration. The FTC is not the only regulator focusing on AI. For example, federal financial agencies recently requested comments about the use of AI, and the European Commission has just issued a proposed Artificial Intelligence Act (following a white paper and resolution on the topic issued last year).**

## Federal Financial Agencies Seek Comments on Use of Artificial Intelligence

*Posted April 5, 2021*

Artificial intelligence continues to remain a focus in 2021, as we predicted at the start of the year. From the FTC, to the EU, to others, regulators of all kinds are paying attention to companies' use of these tools. In the latest, five US federal agencies are seeking input on how financial institutions are using AI tools. Comments from stakeholders are due by June 1, 2021.

These financial agencies recognize and acknowledge the benefits of AI, noting that AI tools have the potential to augment business decision-making and enhance services available to consumers and businesses. These tools, they note, are used by financial services firms for things like flagging suspicious transactions and personalizing customer services. While there are certainly benefits, the agencies recognize that use of AI tools are not without risks, including operational vulnerabilities, cyber threats, heightened consumer protection issues, and privacy concerns.

The agencies are seeking input from the industry on a variety of topics to provide them with a more complete picture of current AI. This is part of their efforts to determine the appropriate levels and types of governance, risk management, and controls over those tools. Areas of input sought include:

- Explainability
- Data quality and data processing
- Overfitting (i.e. when an algorithm "learns" from idiosyncratic patterns in the training data that are not representative of the population as a whole)
- Cybersecurity
- Dynamic updating
- AI use by community institutions
- Use of AI developed or provided by third parties
- Fair lending

While signaling that they may create more guidance, the agencies point out that there are currently many regulations that govern use of AI tools. These include the Fair Credit Reporting Act, Section 5 of the FTC Act, Sections 501 and 505(b) of the Gramm-Leach-Bliley Act, and more. Similarly, there are several general guidance documents that have been issued that can give direction on the use of AI tools.

**PUTTING IT INTO PRACTICE. This request for comment gives financial institutions an opportunity to bring the benefits and challenges from the use of AI to regulators' attention. Comments are due by June 1, 2021. Instructions on how to submit comments to each of the agencies is found at the beginning of the request for comment.**

## Beware BIPA Bifurcation: Plaintiffs' New Gambit to Split BIPA Claims Between State and Federal Courts

*Posted March 16, 2021*

The Illinois Biometric Information Privacy Act (BIPA) has spawned hundreds of class action lawsuits and a raft of unresolved issues. A core issue from a litigation perspective—as well as for companies bracing for potential lawsuits—is one of "standing," and in particular, what BIPA claims can be brought by plaintiffs in what venues.

As we discussed in an earlier post, in a case from last year (*Bryant v. Compass Group USA, Inc.*), the Seventh Circuit ruled plaintiffs have federal standing for claims alleging that a company collected biometric information without written consent (i.e., violated Section 15**(b)** of BIPA). BIPA has other requirements, however. Namely, that companies publicly disclose their biometric retention policy, *and* retain biometric information in accordance with such policy (i.e., violations of Section 15**(a)** of BIPA). While the *Bryant* case found there was standing for violations of Section 15(b), the court found at the same time that a violation of the disclosure requirement (Section 15(a)) does *not* create standing. However, a few months later in *Fox v. Dakkota Integrated Systems*, the Seventh Circuit ruled that a violation of the retention requirement under Section 15(a) *does* create standing.

Companies who are sued under BIPA for their biometric practices often find it desirable to defend themselves in federal court, as under the Federal Rules of Civil Procedure it can be harder to have a class certified than in state court. On the other hand, plaintiffs increasingly favor splitting up BIPA class actions between state and federal court, likely because the outcomes in state court may be more favorable, and having litigation running in two venues can have advantages for them.

What does the *Fox* decision mean in this environment? First, plaintiffs are starting to plead *only* that a company has failed to disclose its biometric retention policy. That way, if the defendant—who wishes to defend itself in federal court—tries to argue that BIPA cases should be heard in federal court, not state court, the plaintiffs can argue the federal court lacks jurisdiction. So far, this strategy has yielded mixed results for BIPA plaintiffs.

**PUTTING IT INTO PRACTICE: Companies that collect biometric information in Illinois should keep in mind that plaintiffs' counsel are actively working to have biometric policy violation allegations heard exclusively in state court, not always a preferred venue. This is a reminder that by having a written policy that specifies a retention and destruction schedule for individuals' biometric information, and making that policy available to those from whom it collects biometric information, companies may be able to avoid these standing battles.**

## What to Watch in Artificial Intelligence in 2021

*Posted February 10, 2021*

Artificial intelligence continues to be a focus and concern for businesses, regulators, and lawmakers alike. As we recently wrote, there was much activity and focus on artificial intelligence and the impact on privacy laws. In addition to legal developments, there have been advancements in AI business technologies by major multinational technology firms, something focused on this post in our sister Intellectual Property Law Blog. There has been an arms race underway by the world's leading economies to win the estimated $13 Trillion of GDP this field stands to award the winner. In a recent podcast episode, partners Siraj Husain and Michael P.A. Cohen discuss these developments, risks, and solutions that businesses are experiencing.

**PUTTING IT INTO PRACTICE: Companies will continue to implement artificial intelligence into their operations. Our recent podcast and other articles can help as companies move forward thinking about integrating these tools while keeping in mind the not insignificant legal risks.**

## Portland's Facial Recognition Law: Impact on National Companies

*Posted February 9, 2021*

Many have been watching facial recognition law developments closely, and saw that Portland became the first US city to regulate the use of such technology by private entities operating "places of public accommodation" within the city. Of particular concern for the Portland city council was the use potentially discriminatory use of these technologies, and its impact on "children, Black, Indigenous and People of Color, people with disabilities, immigrants, refugees, and other marginalized communities and local businesses."

The ordinance applies to use of facial recognition technology in public places (like "lodgings, amusements, transportations"), but does not apply to private clubs, homes, or places of accommodation that are in their "nature distinctly private." The ordinance provides for a private right of action, with the potential of $1,000 per day "for each day of violation." Under the ordinance, public places of accommodation can only use facial recognition technologies for:

1. User verification, when the user is accessing his or her own "personal or employee issued communication and electronic device"
2. For "automatic face detection services in social media" apps
3. To comply with the law

Unlike other laws that impact use of facial recognition technologies (Illinois' biometric law), this ordinance is narrowly focused on "Face Recognition," namely those technologies that help identify, verify, detect, or characterize the facial features of individuals based on their face. Nevertheless, there has been much concern over the wording of the ordinance, given the narrow permitted uses of the technology and the broad definition of places of public accommodation. Several industry organizations and individual companies objected to the law, and some have indicated that they will be pushing for additional exemptions to the broad ban.

**PUTTING IT INTO PRACTICE: We will continue to monitor developments related to this ordinance. In the meantime, for national chains (hotels, restaurants, retailers) and others who have operations in Portland, especially those who have been moving towards increased use of touchless technologies in their interactions with customers and guests, they will want to keep this new ordinance's requirements and restrictions in mind. For more on using facial recognition and artificial intelligence tools more generally, both the FTC's recent decision in this space and our recent AI roundup provide suggestions.**

## Defunct Photo App Agrees to Erase Biometric Data in FTC Settlement

*Posted January 20, 2021*

The Federal Trade Commission recently entered the biometric fray. It settled with a now-defunct photo-storage app over its use of facial recognition technology. According to the FTC, the company engaged in a variety of deceptive and unfair acts, in violation of Section 5 of the FTC Act.

The company, Everalbum, Inc. operated an app that let users organize photos that they uploaded to the app. The app, Ever, had a "Friends" tool that used facial recognition technology to group photos by people's faces. Everalbum told users it would only use facial recognition with consent. However, Friends was in an "opt in" mode only in jurisdictions with biometric laws (Texas, Illinois, Washington, and the European Union). For users in other locations, the technology was automatically turned on unless users opted out. This (being in opt-out mode) did not constitute the promised consent, according to the FTC.

Also of concern for the FTC was the fact that facial recognition technology was used by extracting images from uploaded photos and combining those with other images the company obtained from public datasets. The resulting datasets Everalbum created, the FTC alleged, were used to help develop Friends. The FTC was further concerned that Everalbum did not delete any users' photos upon account deactivation, even though it represented that it would do so. Instead, Ever stored photos indefinitely.

While no civil penalties were imposed, Everalbum agreed to (1) delete all photos collected from users who deactivated their accounts and (2) delete "face embeddings" (i.e., the facial features used for facial recognition) unless the company had obtained express consent for their use. The settlement also establishes recordkeeping requirements. Everalbum also has to complete a compliance report in one year. In a supporting statement, Commissioner Chopra emphasized that absent more restrictions on the use of biometric technology, it was "critical that the FTC meaningfully enforce existing law to deprive wrongdoers of technologies they build through unlawful collection of American's facial images and likenesses."

**PUTTING IT INTO PRACTICE: This case shows that even absent a federal biometric law, the FTC expects companies in many situations to both provide notice and get consent before collecting and using biometric information.**

# CHILDREN'S PRIVACY

## The Impact of the CARU Advertising Guidelines Change On Privacy

*Posted August 26, 2021*

As discussed in our sister blog, CARU's revised Ad Guidelines go into effect on January 1, 2022. While the core principles of the guidelines have not changed, they now include new content to account for today's advertising environment. Several modifications are important to keep in mind for those who collect information from children.

One of them is that the children's privacy guidelines, which were previously included in the advertising guidelines, have been re-located to a separate document. Second, that the guidelines apply to children 13 and under (instead of children under age 12) to provide better uniformity with the COPPA Rule. As we discussed in our sister blog, other modifications include changes to address influencer marketing, blurring, and better promoting diversity.

**PUTTING IT INTO PRACTICE: Advertisers who market to children should keep in mind that the CARU guidelines will be updated beginning next year, and begin to familiarize themselves with the updated guidelines. As new FAQs about the guidelines are released, they were be announced in the CARU section of the BBB National Programs website.**

### A COPPA First: Safe Harbor Program Removed From Approved List

*Posted August 23, 2021*

The FTC recently announced the removal of Aristotle International, Inc. from the list of seven approved safe harbor programs under the Children's Online Privacy Protection Act. Programs that are approved by the FTC must place requirements on participating organizations that are the same -or greater- than the requirements of COPPA. (As we have reported in the past, COPPA requires, *inter alia*, getting verified parental consent before collecting personal information from children online.) Companies that participate in those approved COPPA safe harbor programs are deemed in compliance with COPPA. Such protection can be valuable with a law, like COPPA, that has been found to be confusing to operationalize.

The FTC had expressed concern with Aristotle's monitoring efforts, fearing that the company was not taking steps to ensure that participants complied with the requirements of Aristotle's safe harbor program. The FTC indicated to Aristotle that its response was inadequate, and Aristotle withdrew from the COPPA safe harbor scheme as a result.

**PUTTING IT INTO PRACTICE: Companies that participate in a COPPA safe harbor program might see an increased scrutiny by their COPPA safe harbor provider as a result of Aristotle's removal from the approved list.**

## COMMUNICATION PRIVACY

### Texting Post-Duguid: Can Consent Practices Change?

*Posted May 4, 2021*

Providing business teams with advice for sending text messages can be nothing short of frustrating. For businesses used to sending email marketing, the laws for texting are unexpected. Unlike the CAN-SPAM Act, TCPA requires prior express written consent if autodialed messages are sent that contain advertising content. And unlike CAN-SPAM, TCPA has a private right of action. On its face, the recent Supreme Court decision in *Facebook, Inc. v. Duguid* seemed to bring good news. The decision suggests that companies may be able to send, in several circumstances, automated texts to databases of current customers without running afoul of TCPA. There are still areas of confusion, though.

As we reported in our sister blog, the Court clarified what had been an area of confusion for some time: what *is* an autodialer, or an "automatic telephone dialing systems" (ATDS)? The TCPA regulations define ATDS as equipment that "has the capacity to store or produce telephone numbers to be called using a random or sequential number generator and to dial such numbers." The Court ruled that to fall under ATDS, it was not enough that the equipment had the *capacity* to store numbers and to dial them automatically (as the Ninth Circuit before it had found). Instead, the equipment must either *store or produce numbers using* a random or sequential number generator.

The question, then, is whether a company's texts are sent using technology that not only has the *capacity* but also actually *stores or produces numbers using* a random or sequential number generator. It is possible that company's text campaigns may be sent using technology that only has the "capacity," and they then fall outside of TCPA's scope. On the other hand, the text campaign may be sent using technology that stores or produces numbers using random generators. If that is the case, then the campaign remains in-scope for TCPA.

**PUTTING IT INTO PRACTICE: This decision significantly narrows a company's potential exposure under TCPA. The law does not, however, modify requirements around getting consent to send text messages that might exist at a state level, nor will companies always know if the vendors they are working with are, in fact, avoiding using an ATDS. As such, companies will still want to ensure that their express written (signed) consent mechanisms are in place when collecting cell phone numbers for marketing campaigns.**

## FCC Sets Volume Limits For Some Prerecorded Calls to Home Phones

*Posted January 15, 2021*

The FCC recently adopted new rules that will limit the volume of calls that can be made to residential phones under certain TCPA consent exceptions. The new rules affect non-telemarketing calls that use an artificial or prerecorded voice. For years, companies have been able to make unlimited numbers of these calls to residential lines without the need for prior express consent if the exceptions applied. Beginning later in 2021, companies will need to follow volume limits for the following types of exempted calls, unless they have obtained prior express consent to make more calls. The new limits will apply to calls that fall into one of these consent exceptions:

1. Non-Commercial Calls to a Residence: The new rules limit the number of calls under this exemption to **three calls within any consecutive 30-day period**. This exemption includes calls conducting research, market surveys, political polling, or similar noncommercial activities.
2. Commercial Calls to a Residence that Do Not Constitute Telemarketing: The new rules limit the number of calls under this exemption to **three calls within any consecutive 30-day period**. This exemption includes calls to consumers regarding prescription refill reminders, power outage updates, and data security breaches.
3. Tax-exempt Nonprofit Calls to a Residence: Like the two previous categories, the new rules limit the number of calls under this exemption to **three calls within any consecutive 30-day period**.
4. HIPAA Calls to a Residence: The new rules limit the number of calls under this exemption to **one call per day up to a maximum of three calls per week**.

As long as companies follow these limits, they may still make these calls without obtaining prior express consent. Companies must also let recipients opt out of such calls (as is provided in TCPA). These rules will go into effect six months after they are published in the Federal Register, which we anticipate will happen soon.

**PUTTING IT INTO PRACTICE: Before these requirements go into effect, companies can prepare and test procedures to comply with the volume limits, or consider whether it makes sense to get consent to send more calls than provided for in the rule.**

# CONSUMER PRIVACY

## FTC To Focus Enforcement Efforts on Dark Patterns

*Posted November 9, 2021*

The Federal Trade Commission recently issued a new enforcement policy statement about "dark patterns:" programs that attempt to "trap" consumers into service contracts. These programs usually take the form of negative option marketing programs, according to the FTC, and are regulated under most states' laws as well as the Restore Online Shoppers Confidence Act (ROSCA).

Negative option programs begin as a free service, with a fee charged after a certain period of time. Under both ROSCA and state laws, companies must clearly and conspicuously disclose material terms to consumers before they make a purchase. They must also get express consumer consent to the negative option program, and give people an easy way to cancel.

With this new enforcement policy statement, the FTC is indicating that it will increase its scrutiny of these programs. In the statement, the FTC warned against taking silence for acceptance, reminded companies of their obligations under ROSCA, and warned against engaging in practices that might be viewed as a deceptive or an unfair act. The policy statement gives companies some guidance– and reminders– about what is expected. These include:

- Making clear and conspicuous the terms of the program, such as the fact that the consumer will be charged and that charges may increase after an initial period.
- Disclosures should appear "immediately adjacent to the means of recording the consumers' consent" and before the consumer makes the decision to buy.
- The consent itself should be "express" and "informed." A pre-checked box, the FTC indicated, is not sufficient. And information about the program should not be buried in "extraneous language" that isn't related to the consent.

Finally, the FTC reminds companies of the need to provide consumers with a simple and easy way to cancel negative option contracts.

**PUTTING IT INTO PRACTICE: This enforcement policy statement signals the FTC's increased scrutiny of negative option programs. It also gives direction about what it considers to be appropriate "express informed consent."**

## Impact of NYC's New Delivery Service Data Sharing Requirement

*Posted September 29, 2021*

New York City recently amended its law governing third party delivery services, with the changes going into effect December 27, 2021. The revised law specifically permits restaurants to ask for customers' personal information from the delivery service. The delivery service, in turn, must tell consumers about the potential sharing "in a conspicuous manner" on its website and give people the ability to opt-out of such sharing. That notice needs to indicate that the person's information will be shared with the restaurant, and needs to identify the restaurant.

If requested by the restaurant, the delivery service will need to provide the information on customer-specific, monthly basis and in a "machine-readable format." Delivery services will need to scrub out anyone who has opted out. Restaurants who receive information from the delivery services under this new law cannot sell or otherwise share the information unless they have gotten express consent from the customer. Restaurants also have to let customers opt-out of having their information used by the restaurants. The requirements do not apply to phone orders, and the law makes clear that both parties still need to comply with applicable laws.

The law has been criticized; indeed one delivery service has sued arguing that the provisions violate consumers' privacy. The city, on the other hand, views this as a way to financially support restaurants in light of struggles resulting from the COVID pandemic. It has introduced this measure along with others in its changing approach to regulating food delivery.

**PUTTING IT INTO PRACTICE: Provided that there are no delays in implementation, restaurants operating in New York City will be able to ask delivery services for customer information starting December 27, to the extent that such requests are not already provided for in the contracts between the parties. Delivery services will need to prepare by making the requisite disclosures when collecting customer information.**

## Supreme Court Decision Impacts How FTC May Pursue Privacy Cases

*Posted June 7, 2021*

The Supreme Court recently dealt a potential blow to the FTC's enforcement tool chest. In particular, the decision impacts its ability to seek monetary relief under a theory it has used in a wide variety of cases, included privacy and security ones, that monetary relief constitutes a "permanent injunction" on consumers' behalf. In AMG Capital Management, LLC v. Federal Trade Commission, the Supreme Court held that while the FTC should be able to obtain injunctive relief to stop unfair practices, that power does not extend to seeking monetary relief for injured consumers.

The dispute in front of the Supreme Court involved the interpretation of Section 13(b) of the FTC Act, which allows the Commission to seek "permanent injunctions." Historically, the FTC interpreted that provision to also allow it to seek monetary remedies to return money to injured consumers. The Supreme Court disagreed. At issue in the AMG case were allegations of deceptive payday lending (unfair practices under the FTC Act). The FTC had sought not just injunctive relief, but payment of $1.27 billion in restitution. While the Ninth Circuit allowed the payment, the Court rejected it.

Shortly after this opinion was issued, the FTC signaled its intent to continue pursuing monetary penalties by other avenues, and encouraged Congress to "restore and strengthen the powers of the agency." In the meantime, the agency has indicated that it plans to grow partnerships with state attorneys general, who can seek monetary penalties under state laws. The decision also does not impact the agency's ability to seek civil penalties in the event of a violation of an FTC order (Section 5(l) violations), nor its ability to obtain consumer redress through the (arguably cumbersome) process of Section 19. These two avenues are not as immediate, however, as the permanent injunctive relief the FTC had used prior to the Court's decision.

**PUTTING IT INTO PRACTICE: This decision suggests that the FTC may be more active in bringing joint enforcements in a wide variety of cases -including privacy and security cases- with state AGs. Companies should keep this in mind when planning privacy and data security programs, and would be well served by looking to expectations of fairness not just as signaled by the FTC, but state AGs as well.**

## What Is FTC's Course Under Biden?

*Posted March 11, 2021*

The new acting FTC chair, Rebecca Kelly Slaughter, recently signaled that the FTC may increase enforcement and penalties in the privacy and data security realm. Slaughter pointed to several areas of focus for the FTC this year, which companies will want to keep in mind:

- **Notifying Consumers About FTC Allegations:** Slaughter referred favorably to two recent cases: (1) the Everalbum biometric settlement from earlier this year (which we wrote about at the time); and (2) the Flo Health settlement over alleged deceptive data sharing practices (which we also wrote about at the time). In drawing on these two cases, Slaughter indicated that in future cases the FTC intends to include as part of any settlement a requirement to notify customers of any FTC allegations. This, she said, would allow consumers to "vote with their feet" and help them decide whether to recommend their services to others.
- **FTC Intent to Plead All Relevant Violations**: According to Slaughter, another lesson the FTC is taking from the Flo case is to include in the cases it brings all potentially applicable violations of all relevant privacy-related laws. In the Flo case, Slaughter said the FTC should have pleaded a violation of the Health Breach Notification Rule, which requires that vendors of personal health records notify consumers of data breaches.
- **Focus on Ed Tech and COPPA:** Given the explosive growth of education technology during COVID-19, the FTC is conducting an industry sweep of the industry. Related to this, the FTC is reviewing its Children's Online Privacy Protection Act Rule. This goes beyond the refresh the agency did of their FAQs earlier in the pandemic (which we wrote about at the time). For now, Slaughter reminds companies that parental consent is needed before collecting information online from children under the age of 13.

- **Examination of Health Apps**: The FTC will take a closer look at health apps, including telehealth and contact tracing apps, as more and more consumers are relying on such apps to manage their health during the pandemic.
- **Overlap Between Competition and Privacy**: Slaughter also indicated that it is worth looking at situations where there may be not only privacy concerns, but antitrust as well. Because the FTC has a dual mission (consumer protection and competition) she notes that it has a "structural advantage" over other regulators in that it can look at these issues, especially since -she states- "many of the largest players in digital markets are as powerful as they are because of the breadth of their access to and control over consumer data."
- **Racial Equity and AI/Biometrics/Geotracking:** Slaughter noted that COVID-19 is exacerbating racial inequities. She pointed to the unequal access to technology, as well as algorithmic discrimination (the idea that discrimination offline becomes embedded into algorithmic system logic). The FTC intends to focus on algorithmic discrimination, as well as on the discrimination potentially embedded into facial recognition technologies. (This mirrors concerns that gave rise to the recent Portland facial recognition law, which we recently wrote about). Finally, Slaughter commented on the use of location data to identify characteristics of Black Lives Matter protesters, and said she is concerned about the misuse of location data to track Americans engaged in constitutionally protected speech.

**PUTTING IT INTO PRACTICE: Companies that operate health apps, that are in the education technology space, or that use algorithms or facial recognition tools will want to keep in mind that these are areas of focus for the FTC. And for everyone, keep in mind that the FTC has indicated it will beef up privacy law penalties and will ask for more notification to injured consumers.**

# CROSS-BORDER DATA TRANSFERS

## China Draft PIPL Measures Outlines Thresholds for CAC Security Assessments

*Posted November 11, 2021*

The Chinese agency charged with implementing and enforcing the new Personal Information Protection Law has issued draft measures for cross-border data transfers. Comments are due by November 28. As we detailed previously, the law requires that the Cyberspace Administration of China (CAC) conduct security assessments prior to certain information transfers out of China. Those situations included if the information transferred reached "significant" thresholds. Those thresholds have now been clarified in the draft.

In particular, the draft contemplates security assessments for transfers by entities that handle over one million individuals' personal information. Security assessments would also occur if the entity is either transferring personal information of more than 100,000 people or "sensitive" information of more than 10,000 people. In most situations security assessments would be valid for two years.

Under PIPL, both entities who do not meet the thresholds for a CAC-led assessment, as well as those who do, must complete an internal self-assessment before transferring data outside of China. The draft outlines the specifics of that self-assessment. This includes looking at the risk of data leaks, the volume and scope of information to be transferred, and the like.

The draft also provides more insight into requirements around having a data transfer agreement when sharing personal information with a third party. Elements to include in the agreement are similar to GDPR, such as outlining security measures that will be used, limiting the scope of use by the data recipient, and having contractual penalties for contract violations. Also included is a requirement to indicate where, physically, data will be stored outside of China.

**PUTTING IT INTO PRACTICE: While the law was effective November 1, this draft is still under review. It does, however, provide guidance about expectations about what companies must do under the law, including thresholds for needing a CAC assessment.**

## Free Data Flow to the UK May Continue – EU Adopts Adequacy Decision

*Posted June 28, 2021*

The European Commission announced today a long-awaited decision that the UK data protection standards are adequate under the meaning of GDPR's Article 45, providing a mechanism to enable transfer of data from the EU to the UK without the need for additional authorisation or putting in place additional safeguards. This decision will be in force for four years but can be withdrawn if the UK were to lower its standards and no longer provide EU citizens adequate protection for their personal data. The decision excludes personal data that is transferred for purposes of United Kingdom immigration control.

In the bleak aftermath of Brexit this is a positive development for many businesses on both sides of the English Channel and provides for much needed legal certainty for data flows between the EU and the UK without the need to implement any additional transfer mechanism such as the newly issued EU standard contractual clauses.

A European adequacy decision was expected not least as the UK only recently implemented its Data Protection Act 2018 which is broadly in line with the GDPR. There continue to be concerns that the UK will eventually diverge from EU standards not least given the ongoing political debate in the UK post-Brexit to alleviate UK businesses from the requirements of the GDPR. For now the European Commission was not convinced that these concerns were justified.

**PUTTING IT INTO PRACTICE: The UK now joins the group of other 12 countries (Andorra, Argentina, Canada (commercial organisations), Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, Switzerland and Uruguay) which so far have benefited from an EU adequacy decision.**

## Update on the State of Privacy Law In China

*Posted May 13, 2021*

China is continuing to move forward with its first comprehensive privacy law. China recently issued a second version of the draft Personal Information Protection Law (Draft PIPL) which will be open for public comments until May 28, 2021. (An earlier version of the law was released at the end of 2020.) The law is anticipated to come into effect sometime in the next one to two years.

**Current State of Laws**

China does not currently have a comprehensive data privacy law. There are some rules about data protection and use scattered in existing laws, national standards and governmental guidelines. For example, the country's current Cybersecurity Law, which came into effect in June 2017, is focused on the "critical information infrastructure." Specifically, the law is directed at "network operators" (anyone owning or operating a computer system network), and suppliers of network products and services.

Over the past several years, China has also issued other related guidance. While still in draft form, this includes the Security Assessment on Cross-border Transfer of Personal Information and Guidelines for Personal Information Security Engineering. Other recent sectoral guidance also indirectly impact how companies use and protect information in China. For e-commerce, this includes the Measures for the Supervision and Administration of Online Transactions. There have also been several rules released aimed at improving data governance in China's financial sector (e.g., Guidelines for Data Capacity-Building in the Financial Industry). And other recently released standards touch on facial recognition data and data collected from connected cars.

**Draft Data Security Law**

When thinking about the impact PIPL will have, China's draft Data Security Law (DSL) should also be kept in mind. The second version of DSL was also recently released. The Draft DSL primarily applies to "important data" or data that has national security concerns for China. The Draft DSL It primarily applies to "important data" or data that has

national security concerns for China. Practically speaking, this law may require the need to designate data security personnel and management bodies to ensure responsibility over data security. It may also require conducting risk assessments and submitting reports of those assessments to the applicable authorities. The Draft DSL also calls for mandatory reporting requirements for data security incidents. Once finalized, the PIPL and DSL, coupled with the Cybersecurity Law, will form the over-arching legal framework for data privacy and protection in China.

**Preparing for PIPL**

The Draft PIPL has a broad extra-territorial effect similar to that of the EU's GDPR. Namely, the law applies to processing of personal information that happens outside of China if the purpose of the processing is to (i) to provide products or services to individuals in China, (ii) to "analyze" or "assess" the behavior of individuals in China, or (iii) for other purposes to be specified by laws and regulations. Thus, even if an organization does not have a physical presence or legal entity in China, the law could still apply.

While the law is still in draft form, companies that expect PIPL to apply to them may want to begin thinking now through some of the potential operational changes of this law. Some of these considerations are highlighted below:

**Basis of Processing**. Unlike the current Cybersecurity Law, where "consent" is the only available legal basis for collecting and using of personal information, the Draft PIPL is more like GDPR. It permits multiple legal bases for processing. Nonetheless, there are still some types of processing that must be based on consent. For example, when processing information about someone under 14, sharing biometric-type information for non-security purposes, and processing sensitive information. The law also calls for processing to be based on a "minimum necessary" standard. Like GDPR, there are requirements for engaging in automated decision-making.

**Data Subject Rights**. The Draft PIPL proposes various data subject rights. This includes a right to information and explanation on the data processing. Individuals will also have a right to access, right to correction, right to object processing, right to withdraw consent and a right to deletion.

**Localization**. Critical information infrastructure operators and entities who process personal information of a certain volume (the threshold is currently unspecified) are required to store the personal information collected and generated within the borders of China. If information needs to be transferred overseas, a company will have to pass a security assessment organized by the Cyberspace Administration of China.

**Cross-border Transfers**. In addition to the security assessment for certain organizations, the law requires notice and consent for cross-border transfers. Companies must carry out an internal risk assessment prior to transferring data out of China and keep records of such transfers. A lawful transfer mechanism such as a standard transfer agreement, or a security assessment administered by the Cyberspace Administration of China is also required.

**Data Breach Notification**. In the event of a data breach, the Draft PIPL requires entities to take "immediate" remediation actions and notify the relevant agency and affected individuals. The text itself does *not* provide a time limit for notification (e.g., 72-hours).

**Penalties**. Under the Draft PIPL, an organization that unlawfully processes personal information or fails to take necessary security measures to protect personal information may be subject to a baseline fine up to 1 million RMB. If the violation is considered serious, the fine may be increased up to 50 million RMB or 5% of the organization's annual revenue for the prior financial year.

**PUTTING IT INTO PRACTICE: Companies who are already addressing GDPR or CCPA requirements will find some aspects of China's draft laws familiar. While the laws have not yet been finalized, they are expected to be passed in the next year or two. Now is a good time, then, to start thinking about how to offer GDPR-type rights in China, as well as preparing for breach notice requirements and data transfer issues.**

# DATA BREACH

## Breach of PHI? California AG Reminds Companies of Potential State Notification Obligations

*Posted August 27, 2021*

The California AG recently reminded companies in the healthcare industry of potential data breach notification obligations beyond HIPAA. As ransomware attacks continue to rise, particularly in healthcare, companies should keep in mind the patchwork of state and federal health data privacy laws that may apply.

Companies may have obligations under both federal and state laws to protect information. In the healthcare space, this means that entities subject to HIPAA either as a covered entity or business associate may also be subject to other more stringent state medical information laws or other general data security laws – in addition to the HIPAA Security Rule. *Some* (but not all) of these state general data security laws include certain exemptions for HIPAA-regulated entities, or for information subject to or protected under HIPAA. However, these laws may still apply to health or medical information that is not subject to HIPAA. Similar to OCR's recent reminder about ransomware, the California AG similarly called for entities collecting and storing health-related information to take preventative measures against these attacks. This includes, at minimum:

- keeping systems and software up-to-date,
- installing and maintaining virus protection
- providing regular data security training, including education about phishing
- restrict users from downloading and installing unapproved software; and
- maintain and test regularly data backup and recovery plan.

In addition to obligations to protect information, federal and state laws have specific breach reporting requirements. While some requirements may overlap, the state obligations may trigger notice to additional regulatory authorities. For example, in California, entities subject to HIPAA must also report security breaches of more than 500 California residents to the California's AG's office.

**PUTTING IT INTO PRACTICE: The California AG's bulletin provides insight into what the agency might expect companies to be doing to prevent cyberattacks. It also serves as a reminder of potential state breach reporting obligations for HIPAA-regulated entities. States other than California have similar requirements. It also suggests that AG will likely be keeping a close watch on breaches reported under HIPAA (either through media notices or the OCR breach portal) that go unreported to the office. The AG also signaled in the bulletin that this area will likely be an increasing enforcement priority by noting its authority to bring civil actions for violations of HIPAA.**

## Connecticut Expands Data Breach Notification Law, Changes Effective October 1, 2021

*Posted June 26, 2021*

In addition to recently passing a cybersecurity safe harbor law, Connecticut also updated its data breach notification law. Connecticut joins Texas in passing changes to breach notification requirements this year. There are three key changes included in this amendment.

- **Expansion of the definition of "personal information"**. Falling in line with many other states, the law now broadens "personal information" to also include (i) taxpayer identification number; (ii) IRS identity protection personal identification number, (iii) passport number, military ID or other government ID; (iv) certain medical

information; (v) health insurance policy information; (vii) biometric information; and (viii) a user name or email address in combination with a password or security question and answer (regardless of whether or not the individual's name is accessed in combination with it), in addition to the other existing elements.

- **Shortened Notification Requirements**. The time businesses have to notify affected Connecticut residents and the Office of the Attorney General of a data breach has been shortened from 90 days to no later than 60 days after discovery of the breach. Further, if notice cannot be made within the new 60-day window, companies are to provide preliminary substitute notice to individuals and follow up with direct notice as soon as possible.
- **HIPAA/HITECH Exemption, Except for AG Notice**. If notice is provided to Connecticut residents in compliance with HIPAA and HITECH, then the notice is deemed compliant with Connecticut requirements. However, notice must still be provided to the Connecticut Attorney General (no later than when notice is provided to residents).

**PUTTING IT INTO PRACTICE: Beginning October 1, companies who suffer a breach impacting Connecticut residents will want to keep in mind these changes. Namely, the expanded definition of personal information and shortened notification timelines.**

## Texas Breach Notification Law Amended, Changes Effective September 1, 2021

*Posted June 28, 2021*

Texas's data breach notification law was recently amended to require the state's Attorney General to post notice of data breaches on a public website within 30 days of receiving notice of the data breach. It also requires companies to provide the AG with more information when notifying the AG of a breach.

Under existing Texas law, data breaches that impact 250 or more Texas residents must be reported to the state Attorney General within 60 days of becoming aware of the breach. Such notice currently requires companies to describe the breach, steps taken "regarding the breach," whether law enforcement was involved, and the number of impacted state residents. Under the amended law, businesses will also be required to report the number of impacted Texans *who were sent notice of the breach*.

The new amendment also requires the Texas Attorney General to maintain a publicly accessible list of breach notifications submitted to the Attorney General's Office. Within 30 days of receiving a data breach notification, the Texas AG must post a notice of such breach to their website. In posting such notice, the AG is instructed to exclude reported sensitive personal information, information that may compromise a system's security or information that is confidential by law. Such notice is to be removed from the website after one year if the business reporting such breach does not report another breach during that period.

**PUTTING IT INTO PRACTICE: This change means that Texas, like Puerto Rico, will now require the Attorney General to publicly post the breach notices it receives from companies. While other states' AGs do engage in this practice, it will be mandated under Texas law. Companies should keep this in mind when drafting any potentially required notice to the Texas AG.**

## Booking.com Fined By Dutch DPA For Breach Notice Delay

*Posted April 29, 2021*

The Dutch Data Protection Authority recently imposed a €475,000 fine ($558,000) against the hotel website Booking.com for waiting longer than 72 hours to report a data breach. According to the Dutch DPA press release, Booking.com learned of the breach on January 13, 2019 and reported it to the DPA on February 7, 2019. The DPA did not make it clear in that release whether Booking.com had, in fact, determined on January 13, 2019 that a security breach impacting personal information of Dutch citizens had occurred or whether January 13, 2019 was date that Booking.com was first alerted to suspicious activity.

The situation arose when hackers persuaded hotel staff to reveal their Booking.com account log-in details. The hackers then used these credentials to log into Booking.com, and stole information of more than 4,109 Booking.com customers, including names, addresses, phone numbers and details about their bookings. Also taken was a smaller number of credit card numbers (283) and along with security codes for a smaller percentage (97). Booking.com notified impacted individuals on February 4, 2019, three days before it notified the Dutch DPA. The DPA decision was based only on late notification, not for causing or being at fault for the underlying breach.

**PUTTING IT INTO PRACTICE: This decision is a reminder that EU regulators expect to be notified within 72 hours of a company "becoming aware of a personal data breach." This would in almost all circumstances occur *before* notification to individuals. Companies should take care to continuously scrutinize the facts being gathered and discovered during an investigation to be able to track the date on which they first discover facts that would confirm or suggest a personal data breach has occurred.**

## Utah Creates Data Breach Safe Harbor

*Posted April 12, 2021*

Utah recently amended its breach notice law to provide certain defenses to companies who suffer a data breach. It is now the second state, after Ohio, to include such provisions. Specifically, entities that create and reasonably comply with a written cybersecurity program may have an affirmative defense to litigation resulting after a data breach. For the safe harbor to apply, the written cybersecurity program must:

- be designed to protect against the security, confidentiality and integrity of personal information and anticipated threats and hazards;
- reasonably conform to a recognized cybersecurity framework like NIST 800-171 or 800-53, ISO 27000, PCI DSS, and federal laws such as HIPAA and GLBA (among others); and
- be appropriate to the "scale and scope" of the company, the information it collects, the activities in which it engages, and its resources and tools available.

Even if a written cybersecurity program is in place, there are certain exceptions. For example, if the entity had actual notice of a threat to the security of the personal information. Or, if it did not act in a reasonable amount of time to take known remedial efforts to protect the personal information.

**PUTTING IT INTO PRACTICE: The Utah and Ohio laws provide incentives for companies to protect information in light of the safe harbor from certain litigation claims after a data breach. As a reminder, beyond these laws, many states require a written cybersecurity program as part of their data security laws.**

## Successful Dismissal of PayPal Class Action Over Breach Disclosures Serves as Risk Reminder

*Posted February 4, 2021*

A class action lawsuit filed against PayPal in connection with a breach it suffered in 2017 was dismissed recently because the plaintiffs did not adequately allege PayPal's intent to deceive investors. The litigation began after PayPal's acquired TIO Networks Corporation, a smaller payment processor and platform. Post-acquisition, PayPal announced that it had discovered "security vulnerabilities" in TIO's operations and it thus suspended TIO's operations. At that point, TIO had not yet been integrated into PayPal's platform. PayPal confirmed that it was investigating TIO's security measures with the help of outside assistance, and that PayPal customers' data remained secure. PayPal further confirmed that it was not aware of any breach of personal information maintained by TIO. The following month, however, PayPal announced that a breach of personal information had in fact occurred. Confidential information belonging to 1.6 million customers had been potentially compromised, causing PayPal's stock price to drop by 5.75%.

Plaintiffs, who bought stock between the two announcements, filed a putative class action lawsuit in California, alleging that they had purchased PayPal stock at fraudulently inflated prices. Plaintiffs alleged that the prices had been inflated because PayPal did not disclose the security breach and its potential magnitude in its original announcement. The district court dismissed the case for failure to plead sufficient facts. Namely, the plaintiff stockholders had not shown a "cogent and compelling" inference that PayPal made material representations with intent or "deliberate recklessness."

The stockholders appealed, but the Ninth Circuit affirmed the district court's ruling in PayPal's favor. The court did not believe that the original disclosure was misleading, noting that PayPal had disclosed what information it had at the time. In reaching its decision, the Ninth Circuit also pointed to the fact that none of the defendants had sold stock during the intervening period between the two announcements. This suggested that they had no material, non-public information that they were taking advantage of.

**PUTTING IT INTO PRACTICE: This decision is a reminder of the risks associated with public announcements relating to potential data security incidents, as well as the close scrutiny that individuals, regulators, and courts may subsequently take when looking at a company's cybersecurity risk disclosures and the timing of stock sales. Companies should consult closely with counsel when making a public announcement regarding a potential or confirmed data security incident to ensure they are thinking through the potential regulatory and litigation risks, whether a trading blackout period is appropriate during the period of investigation, and whether existing cybersecurity risk disclosures in the company's public filings should be amended.**

## Companies Have Until March to Comment on EDPB Data Breach Notification Guidelines

*Posted February 1, 2021*

Many supervisory authorities across Europe have reported increasing numbers of data breach notifications since the introduction of GDPR. While most companies are now familiar with the 72-hour reporting obligation for controllers to supervisory authorities, whether such obligation has been triggered continues to present unique and complex questions in each specific security event. To help aid companies sorting through these potential legal notification obligations in the aftermath of a security event, the EDPB recently released draft guidance, which is open for comment until 2 March 2021.

The guidelines are intended to supplement the October 2017 general guidance provided by the Article 29 Working Party, the predecessor to the EDPB. The guidelines walk through 18 examples covering the most common security event scenarios, including ransomware attacks, data exfiltration attacks, human errors lost or stolen devices and paper documents, "mispostal," and social engineering, such as identity theft and email exfiltration. For each example scenario, the EDPB identifies whether notification would be required to the relevant supervisory authority or data subjects, as well as mitigation measures.

The guidelines also note several recommendations for data breach management such as implementing plans, procedures and guidelines, regular employee training, and documenting breaches in each and every case, irrespective of the risk they pose.

**PUTTING IT INTO PRACTICE: Notification obligations are very fact specific and will depend on the circumstances of each unique event. Organizations are reminded of the importance of data breach preparedness efforts. This includes activities such as preparing incident response plans and playbooks, training of those plans, simulating an event through a tabletop scenario, and reviewing cyber insurance policies. The EDPB guidelines are open for public comment until March 2, 2021. Feedback may be submitted here.**

## New York and Others Settle with CafePress Over 2019 Data Breach

*Posted January 12, 2021*

The operator of CafePress, an online retailer that sells customizable mugs and other products, has reached an agreement with New York State Attorney General Letitia James and six other State Attorneys Generals to settle claims related to a 2019 data breach. The breach stemmed from a cyberattack that the company suffered in early 2019. Upon learning of the attack, the company engaged a third-party investigation firm that identified a vulnerability in the company's Structured Language Query (SQL) protocols. As a result, CafePress looked at its database and two weeks of logs but did not find evidence of any data breach. Regardless, CafePress released a security patch to fix the vulnerability and automatically reset the passwords of all customer accounts, requiring all users to reset their passwords upon logging in.

Several months later the website "Have I Been Pwned," a site that lets people see if their personal information has been compromised online, added the email addresses associated with the CafePress customers compromised by the breach to its website. At that point, according to the settlement, CafePress launched a full-scale investigation into the matter. It found that customer information was available for sale on the dark web. In the end, the company determined that as many as 22 million customer accounts, including consumer names, email addresses, passwords, physical addresses and phone numbers as well as 186,179 social security and/or tax identification numbers had been impacted. Although CafePress notified those impacted and offered two years of credit monitoring and theft resolution services to customers whose social security numbers were compromised by the breach, Attorney General James was concerned both that CafePress failed to provide sufficient protection for its customers' personal information and also that CafePress failed to notify their customers of the data breach promptly. The other states in the coalition led by Attorney General James were Connecticut, Indiana, Kentucky, Michigan, New Jersey, and Oregon.

The multi-state settlement agreement announced on December 18, 2020 requires CafePress to make a $2 million payment to the multi-state coalition, $750,000 of which will be divided among the states affected, and the remainder of which will be held in a suspended account. PlanetArt, LLC, the company who purchased substantially all of CafePress's assets, has agreed to all provisions of the settlement. As part of the settlement, the company has also agreed to several specific data security steps it will take moving forward. Namely, that it will:

- create and update a comprehensive information security program to keep pace with technological improvements and security threats, and report security risks to the company's CEO;
- design and implement an incident response and data breach notification plan to address threat preparation, detection and anaFlysis, eradication, and recovery, which plan requires investigation of incidents that are suspected to be security events;
- ensure that personal information safeguards and controls are in place, including encryption, segmentation, penetration testing, logging and monitoring, and risk assessment, password management and data minimization plans;

- provide clear notice to consumers regarding account closure and data deletion; and
- ensure that third-party security assessments occur for the next five years.

**PUTTING IT INTO PRACTICE: This settlement serves as a reminder that state regulators expect companies not only to provide appropriate protection to data they hold, but also to appropriately investigate cyber-attacks and other suspected security incidents.**

# DATA SECURITY

## 2021 Cybersecurity Recap for Government Contractors (and What to Expect in 2022) – Part 4 of 4: Cybersecurity Maturity Model Certification ("CMMC") 2.0

*Posted December 22, 2021*

As 2021 draws to a close, we wanted to share a recap of some of the most important cybersecurity developments we covered this past year along with some suggestions on what companies (particularly those that do business with the federal government) should expect in 2022. This is part four of a four-part series (you can read Part 1 here, Part 2 here, and Part 3 here.

In November 2021, the Department of Defense (DOD) announced an updated version of its cybersecurity certification program – CMMC 2.0 – which includes several changes as compared to the original CMMC program. CMMC 2.0 takes a risk based approach to protecting sensitive defense information in company systems through rigorous security requirements and third party certifications or company self-attestations. We discussed the specific revisions and related implementation timeline here and here.

**PUTTING IT INTO PRACTICE: What to expect in 2022: We expect the formal rulemaking process (including opportunity to comment) for CMMC 2.0 to begin sometime in 2022 (although CMMC generally has been plagued by delays). Once it begins, DOD estimates the rulemaking process will take anywhere from 9-24 months. In the meantime, companies that work in the DOD space should be following closely all proposed cybersecurity developments and prepare for the implementation of CMMC 2.0 by continuing to monitor and enhance their cybersecurity posture.**

## 2021 Cybersecurity Recap for Government Contractors (and What to Expect in 2022) – Part 3 of 4: Cyber Incident & Ransomware Payment Reporting Legislation

*Posted December 21, 2021*

As 2021 draws to a close, we wanted to share a recap of some of the most important cybersecurity developments we covered this past year along with some suggestions on what companies (particularly those that do business with the federal government) should expect in 2022. This is part three of a four-part series (you can read Part 1 here and Part 2 here).

We have been keeping a close eye on proposed legislation related to cyber incident and ransomware payment reporting. Certain proposed legislation initially included in draft versions of the 2022 National Defense Authorization Act (NDAA) would have required critical infrastructure providers and contractors to report cyber incidents within 72 hours and ransomware payments within 24 hours. Despite widespread bipartisan support, these provisions were removed from the final version of the NDAA.

**PUTTING IT INTO PRACTICE: What to expect in 2022: Many lawmakers appeared genuinely disappointed that the language was removed from the NDAA and have indicated enacting the proposed legislation will be a priority in the new year.**

## 2021 Cybersecurity Recap for Government Contractors (and What to Expect in 2022) – Part 2 of 4: Department of Justice (DOJ) Civil-Cyber Fraud Initiative

*Posted December 20, 2021*

As 2021 draws to a close, we wanted to share a recap of some of the most important cybersecurity developments we covered this past year along with some suggestions on what companies (particularly those that do business with the federal government) should expect in 2022. This is part two of a four-part series (you can read Part 1 here).

On October 6, 2021, the DOJ announced a new Civil Cyber-Fraud Initiative to enforce cybersecurity standards and reporting requirements. The Initiative will use the False Claims Act to pursue companies that do business with the government as well as federal grant recipients that "knowingly provid[e] deficient cybersecurity products or services, knowingly misrepresent[] their cybersecurity practices or protocols, or knowingly violat[e] obligations to monitor and report cybersecurity incidents and breaches." You can read our article about the initiative here.

**PUTTING IT INTO PRACTICE: What to expect in 2022: We expect DOJ will pursue enforcement actions against companies next year. As these actions progress – in addition to the possibility of companies agreeing to pay hefty amounts to settle – we hope to gain additional insight into the specific types of cybersecurity infractions the government intends to pursue. In the meantime, companies should keep this enforcement initiative in mind as they develop or enhance their cybersecurity policies or take on new cybersecurity contract clauses and seek to limit risk by ensuring they understand, and can comply with, government data security and reporting requirements.**

## 2021 Cybersecurity Recap for Government Contractors (and What to Expect in 2022) – Part 1 of 4: Biden's Cybersecurity Executive Order (EO 14028)

*Posted December 17, 2021*

As 2021 draws to a close, we wanted to share a recap of some of the most important cybersecurity developments we covered this past year along with some suggestions on what companies (particularly those that do business with the federal government) should expect in 2022. This is part one of a four-part series.

On May 12, the Biden Administration issued its much anticipated "Executive Order on Improving the Nation's Cybersecurity," which – with over 55 deliverables – has been the driving force behind may of our updates this year. In addition to many internal government initiatives, the EO calls for new data security and incident reporting regulations, publication of requirements for secure software development practices, and establishment of criteria for consumer labeling programs for software and Internet of Things (IoT) devices. You can review our initial article on the EO here, and some additional related articles here (discussion relating to "critical software"), here (draft guidance relating to cloud computing), here (comments on Zero Trust architecture), and here (publication relating to cyber supply chain risk management).

**PUTTING IT INTO PRACTICE: What to expect in 2022: The next EO deliverables are due in February 2022 and relate to solidifying practices for enhancing the security of the software supply chain, and publicizing criteria for the software and IoT consumer labeling programs. Additionally, companies that do business with the federal government (either directly or indirectly through a supplier or reseller) should be keeping an eye out for new proposed rules (e.g., FAR Case 2021-017) that likely will increase instances in which information about cyber threats and incidents must be shared with the Government by certain providers.**

## Updates Announced to Department of Defense Cybersecurity Certification Program

*Posted November 10, 2021*

The Department of Defense (DOD) recently announced several changes to its Cybersecurity Maturity Model Certification program. The program applies to those who serve as contractors and suppliers to the DOD. As described in our sister blog, the new version of the program – "CMMC 2.0" – has several important differences from the original program. CMMC 2.0 is anticipated to go into effect anywhere from nine to 24 months from now.

Key differences include:

- Restructuring the program to allocate information systems into three levels (rather than five) depending on the type of information companies maintain within those systems. Depending on level, companies need to provide different levels of security for the information they handle.
- Allowing Level 1 companies to self-assess (rather than having assessment and certification by a third-party). Also allowing self-assessment for certain acquisitions at Level 2.
- Aligning the required practices with National Institute of Standards & Technology (NIST) cybersecurity standards.
- Increasing oversight of third-party assessors.

Allowing companies who have not yet met compliance requirements to remediate under strict timelines. Also includes waivers in limited circumstances.

The new program aligns with current regulations regarding protection of Controlled Unclassified Information (CUI). These regulations already require NIST SP 800-171 as the minimum level of security for CUI. They also require a self-assessment or DOD assessment against the NIST SP 800-171 controls and an associated report to DOD.

**PUTTING IT INTO PRACTICE: Companies who contract with the DOD (or are part of the DOD supply chain) will want to review their cybersecurity program and update their compliance plans to ensure that they are working towards the new streamlined CMMC 2.0.**

## Do You Have a Risk-Based Sanctions Compliance Program?: In the Event of a Ransomware Attack, OFAC Wants to Know

*Posted October 4, 2021*

In the wake of increased ransomware attacks over the course of the last several months, the US Department of Treasury's Office of Foreign Assets Control (OFAC) has updated a guidance it released last year on potential sanction risks if facilitating ransomware payments. As indicated in the original guidance, OFAC has designated several threat actors as "malicious cyber attackers," including the developers of Cryptolocker, SamSam, WannaCry, and Dridex. OFAC has indicated that it will impose sanctions on those who financially (or otherwise support) these actors, including by making ransomware payments to them. Sanctions can range from non-public (for example No Action Letters or Cautionary Letters) to public actions (including for example payment of civil monetary penalties).

In this new guidance, OFAC has indicated what factors would be "more likely" result in the matter closing with a non-public action. They are improving cyber security practices prior to an incident and working closely with law enforcement in the event of an incident. Improvement measures mentioned by the guidance include keeping backups (offline), having an incident response plan, conducting training, updating virus software, using authentication protocols, and otherwise following the Cybersecurity and Infrastructure Security Agency's 2020 guide on ransomware. In other words, a risk-based compliance program to mitigate potential exposure if a company finds itself in a position of potential exposure to sanctions' violations. This guidance came on the heels of OFAC's sanctions of a cryptocurrency for its involvement in payment to ransomware threat actors (see article on our sister blog).

**PUTTING IT INTO PRACTICE: Is your organization prepared for a potential cyber incident? The cyber security practices outlined in OFAC's guide can not only help a company be prepared for a potential incident, but also put it in a better posture in the event a ransomware demand is made.**

## FTC Surveillance App Settlement Signals Concern Over Deceptive Tracking

*Posted September 22, 2021*

The FTC recently settled with a surveillance app operator over allegations that the company facilitated the secret harvesting of personal information. According to the FTC, the main users of Support King, LLC's "SpyFone" app were bad actors who used the tool to remotely monitor users' physical and digital activities. The FTC dismissed the company's argument that the users were employers and parents as a "pretext." It felt neither group would want to use the product, which to install required minimizing the device's security settings and potentially voiding the device warranty.

Service King failed to take reasonable steps, the FTC felt, to make sure the app was used for legitimate reasons and not by potential stalkers. The FTC also found the company's practices deceptive. Namely, the company said it "took all reasonable precautions" to protect personal information. The FTC disagreed. Instead, it said, the company's insufficient security practices resulted in a 2018 data breach. The company also -according to the FTC- deceptively indicated that it had "coordinated with law enforcement authorities" and "leading data security firms" on the incident, when in fact it had not done so.

As part of the settlement, Support King has agreed to cease marketing and selling its app, to delete personal information collected from its software, and to notify affected individuals. The company also agreed to create an information security program and obtain regular third-party assessments.

**PUTTING IT INTO PRACTICE: This case, which arose after a data breach, is a reminder that when products facilitate tracking and monitoring users, the FTC will take a careful look at a company's practices. This includes examining the typical users of such products.**

## SEC Fine Highlights Importance of Cybersecurity Disclosures

*Posted August 25, 2021*

The SEC recently announced a settlement with Pearson plc where the company has agreed to pay $1 million to settle charges that it misled investors about a 2018 cyber incident. According to the order, Pearson made misleading statements and omissions about a 2018 data breach involving the theft of student data and administrator credentials in its July 2019 semi-annual report.

Pearson is a UK-based education and publishing company, and provides services to both K-12 schools and universities. As part of the provision of its services, school administrators are provided with login credentials, and 13,000 of those credentials -as well as student emails and dates of birth- were impacted in the cyber incident. Pearson learned of the incident in March 2019, and four months later, after its investigation, notified impacted individuals. Pearson's management determined that no public statement needed to be issued, and the day after the board met (and seven days after notice was sent to impacted individuals), the company issued its semi-annual report (Form 6-K) which did not mention the cyber incident, instead referring to data privacy incidents as a hypothetical risk – mirroring language from past reports. After issuing its 6-K, Pearson was contacted by a national media outlet about the incident, and only then did it release a statement to the media and post information about the incident to its website.

The SEC cited Pearson with violations of the Securities Act and the Exchange Act for failure to have appropriate processes and procedures around the drafting of its Form 6-K Risk Factor disclosures, for misleading and inaccurate details in its disclosures, and for omitting key details about the incident (such as the volume and type of data impacted) in its media statement. While Pearson did not admit wrongdoing, it agreed to pay a $1 million penalty as part of the settlement.

**PUTTING IT INTO PRACTICE: This case highlights the importance of appropriately analyzing incidents and assessing their materiality to determine if they need to be disclosed in company filings. Companies would be well served to review their controls and procedures, including how incidents are reported to management, what processes management has in place for analyzing materiality, and how its disclosures can quickly and effectively be modified or updated as the result of an incident.**

## Connecticut Enacts New Cybersecurity Safe Harbor

*Posted July 22, 2021*

Connecticut recently enacted cybersecurity legislation that provides a safe harbor for businesses that implement a written cybersecurity program. Under the legislation, set to go in effect on October 1, 2021, punitive damages will not be assessed on a business that has suffered a data breach, in the event that there are causes of action alleging a failure to implement reasonable cybersecurity controls, which failure resulted in the breach.

To take advantage of this safe harbor, businesses must implement a written cybersecurity program which contains administrative, technical and physical safeguards that conforms to an industry recognized cybersecurity framework. The recognized frameworks include NIST SP 800-171, NIST SP 800-53, and the ISO/IEC 27000-series. Businesses regulated by HIPAA/HITECH or GLBA may also meet the safe harbor cybersecurity requirements by conforming to the applicable regulatory requirements.

**PUTTING IT INTO PRACTICE: Businesses operating in Connecticut should review their cybersecurity program and consider implementing any additional measures, to the extent necessary, to take advantage of this new safe harbor.**

## New Decision Narrows Scope of Georgia Computer Trespass Statute

*Posted July 9, 2021*

The Georgia Supreme Court recently concluded that Georgia's equivalent of the CFAA should be viewed narrowly, similar to the US Supreme Court's recent, similar decision in *Van Buren*. In Kinslow v. State, the Georgia Supreme Court held that even if there is unauthorized use of a computer or computer network, there must be enough evidence to prove that the defendant used the computer network knowingly without authority and with the intention of obstructing or interfering with the use of data.

The court acknowledged that in the case at hand, the defendant lacked authority when he altered his employer's computer network settings in such a way that his supervisor's emails were forwarded to defendant's personal email address. However, there was not enough evidence to prove that the defendant had the intention to obstruct or interfere with the flow of data in the form of emails, as the supervisor still received emails that were intended for him. The court went through a deep analysis of each of the elements of the statute. Applying the canons of construction, it found that there must be evidence of the intention to obstruct and interfere, which was lacking in this case. As a result, the court overturned the defendant's felony conviction under Georgia's computer trespass law.

**PUTTING IT INTO PRACTICE: This case shows that the scope of state computer trespass/fraud statutes may be narrowed, similar to the narrowed scope of CFAA. As we noted following the *Van Buren* decision, companies should think about regularly auditing and updating access rights to their IT systems.**

## FTC Settles Security Claims With Both MoviePass and Its Owners

*Posted June 25, 2021*

MoviePass, a movie subscription service, has agreed to a proposed settlement with the FTC over alleged deception and lack of security allegations. The now-defunct company not only allegedly marketed its service as a "one movie per day" service – yet took steps to actively deny subscribers such access – it also failed, according to the FTC, to secure subscriber's personal data. The company also was alleged to have violated the Restore Online Shoppers' Confident Act, which impacts the offering of "negative option" (subscription) services.

With respect to the security allegations, MoviePass's privacy policy stated that it used reasonable measures to protection personal information. Statements included that the company "takes information security very seriously," that it "uses reasonable administrative, technical, physical, and managerial measures to protect [consumers'] personal details from unauthorized access" and that email addresses and payment information were encrypted. Notwithstanding these statements, the FTC said the company failed to take security sufficiently seriously. Of particular concern, a database containing subscribers' personal information, including emails and payment information, was both unencrypted and exposed, resulting in a 2019 data breach impacting about 28,000 individuals' financial details.

Under the proposed order, with respect to the alleged security violations, MoviePass's operators must implement a comprehensive information security program. The program must have a "qualified" employee who oversees it, it needs to be designed to address risks that face the company, must provide for employee training, and will be subject to FTC oversight and biennial third-party audits. The order also requires that senior executives annually certify the program, and that the company notify the FTC directly of any future data breaches. The settlement terms will be in effect for 20 years, and are with the company, its parent, as well as the two principal owners, who will be required to follow its terms for any business they control.

**PUTTING IT INTO PRACTICE: This settlement is a reminder that the FTC will use security statements in a company's privacy policy to enforce its expectations under theories of deception. Also of interest is the defunct nature of the company. The FTC often brings claims -and seeks settlement- against both the company and its owners. Here, though, since the company is no longer operational, the practical effect will be that this settlement is principally against the owners.**

## The Impact of the Narrowed Scope of CFAA Liability in the Privacy and Security Realm

*Posted June 14, 2021*

The Supreme Court's recent decision in *Van Buren* addressed the meaning of the term "exceeds authorized access" under the Computer Fraud and Abuse Act (CFAA). The Court held, in a criminal case that alleged that the person used information for an improper purpose, that the law's definition of this term does not include situations when people have improper motives for obtaining computerized information they are otherwise authorized to access.
As we outlined in our sister blog, the Court found that individuals "exceed authorized access" only if they obtain files or folders that should have been off limits. In the particular case, authority was not exceeded because the individual was authorized to retrieve the information in question. Although *Van Buren* was a criminal case, the structure of CFAA strongly suggests that the Supreme Court's holding will apply in civil cases as well, where controlling decisions in the First, Fifth, Seventh and Eleventh Circuits held the "exceeds authorized access" clause applies to those who misuse their authorized access.

The CFAA has often been used in data privacy and security lawsuits, where companies argue that there is "unauthorized access" under the CFAA because an individual does not comply with terms of service, computer use policies, or other documents requiring privacy and security protections. This "improper purpose" theory will be eliminated if lower courts apply *Van Buren's* holding to criminal and civil cases alike.

**PUTTING IT INTO PRACTICE: This case may eliminate a potential cause of action if an individual acts improperly by misusing personal information or failing to protect it as required by law. That does not mean, however, that companies should necessarily strike such requirements from their policies and terms. CFAA is not the only cause of action that can be brought, and making expectations clear in terms can help guide behavior. This decision does, though, remind companies to think about who has (or should have) access to what systems and to regularly audit and update access rights as people's roles change.**

## Cybersecurity Guidance Issues to Retirement Plan Sponsors

*Posted June 7, 2021*

The Department of Labor recently issued cybersecurity guidance to retirement plans. The department's Employee Benefits Security Administration (EBSA) issued guidance in three areas: (1) hiring and working with vendors and service providers; (2) implementing an internal cybersecurity program for the plan; and (3) online security for plan participants and end-users.

Recommendations made to plan sponsors and administrators include:

- Asking vendors what security practices they use and how those measures are validated;
- Determining the type and scope of vendors' cyber insurance;
- Putting a formal cybersecurity program in place and conduct annual risk assessments;
- Using security measures like encryption, and conducting periodic training;
- Giving users information about common risks, like free WiFi or improper password hygiene.

These guidelines provide clarity on how EBSA will interpret regulations on electronic recordkeeping, (which require plan administrators to put in place reasonable controls and adequate records management) and those that relate to plans' fiduciary responsibilities. While these cybersecurity recommendations were the first from EBSA, they will be familiar to those acquainted with other frameworks like the NIST Cybersecurity Framework and other agency guidance about managing vendors. This includes the recent NYDFS supply chain management guidelines.

**PUTTING IT INTO PRACTICE: This first cybersecurity guidance from the EBSA signals its expectations around cybersecurity. Of note is the focus made on vetting and onboarding service providers. These cautions are particularly helpful when considering vendors who have automated protection processes and/or intimate knowledge of their clients' IT systems (knowledge that could be exploited by a bad actor). Plan sponsors and other fiduciaries with existing cybersecurity programs will want to compare their controls and vendor management programs to these three newly issued guidance.**

## NYDFS Issues Supply Chain Management Guidance

*Posted May 25, 2021*

The New York State Department of Financial Services recently issued recommendations to financial institutions in the aftermath of the SolarWinds cyberattack. In that attack, hackers inserted malware into SolarWinds software which was then distributed to SolarWinds' customers (many of which were financial institutions). After discovery, SolarWinds released a series of hot fixes to address vulnerabilities in their software associated with the attack. Although NYDFS found that most companies responded quickly to patch the vulnerabilities, it did identify additional steps to reduce supply chain risk:

- Properly diligence third party service providers' potential cybersecurity risks, and include in vendor contracts -particularly critical vendors- provisions that ensure cybersecurity practices and cyber hygiene can be monitored, and that require immediate notice of any cyber event that could impact the company.
- Assume any software from service providers might be compromised. Thus authorize only as-needed access and monitor for malicious activity.
- Have a vulnerability management program with patch rollback procedures to ensure timely patches.
- Update incident response plans to address supply chain compromises.

As we have reported recently, NYDFS is actively enforcing the cybersecurity rules, and these recommendations can be read in context of those rules.

**PUTTING IT INTO PRACTICE: These NYDFS cybersecurity recommendations highlight for financial services companies the expectations the department has of them with regard to supply-chain risk. Companies would be well-served to review their vendor management practices against these latest recommendations.**

## Two Other States Adopt Model Data Security Law for Insurance Industry

*Posted April 19, 2021*

Maine and North Dakota recently adopted the National Association of Insurance Commissioners (NAIC) data security model law. They join at least 11 others states who have already adopted the model law. The model law applies to insurers, insurance agents and other entities licensed by the state department of insurance.

As we wrote about in our insurance certifications round-up, among other requirements, the model law requires organizations subject to the law to have:

- A comprehensive written information security program commensurate with the company's size and complexity
- A written incident response plan
- Employee training
- Appropriate oversight by the company's board of directors

Neither law will take effect right away. Maine's Model Law is not effective until January 1, 2022, with one section regarding compliance with third-party service provider arrangements effective January 1, 2023. The North Dakota law takes effect later, on August 1, 2022, with one section regarding the obligation to document and report cybersecurity events and related incident response activities effective August 1, 2023.

**PUTTING IT INTO PRACTICE: We anticipate more states will continue to adopt the NAIC model security law. Those in the insurance field should keep these security obligations in mind when assessing the sufficiency of their practices.**

## Managing the World of Cybersecurity in a New Era

*Posted February 24, 2021*

Cyberattacks have become big business from the standpoint of attackers. Threat actors range well beyond cults of old, and now including sophisticated state actors, large businesses organized for the very purpose of cyber breach and theft, and complex threat networks that aggregate information formerly treated as innocuous. This is a real risk for companies as we look forward to the remainder of 2021. At the same time, ransomware is changing the state of cyber insurance, with regulators across the globe entering the field to govern the conduct of attacked businesses in this climate. Regulations cover terms of ransom payments and subsequent obligations to persons whose information goes out the pipes. For more on these risks, you can listen to the recent *Nota Bene* podcast episode (on Apple Podcasts, Google Podcasts, Spotify, or Stitcher) with Sheppard Mullin partners Kari Rollins and Michael Cohen.

**Putting it Into Practice: With this landscape, companies should take care to examine the state of their existing information security posture and preparedness, test systems vulnerabilities, and audit cybersecurity compliance to mitigate the ever-expanding cybersecurity risks and potential liability to any global or domestic business organization.**

## FTC Settles Over Alleged Failure to Manage Service Providers

*Posted January 7, 2021*

The FTC recently settled with Ascension Data & Analytics for failure to oversee service providers. Ascension provides services to mortgage companies within its corporate family of entities. According to the complaint, Ascension uses third parties to provide some of its services. One of those, OpticsML, had access to tax returns for approximately 60,000 customers. OpticsML stored the information on a cloud-based server which server was publicly accessible for a year. During that time the tax documents were accessed by unauthorized individuals. The originating IP addresses were in Russia and China. Although the security incident was that of OpticsML, the FTC alleged that Ascension violated the Gramm-Leach-Bliley Act's Safeguards Rule. Namely, the company failed to properly oversee its service providers and it failed to adequately assess risk. In particular, the FTC alleged that:

- Ascension did not take steps to actually assess third parties' security capabilities, even though it did have a policy in place requiring such due diligence.
- Ascension failed to contractually require its service providers to implement specific safeguards. Instead contract stated only that nonpublic personal information be protected as required under GLBA and not disclosed without consent.
- Ascension did not adequately assess risk, insofar as it only did risk assessments for a small subset of third parties (which did not include OpticsML).
- Ascension has agreed to implement a comprehensive data security program and obtain initial and biennial assessments of its data security program for ten years. It has also agreed to annually certify to the FTC as well as to report any security incidents to the FTC.

**PUTTING IT INTO PRACTICE: This settlement is a reminder that the FTC expects companies to take steps to ensure their third party providers secure personal information. Measures include specific contractual terms and conducting appropriate due diligence.**

# EU PRIVACY

## European Securities Watchdog Fine Highlights Importance of Data Integrity and Regulatory Access

*Posted September 27, 2021*

The European Securities and Markets Authority (ESMA), the EU's securities markets regulator, recently announced that it fined UnaVista Limited, a UK-based trade repository, €238,500 ($280,000) for eight breaches of the European Market Infrastructure Regulation (EMIR). The EMIR includes rules regulating the conduct of trade repositories, and in conjunction with its role as the supervisor of trade repositories under EMIR, ESMA is empowered to file enforcement actions in response to infringements of EMIR by trade repositories.

Under the EMIR, trade repositories are required to provide data to regulators, including access to details of derivatives contracts in the form of periodic and ad hoc open trade state reports. According to the Public Notice, between 2016 and 2018 the trade repository failed to:

- Ensure the integrity of its data by providing incorrect field ordering logic, mapping rules, and crossed date boundaries, which led to generating incorrect or unreliable reports for regulators; and
- Provide regulators with direct and immediate access to trade state reports and historic trade state reports, due to missed data exports and to non-existent functionality.

Based on these failures, the Board of Supervisors found that UnaVista did not meet the special care expected from a trade repository as a professional firm in the financial services sector, and had committed the infringements negligently and was liable to a fine. UnaVista may appeal against this decision to the Joint Board of Appeal of the European Supervisory Authorities.

**PUTTING IT INTO PRACTICE: This case highlights the importance of complying with obligations of data integrity and regulatory access. Companies would be well-served to review their controls and procedures, including performing risk-based data validation to reveal potential systemic weaknesses in your organizations, and ensuring the provision of timely and accurate data to regulators.**

## Understanding When to Use Two New Sets of Standard Contractual Clauses Issued by the EU

*Posted June 16, 2021*

Starting this fall, companies transferring personal data from the European Economic Area (EEA) will likely begin to see a flurry of contract renegotiations. On June 4, 2021, the European Commission adopted long awaited new Standard Contractual Clauses (SCCs) for transfers out of the EEA. SCCs have been one of the more popular ways for Companies to transfer personal data from the EEA to third countries whose privacy laws have not been deemed "adequate" (like the US). The prior SCCs pre-date GDPR (see our discussion here), and have been updated to (1) more directly address GDPR and (2) because of comments in *Schrems II* last July, which called into question their use (the court noted that even under SCCs, certain "supplementary measures" might be needed for cross-border transfers).

*So what's new?* Among other changes, two of the biggest differences in these new "cross border" SCCs is the modular approach and provisions to address *Schrems II*. The new SCCs combine a set of non-negotiable, standard clauses, along with a modular approach, so companies can adapt the SCCs to different data transfer scenarios. The previous SCCs contemplated only two transfer scenarios: controller-to-controller transfers and controller-to-processor transfers. Now, the SCCs contemplate more realistic transfer situations, including Controller-to-Controller transfers (Module 1); Controller-to-Processor transfers (Module 2); Processor-to-Processor transfers (Module 3); and Processor-to-Controller transfers (Module 4). In relation to the *Schrems II* ruling, the new SCCs allow organizations to take a risk-

based approach when assessing the possibility of (foreign) public authorities accessing the data under their local laws. This means, for example, that a data importer's mere eligibility to receive data disclosure directions under Section 702 of the U.S. FISA Act should not automatically stop the ability to transfer data, if the parties can demonstrate that the likelihood of such disclosures is sufficiently low.

*What's the timing?* The new cross-border SCCs can be used instead of the old terms starting June 27, 2021. From June 27, 2021 until September 27, 2021, both the "old" SCCs and the new SCCs can be used for *new* contracts. However from September 27, 2021 onwards, only the new SCCs can be used for new contracts. There is an 18 month grace period for existing contracts under the old SCCs. This means that by December 27, 2022 onward, all existing contracts using the old SCCs will need to be replaced by the new terms.

*So what is the second set of SCCs?* The EC has also issued SCCs for transfers of information between controllers and processors. These clauses can be used by entities operating solely within the EU, and can be incorporated into a broader contract between the parties. Provisions include those contemplated under GDPR, including that processors will use information only as set forth in the SCCs, and will provide security for information processed. While companies are not required to use these controller-processor SCCs and could instead negotiate and include each of the elements required to be contained in a controller-processor agreement under GDPR, using these SCCs could make the contracting process simpler. (These SCCs do not contain cross-border provisions, which would still need to be addressed where relevant.)

**PUTTING IT INTO PRACTICE: During this grace period, companies relying on old SCCs for cross-border data transfers should start inventorying existing arrangements and prepare to implement the new cross-border SCCs. Even though these new SCCs have been designed to largely address the requirements of *Schrems II*, companies will still need to assess whether the cross-border SCCs alone will suffice or whether any other additional measures are needed. For data importers in particular, this may include preparation of a transparency report and transfer impact assessments. With respect to intra-EU transfers between controllers and processors, companies can rely on these new SCCs to address GDPR obligations.**

## Portugal Puts Halt on Data Transfers Between INE and Cloudflare

*Posted May 10, 2021*

The Portuguese data protection authority issued a recent resolution ordering the Portuguese National Institute of Statistics (or INE) to stop sending personal census information to any countries outside of the EU that do not provide "adequate" levels of data protection. Among those countries are the United States.

Prompting the resolution was the INE's use of the US company Cloudflare, Inc. The parties had standard contractual clauses in place, and relying on those, the INE transferred Portuguese resident data from the 2021 census surveys to Cloudflare. Citing the Schrems II decision, the Portuguese data protection authority (CNPD) concluded that the SCCs were not sufficient, since Cloudflare is subject to US surveillance laws, which could require the company to share personal information with US authorities.

Noting that as a data protection authority, it was required to stop data transfers if there were insufficient guarantees that the transferred information was protected, the CNPD made the decision to order the data transfers to be stopped. The parties had only 12 hours to comply.

**PUTTING IT INTO PRACTICE: This resolution, which comes just a month after a similar decision from Bavarian authorities, signals that EU data protection authorities are watching data transfers to the US closely. While we await updated SCCs, recommendations from the EDPB about data transfers can be helpful.**

## Bavarian DPA Holds SCCs Alone Not Enough for European Use of US Email Service

*Posted April 13, 2021*

In a notable application of the European Court of Justice's "Schrems II" decision, the data protection authority for the German state of Bavaria recently held that use by a German entity of US-based MailChimp (which use involved transferring personal information to the US) violated GDPR. As we previously wrote, the Schrems II decision turned on concerns around lack of sufficient safeguards under US law. The court cautioned, and the EDPB has since clarified further, that for standard contractual clauses to be used companies must determine whether the information will have the same level of protection under the laws of the receiving country. If not, additional "supplementary measures" must be implemented.

As many may be aware, MailChimp is a popular email vendor. Here, the German company that hired MailChimp sent its European customers' email addresses to MailChimp, in the US, so that MailChimp could then send the customers email newsletters. Even though the transfer was made pursuant to standard contractual clauses, the Bavarian DPA held that the transfer failed to adequately protect EU data subject rights.

In reaching its decision, the Bavarian DPA pointed to the potential of US intelligence services' ability to access information held by MailChimp under US law. This was a concern for the DPA. It concluded that this failed to provide European individuals "protection" from such access, thus not giving the same level of protection as if the information remained in the EU. The Bavarian DPA did not provide direction on what supplemental measures could have been used. The EDPB, though, has suggested (para 48) that in such circumstance a technical measure may be the only option. Faced with the DPA's determination, the data controller promised to stop using MailChimp.

**PUTTING IT INTO PRACTICE: When sending personal data from the EU to the US using standard contractual clauses, businesses should evaluate whether the SCCs alone will provide the same level of protection for the data as under EU law. If not, businesses should consider whether they can employ additional security measures. Although no direction was provided in this case by the Bavarian DPA, the EDPB guidance can be of help.**

# FINANCIAL PRIVACY

## Beginning in May 2022 Banks Will Have 36 Hours to Disclose Certain Types of Cyber Incidents

*Posted December 9, 2021*

Federal banking regulators issued a final rule that impacts how banks and other regulated entities report certain data incidents. Those subject to these new reporting requirements include U.S. banks and bank service providers. The rule is effective April 1, 2022, and covered entities are expected to comply with the final rule by May 1, 2022. The new requirements reflect ongoing concern to identify and stop computer security incidents before they become systemic.

As we detail in our sister blog here, banks will have to 36 hours to notify their primary regulator after determining that they suffered a computer-security incident that rises to the level of a notification incident. Two definitions are important for understanding when such notice is required. First, a *computer-security incident* is one that would result in actual harm to either information systems or underlying information in those systems. Second, a *notification incident* is one that materially disrupts a banking organization's operations or lines of business.

For notices that fall in this 36 hour time frame, the notice can occur to the regulator in a variety of ways. This includes email or phone. The rule also provides for regulators to create alternate methods for notice to be submitted.

Under the rule, bank service providers will also have to notify bank clients "as soon as possible" if there is a computer-security incident that is -or is likely- to materially interferes with covered services for four or more hours. The parties can design a notice method that works best, provided that clients get the notice in a timely manner.

**PUTTING IT INTO PRACTICE: Banks have six months to prepare for this upcoming rapid-notice requirement. During this time they can determine how they will identify and address computer-security and notification incidents. They will also want to work with clients to determine how best to provide the four-hour notice, if such notice is ever needed.**

## Non-Banking Institutions Will Want to Review Security Measures in Light of Update to Safeguards Rule

*Posted November 4, 2021*

The FTC recently announced a final rule updating its GLBA Safeguards Rule to "strengthen the data security safeguards" of consumer financial information. The FTC reported that it was making these changes in response to widespread data breaches and cyberattacks. As we reported in our sister blog, the changes will mean that a broad range of non-banking financial institutions may need to make updates to their data security policies and procedures. The new requirements go into effect in November 2022.

The final rule adds specificity to the existing rule's requirements around data security measures. The update specifies several measures entities need to have in place. This includes having access controls, authentication and encryption as part of the organization's overall information security program. It also requires them to have a single qualified individual to oversee their information security program. The update adds a requirement of periodic reports to boards of directors, having a written risk assessment and incident response plan, as well as conducting periodic assessments of service providers.

The update also expands the definition of "financial institution" to include entities engaged in activities that the Federal Reserve Board determines to be incidental to financial activities. This change adds "finders"– companies that bring together buyers and sellers of a product or service – within the scope of the Rule.

**PUTTING IT INTO PRACTICE: Covered non-banking financial institutions should review their current data security measures to ensure they address the new specifics outlined in the update to the Safeguards Rule. These include access authentication, a person in charge of security measures, and service provider assessments.**

## NYDFS FAQ Provides Clarity on Breach Notification and Security Requirements

*Posted September 21, 2021*

The New York Department of Financial Service recently clarified security incident notification requirements and the use of multi-factor authentication. On its FAQ page, the NYDFS added two new questions and answers for financial services companies subject to 23 NYCRR Part 500.

The first answer explains that covered entities must notify the NYDFS of security incidents that occur at a third party service provider. Even if the third party notifies NYDFS on the covered entity's behalf, covered entities still must directly notify the department. This requirement helps the NYDFS quickly identify threats and appropriately respond.

The second answer clarifies when covered entities must use multi-factor authentication. Namely, MFA should be used whenever accessing internal networks from an external network. This includes email, document hosting, and related

services (whether on-premise or cloud-based). MFA may not be necessary if a covered entity's CISO documents approval of similar or more secure access controls.

**PUTTING IT INTO PRACTICE: These updates highlight the importance of having proper breach notification procedures and security controls. Companies are reminded to notify the department of relevant breaches and to enable MFA by default for accessing internal networks.**

## NYDFS Issues Ransomware Guidance

*Posted July 12, 2021*

The New York State Department of Financial Services recently announced new guidance addressing ransomware attacks, and highlighting cybersecurity measures to significantly reduce the risk of an attack. The guidance comes as ransomware rates have been increasing, and builds on the post SolarWinds guidance from NYDFS about supply chain management. It was released just prior to the most recent large attack, namely the July 2nd supply-chain ransomware attack centered on the U.S. information technology firm Kaseya.

The guidance was generated from reports to NYDFS of 74 ransomware attacks from NYDFS-regulated companies between January 2020 and May 2021 which it said followed a similar pattern: "hackers enter a victim's network, obtain administrator privileges once inside, and then use those elevated privileges to deploy ransomware, avoid security controls, steal data, and disable backups." NYDFS – in step with the FBI – recommends against paying ransoms because such payments (i) may violate the Treasury's OFAC sanctions, (ii) do not guarantee that the company will regain access to all its data, or that the company's data will not be leaked later anyway, and (iii) will likely not prevent subsequent attacks. Instead, in the guidance NYDFS urged all regulated entities to implement the following multi-layered approach to cybersecurity:

- Train employees about email filtering and anti-phishing;
- Implement a vulnerability and patch management program;
- Use multi-factor authentication;
- Disable RDP access from the internet wherever possible;
- Use strong, unique passwords;
- Employ privileged access management so that each user has the minimum level of access necessary to perform the job;
- Monitor systems for intruders;
- Segregate and test backups; and
- Include a ransomware-specific incident response plan that is tested.

**Putting it Into Practice: This guidance is a reminder that while supply-chain cybersecurity threats have been gaining headlines, cyberattacks can and do just still occur as a result of phishing attacks, human error, and failures in controls. Teaching employees about good cyber hygiene helps to mitigate the risk that employees will fall prey to sophisticated phishing or socially-engineered fake emails. Companies should couple their employee cybersecurity training with the implementation of a robust cybersecurity program that utilizes diversified security measures and tests controls to ensure system endpoints are protected from threats.**

## Insurance Cybersecurity Certifications: A State Roundup

*Posted February 18, 2021*

Many states require insurance providers that do business in their states to complete annual certifications of compliance. As examples, the deadline in New Hampshire is coming up on March 1. The deadline in Alabama, Connecticut, Delaware, Louisiana, Michigan, Mississippi, Ohio, and South Carolina was February 15. (The deadline under new laws in Michigan and Virginia will be February 15 as well, starting in 2022 and 2023, respectively.) The deadline in New York is April 15.

This certification requirement is captured in the model National Insurance Data Security Law endorsed by the National Association of Insurance Commissioners. That model law, and those states that have implemented it, require insurers not only to have information security programs in place, but also to attest compliance. There are some exemptions, including for small businesses with fewer than ten employees, licensees subject to and in compliance with HIPAA requirements, and employees, agents, and representatives of licensees. As part of the certification process, companies typically need to submit written confirmation that they comply with the law, and thus have, among other things:

- A comprehensive written information security program commensurate with the company's size and complexity
- A written incident response plan
- Employee training
- Appropriate oversight by the company's board of directors

Once submitted, companies must maintain the records and data supporting their certifications. In most states that retention period is five years.

**PUTTING IT INTO PRACTICE: When fulfilling certification obligations, companies should keep in mind the underlying requirements to which they are certifying. Now, in the midst of certification season, is a good reminder to regularly take stock of ongoing compliance obligations and efforts.**

# HEALTHCARE PRIVACY

## FDA Joins Other Regulators in Focus on AI and Machine Learning

*Posted November 22, 2021*

The Food and Drug Administration recently sought comments on the role of transparency for artificial intelligence and machine learning-enabled medical devices. The FDA invited comments in follow up to a recent workshop on the topic.

The workshop was part of a series of efforts the FDA has had in this space. These include its Digital Health Center of Excellence and a five-part Action Plan for AI and machine-learning enabled medical devices. As part of the action plan, the FDA indicated it wants to issue guidance on software learning over time and help the industry be "patient-centered." In other words, that companies be transparent when using AI and machine learning-enabled software with patients. These initiatives are especially important given the increase in AI/ML in healthcare.

Workshop participants explored how to provide transparency. One idea proposed was using a "nutrition fact label" approach to give individuals enough information to make informed decisions. The graphic would be similar to a food label, disclosing quickly and visually the key things patients might want to know. (This is similar to an approach launched by Apple late last year, which we discussed here.) Other agencies have looked at machine learning and AI

with similar transparency recommendations. We have written about those in the past, including for the financial services industry. Advice about use of these tools has also been issued by the FTC and the EU.

**PUTTING IT INTO PRACTICE: While the FDA continues to explore this area, companies are reminded that the FDA (like other regulators) expects transparency with consumers. From a privacy perspective, the workshop reminds digital health companies this includes telling users when AI or ML-enabled software is being used.**

## Florida Imposes Criminal Penalties for Improper Processing of DNA

*Posted November 1, 2021*

Florida recently passed a law governing DNA samples. The Act places several restrictions on the use, retention, and sharing of DNA samples. Those that violate the Act may face criminal liability.

### Requirements under the law

Requirements under the Act are tied to "DNA samples" which include any human biological specific from which DNA can be extracted or the extracted DNA. To process a person's DNA, entities must first obtain express consent. The Act defines "express consent" as an "authorization…evidenced by an affirmative action demonstrating an intentional decision." With consent, there must also be a clear and prominent disclosure describing the manner of collection, use, retention, maintenance, or disclosure of a DNA sample. The notice must also describe the purpose of processing or the use of the DNA.

### Penalties for violating the law

The Act creates criminal liability of varying degrees for failure to obtain express consent. Willfully collecting or retaining DNA without express consent and with the intent to perform DNA analysis is a misdemeanor. It is a felony to willfully disclose another person's DNA analysis results to a third party without express consent. To willfully sell or transfer a person's DNA sample or the results of a DNA analysis to a third party without express consent, regardless of whether the sample was collected with express consent in the first place, is also a felony.

### Exemptions

There are certain uses of DNA samples exempt from these requirements. For example, use in a criminal investigation or prosecution, or if complying with a court order. Provided certain conditions are met, uses in medical diagnosis, patient treatment, quality assessments, and improvement activities are also exempt. Namely, that the health care practitioner who originally collected the DNA obtained express consent or a CMS certified clinical laboratory performs the activities.

**PUTTING IT INTO PRACTICE: Companies that collect DNA samples should review their notice and consent practices to ensure they meet the requirements of this new law. States are continuing to impose new restrictions on the processing of biometric and genetic data. Civil, and potentially criminal penalties await companies under these laws.**

## California Broadens Security and Breach Laws, Includes Genetic Data

*Posted October 18, 2021*

California recently updated both its data security and breach notice laws to include genetic data. With the passage of AB 825, the data security law now includes in the definition of "personal information" genetic data. The information needs to be "reasonably protected." While many other states have similar "reasonable protection" requirements in their data security laws, California is one of a handful to specifically list genetic information.

Genetic is now "personal information" subject to data breach notification requirements. This includes the breach notification law that applies to state agencies as well as companies. Genetic data is any data that results from an analysis of a biological sample or an equivalent element from a consumer that concerns genetic material. This includes DNA, RNA, genes, chromosomes, alleles, genomes, alterations or modifications to DNA or RNA, and SNPs.

Both modifications go into effect January 1, 2022.

**PUTTING IT INTO PRACTICE: Companies will want to review their incident response policies and data security programs prior to the effective date to ensure genetic data is addressed. The inclusion of genetic data into both of these laws shows the increasing regulation of health and medical data outside of HIPAA. (In addition to these amendments, California concluded its 2021 legislative calendar passing a law aimed at direct-to-consumer testing companies collecting genetic data (which we discussed here)).**

## California Enacts New Privacy Law for Genetic Data

*Posted October 12, 2021*

California's governor recently signed SB 41 into law. The bill enacts the Genetic Information Privacy Act (GIPA). The governor rejected a similar bill last year over concerns about COVID-19 public health efforts. To address that concern, this bill exempts tests used to diagnose whether an individual has a specific disease.

California's law adds to the existing federal and state patchwork of laws governing genetic information. It largely mirror's Utah's Genetic Information Privacy Act enacted earlier this year (we discussed here). Generally, the law creates requirements for: (1) notice; (2) consent; (3) data security; and (4) individual rights, which we discuss in more detail below.

***Applicability:*** The law applies to a "direct-to-consumer genetic testing company" that collects genetic data from "consumers" (i.e., California residents). "Genetic data" broadly means any data that results from an analysis of a biological sample or an equivalent element from a consumer that concerns genetic material. This includes DNA, RNA, genes, chromosomes, alleles, genomes, alterations or modifications to DNA or RNA, and SNPs. The definition does *not* include deidentified data or data that is processed exclusively for condoned scientific research.

***Requirements:*** The obligations under the law are described in more detail below.

- **Notice.** Companies subject to GIPA must provide consumers with a clear and complete summary of its privacy practices. This includes giving information about the company's use, maintenance, and disclosure of genetic data. As a separate requirement, companies must also display a prominent and accessible privacy notice. The notice must include "complete" information about the company's data collection, consent, use, access, disclosure, maintenance, transfer, security, and retention and deletion practices. It must also explain how to file a complaint under the Act. Lastly, the law requires notice to consumers that deidentified genetic information may be shared with third parties for research purposes.

- **Data Use and Consent**. Under GIPA companies must get consumers' express consent for collection, use, and disclosure of genetic data. Separate, express consent must also be obtained for (1) the storage of a biological sample after initial testing has been fulfilled; (2) use of genetic data beyond the primary purpose of the testing or service; and (3) transfer of genetic data to a third party (other than a service provider). Express consent is also required for direct marketing based on a consumer's genetic data or third party marketing based on the consumer's order, purchase, reception, or use of a genetic testing product or service. However, consent is *not* needed to market on the company's own website or mobile application, so long as the marketing is not based on information specific to the consumer. If a company conducts this kind of marketing, the ad itself has to be "prominently labeled as advertising" and include the name of any third parties who "contributed to the placement" of the ad. Companies must provide mechanisms for a consumer to revoke consent after it is given. Requests to revoke consent must be honored no later than 30 days after receipt of the request.
- **Data security.** Companies must implement and maintain reasonable security procedures and practices. Those practices need to be designed to protect a consumer's genetic data against unauthorized access, destruction, use, modification, or disclosure.
- **Individual rights.** GIBA requires that companies put procedures in place so consumers can access their genetic data. Consumers must also be able to delete their account or genetic data and to destroy biological samples. Companies cannot discriminate against consumers for exercising any of these rights.

***Enforcement:*** GIPA may be enforced by the Attorney General, district attorneys, county counsel, and city attorneys and prosecutors with appropriate authorization. In addition to court costs, these actors can recover up $1,000 in civil penalties for a negligent violation and up to $10,000 for willful violations. Any recovered penalty will be paid to the individual whose genetic data is at issue.

***Effective Date:*** The law is expected to go into effect on January 1, 2022.

**PUTTING IT INTO PRACTICE: Direct-to-consumer companies are facing increased notice and consent requirements under state laws. This is particularly true for companies collecting health, medical, genetic, or biometric data that are not regulated by HIPAA. As more states develop genetic privacy laws, these companies should continue to be mindful of requirements around notice, individual rights, and data security.**

## FTC Warns Digital Health Industry to Comply with its Breach Notification Rule

*Posted September 20, 2021*

The use of apps, wearables, and other devices used to track health and wellness data have continued to rise. The FTC again signaled its focus on this growing industry in a statement on the scope of the Health Breach Notification Rule. In the statement, the FTC called out specific types of apps and trackers that it views as having notification obligations under this rule.

The rule is intended to address those entities that collect health information, but are *not* covered by HIPAA. Under the rule, vendors of personal health records (PHR) and PHR-related entities must notify consumers, the FTC, and, in some cases, the media, if there has been a breach of unsecured identifiable health information. The statement provides guidance on which health-related apps are subject to the rule, clarifying that newer health apps and fitness trackers would be covered under the rule. Based on this statement, the FTC views developers of health apps or connected devices to be a "health care provider" because it "furnishes health care services of supplies." As an example, the FTC said a blood sugar monitoring app drawing health information only from one source (e.g., a consumer's inputted blood sugar levels), but also taking non-health information from another source (e.g., dates from your phone's calendar), would be covered under the rule. The FTC also clarified that a "breach" includes not only incidents

of unauthorized access, but sharing of covered information without an individual's authorization. In two different dissenting statements, Commissioners Wilson and Phillips generally argued that the FTC is broadly expanding the scope of key terms under the rule (PHR, "multiple source" and breach) and circumventing the rulemaking processes.

**PUTTING IT INTO PRACTICE: The FTC has not enforced the Health Breach Notification Rule since it went into effect. However, this statement, coupled with statements in a more recent FTC enforcement action involving a digital health app, and other enforcement priorities suggests that enforcement is forthcoming. While many of these companies collecting "health" or "medical" information may have otherwise had notification obligations to individuals and/or state attorneys' general under state data breach notification laws, companies are reminded that they may also have notification obligations to the FTC, and in some cases, the media. Companies that don't comply with the Health Breach Notification Rule could be subject to up to $43,792 in monetary penalties per violation per day.**

## FTC Signals Focus on Healthcare and Technology Platforms, Among Others

*Posted August 12, 2021*

The FTC recently voted to authorize the use of compulsory processes—the FTC's primary investigatory tools—on what it calls "key law enforcement priorities." The resolutions allow investigators to take actions like issuing subpoenas and civil investigations demands (commonly referred to as "CIDs") in a variety of areas. Of note is the inclusion of both healthcare markets and technology platforms, signaling a potential FTC interest in those sectors.

These resolutions compliment the agency's existing authority to investigate deceptive or unfair acts, and comes on the heels of the blow the FTC suffered as a result of the Supreme Court's *AMG* decision. For those in the healthcare and technology platform space, this may signal an increase in privacy and data security scrutiny by the FTC.

**PUTTING IT INTO PRACTICE: The authorization of the use of compulsory processes suggests that the FTC will not be backing off from bringing actions to enforce against unfair and deceptive practices. We will continue to monitor to see the impact this may have on privacy and data security cases brought by the agency in the healthcare and technology platform industries.**

## OCR Urges Private Sector to Beef Up Ransomware Protections

*Posted July 14, 2021*

Echoing other agencies in recent weeks, the U.S. Department of Health and Human Services' Office for Civil Rights (OCR) issued an alert sharing resources to address and protect institutions against the recent influx of ransomware attacks. Resources included a White House Memo urging companies to strengthen their commitment to cybersecurity. Similar to other recommendations we have recently written about (for example those from NYDFS), OCR recommends that the private sector:

1. Implement the five best practices from the President's May 2021 Executive Order on Cybersecurity: (a) multifactor authentication, (b) early detection of cybersecurity vulnerabilities, (c) robust response to cybersecurity incidents, (d) encryption, and (e) dedicated security teams;
2. Back up all information and data, regularly test backups, and keep the backups offline and not connected to core business systems;
3. Update and patch operating systems, applications, firmware and other systems promptly;
4. Test and optimize incident response plans;

5. Run third-party checks to ensure system security; and,

6. Segment networks to minimize damage in the event of a system compromise.

**PUTTING IT INTO PRACTICE: Though these guidelines have no binding effect, they provide timely insight into OCR's expectations for HIPAA covered entities and business associates to protect against cyberattacks. Failure to implement the above guidance may leave companies at risk not only to ransomware attacks but also greater scrutiny from the government in the event of a data breach.**

## NIST Plans to Update HIPAA Security Guidance – Asks for Comments

*Posted May 14, 2021*

Recently, the National Institute of Standards and Technology (NIST) requested comments to its Resource Guide for implementing the HIPAA Security Rule. (i.e., SP 800-66). This Guide, first released in 2008, summarizes the HIPAA Security Rule standards and explains the structure and organization of the Security Rule.

Since the Guide's original publication, cyberattacks and threat conditions have changed significantly. As such, NIST is seeking stakeholder input to improve the Guide. Namely, it wants to understand how covered entities and business associates have used and applied the Guide in implementation of cybersecurity programs. NIST's three key objectives with the Guide are to:

- educate readers about information security terms used in HIPAA Security Rule,
- amplify awareness of non-NIST resources relevant to the HIPAA Security Rule, and
- provide detailed implementation guidance for covered entities and business associates.

Specifically, NIST has asked for feedback about what components of the Guide are used, including which aspects are least helpful and what sections might be missing. NIST also wants to understand how the Guide could be more useful and relatable to a variety of audiences, such as small health care providers, health plans, and health care clearinghouses (among others). NIST is also looking for information about how the guide is used in a practical manner to implement a data security program. For example, organizations submitting comments may want to provide input about the tools, resources, or techniques used to implement the HIPAA Security Rule.

**PUTTING IT INTO PRACTICE: The NIST website provides a more detailed list of suggested areas for feedback. NIST invites comments through June 15, 2021 at sp800-66-comments@nist.gov. In the subject field, comments should be labeled as "Resource Guide for Implementing the HIPAA Security Rule Call for Comments". After that date, a revised version will be provided for public review and comment.**

## States Continue to Step in to Safeguard Genetic Information

*Posted March 29, 2021*

Utah's governor recently signed into law SB 227, creating the Genetic Information Privacy Act (GIPA). The law, which is anticipated to go into effect in May, is aimed at protecting genetic data collected from direct-to-consumer genetic testing companies. Generally, the law creates requirements for (i) notice; (ii) consent for certain data uses; (iii) data security obligations; and (iv) access, deletion, and destruction rights.

Overview of Current Legal Framework for Genetic Information

To understand this new law, it's helpful to put it in context. Like many areas of data privacy and security law in the United States, the laws governing genetic information very much remain a patchwork. At the federal level, the Genetic Information Nondiscrimination Act, passed in 2008, generally protects individuals against discrimination based on their genetic information in the health coverage and employment context. The law does not preempt state laws that provide equal or greater protection with respect to genetic discrimination and privacy. Other federal laws such as the Federal Policy for the Protection of Human Subjects aka the "Common Rule," or the 21st Century Cures Act, may also impose requirements on how genetic information is collected and used. Such information, depending on the context in what it is collected or shared, might also be subject to the Health Insurance Portability and Accountability Act. The Clinical Laboratory Improvement Amendments and the Affordable Care Act may also impact the collection and use of genetic information. Claims about how genetic information is used (or not) would also be subject to regulation from the FTC under Section 5 authority.

In addition to these myriad of federal laws, states have continued to enact laws applying to genetic information. Some of these states have similarly focused on prohibiting discrimination based on genetic information by certain parties (i.e., insurers or employers). Other laws require informed consent to perform a genetic test or to obtain genetic information. While more comprehensive in terms of the scope of information subject to the laws, California's Privacy Rights Act and Virginia's Consumer Data Protection Act (both set to come into effect in 2023) specifically contemplate "genetic data" in their definitions of "sensitive" personal information. However historically, legislation specifically aimed at the privacy of information collected by consumer genetic testing companies has been rarer. Just last fall, California's governor vetoed a somewhat similar (but broader) law aimed at direct-to-consumer (DTC) companies, which we wrote about here. In 2018, the Future of Privacy Forum issued industry self-regulating privacy best practices for DTC genetic testing companies.

Applicability and Requirements of Utah's Law

Utah's law applies to a "direct-to-consumer genetic testing company" that collects "genetic data" from residents of Utah. "Genetic data" broadly means any data, regardless of format, concerning a consumer's genetic characteristics. This includes: (i) raw sequence data that result from sequencing all or a portion of a consumer's extracted DNA; (ii) genotypic and phenotypic information obtained from analyzing a consumer's raw sequence data; and (iii) self-reported health information regarding a consumer's health conditions that the consumer provides to a company that the company: (A) uses for scientific research or product development; and (B) analyzes in connection with the consumer's raw sequence data. Genetic data does not include de-identified data.

As noted above, the law imposes other obligations around notice, data use, data security and individual rights, described in more detail below.

- **Notice**. Companies subject to this law must provide a prominent, publicly available privacy notice that includes information about the company's data collection, consent, use, access, disclosure, transfer, security, retention, and deletion practices. This is likely to impose little new requirements for those companies already meeting other US (or EU) privacy notice legal obligations.
- **Data uses and consent**. The law requires separate (and sometimes "express") consent for various uses of genetic data. Initially, express consent must be obtained for the collection, use, or disclosure of genetic information. This express consent must disclose who has access to test results and how the company may share genetic data.

Separate express consent is also required for: (i) transfers or disclosures of genetic data to any person (other than vendors); (ii) use of the information beyond the primary purpose of the genetic testing; or (iii) retention of the biological sample following completion of the initial testing service. Express consent is also required for direct or third party marketing activities. However, companies with a first party relationship may, *without* express consent, provide customized content or offer's on the company's website or through the app/service. There are also consent requirements for disclosing genetic data to third parties for research purposes, health insurance companies, and/or a consumer's employer. The law also requires companies to have a valid legal process for the company's disclosure of a consumer's genetic data to law enforcement or any government entity without the consumer's express written consent.

- **Data security**. Companies subject to this law must develop, implement, and maintain a comprehensive security program to protect a consumer's genetic data against unauthorized access, use, or disclosure.
- **Individual Rights**. There must be a process in place for consumers to access their genetic data, delete their account and genetic data, and destroy the biological sample.

Enforcement and Effective Date

The attorney general may initiate a civil enforcement action and recover actual damages, costs, attorney fees, and up to $2,500 for each violation. The law does not contemplate a private cause of action. In Utah, unless specifically noted otherwise in the bill, a law becomes effective 60-days after adjournment. Given that March 5, 2021 was the last day of the annual general session, the law is anticipated to go into effect early May 2021.

**PUTTING IT INTO PRACTICE: Companies operating in the growing DTC industry should continue to be mindful of the increasing appetite for legislation in this area (as well as the patchwork of existing laws), and growing expectations around notice, consent, and data security. With the continued proliferation of the use of digital health and other direct-to-consumer and at-home health and wellness testing and wearable devices, more regulation in this area is likely.**

## What Does the Fifth Circuit's Vacating of HHS HIPAA Fines Mean for Companies This Year?

*Posted February 8, 2021*

Will HHS' approach for imposing penalties in the aftermath of a data breach become a little clearer in 2021? This is a distinct possibility in the wake of a Fifth Circuit decision vacating penalties against MD Anderson Cancer Center. The hospital suffered three data breaches, leading HHS to impose over $4 million in civil penalties. That fine was reversed recently by the Fifth Circuit as arbitrary, capricious, and contrary to law.

MD Anderson first reported to HHS a lost unencrypted laptop that contained ePHI of 29,021 individuals in 2012. It also misplaced two unencrypted USB thumb drives in 2012 and 2013, the first had ePHI of over 2,000 individuals, and the other had ePHI of nearly 3,600 individuals. On February 8, 2019, following HHS's inquiry and investigation, an HHS Appeals Board affirmed an Administrative Law Judge's decision sustaining HHS's civil monetary penalties for the company's alleged (i) failure to implement encryption or adopt an alternative and equivalent method to limit access to ePHI stored on electronic devices, and for (ii) unauthorized disclosure of protected health information in violation of HIPAA and the HITECH Act.

According to the Fifth Circuit, the HHS ruling on the company's encryption measures was incorrect. The Security Rule does not address the effectiveness of an encryption mechanism, only that a covered entity must implement an encryption mechanism or adopt an alternative and equivalent method to protect ePHI. While these particular devices in question were not encrypted, MD Anderson did have an encryption mechanism in place. Thus, the court found that MD Anderson did meet the Security Rule's encryption requirement. On the ruling regarding the disclosure of ePHI, the Fifth Circuit held that HHS had failed to establish that MD Anderson disclosed ePHI to someone outside of the covered entity. The court clarified that under HIPAA's definition of disclosure, a disclosure required an affirmative

act to disclose information and that HHS must prove that the information was actually disclosed to someone outside of the covered entity.

The court found that the penalty imposed by HHS was arbitrary and capricious because it enforced the civil monetary penalty rules against some entities and not others. As an example, the court pointed to another hospital that also lost an unencrypted laptop containing ePHI of more than 33,000 patients, which HHS investigated and imposed no penalty at all. Finally, the court was concerned that HHS had misinterpreted the per-year cap at $1,500,000 when, the Fifth Circuit stated, it is really $100,000. HHS had previously admitted it had misinterpreted the statute back in 2019.

**PUTTING IT INTO PRACTICE: This decision may result in more consistency in penalties and decisions imposed by HHS after companies report data breach incidents to the agency.**

## Learning from the Mistakes of Others: OCR Releases Audit Report

*Posted January 19, 2021*

The HHS Office for Civil Rights released, at the end of last year, findings from audits it conducted in 2016 and 2017 of 166 covered entities and 41 business associates. The report represents the periodic audit that the Department of Health and Human Services must periodically conduct of covered entities and business associates for compliance with the requirements of HIPAA and the HITECH Privacy, Security, and Breach Notification Rules. There are many practical take-aways for businesses from the OCR's report.

OCR concluded that most covered entities and business associates met the timeliness requirements for providing breach notification to individuals, and most covered entities (that maintained a website about their customer services or benefits) also satisfied the requirement to prominently post their Notice of Privacy Practices on their website. However, OCR also found that most covered entities and business associates failed to meet the requirements for other selected provisions in the audit. Covered entities and business associates can keep these findings in mind as they build out and review their privacy and security measures. Concerns raised by OCR included, among others, that the entities failed to:

- Properly implement the requirements of the HIPAA Right of Access, which includes providing access to or a copy of PHI within 30 days of receiving a request and only charging a reasonable cost-based fee for access.
- Implement the HIPAA Security Rule requirements for risk analysis and risk management.
- Satisfy regulatory content requirements for breach notification letters (e.g. failing to include a description of the electronic personal health information (ePHI) breached and steps individuals can take to protect themselves from additional harm).

**PUTTING IT INTO PRACTICE: As HIPAA covered entities and business associates enter the new year, they can use the report as a tool to enhance their awareness of their HIPAA compliance obligations. Steps to consider include access rights, risk management, and including correct content in breach notices.**

# MOBILE PRIVACY

## Google's Privacy "Data Safety" Form Is Now Available

*Posted November 24, 2021*

Google Play's "data safety form" is now live. Developers can now submit the form for early review and feedback. Starting in April 2022, Google will require this label and a privacy policy for all new and existing apps. This is similar to Apple. Before, only apps that collected personal and sensitive user data needed to share a privacy policy in Google's store.

An app's store listing will automatically update with the data safety information in February 2022. If an app has not submitted this information yet or it has been rejected, users will see "no information available." By April 2022 all apps must have this data safety section approved. In the data safety form, apps will have to state what data the app collects. Developers will also have to note activities involving data "sharing." The form also asks about measures taken to protect data. Apps will need to note if there are user rights, such as deletion. Developers are ultimately responsible for the accuracy of the information disclosed in this form.

There are a number of FAQs available as companies work through completing this form. For example, the FAQs note that the form should reflect the global representation of data practices. Thus, those companies that have different practices by geography will have to share version-specific information in the "about this app" section. The launch of the form is on track from Google's initial announcement, which we reported on. Companies that fail to timely comply with this requirement may be subject to blocked updates or removal from Google Play.

**PUTTING IT INTO PRACTICE: Companies that have mobile apps available in the Google Play Store should work with counsel to complete the data safety form. This may involve also reviewing the company's privacy policy. Data practices must be accurately described in both the data safety form and privacy policy to address potential UDAAP exposure.**

## Apple To Require Ability to Delete Accounts In-App

*Posted October 27, 2021*

Apple has issued new guidelines for apps that let people create accounts. The guidelines will require these apps to give people a way to delete their accounts. This requirement is broader than CCPA and GDPR deletion rights, as it applies to all users (not just those from specific territories). The requirements go into effect for submissions starting January 31, 2022.

From a process standpoint, apps will need to let users "*initiate* deletion of their account *from within the app*." This suggests that to comply apps could have a deletion button, link or other process accessible from *within* an app. That could then re-direct users to a browser to complete the deletion request. Provided that the UX for deleting an account is not filled with "dark patterns," apps will likely be permitted to ask users to confirm a request to delete an account.

The guidelines do not make clear if the intent is for apps to also delete data associated with the account. Or, simply, to delete the account. Companies that currently have a CCPA or GDPR process that allows users to delete data may want to consider setting up a new process for this new Apple requirement. In other words, this could be a process that allows a user to delete an account, separate from any jurisdiction-specific process the company already has for users to request that the company delete data.

The new requirements under Apple's guidelines will overlap with certain privacy laws. This is particularly true depending on whether a company takes a "data deletion" or "account deletion" approach. Companies will need to analyze their obligations under relevant privacy laws when requests come in as a result of the guidelines. This includes exceptions to deletion obligations under CCPA and GDPR.

**PUTTING IT INTO PRACTICE: Companies that offer an ability to create an account *in-app* should begin working with stakeholders to develop an approach to meet the account deletion requirement. This includes determining how the back-end will differ (or not) from any other deletion requests the company may be processing.**

## Time to Update Your Privacy Disclosure Creation Checklists? Google Will Add to Mobile Privacy Disclosure Requirements

*Posted May 17, 2021*

Google recently announced that beginning next year it will require Android mobile apps to provide privacy disclosures. These disclosures will live in a new "safety section" in Google Play. The requirements include disclosing:

- What information the app collects and how information is used;
- How the app protects information and if it uses encryption;
- If information is shared and if users have a choice about sharing;
- If users can request data deletion; and
- If the disclosures made in the safety section have been verified by an independent third party.

App developers will need to confirm to Google that the disclosures are accurate. This announcement follows on the heels of Apple nutrition label requirement, which we reported on recently. Companies can start creating these disclosures at the end of this year, even though the deadline for providing these disclosures is not until mid-2022.

**PUTTING IT INTO PRACTICE: To avoid UDAAP issues, care should be taken to accurately describe practices when completing the Google process. Companies will want to make sure the disclosures match what other privacy representations it makes. Those might be in privacy policies or elsewhere.**

## Apple's App Tracking Transparency Now In Effect

*Posted April 29, 2021*

As of this week, Apple's requirements for apps to follow its AppTrackingTransparency are now in effect. These requirements went hand-in-hand with the iOS 14.5 launch, and impacts how an app can track users and access their advertising device IDs. In particular, consumer consent is now required if the app collects consumer information and shares it with others "for purposes of tracking across apps and web sites." Apple has provided developers with specific implementation steps, which will be reviewed when apps are submitted to Apple for approval. As part of the submission, companies need to explain why they want to track users, as required under Apple's guidelines.

As implemented, the process will mean that the app user would receive a pop-up telling them that the app wants to access the user's unique device ID for advertisers. The pop-up asks the user if they want to be tracked and why the app they are using wants them to opt-in. The "why" is something that the app developer will need to draft and have contained within the pop-up.

**PUTTING IT INTO PRACTICE: As we discussed with the implementation of the privacy "nutrition labels," companies who are engaging in covered tracking activities should take care that descriptions submitted to Apple are accurate.**

## FTC Settles with Fertility Tracking App For Alleged Deceptive Data Sharing Practices

*Posted February 16 , 2021*

The FTC recently settled with Flo Health, Inc., a popular fertility-tracking app, based on promises made about how health data would be shared. In its complaint, the FTC alleged that while Flo promised to keep users' health data private and only use it to provide the app's services to users, in fact, health information of over 100 million users was being shared with popular third party companies. Namely, third parties who provided marketing and analytics services to the app.

Like many app developers, Flo tracked both standard app events such as launching or closing the app, as well as "custom" app events. Custom app events record user-interactions unique to those using the Flo app. For example, if a user enters a menstruation date, that interaction is logged as a custom app event. Flo used those custom app event to improve app functionality and identify features that might be of interest to the user. Flo also gave each custom app event a descriptive title, such as "R_PREGNANCY_WEEK_CHOSEN." These custom app events, with that descriptive title, thus conveyed information about users' menstruation, fertility, or pregnancies.

In its app, Flo integrated various third-party tools (software development kits or SDKs) that gathered advertising or other unique device identifiers. When doing this, the SDKs also gathered the custom app events revealing certain health information about users. The FTC alleged that this was sharing health information with third parties and directly contradicted statements in Flo's privacy policy claiming to never share health data (e.g., "We may share certain non-identifiable information about you and some Personal Data (*but never any data related to health*)."). In addition, Flo did not limit what these companies could do with the users' information, agreeing to each company's standard terms of service. Besides allegedly violating its privacy policy, the FTC also pointed that out that this kind of sharing violated several of the third parties' own terms of service/use. Those terms prohibited the sharing of health or sensitive information.

Interestingly given the current status of the EU-U.S. Privacy Shield program, the FTC also alleged that Flo violated both that program and the Swiss-U.S. Privacy Shield framework. In particular, the provisions of the programs that require notice, choice, and protection of personal data transferred to third parties. These allegations are somewhat unique given that to-date, most FTC complaints enforcing the EU-US Privacy Shield have dealt with instances where companies were representing they were participants of the framework when in fact, they were not. Two commissioners also issued a joint statement concurring in part and dissenting in part, arguing that that Flo also violated the Health Breach Notification and the FTC should have enforced it. The Health Breach Notification rule has not been enforced by the FTC to-date. This rule, which the Agency sought public comment on last year, imposes breach notification requirements on vendors of "personal health records" (PHRs) that are ***not*** covered entities, business associates, or subcontractors subject to HIPAA.

While no financial penalty was invoked, as part of the settlement, Flo agreed to a number of terms invariably having some financial impacts. Among other requirements, Flo must notify affected users about the disclosure of their personal information and instruct any third party that received users' health information to destroy that data. In addition, separate from disclosures in any privacy policy or terms of use, before sharing any health information with a third party in the future, Flo must disclose the categories of health information that will be shared, the identifies of the third parties, the purpose of such disclosure and how information will be used, and obtain the users *affirmative express consent*.

**PUTTING IT INTO PRACTICE: Apps collecting sensitive or health information should be aware that descriptive custom app event titles could inadvertently convey information not intended to be shared with third parties. This information could be viewed as sharing of personal information, and thus the FTC (and others) will expect that it be correctly described in the company's privacy policy and elsewhere that representations about data use and sharing are made. Companies who have not done so already will want to think through app event titles and information that gets shared as part of SDK integrations and align that with their privacy disclosures. This case is also a reminder that companies in the health and wellness space have privacy and security obligations even if outside the scope of HIPAA applicability.**

# PRIVACY MANAGEMENT

## FTC 2022 Regulatory Priorities to Include Privacy and Security

*Posted December 22, 2021*

As we look to 2022, a question on many companies' minds is what actions we will see from the FTC. Two recent developments are important on that front.

First, the FTC recently signaled its intent to initiate rulemaking on issues of privacy and security. The Commission indicated that it wants to curb lax security practices and limit privacy abuses. It is also interested in making sure that algorithmic decision-making does not result in unlawful discrimination. The FTC signaled this intent through an Advanced Notice of Proposed Rulemaking, which has a deadline of February 2022. At that time, interested parties can respond to the proposed rulemaking and provide suggestions or alternative methods for achieving the objectives. The FTC may then decide to begin its rulemaking process.

Second, the FTC recently published its annual Statement of Regulatory Priorities. This statement provided updates on a number of different priorities, including several relating to privacy and security. Topics included issues relating to the collection of information from children, health care privacy, and privacy and data security for those in the financial services space. Each are summarized below:

- **Children's Online Privacy Protection Act (COPPA)**. FTC staff are reviewing public comments submitted in response to the agency's 2019 request for comment to its COPPA Rule. The FTC had requested comment on all major provisions of the COPPA Rule. For example, definitions and the notice and parental-consent requirement. This also includes exceptions to verifiable parental consent and the safe-harbor provision.
- **Health Breach Notification Rule (HBNR)**. The Commission initiated a periodic review of the HBNR in May 2020. The comment period then closed in August 2020. The staff intends to submit a recommendation to the Commission by January 2022. In light of some of the controversial and new interpretations to this rule released in 2021, additional clarity about the scope of the rule will be welcomed by industry.
- **Identity Theft Rules**. FTC staff is reviewing the public comments to the Identity Theft Rules and anticipates sending a recommendation by January 2022. The Identity Theft Rules includes the Red Flags Rule and Card Issuer Rule.
- **Safeguards Rules**. In October 2021, the Commission updated the GLBA Safeguards Rule, providing additional requirements for security programs. It also announced the issuance of a Supplemental Notice of Proposed Rulemaking. That notice sought comment on whether financial institutions should be required to report certain data breaches and other security events to the Commission.
- **Fair Credit Reporting Act Rules (FCRA)**. On September 8, the FTC approved final revisions that would bring several rules implementing parts of the FCRA in line with the Dodd-Frank Act.

The Commission's plan to take up additional privacy rulemaking in the new year is unsurprising in light of its vote earlier in the summer to streamline the rulemaking process under Section 18 of the FTC Act. Those changes included giving the FTC chair oversight authority and removing some of the public comment periods.

**Putting it into Practice: These rulemaking initiatives may add further complexity in 2022, especially as companies begin to prepare for forthcoming laws in Colorado, Virginia, and updates in California.**

## Implications of SEC's Scrutiny of Data Use Representations

*Posted November 16, 2021*

The SEC's enforcement action with a leading seller of market data (App Annie Inc.) signals its concern with misleading data use representations. While the data at issue was not "personally identifiable" information, but instead corporate confidential information, the SEC's concerns mirrored those that we have previously seen from that agency, as well as others, regarding representations made about personal information.

App Annie provides investment insights to help its trading firm clients identify potential investment opportunities. Information it provides includes information about mobile application performance, like app downloads, usage, and revenue. One of App Annie's products, App Annie Connect, provides statistical model-generated "estimates" of application performance for its customers based on "aggregated pools of information." The App Annie Connect Terms of Service indicate this is done in order to ensure the data cannot be identified as coming from a particular company. According to the SEC, App Annie falsely assured its clients that the company had policies in place to prevent the disclosure of nonpublic information, when in fact App Annie used its non-aggregated, non-anonymized, nonpublic confidential data to alter its model-generated estimates to make them more accurate and more valuable to trading firms.

The SEC claimed that these actions constituted fraud in connection with the purchase or sale of securities, in violation of Section 10(b) of the Securities Exchange Act, because App Annie's clients used the "estimates" to make purchases and sales of securities. Without admitting fault, App Annie consented to a cease and desist order and payment of $10 million penalty.

**PUTTING IT INTO PRACTICE: This settlement is a reminder that the SEC is looking closely at companies' representations about data use, and expects that representations made will be followed.**

## Privacy Playing Increased Role in Antitrust Enforcement

*Posted October 5, 2021*

Policymakers, regulators, and litigants are starting to bring privacy into antitrust matters. This is a move beyond the traditional focus on price restraints. Privacy are playing both offensive and defensive purposes, as we wrote recently.* Antitrust plaintiffs are starting to argue that tech giants unlawfully maintain market power. They argue this minimizes privacy innovation. They argue that if the defendant company faced more competitive pressure, it would develop products with better privacy protection. The United States Department of Justice and several state attorneys general made this argument in their ongoing lawsuit against Google. But for Google's anticompetitive restrictions, the complaint alleged, Google would be forced to compete against more privacy-oriented search engines, such as DuckDuckGo. The case is currently pending.

Antitrust defendants have also invoked privacy, to defend against allegations of anticompetitive conduct. They have argued, for example, that conduct appearing to limit competition actually increases privacy protection. In *Texas v. Google*, 15 state attorneys general filed a complaint alleging in part that updates to Google Chrome was anticompetitive as the cookie-restricting technologies were a barrier for others to enter the market. Google argued in its defense that it was responding to consumer privacy expectations, not trying to be anti-competitive. This case is also pending.

**PUTTING IT INTO PRACTICE: Privacy practitioners should prepare for questions from their antitrust colleagues, as companies witness more privacy-based arguments on both sides of antitrust disputes. Government enforcers in particular have signaled that they intend to expand the scope of antitrust law beyond price to include other considerations.**

*"Privacy Now Looms Large in Antitrust Enforcement" published by Competition Law360 on Sept. 20, 2021. Reprinted with permission of Portfolio Media, Inc.

## Tools for Understanding Global Privacy Obligations

*Posted September 8, 2021*

Companies are struggling to understand how to comply with rapidly changing and sometimes conflicting privacy obligations. For entities outside of the US seeking to do business in the States, approaching and understanding the patchwork of state and federal privacy laws can be daunting, especially since US privacy laws vary depending on the type of activities in which companies engage, the individuals from whom they gather or use information, and the industry in which the company operates. While there are some "general" privacy laws (notably in California and Virginia) those are the exception rather than the rule.

Rather than think about legal requirements on a law-by-law basis, it can be helpful to group obligations by activity. What restrictions exist when collecting personal information? What notices need to be given? What type of choices should individuals be provided about how their information is used? Do those choices need to be affirmative (opt-in) or retroactive (opt-out)? How can companies use information? Can they send marketing emails? Text messages? In our recent *Nota Bene* podcast episode, Michael P.A. Cohen and Liisa Thomas discuss ways to approach these requirements, and the support the recent treatise, *Thomas on Big Data: A Practical Guide to Global Privacy Laws* released by Thomson Reuters, provides for organizations.

**PUTTING IT INTO PRACTICE: Privacy laws are continuing to modify and adapt, and companies will need to stay on top of these developments as they continue with their privacy compliance efforts. Along with our ongoing blog posts, we are happy to provide other tools (like this new treatise) for our clients -and for the industry generally- to help make clarity in this sea of ongoing confusion.**

## Understanding Risk in An Increasingly Risky World

*Posted March 30, 2021*

As the first quarter of 2021 comes to a close, cyberattacks are only gaining momentum. As we reported last month, these attacks have become big business for threat actors, and companies are working hard to be prepared. Taking stock of potential risks – and risk management techniques – can be a useful exercise in this environment. For this, tools from change management can help. Change management, particular sustainable change management, teaches us not to jump head-first into action, but first to take stock of what actions will be most helpful.

To mitigate cyber risks, several actions of course are useful, and indeed several are required by data security laws. These include identifying and preparing for known risks, updating policies, implementing operating procedures to execute on those policies, strengthening internal controls and auditing compliance. These steps can help with both preventable risks -i.e., those that are internal and controllable; or are strategic – i.e., risks that one might be willing to accept for some benefit. However, those are only two of three types of risk, according to management theorists Robert Kaplan and Anette Mikes.[i] The situations companies are facing today -with multiple potential cyberattacks arriving at unknown times, in unknown ways, by unknown threat actors- fall into a third category of risk. External risks. Risks outside of a company's control; risks that are not predictable.

To manage external risks, companies can include more tools in their prevention toolbox, Kaplan and Mikes explain. In preparing for cyberattacks we can think about their suggestions. For them, the focus with external risks should be on identifying them when they happen (often easier said than done) and mitigating the potential negative impact. A written policy may not be able to prepare a company (how can the policy anticipate every potential bad outcome?), but tabletop exercises that focus on teamwork -rather than on preparing for a specific type of incident- could. Other tools include short checklists, along the lines used by pilots (including in disaster situations).[ii]

Some data incidents may arise from risks that fall into multiple categories. Thus having multiple mitigation strategies in place can be important. These steps, like being strategic about privacy compliance generally, can help companies' overall privacy compliance efforts, as we outlined in our articles on right-sized privacy programs at the beginning of this year.

**PUTTING IT INTO PRACTICE: Given the external nature of cyber risks facing companies, now is a good time to take stock of mitigation strategies in place. Thinking proactively – even where much may be unknown – can help companies be prepared if the worst happens. Rather than only tabletop exercises that prepare for a specific type of situation, companies may also want to add those that deepen relationships and teamwork.**

FOOTNOTES
[i] Kaplan, Robert S. and Mikes, Anette. *Managing Risks: A New Framework*. Harvard Business Review (June 2012).
[ii] Gawande, Atul. The Checklist Manifesto: How to Get Things Right. (2010).

## Elements of Right-Sized Privacy Program: Addresses the Law

*Posted January 28, 2021*

An effective privacy program takes into account legal requirements and litigation risk. While this series advocates for starting with strategy and designing a customized approach, this does not mean that legal obligations and risks should be ignored. Instead, by starting with strategy and focusing on customization, many legal risks can be better managed. If the legal requirement in a given law is that a data security policy addresses the risks a company faces, for example, a company is better off with a customized policy. For this reason, addressing the law can be thought of as the middle of the project, rather than the start. (See more in a recent article we published.)

When addressing the law, companies should avoid thinking of them as static requirements. Not only will existing laws change (for example, the many modifications that were made in 2020 to California's privacy law and related regulations), but new laws are constantly on the horizon. Litigation similarly is on the rise for an expanding set of corporate activities (see, for example, lawsuits around a collection of biometric information, an activity almost unheard of ten years ago).

**PUTTING IT INTO PRACTICE: Any privacy program needs to take into account a wide variety of issues, and legal risks should not be overlooked. Properly addressing them, though, requires more than just reviewing their requirements, but also thinking about how the company can, practically, put appropriate policies and procedures in place.**

## Elements of Right-Sized Privacy Program: Customized

*Posted January 27, 2021*

As mentioned in the prior post in this series, a strategically developed privacy program can help support companies in a rapidly changing legislative and enforcement environment. As part of taking a strategic approach, companies attempting to create a right-sized privacy program will want to customize their program to their company. Privacy and data security laws place bespoke obligations on companies. Privacy notices need to describe the *company's* practices. Data security laws anticipate policies that are designed for the risks that the *company* faces.

To customize a program, the start is not taking an off-the-shelf policy or copying the approach of a competitor. Instead, privacy professionals will look at their organization's strategic needs, and weigh those against its strengths, weaknesses, opportunities and threats. (Yes, a SWOT analysis!) From there, a company could borrow from strategic management tools and take a "scorecard" approach, along the lines developed by Robert Kaplan and David Norton. Using this approach, the privacy office can think through what personnel and infrastructure it needs to reach the strategic goals it has set out. To help underscore the need for those resources, it can then reflect on what the impact will be on its "consumers" (i.e., the internal stakeholders whom it supports). Similarly, how having those resources will support the company's financial goals.

**PUTTING IT INTO PRACTICE: Change management tools can help privacy professionals customize their approach and develop a truly right-sized approach for privacy compliance. This one-sheet can help your organization think through developing a strategic privacy approach.**

## Elements of Right-Sized Privacy Program: Strategic

*Posted January 26, 2021*

One of the biggest difficulties companies may face for effective privacy program implementation arises if they neglect strategy and focus only on the law. Namely, developing policies and procedures that mention legal requirements, but fail to address the underlying business purpose of those policies and procedures. Certainly, compliance with the law is critical. But it is not the only part. And, importantly, since regulators expect companies to follow their policies and procedures, taking time to strategize -and address *how* a company will comply with its policies and procedures- is critical.

Professionals implementing a right-sized privacy program, from a strategic perspective, can take several steps:

- First, a strategic program is one that takes into account and supports the underlying business needs. What are the goals of the organization? What is the current environment in which it is operating? What challenges does it face? What are its existing strengths? The program is then designed around that reality.
- A strategic program is also one that is implementable, not aspirational. It is one that can be easily understood by company personnel (and thus followed), and training to adhere to the program is achievable.
- Finally, a strategic program is one that takes into account the fact that corporate activities are ever-changing, as are privacy and data security laws. A strategic program anticipates that modifications will be needed, and is not designed with a "set it and forget it" approach.

**PUTTING IT INTO PRACTICE: Companies face ever-shifting privacy requirements. Developing a flexible, holistic and right sized privacy program can help in this rapidly-changing world. The next article in this series will look further into how a program can be customized to the company.**

## Developing a Right-Sized Privacy Program

*Posted January 25, 2021*

Later this week, January 28, 2021 will mark International Privacy Day: a day corporations release educational efforts around privacy and data protection. There are many reasons to approach privacy proactively in 2021: (1) January 28 will mark the second week of a new US administration, one which will likely focus more on privacy and data security; and (2) laws and enforcement in this area continue to change and develop, as we reported last year. With this in mind, privacy and data security practitioners may find themselves behind with reactive approaches. Reactivity is also costly, both monetarily and resource-use wise.

To be proactive, companies can take an adaptive approach to customized privacy compliance to their organization. One that, instead of needing constant modification as laws or practices change, can grow and adapt as those inevitabilities occur. An adaptive privacy program, most critically, is both aligned with and supportive of the organization's underlying mission, vision and goals. Such a program is bespoke to the organization, and avoids extraneous elements or those that do not account for the company's ultimate activities and needs. The program also takes into account both regulatory and litigation risk, and is flexible enough to adapt as those change. Finally, it is a program that the organization can get behind and support. From line managers to senior leadership, it is a program that is digestible and around which people can easily be trained.

**PUTTING IT INTO PRACTICE: In recognition of Privacy Day 2021, this week's blog series walks through core elements for developing a right-sized privacy program, one that will ideally provide better legal protections than taking an off-the-shelf, create-it-as-you-fly-the-plane approach.**

## Elements of Right-Sized Privacy Program: Appropriately Addresses Third Parties

*Posted January 21, 2021*

To round out this series on right-sizing a privacy program, our last stop is thinking about the impact of working with third parties. There are many legal requirements to assess and/or to address in third party contracts when personal information is being gathered or is changing hands.

Unfortunately, the legal requirements in this area are not static. As many are aware, the terms that exist in this vein in the EU are in the process of changing. They are also ever-growing. In the US, many laws provide certain protections -or require certain hurdles- if contractual provisions are not in place (California's CCPA, for example). While many are aware of the CCPA provisions regarding third parties, other laws impact contracting with third parties, including in the data security realm. For example, state data protection laws in California, Illinois, Massachusetts, and New York, as well as several others.

When faced with such a large number of legal requirements, it often helps to take a step back. Critical for a right-sized approach is understanding what information is flowing to which partners. With that diligence –done perhaps in coordination with IT or IS teams' efforts– privacy professionals can work on having the appropriate contractual terms in place. While standardized language is ideal, it is not always feasible. Knowing when and where to push back, or when and where to have customized language, is one of the potential benefits of a right-sized approach.

**PUTTING IT INTO PRACTICE: As our "Privacy Day" week draws to a close, we hope that these insights and ideas with respect to strategizing and customizing as well as legal and vendor considerations help you think through creating a right-sized privacy program at your organization. In sum, we suggest initiating efforts with a focus on strategy, establishing and keeping track of measurable goals, and obtain the resources you need to keep implementation going. This one-sheet is a handy resource for the various elements discussed over the course of this series.**

## 2020 Privacy Year in Review

*Posted January 21, 2021*

As we reach the end of January 2021, it is becoming increasingly clear that this will be a busy year in the areas of privacy and data security. Following up on our posts discussing some of the important trends from last year, the Sheppard Mullin Privacy and Cyber Security team has put together a comprehensive resource containing all of our posts from last year. From a focus on artificial intelligence, to international data flow and vendor transfer concerns, to ongoing enforcement of a patchwork of laws, we anticipate many of the issues facing companies in 2020 will not go away this year.

# US GENERAL PRIVACY LAWS

## California Publishes Initial Public Comments to CPRA

*Posted December 20, 2021*

The California Privacy Protection Agency recently published public comments received in response to its preliminary rulemaking activities for the California Privacy Rights Act (CPRA). The comments were originally solicited in September and due by November 8. The public feedback totals nearly 900 pages. It includes comments from various companies, industry associations, and other interested parties.

The Agency intends to have additional informational hearings to gather more feedback. Its October meeting minutes suggest that the hearings may address topics such as how the procedures for exercising rights is operating, and the "opt out preference signal" or "global privacy control." Formal rulemaking activities will begin at the conclusion of the agency's fact gathering. There is no set timetable. That said, the rule-making authority is tied to 6 months *after* the agency provides notice to the Attorney General (discussed here).

We anticipate that the Agency will not only update existing CCPA rules, but issue new ones. This includes potentially addressing at least 15 topics not originally identified in the CCPA. For example, the access and opt-out rights for processing using automated decision making. This also includes the annual "cybersecurity audit."

**PUTTING IT INTO PRACTICE: As companies begin to plan and prepare budgets and resources for 2022, keeping an eye on developments and the procedural process for the CPRA regulations will be important. As we approach the new year, companies are also reminded that information collected in 2022 will be subject to CPRA's 12-month look back period.**

## Virginia Privacy Law Continues to Progress Towards 2023 Implementation

*Posted December 13, 2021*

Virginia edges closer to its privacy law January 2023 implementation. A new working group report gives some insight on implementation focus. The working group is tasked with giving advice on implementing the Virginia Consumer Data Protection Act. It held a series of meetings with companies and other stakeholders throughout the year. This current report summarizes "points of emphasis" from those meetings. Those included that law be interpreted strictly. For example, sunseting companies "right to cure" after two years. Another point raised was whether to let the attorney general seek actual damages based on harm.

During the meetings some raised whether sample forms should be created to help smaller companies. Other issues included procedural items like funds to staff more AG employees. Education proposals were also put forward. That included education initiatives directed to smaller corporations and a consumer-education focused website.

**PUTTING IT INTO PRACTICE: This report highlights the ongoing focus we expect next year on implementing this new comprehensive privacy law. As a reminder, the law will apply -with some exceptions- to companies that collect information on 100,000 or more Virginian consumers.**

## California Bill Clarifies Timing for CPRA Rulemaking Authority

*Posted October 8, 2021*

California recently passed AB 694, which makes a few "technical" changes to the California Privacy Rights Act (CPRA). Importantly, this amendment clarifies the timing for the new California Privacy Protection Agency's (CPPA) rulemaking authority.

Previously, CPRA provided two different dates for when the Agency would assume responsibility for rule-making. One section said it was the *earlier* of July 1, 2021, or six months after the Agency provides notice to the Attorney General that it is prepared to begin rulemaking. However, a different section of the statute said it was the *later* of these two dates. Because the appointments to the CPPA were just made, the amendment clarifies that it is the *later* of these two dates – i.e., six months after notice to the Attorney General.

**PUTTING IT INTO PRACTICE: Though in the past, Companies now have clarity that CPPA's rule-making authority was not in fact tied to July 1, 2021. Instead, the Agency's authority will be tied to 6 months *after* it provides its notice of proposed rule-making (which we expect later this year/early 2022 as discussed here).**

## California's New Privacy Agency Seeks Feedback on CPRA

*Posted September 28, 2021*

California's new privacy protection agency recently issued an invitation for public comments as part of its preliminary rulemaking activities for the California Privacy Rights Act (CPRA). Introduced and passed by ballot initiative in November 2020, CPRA amends and introduces several new concepts to CCPA.

CRPA required the creation of a new administrative entity – the California Privacy Protection Agency (CCPA) – tasked with implementing and enforcing the law separate from the attorney general's office. Appointed in March, the agency's five-member board is made up of lawyers and academics. In advance of the January 1, 2023 effective date, the agency seeks comments on both the new CPRA rules, as well updates to CCPA's existing rules. While the agency is supposed to issue final CPRA regulations by July 1, 2022 (*before* the amended law goes into effect), many are skeptical of this timing in light of the process and timing for the CCPA regulations.

In particular, the Agency seeks feedback on the "new and undecided" issues introduced by CPRA, including:

- Processing that presents a significant risks to consumers' privacy or security
- Cybersecurity audits and risk assessments
- Automated decision-making
- Rights to delete, correct, and to know
- Right to opt-out of selling or sharing of personal information
- Right to limit use and disclosure of sensitive personal information
- Definitions such as "sensitive personal information" and "deidentified" (among others)

**PUTTING IT INTO PRACTICE: Comments are due by November 8, 2021. Tips for submitting effective comments are available here. Public hearings are expected to be heard in Winter/Spring of 2021 – 2022. This invitation for comments is *not* the same as a proposed rulemaking action. The public will have the opportunity to provide additional comments on proposed regulations or modifications when the agency proceeds with a notice of proposed rulemaking action (expected later this year). The agency's next board meeting is scheduled for October 18, 2021 at which time we may learn other additional information about this process and expected timelines.**

## AG Implements Tool to Allow Consumer Reporting of Alleged DNS Violations

*Posted August 24, 2021*

Changes The California attorney general has created a tool for consumers to report situations where companies sell information but do not have an opt-out of sale link on their website. The release of the tool came at the same time as the AG's update on its CCPA enforcement actions. In that update, the AG highlighted one of the most common problems it had found: not having appropriate disclosures around "sales."

Under CCPA, companies (for whom the law applies) must indicate if they do or do not sell information, as that term is defined. If a company does sell information it needs to provide individuals with the ability to opt out of such sales. Failure to comply with this requirement of CCPA carries no private right of action. Instead, after being notified of noncompliance, a company has 30 days to cure. If the company fails to do so, the AG may bring action.

The advent of this tool creates an interesting wrinkle to the 30 day period. Using the tool, individuals can create a "notice of noncompliance to send" to businesses they believe are not complying with the do-not-sell provisions of CCPA. According to the AG, the notice a consumer sends "may satisfy [the 30 day notice] prerequisite." If a business does not cure a violation then the consumer is directed to report the issue to the AG.

For now, the tool only allows consumers to notify of do-not-sell concerns. The AG has signaled that it may update the tool to allow for consumers to submit notices about other issues. If the AG report on enforcement actions gives any direction, those other issues might be lack of required disclosures in privacy policies, not giving people a way to exercise rights, or not telling people about whether information was (or was not) sold. All three of these, according to the report, were common areas of non-compliance.

**PUTTING IT INTO PRACTICE: Business subject to CCPA should be on the lookout for potential notices generated by this tool. The suggested subject line generated by the tool is "Notice of Noncompliance with the California Consumer Privacy Act (CCPA)." The consumer is not given instructions about what point of contact to use with the company. It may thus be useful to train those who monitor the most common entry points such as general "help" or "info" email addresses on how to handle these notices, as well as to work with the CEO or President (to whom the form notice is drafted) and those who monitor that email address (if others do monitor it).**

## And Then There Were Three: Colorado Passes Privacy Law, Effective July 2023

*Posted July 13, 2021*

Colorado recently joined Virginia and California in passing a more comprehensive privacy law. The Colorado Privacy Act (CPA) will go into effect July 1, 2023. This is six months after Virginia's law (CDPA) and California's Privacy Rights Act (CPRA), which amends the existing CCPA, go into effect. The law does not have a private right of action, and the AG is to adopt regulations on certain aspects by July 1, 2023.

**Applicability**. Like CDPA, Colorado's law covers information about "consumers" which are people acting in their personal capacity, it does *not* apply to information about employees. The law will apply to companies that conduct business in Colorado and meet one of the following: (1) control or process personal data of 100,000 Colorado consumers during a calendar year, or (2) derive revenue or receive a discount on the price of goods or services from the sale of personal data and processes or controls the personal data of 25,000 consumers or more. Like Virginia's CDPA, the law exempts financial institutions (subject to GLBA). While other types of data, including certain health care information is exempt, covered entities and business associates subject to HIPAA are not wholesale exempt (unlike CDPA). The law does not apply to other types of data regulated by various laws (such as COPPA and FERPA, among others). Unlike in California and Virginia, non-profits are in-scope, and will *not* be exempt.

**Individual Rights**. Colorado consumers will have rights similar to those under other US laws and GDPR. For example, a right of access and to correct. There are also rights to deletion and data portability. Like Virginia and the CCPA, there is a right to opt out of selling information. Also like Virginia, there is a right to opt out of targeted advertising and profiling. For targeted advertising, this will not be a new concept, since companies will already be addressing this by following the DAA and FTC self-regulatory schemes. Consumers will need to be able to action their rights through a universal opt-out mechanism: the Colorado AG will issue regulations on this topic. Also like California and Virginia, these rights requests must be honored within 45 days (with an extension available in certain circumstances). Colorado's new law, as with that of Virginia, includes some of GDPR's "sensitive information" concepts, requiring opt-in consent to process any such information.

**Contractual Requirements**. Like Virginia and GDPR, contracts between controllers and processors should outline certain obligations. (CPA uses the "controller" and "processor" terminology, similar to Virginia and GDPR, but unlike California which refers to parties as "businesses," "service providers" and "third parties.") Contractual obligations include instructions about the nature, purpose, and duration of processing. Contracts will also need to include requirements around sub-contractors, data security, termination procedures, and cooperation (among others).

**Accountability and Governance**. CPA introduces data minimization concepts: i.e., collection of information must be limited to what is reasonably necessary for the processing. This is like CDPA, CPRA, and GDPR. While not a new concept to data use activities, CPA more explicitly introduces a duty to avoid secondary uses of data. This means that personal data should not be processed except for those purposes for which the data was collected, unless the consumer consents. CPA also calls for the documentation of data protection assessments, similar to CPRA (but not CCPA), CDPA, and GDPR. These assessments are required for specific types of processing activities listed in the statute. Those activities include the sale of personal data and processing of sensitive data. It also includes targeted advertising where profiling may present certain risks.

**Enforcement**. There is no private right of action under this new Colorado law. The attorney general and district attorneys have exclusive enforcement authority. The AG is required to provide a 60-day written notice to companies it believes are in violation of the law and an opportunity to cure prior to initiating any action. However, there is a sunset provision for the cure period starting January 1, 2025. Violations of the CPA constitute deceptive trade practices and therefore are subject to a $20,000 per violation fine pursuant to the Colorado Consumer Protection Act.

**PUTTING IT INTO PRACTICE: The CPA blends together concepts from existing California and EU law, as well as the upcoming (January 1, 2023) requirements in Virginia and California. Companies working on updating their privacy compliance programs for those two will want to add Colorado residents into the mix, and consider more broadly how they will comply with these requirements across states. For those already adhering to GDPR, the additional requirements may not be burdensome, but some level of gap analysis will be needed.**

## Nevada Broadens its Privacy Law

*Posted June 15, 2021*

Nevada's governor recently approved an amendment to their privacy law. As we covered previously, generally, this law affords consumers a right to opt out of the "sale" of their data to third parties. The amendment broadens (1) the scope of the law to also apply to "data brokers" and (2) consumers right to opt-out of sale. The changes are expected to go into effect October 1, 2021.

Nevada is the not the first state to regulate "data brokers." California and Vermont also have laws that apply to companies that are in the business of buying and selling information about consumers. In Nevada, a data broker is defined as "a person whose primary business is purchasing covered information about consumers with whom the

person does not have a direct relationship and who reside in this State from operators or other data brokers and making sales of such covered information."

Nevada's previous definition of "sale" was relatively narrow in scope, requiring that there be an exchange for monetary consideration *and* an onward license or sale of the data to other third parties. While still not as broad as "sale" under California's CCPA (which defines sale to also include "other valuable consideration"), the amendment removes the requirement that the exchange be for the purpose of the other person licensing or selling covered information to additional persons. Thus, Nevada still maintains the requirement that there be "monetary consideration" which aligns more closely to Virginia's impending privacy law.

**PUTTING IT INTO PRACTICE: While the amendments to Nevada's law likely will not significantly broaden what activities might constitute a "sale," companies should still confirm that any existing disclosures in privacy policies about Nevada's law remain accurate in light of these changes. Data brokers should also review and assess whether any existing processes will need to be updated.**

## Changes to CCPA Regulations are Approved and in Effect

*Posted March 22, 2021*

On March 15, 2021, the California Office of Administrative Law ("OAL") approved additional regulations to the CCPA. These regulations were originally proposed at the end of 2020 (which we covered here). The changes are effective immediately. The modifications largely focus on (1) changes impacting those companies that "sell" information, and (2) the verification process for rights requests made by authorized agents.

Specifically, the regulations touch on the following areas:

- **"Offline" notices**. Organizations 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. For example, brick-and-mortar stores may post signage where the information is collected directing individuals where the information to opt-out can be found online.
- **"Opt-out" icon**. For companies selling information, the regulations provide an icon that may be used in addition to (and *not* in lieu of) having the link on the bottom of a website for consumers to opt-out. 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.
- **Requests to opt-out**. Methods for submitting requests to opt-out should not be designed with the purpose of subverting a consumer's choice to opt-out. The regulations provide a number of illustrative examples for avoiding these kind of "dark patterns." For example, requiring consumers to click through or listen to unnecessary reasons why they should not submit a request to opt-out before confirming their request. Companies should also not require a consumer to provide personal information that is unnecessary to implement an opt-out request. Consumers should also not be required to search or scroll through the text of a privacy policy once they have clicked on the "Do Not Sell My Personal Information Link" in order to find the request to opt-out mechanism.

**PUTTING IT INTO PRACTICE. These updates to the regulations will likely have little to no impact to those organizations that are not "selling" information or receiving a high volume (or any) rights requests from authorized agents. However, organizations that are "selling" information may want to confirm that the userflow for their do-not-sell link, notice and mechanism are transparent and do not require any unnecessary steps. In the Final Statement of Reasons, the Attorney General noted that these changes stemmed in part from the office's experience in enforcing the CCPA. Thus now given some of these itemized examples, particularly for opt-out requests, this is likely to be an area that the OAG's office will continue to look to for potential non-compliance.**

## Virginia is for…Privacy: Comprehensive Law Passed, Effective January 2023

*Posted March 3, 2021*

Virginia is now the second state, after California, to pass a comprehensive privacy law. The Consumer Data Protection Act ("CDPA") will come into effect January 1, 2023 (the same time as the modification to California's Consumer Privacy Act ("CCPA"), namely the California Privacy Rights Act). Although this new Virginia law has been compared by many to California's current CCPA and the EU's GDPR, there are some differences. Businesses will find most of the differences a relief, although the law does introduce a few new concepts.

- **Virginia's law applies more narrowly than CCPA and GDPR**. The law covers information about "consumers," which are people acting in their personal capacity, not employees (thus unlike CCPA and GDPR). It applies to companies that conduct business in Virginia and meet one of the following: (1) control or process personal data of 100,000 Virginian consumers during a calendar year, or (2) control or process personal data of 25,000 Virginian consumers and get 50% of gross revenue from the sale of personal data. Virginia also exempts financial institutions (subject to GLBA) and health care covered entities and business associates (subject to HIPAA). This is unlike CCPA, where the exemptions largely apply to *types* of information subject to other regulated laws, but not the entities subject to those other laws altogether. That said, Virginia also exempts several types of information. Nonprofits are also exempt.
- **Virginia, like California, has no private right of action**. The AG has exclusive enforcement authority over CDPA. Moreover, the AG is required to provide a 30-day written notice to companies it believes are in violation of the law and an opportunity to cure prior to initiating any action. If after time the violation remains, the AG may initiate an action and seek $7,500 in damages for each violation.
- **Virginia provides for individual rights similar to those found under CCPA, and also adds some found in GDPR**. The process for responding to rights requests appears simpler than CCPA and GDPR, however unlike those two laws, in Virginia there are fewer exceptions to honoring rights requests. Virginia also goes beyond CCPA and includes GDPR's "rectification" right, and GDPR's right to object to automated decision making and profiling. Like CCPA, there is a right to opt out of selling information, but Virginia adds a right to opt out of targeted advertising. While the latter is not contained in CCPA, this concept is already addressed by those who follow the DAA and FTC self-regulatory schemes. This addition appears to be designed to help clarify some of the different interpretations under CCPA about whether targeted advertising is a "sale." Although the CDPA rights process is generally more straightforward than CCPA, Virginia does add an appeals process. At the conclusion of that process, companies must direct consumers to the AG for any unresolved issues. The Virginia law also includes some of GDPR's "sensitive information" concepts, requiring opt-in consent to process any such information.
- **Virginia goes beyond CCPA by mirroring GDPR's collection and use limitations; contains data security obligations similar to many jurisdictions**. Like certain concepts in GDPR, under the new Virginia law companies should only collect information needed for the purposes of the processing. Further, information should only be used for the purposes reasonably necessary and compatible with a company's stated disclosures. This is unlike CCPA, and one area where companies may need to focus their efforts. A related concept under CDPA is to protect what information a company does maintain. This is similar to that which exists in many other US states as well as GDPR, and requires companies to implement and maintain reasonable administrative, technical, and physical data security practices to protect the confidentiality, integrity, and accessibility of personal data. These practices should be appropriate to the volume and nature of the personal data at issue.
- **Virginia's law goes beyond CCPA in including certain GDPR-like accountability and governance requirements**. CDPA calls for the documentation of data protection assessments, similar to GDPR, but unlike CCPA. These assessments are to be conducted for specific types of processing activities listed in the statute including targeting advertising and the sale of personal data. The Attorney General may request copies of these as part of a civil investigative demand. The assessments are to apply to processing activities created or generated after January 1, 2023, and are not retroactive. CDPA also, like GDPR, requires agreements between controllers and processors (i.e., service providers) with specific language in those contracts.

**PUTTING IT INTO PRACTICE:** Companies will have some time before this law becomes effective, and may take comfort that its scope is more narrow than the general privacy laws of Europe and California. Indeed, for those already adhering to both GDPR and CCPA, the additional requirements may not be excessively burdensome. There will be some review and potential modifications needed nevertheless. Areas to examine include vendor contracts and privacy policy disclosures. For others, the lift may be heavier, especially if a company is currently not subject to the GDPR-like items listed above. This new law also serves as a reminder for companies to evaluate whether their current privacy program is sufficiently flexible and adaptive. Developing a principle-based program that can grow can be particularly helpful as other states look at passing similar types of broader privacy laws.

As you move forward in planning and implementing your privacy efforts this year, we hope that this compilation serves as a useful tool.

# 2021 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

**Michael Cohen**
*Partner*
mcohen@sheppardmullin.com
202.747.1958

**Michael Scarborough**
*Partner*
mscarborough@sheppardmullin.com
415.774.2963

**Morgan Forsey**
*Partner*
mforsey@sheppardmullin.com
415.774.3254

**Moorari Shah**
*Partner*
mshah@sheppardmullin.com
213.617.4171

**Allison Fulton**
*Partner*
afulton@sheppardmullin.com
202.747.2195

**Sara Shanti**
*Partner*
sshanti@sheppardmullin.com
312.499.6358

**David Garcia**
*Partner*
drgarcia@sheppardmullin.com
310.228.3747

**Michael Zhang**
*Partner*
mzhang@sheppardmullin.com
86.21.2321.6000

**Oliver Heinisch**
*Partner*
oheinisch@sheppardmullin.com
44.203.178.7833

**Sarah Aberg**
*Special Counsel*
saberg@sheppardmullin.com
212.634.3091

**A.J. Dhaliwal**
*Special Counsel*
adhaliwal@sheppardmullin.com
202.747.2323

**James Fazio**
*Special Counsel*
jfazio@sheppardmullin.com
858.720.7418

**Tenaya Rodewald**
*Special Counsel*
trodewald@sheppardmullin.com
650.815.2664

**Ana Anvari**
*Associate*
aanvari@sheppardmullin.com
310.228.2292

**Samuel Cohen**
*Associate*
sjcohen@sheppardmullin.com
212.896.0663

**Anne-Marie Dao**
*Associate*
adao@sheppardmullin.com
858.720.8963

**Snehal Desai**
*Associate*
sdesai@sheppardmullin.com
415.774.2960

**Charles Glover**
*Associate*
cglover@sheppardmullin.com
212.896.0679

**Susan Ingargiola**
*Associate*
singargiola@sheppardmullin.com
212.869.0624

**Julia Kadish**
*Associate*
jkadish@sheppardmullin.com
312.499.63340

**Yarazel Mejorado**
*Associate*
ymejorado@sheppardmullin.com
858.720.8955

**Elfin Noce**
*Associate*
enoce@sheppardmullin.com
202.747.2196

**David Poell**
*Associate*
dpoell@sheppardmullin.com
312.499.6349

**Bridget Russell**
*Associate*
brussell@sheppardmullin.com
310.228.2273

**Harrison Schafer**
*2021-2022 Privacy Fellow*
hschafer@sheppardmullin.com
312.499.6371

**Alyssa Shauer**
*Associate*
ashauerr@sheppardmullin.com
424.288.5305

**Nikole Snyder**
*Associate*
nsnyder@sheppardmullin.com
202.747.3218

**Ariana Stobaugh**
*Associate*
astobaugh@sheppardmullin.com
424.288.5301

**Brittany Walter**
*Associate*
bwalter@sheppardmullin.com
858.876.3525

**Dhara Shah**
*Associate*
dshah@sheppardmullin.com
312.499.6336

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