SheppardMullin

Eye On Privacy: 2022 Year in Review

These articles appeared in the “Eye On Privacy” Blog in 2022 (www.eyeonprivacy.com)

Sheppard Mullin's 2022 Eye on Privacy Year in Review

As we start down the path of 2023, with the pandemic not quite behind us and economic uncertainty looming, the world can seem unsettled. Some things do appear to be a constant. Included in those are regulatory and court scrutiny on privacy and cybersecurity. As companies' privacy and security teams make plans for their 2023 compliance efforts, it can be helpful to look back at last year's developments.

From the expansion of "general privacy" laws in US states and concerns over cross-border data transfers, to global focus on artificial intelligence, surveillance and dark patterns, 2022 was a busy year in privacy. As we have done in years past (including 2021, 2020, 2019 and 2018), we have created a comprehensive resource of all our www.eyeonprivacy.com posts from 2022, covering these topics and more. We hope that this is again a useful tool to help prepare for privacy and cybersecurity program plans for the year.

Sheppard Mullin Privacy & Cybersecurity Team

Our group includes some of the most respected lawyers in the privacy space, including 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

CHILDREN'S PRIVACY

Impact on Companies of California's Children's Privacy Law – Effective 2024

Posted September 28, 2022

The California governor recently signed into law the California Age-Appropriate Design Code Act, which will go into effect July 1, 2024. The law applies to "businesses" (as defined by CCPA) that provide online services or features "likely to be accessed by children." To understand if the product or service is likely to be accessed by children, companies should look at factors like audience composition, if there are child-directed ads, or elements known to be of interest to children. Children are those who are under 18 (as opposed to the federal Children's Online Privacy Protection Act, applicable to collection of personal information of those under 13).

Unlike COPPA, the law is not focused on parental consent. Its prohibitions and requirements are much broader. By way of example, the law prohibits companies from several activities, including:

1. Using information in a way that harms children
2. Profiling children (subject to certain exceptions)
3. Collecting or using children's precise geo-location information (again, subject to some exceptions)
4. Use "dark patterns" to get children to provide too much information or engage in activities detrimental to their health or well-being

The law contains data minimization provisions, and will require entities to conduct a data protection impact assessment before launching a product or service "likely to be accessed" by children. That assessment needs to examine whether the product or service will be "harmful" to children or could exploit children, among other things. These assessments must be made available to the Attorney General upon request. The law calls for a working group to provide a report on (among other things) how to best protect children, which report will be provided on January 1, 2024 and every two years thereafter until January 2030.

Putting It Into Practice: Companies who are subject to CCPA can take two steps now to begin preparing for this law. First, begin to assess if their sites are likely to be accessed by those under 18. If so, then second, companies can look to the laws data protection impact assessment requirements, and begin now in thinking through how they would conduct such an assessment for their online products and services.

CARU Strikes Again: Another Mixed-audience App Settles Over COPPA Allegations

Posted September 27, 2022

The Children's Advertising Review Unit recently found that Tilting Point Media violated COPPA and CARU's Self-Regulatory Guidelines for Advertising and for Children's Online Privacy. Tilting Point is the operator of the SpongeBob: Krusty Cook-Off app. The case arose as part of CARU's routine monitoring of child directed content.

CARU determined that the app was a "mixed audience" app, meaning that it was directed to both adults and children under 13. In making this determination, CARU took into account a variety of factors, including the fact that Spongebob Squarepants is appealing to children, as well as the app's use of music and animation that is also appealing to children.

CARU found that Tilting Point collected personal information from children under the age of 13 and had no mechanism for obtaining verifiable parental consent. As a mixed-audience site, it was however required under both CARU's Guidelines and COPPA to obtain verifiable consent. CARU noted that while Tilting Point had an age screen

on its app, it was not a neutral and effective age screen. The age screen just required a user to accept the app's terms and privacy policy, which a minor under 13 could easily do.

In addition to the consent problems, CARU also found that the app served automated ads that could not be stopped or dismissed until users downloaded the advertised app or watched the entire ad. Users were induced to watch ads with the promise of virtual currency rewards. CARU concluded that these ads interfered with gameplay and manipulated children to watch the ads. CARU also found that some of the ads that were displayed were inappropriate and unsafe for children.

Pursuant to CARU's recommendations, Tilting Point Media agreed to take corrective actions, including updating its age screen and privacy policy to align with COPPA and changing its advertising practices, including taking active steps to prevent unsafe ads from displaying to children.

PUTTING IT INTO PRACTICE: CARU has increased its focus on mixed audience sites. These platforms should keep in mind that under both COPPA and the CARU Guidelines, they will need an age gate or a process for obtaining verifiable parental consent before collecting information from children online.

Children's App Settles with CARU Over COPPA and Guideline Violation Allegations

Posted August 25, 2022

Firefly Games agreed to take corrective action in response to the Children's Advertising Review Unit's allegations that the company had violated COPPA by inaccurately (and confusingly) explaining its privacy practices. The app in question, LOL Surprise! Room Makeover, featured dolls and characters intended for children and animated characters. It also included content directed to adult users. CARU concluded as part of its routine reviews that, *inter alia*, the app was "mixed audience." As such, the app needed to comply with not only CARU's guidelines, but the Children's Online Privacy Protection Act as well.

CARU reviewed both the company's main privacy policy, as well as an app-specific privacy policy. CARU found that the two were inconsistent. For example, the main privacy policy did not describe collection and use of children's information, while the app's privacy policy did. The two policies were also inconsistent in their description of cookies, geo-location data, and other items. Moreover, CARU alleged, the policies did not accurately reflect the company's actual practices. CARU found these inconsistencies a violation of COPPA insofar as parents were not given information about how children's information would be used. CARU also found that there was no age verification process, and as such, no ability to obtain parental consent before collecting information from children under 13. Such age verification was needed under COPPA, CARU stated, as the site was found to be a mixed audience site.

In response to CARU's concerns, Firefly Games noted that the app had passed Google's review process for family advertising. CARU found this unpersuasive, stating "that an app developer cannot rely on a platform's guidelines or requirements as a substitute for complying with the CARU Ad Guidelines." Firefly Games agreed to take corrective action to address CARU's concerns.

PUTTING IT INTO PRACTICE: This case is a reminder that mixed audience sites are expected to have a process for obtaining verifiable parental consent if collecting personal information from children. Additionally, it serves as a caution to child-directed and general audience websites alike to ensure that privacy statements are consistent, and are an accurate reflection of actual practices.

FTC Continues Focus on Children's Privacy

Posted May 27, 2022

The FTC recently took two well-publicized steps in the children's privacy space. First, it penalized WW International (formerly, Weight Watchers) and its subsidiary, Kurbo, for alleged COPPA violations. Second, it unanimously voted to adopt a new policy statement on education technology and COPPA. These actions follow its March COPPA settlement with TickTalk Tech.

Kurbo

Kurbo is a wellness app marketed to children as young as eight. According to the FTC, the registration process contained a non-neutral age gate: children who self-identified as under 13 were prompted to register through a parent portal. Those over 13 could register on their own. The FTC found that while the age gate was theoretically intended to screen users under 13, it lead children towards the 13+ option: an option that allowed them to successfully register and give Kurbo personal information without parental consent. Moreover, children who initially entered false birth dates to access the app were later able to correct their birth dates.

Hundreds of users revised their ages after signing up, putting Kurbo on notice that they were under 13. Kurbo deactivated those accounts only after receiving notice from the FTC in late 2021. At that time, Kurbo provided notice to parents about its information collection practices. It did not attempt to get parental consent or confirmation, however. The notice also did not tell parents that persistent identifiers were collected through the website and app. Also of concern for the FTC, until late 2021 Kurbo kept user information indefinitely, in violation of the COPPA (which allows information retention only for as long as needed for the collected purpose).

Kurbo has agreed to pay $1.5 million and delete personal information that was improperly collected from children. As part of the settlement, Kurbo also agreed to destroy any models or algorithms developed in whole or in part using personal information collected through the app. This is a unique penalty that the FTC had not imposed before.

EdTech

This action against Kurbo is likely *not* the last COPPA case we will see in 2022. The FTC recently indicated that it will "crack down on" EdTech companies that improperly surveil students while they use EdTech tools for learning. This warning accompanied the FTC's EdTech policy statement. In that statement, the FTC reminded companies of several important elements of COPPA.

These elements include not conditioning a child's participation in an activity on providing more information than necessary. (This restriction is similar to the EDPB's recent "dark patterns" warning.) It also includes securing information and not retaining information longer than necessary. Finally, the FTC also reminded companies who provide EdTech tools under school authorizations that they can collect and use information only for the requested online education service. They cannot use the information for unrelated commercial purposes like marketing and advertising.

PUTTING IT INTO PRACTICE: In light of the recent EdTech warning, and the settlements with Kurbo and TickTalk, we anticipate more COPPA decisions from the FTC in the coming months. Companies should keep in mind cautions about data limitation, and keep in mind settlement terms that include destroying information – and the analytics derived therefrom.

Smart Watch Maker Settles with CARU Over Privacy Policy and Parental Consent

Posted April 14, 2022

The Children's Advertising Review Unit recently settled with TickTalk Tech, LLC over its information collection practices. CARU, a self-regulatory body that reaches voluntary settlements with companies, conducts regular audits of privacy practices by companies in the child space. During one such audit, it identified concerns over TickTalk Tech's kids smart watch, TickTalk4.

In particular, CARU was concerned that the product privacy policy was not prominent and did not explain in an easy-to-understand way how children's information would be used. While parents were told in on-screen advertising that the watch had geo-location tracking services, the privacy did not clearly explain, for example, what information would be passively gathered from children. CARU's noted that while the company worked to obtain consent during the product registration process, the consent was meaningless because parents couldn't tell from the privacy policy what its practices were. The lack of valid consent and the unclear disclosures constituted, according to CARU, a violation of both its guidelines and COPPA. To resolve the matter, the company has agreed to:

- ensure that its privacy policy clearly discloses its data collection practices regarding children;
- ensure that the privacy policy is conspicuous and not hidden or difficult for parents to find;
- explain its data retention and deletion policies are regarding children's data;
- explain how parents can limit use of their children's data; and
- obtain verifiable consent from parents before collecting children's information.

PUTTING IT INTO PRACTICE: This settlement is a reminder that companies should take care to describe their information collection practices clearly and accurately in their privacy policies. This is particularly true for products directed towards children. This settlement is also a reminder that CARU is actively looking at connected devices for compliance with its guidelines and COPPA. Both require, among other things, obtaining (informed) parental consent before collecting information online from children.

OpenX Ad Exchange Settles With FTC Over Alleged COPPA and Other Violations

Posted January 14, 2022

OpenX Technologies recently agreed to pay $2 million to settle FTC allegations that the advertising platform violated the FTC Act and the Children's Online Privacy Protection Act. OpenX runs a programmatic ad exchange, running a bidding platform that auctions online ad space. The company contracts with publishers who have open ad space as well as ad networks with inventories of ads they are seeking to publish online.

According to the FTC, while OpenX indicated in its privacy policy that users could opt out of having location information collected or used by "*using the location service controls in your mobile device's setting*" in fact, it continued to collect and use location information from those who had followed the opt-out process. The FTC argued this was deceptive in violation of Section 5 of the FTC Act.

In addition, according to the FTC, OpenX posted ads on sites that its human quality team identified as child-directed. The FTC complaint indicated that millions (if not billions) of ad requests were received from these sites and aps, and these bid requests contained personal information of children. Ads were then placed on those sites. The FTC found that because of the placement of programmatic ads on these child sites, OpenX needed to have complied with COPPA's parental notice and consent requirements, since the serving of these ads involved the collection of personal information from children. The FTC found incorrect the standard language OpenX had in its privacy policy. Namely, stating that the company did not "*engage in activities that require parental notice or consent*" under COPPA.

In addition to the monetary penalty, OpenX has agreed to delete all data that it collected in violation of the COPPA Rule. OpenX has also agreed to implement a comprehensive privacy program to ensure COPPA compliance.

PUTTING IT INTO PRACTICE: This case serves as a reminder that the FTC will look closely at companies' underlying technologies and practices when determining privacy compliance, including whether companies are adhering to their stated privacy notice. (In other words, not doing anything the FTC might consider a deceptive practice.) This case is also a reminder that the FTC takes the perspective that the serving of targeted advertising in many circumstances involves the collection of personal information.

CONSUMER PRIVACY

Illinois Appellate Court Weighs in on Biometric Data Policies

Posted December 14, 2022

An Illinois state appellate court's recent ruling will impact how companies consider compliance with Illinois' Biometric Information Privacy Act (BIPA). That court ruled companies must have a BIPA-compliant written retention-and-destruction policy in place before collecting and possessing biometric data. The decision makes clear that mere possession of biometric data triggers the duty to develop the necessary written BIPA policy. In relevant part, under BIPA's section 15(a), companies must establish a written, publicly-available policy that governs their retention and destruction of biometric data.

The plaintiff in the case (*Mora v. J&M Plating, Inc.*) began clocking into his job via biometric fingerprint scan in September 2014. His company, however, did not implement a biometric data policy until May 2018. On these facts, the trial court granted summary judgment for defendant. The trial court found that Section 15(a) established no time limit for the implementation of a BIPA policy and therefore concluded defendant's implementation of a BIPA policy in 2018, four years after initial collection, satisfied Section 15(a).

The appellate court reversed the decision on appeal. According to the appellate court, the 2014 collection of plaintiff's biometric data triggered defendant's duty to implement a written policy. Putting it in place four years later was insufficient to retroactively shield defendant's otherwise non-compliant collection of plaintiff's biometric information from 2014 to 2018. There is still an opportunity for the defendant to appeal to the Illinois Supreme Court, and the decision is not binding outside of Illinois's second appellate district.

PUTTING INTO PRACTICE: This case suggests that -at least in one Illinois jurisdiction- companies will need to have a written retention-and-destruction policy in place for biometric data *before* collecting such information. Doing so will minimize risk under Section 15(a) of BIPA.

White House Releases Guidance on AI

Posted November 10, 2022

The White House recently released its Blueprint for an AI Bill of Rights in an effort to guide the discussion on the design, use and deployment of AI in systems that impact the American public. The Blueprint outlines the following five guiding principles:

- **Safe and Effective Systems:** Systems should be developed and monitored to ensure they are safe and effective. This should include independent evaluation and reporting.
- **Algorithmic Discrimination Protections:** Systems should be continuously monitored to protect against algorithmic discrimination. This may include equity assessments, disparity testing, and organizational oversight.
- **Data Privacy:** Privacy by design should guide the systems. Privacy protections should seek individual permission and respect choices made regarding the collection, use, access, transfer and deletion of data.
- **Notice and Explanation:** Use of AI should be explained in a manner that is clear, timely, and accessible.
- **Human Alternatives, Considerations, and Fallback:** Individuals should have the option to opt out of AI systems in favor of a human alternative.

This Blueprint is non-binding on companies and provides only a starting point on the discussion of how best to protect the American public from potential harms from the use of automated systems. A technical companion included with the Blueprint provides examples and steps companies can use to implement the principles.

PUTTING IT INTO PRACTICE: While not binding, this blueprint is a reminder that AI is receiving increasing scrutiny, which we anticipate will continue in the United States and worldwide.

New York City Set To Regulate Employment Decisions Made By AI

Posted September 28, 2022

Beginning January 1, 2023, New York City will restrict employers from using artificial intelligence to make employment decisions unless they follow certain guidelines. The local law applies to employment decisions made "within the city" regarding job applicants and promotion decisions.

The law contains two major provisions. First, employers must provide notice to evaluatees ten business days before employing an AI system, provide them an opt-out, and list the qualifications and characteristics used by the system. Second, the system itself must be audited for bias annually. The results of the audit must be publicly posted on the employer's website. Employers are also required to publicly post or make available upon request the sources of data used by the system and the organization's data retention policy.

PUTTING IT INTO PRACTICE: Organizations that use AI to make employment decisions in New York City should take time before January 1 to review these systems and develop appropriate notice and choice procedures.

FTC Renews Focus on Dark Patterns

Posted September 27, 2022

Following its 2021 Dark Patterns enforcement policy, the FTC recently issued a staff report on the practice. The report summarized many of the cases the agency has brought against companies it alleges have engaged in "dark patterns" designed to "get consumers to part with their money or data." These include using design elements that induce false beliefs, that delay important and material information, that lead to unauthorized charges, or that subvert or confuse privacy choices.

In this new report, the FTC provides businesses with strongly-worded instructions about how to avoid collect personal information from consumers in a way that might be viewed as a dark pattern. These include:

- Not setting system defaults to collect more information than a consumer would expect, or to use information in a way that consumers would not expect.
- Making it easy for consumers to choose how their information gets used. Specifically, the FTC cautions against having multiple screens through which a consumer needs to navigate to exercise choice, or having ambiguously or confusingly worded toggle buttons.
- The FTC also urges companies to look at the user interfaces they create from the perspective of the consumer.
- Finally, the FTC provides specific direction about collecting and using sensitive information. Companies should make choices about how this information is going to be used clear and understandable, and give people the tools and information they need to exercise their choices. If sensitive information is sold, companies should vet the purchasers, how the purchasers will use the information, and importantly, monitor buyers' use of the sold information.

PUTTING IT INTO PRACTICE: This report follows on the heels of the FTC's proposed privacy rulemaking and signals its ongoing concern that notice and choice presented to consumers be clear and understandable. Much of the advice in the report is familiar and indicate the FTC's expectations of companies. Of note are (1) the direction to review user interfaces and (2) to monitor use of information (especially sensitive information) after it has been sold to third parties.

NAD Examines Privacy Statements Made by DuckDuckGo in Online Ads

Posted July 28, 2022

Following, by a day, a privacy-related claim challenge brought against another advertiser, the National Advertising Division found that advertiser DuckDuckGo had sufficiently substantiated its privacy claims. These cases are significant reminders in two ways. First, that claims made about privacy and security can be viewed through an advertising lens and examined to see if they are properly substantiated. Second, that the NAD, the self-regulatory body that actively examines truth and accuracy of advertising, is looking at privacy claims. As those familiar with the NAD are aware, it refers those who do not cooperate to the FTC for priority action to examine if there have been violations of Section 5 of the FTC Act.

DuckDuckGo provides a browser and mobile app search engine. In a promotional YouTube video, it claimed that using its products were the "best, quickest and easiest steps you can take for your privacy health." The NAD assessed these and similar claims to understand how they would be perceived by consumers. It found that they conveyed that the company's products were a way to protect against the sharing of individuals' data. There was also an implied claim that the company did not share personal data.

The NAD found the claims supported by the evidence which included a third-party expert confirming that the company's measures (encryption, tracker blocking, and private searches) protect against the three largest categories of personal data collectors. Additionally, the NAD found evidence that no special configurations to receive privacy protections were needed (unlike the company's competitors) – support "best" claims. DuckDuckGo confirmed -through proof of regular audits and implementation of blocking technologies in its products- that it did not share personal data.

In reaching its conclusions, the NAD did caution DuckDuckGo to take care not to imply that its protections extended to search engines or apps that fell outside of its platforms' solutions. Namely, through claims that one would be protected "no matter where the internet takes you."

PUTTING IT INTO PRACTICE: This case is another reminder that privacy representations may be examined through an advertising lens. Companies should take care to ensure that they have substantiation that supports both the express and implied claims that they make about how they use personal data.

NAD Brings False Advertising Claims Over Privacy Representations

Posted July 26, 2022

The National Advertising Division, a self-regulatory body that examines the truth and accuracy of advertising claims, recently examined privacy claims made by Brave, Inc. Using the same analysis given to other advertising claims, the NAD analyzed Brave's statements about consumer privacy. It assessed both the implied as well as the express claims made by the company as well as the extent to which the substantiation Brave had for the claims supported those claims.

Brave provides consumers with a web browser that it promoted as "stop[ping] online surveillance" and one that could shield "everything… that can destroy your privacy." The NAD also felt Brave was making an implied claim, namely that information was not shared with third parties. The NAD came across these claims as part of its regular monitoring, believing they were unqualified affirmative promises that needed to mirror the data relied on for substantiation. In response to the inquiry, Brave provided substantiation to the NAD supporting the claims. Included in its evidence were its own studies of its browsers' performance, as well as third-party expert analysis.

The NAD compared the substantiation provided to the claims. It found that the express claims about stopping surveillance and shielding from destruction of privacy were not supported. While the evidence might show that Brave might use industry best practices, the NAD argued, this did not support the broad unqualified claims made by Brave. The NAD found, though, that the implied claim of not sharing with third parties was supported by evidence that Brave does not store users' information, nor does it share it with third parties.

While disagreeing with the NAD's conclusions about its express claims, Brave agreed to comply with the NAD's recommendations. It further stated that it is no longer using the claims in question. Advertisers who decline to follow NAD recommendations can be referred to the FTC for further action under Section 5 of the FTC Act, and the FTC takes these referrals on a priority basis.

PUTTING IT INTO PRACTICE: This case is a reminder that privacy representations may be viewed as advertising claims. As such, they need to be accurate and supported by the evidence. Additionally, claims will be examined not only for what they expressly communicate, but also their implied message.

What's the Big Deal About Dark Patterns?

Posted May 25, 2022

Dark patterns have been a recent regulatory focus. The FTC issued an enforcement policy late last year, and the European Data Protection Board followed suit with guidelines this spring. The two have slightly different takes on what constitutes a dark pattern. The European focus is on misleading consumers into providing more information than they would have otherwise, or in providing unwitting consent for use of information. For the FTC, the focus is on programs that "trick" consumers into making purchases, including signing up for ongoing services. For both entities, the concern is on misleading consumers into providing unwilling consent or agreement.

In the U.S., as we have written, dark patterns may violate negative option laws, including the Restore Online Shoppers Confidence Act. In Europe, dark patterns can violate various parts of GDPR, including Articles 4, 5 and 7. Regulators have brought action for dark pattern violations. This includes a recent action by the U.S. Consumer Financial Protection Bureau, as we wrote about on our sister blog.

The term "dark pattern" suggests nefarious activity in which an upstanding corporate citizen would not engage. Companies might therefore be tempted to ignore this guidance. That would be a mistake. The activities over which regulators have expressed concern might be something in which a "normal" company might engage. This is especially true in the privacy realm. On that front, the EDPB provides helpful examples of what activities might be a dark pattern. Examples include repeatedly asking a user to provide information (continuous prompting), sending users through too many pages to find privacy-related information (privacy maze), designing an interface in such a way that a user fails to think about data protection (skipping), or using formatting and other techniques to direct a user towards more privacy-invasive options (hidden in plain sight).

What are some top takeaways from these various regulatory guidance? What can companies do to avoid being viewed as engaging in a dark pattern? The following are a few steps to take:

- ***Be clear.*** As the EDPB recommends, keep in mind concepts of deception and fairness. Related to this, make disclosures – especially about data usage – clear and prominent. The EDPB gives case study examples of "mistakes," including a company with a 70-page, header-less, privacy policy.
- ***Do not deceive***. This is a fundamental tenant for the FTC, enforced under Section 5 of the FTC Act. The EDPB provides case study examples, including in the context of privacy use FAQs. Those FAQs should not negate other disclosures, or contain internal inconsistencies.
- ***Give options.*** For negative option programs, the FTC reminds companies that users need a way to opt-out. For privacy use decisions, the EDPB emphasizes giving users ways to modify decisions they have made during a sign-up process.

PUTTING IT INTO PRACTICE: The term "dark patterns" can cover a variety of activities. Regulators are particularly concerned right now with companies that use formatting, technologies and other mechanisms to guide users into making decisions that they would not have made otherwise. When putting together user interfaces, companies would be well served to keep in mind the concepts of clarity and choice to avoid potential dark pattern allegations.

DAA Issues Warning On Device Fingerprinting

Posted March 23, 2022

The Digital Advertising Accountability Program, which enforces privacy principles for digital The Digital Advertising Accountability Program, which enforces privacy principles for digital advertising, issued a compliance warning to advertisers regarding device fingerprinting. This warning is worth keeping in mind, since the "fingerprinting" practice is rising in more and more industries.

Device fingerprinting is using technological tools to recognize unique devices. It typically occurs by combining device characteristics (like device IP address, operating system, type and version of web browser) to identify unique devices. This information can be collected across applications, and thus falls within the guidelines. In particular, as "Cross App Data," which is that which is collected from a particular device regarding application use over time and across non-affiliate applications. Under the DAA guidelines, companies need to provide notice and consent when using Cross-App Data for certain purposes—including for interest-based advertising (also known as targeted advertising).

Until recently, notice and consent was put in place when advertisers (engaged in interest-based advertising) used advertising identifiers ("Advertising IDs"). Advertising IDs associate the user of a particular app with a particular

device at a particular time. The DAA's recent warning, though, explains that the guidelines are intended to apply more broadly. They impact *any* technology that is used to identify a device or user for interest-based advertising.

In short, the compliance warning makes it clear that advertisers using device fingerprinting as a method to identify users or devices for purposes of interest-based advertising must provide the "same level of transparency and choice to consumers as they would if using an Advertising ID for the same purpose." To comply with these requirements, advertisers may need to provide notice, enhanced notice or garner consent from the user, depending on the advertiser's relationship to the user and the details of collection.

PUTTING IT INTO PRACTICE: Companies who use device fingerprinting for interest-based advertising, whether online or on mobile devices, should keep in mind the DAA's notice and choice requirements.

CROSS-BORDER DATA TRANSFERS

EU's Initial Response to US Proposed Data Transfers Framework

Posted December 22, 2022

The EU released its draft adequacy decision for the EU-US Data Privacy Framework, but all is not smooth sailing. As we wrote in October, the US developed the proposed new framework in response to the declared inadequacy of the EU-US Privacy Shield program.

For those keeping track, this is the third attempt at a transborder agreement for transfer of information from the EU to the US. The two previous programs, Safe Harbor and Privacy Shield, were both ultimately determined to be insufficient by the EU after challenges from the privacy activist Maximilian Schrems.

In releasing this draft adequacy decision, does that mean that all in the EU think the ailments that plagued the Privacy Shield have been cured? Privacy activists, including Schrems, think not. And the framework's journey through the EU system has only just begun. It still needs to be reviewed by the European Data Protection Board, a committee of Member State representatives before being assessed by the European Parliament. During that time and at each stage, it is expected that the framework will continue to receive heavy scrutiny.

PUTTING IT INTO PRACTICE: As the saga continues, as we wrote in the past, companies will need to continue to take appropriate measures to address EU legal requirements for transfers of personal information out of the EU including standard contractual clauses, transfer impact assessments, and supplemental measures.

EU To Review New EU-US Data Transfers Framework

Posted October 10, 2022

President Biden signed a new executive order on Friday, with a framework that seeks to replace the existing Privacy Shield program. That program was found to be an invalid mechanism for transferring personal data between the EU and the US in 2020 (the Schrems II decision). Since then, companies have struggled to establish an appropriate mechanism for transfer of information from the EU to the US.

As many are aware, under EU law, personal information cannot go from the EU to a third country unless it has been deemed to have "adequate" protections of personal information — except in limited circumstances. Prior to Schrems II, the EU-US Privacy Shield was one such circumstance. It was struck down, in part, however, because of the EU's concerns with EU residents' personal information being collected and used by US intelligence agencies. Under the newly proposed program, those agencies' ability to process such data is restricted: their use of "signals intelligence"

limited, *inter alia*, to that which is necessary to further a "validated" intelligence activity and use proportional to that activity. The order also creates a review process to oversee how agencies access individuals' information for intelligence surveillance purposes.

The program is now with the EU to review, and an agreement may be in place in March 2023. Privacy activists, including Schrems, however, have already begun criticizing the program as insufficient. For those keeping track, this is the third attempt at such a transborder agreement, with the Shield's predecessor -the EU-US Safe Harbor- struck down in 2015.

PUTTING IT INTO PRACTICE: As we wrote in April, companies right now will need to continue to take appropriate measures to address EU legal requirements for transfers of personal information out of the EU. For transfers to the US, this might include standard contractual clauses, transfer impact assessments, and supplemental measures.

Working Through the New EU SCCs? European Commission Releases FAQs

Posted May 26, 2022

The European Commission recently released a set of FAQs for the new EU standard contractual clauses (SCCs). The FAQs are based on feedback received from various stakeholders and currently address 44 different questions. Additional content is expected to be added as new questions come up. The long-awaited SCCs for transfers out of the EEA were adopted about one year ago. Among other changes, two of the biggest differences in the new cross-border SCCs is the modular approach and provisions to address *Schrems* II. The FAQs cover some general questions about the SCCs for companies that might be newer to using this mechanism for data transfers. In addition, the FAQs respond to a number of more mechanical questions added by the new terms. This includes handling the "docking clause," limits of liability, applicable law, and requirements around government access.

PUTTING IT INTO PRACTICE: For parties working through the challenges of filling out these new terms for data transfers, the FAQs shed additional light on many of the new sections. As of September 27, 2021, all *new* contracts should be relying on the new SCCs. By December 27, 2022, all *existing* contracts using the old SCCs will need to be replaced by the new terms.

Formation of CBPR Forum Signals Continued Movement

Posted May 2, 2022

As we have written in the past, APEC's Cross-Border Privacy Rules (CBPR) program is intended to help companies more easily transfer personal data across borders. Participating companies complete self-assessments and participate with their local countries' "accountability agent." There are currently seven participating economies, which include the US, Canada, Japan. Those participating economies recently announced the development of a "Global CBPR Forum." The Forum is tasked with, *inter alia*, creating an international certification system, reviewing members' privacy standards, and ensuring that the program is "interoperable with other data protection and privacy frameworks."

For companies interested in participating in the CBPR program, the current country accountability agents will continue to provide certifications, the US Department of Commerce clarified. There will be a transition from those agents to the process created by the CBPR Forum, but only upon 30 days prior notice. Those companies who currently have been certified under the existing system will be automatically recognized under the new regime.

PUTTING IT INTO PRACTICE: While this announcement will not have an immediate effect on companies, it signals a desire by participating countries the streamlining and simplifying of the cross-border data transfer process.

Waiting on a new EU-US Privacy Shield

Posted April 28, 2022

It has been almost two years since the Privacy Shield was struck down as a valid data transfer mechanism in *Schrems* II. Many have been wondering "what's next"? Will there be a replacement framework? When will that be released? Will the replacement be invalidated? Well, the European Commission and US recently announced an "agreement in principle" to replace the EU-US Shield Privacy Shield. The EDPB also recently released a statement welcoming the announcement, but reminding companies that the announcement is *not* actually a legal framework. Thus, nothing has changed… yet.

The new framework is intended to address several of the key concerns raised in *Schrems* II. The US highlighted that the framework will help ensure that:

- intelligence collection may be undertaken only where necessary to advance legitimate national security objectives, and must not disproportionately impact the protection of individual privacy and civil liberties;
- EU individuals may seek redress from a new multi-layer redress mechanism that includes an independent Data Protection Review Court; and
- U.S. intelligence agencies will adopt procedures to ensure effective oversight of new privacy and civil liberties standards.

PUTTING IT INTO PRACTICE: For the time being, companies must continue to take necessary measures to comply with data transfer requirements of GDPR in light of *Schrems* II. This includes putting in place standard contractual clauses (or other appropriate safeguards), conducting transfer impact assessments, and putting in place any supplementary measures that might be needed. While a draft is expected to be released this year, it will then need to go through the adequacy decision process.

European Commission Adopts Korean Adequacy Decision

Posted January 6, 2022

The European Commission recently adopted an adequacy decision regarding the Republic of Korea's data protection laws. As a result of this decision, personal data can freely flow between the EEA and South Korea without the need for additional transfer mechanisms.

Without such a finding of adequacy, EU law prohibits the transfer of data out of the EU without certain measures being in place. These include, for example, the transferring entity and the recipient entering into Standard Contractual Clauses, or the recipient having Binding Corporate Rules in place. South Korea now joins 13 other countries that are able to freely transfer data from the EEA. This list includes Andorra, Argentina, Canada (commercial organizations), Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, Switzerland, United Kingdom, and Uruguay.

This decision follows the EDPB's September opinion on the Commission's draft Korea adequacy decision. The decision covers transfers of data to both commercial operators and public authorities. A list of common Q&As can be found here. Whether the UK will grant South Korea this same adequacy status remains to be seen. Unlike the recent UK adequacy decision, which contains a sunset provision, the conclusion about the adequacy of South Korea's data privacy laws is not time-limited. Instead, the decision will be subject to a regular review every three to four years. The decision will continue so long as the level of data protection remains.

PUTTING IT INTO PRACTICE: Companies who regularly engage in cross-border data transfers will not need additional measures -like SCCs- if the data transfers are from the EU to Korea.

DATA BREACH

Pennsylvania Amends Breach Notification Law

Posted November 29, 2022

Pennsylvania recently amended its data breach notification law to expand its definition of personal information and provide for a HIPAA exception. The process for providing notice in the event of a username/email breach has also changed. The amendments will not be effective until May 2, 2023.

As amended, personal information will include medical and health insurance information. This mirrors many other states, which have also recently expanded their definitions of personal information to include these data elements. Pennsylvania's breach notice law will also mirror that of almost half of the other US states in including in its definition of personal information usernames or e-mail addresses, in combination with a password or security question that would permit access to an online account.

In addition to amending the definition of personal information, Pennsylvania will add a HIPAA compliance exception to the breach notice law. Under that exception, entities that are both subject to *and in compliance with* HIPAA's privacy and security standards will be deemed compliant with the state's breach notice law.

Finally, beginning in May 2023, if there has been a usernames/email accounts breach, companies can provide "electronic notification." To be sufficient, it needs to tell the individual to change their password or take other protective measures.

PUTTING IT INTO PRACTICE: Pennsylvania's changes will not have a significant impact for those entities who maintain incident response programs that address the requirements of all US jurisdictions. Companies will want to keep in mind that medical and health insurance information, as well as usernames/email account and passwords will become personal information under the breach notice law beginning May 2023.

Lessons From New York AG Scrutiny of Breach Investigation and Response

Posted November 14, 2022

New York's Attorney General Letitia James recently secured a $1.9 million settlement from online retailer Zoetop Business Company, Ltd. to settle allegations that Zoetop had improperly handled a 2018 data breach and subsequent consumer notification. The scrutiny given to Zoetop provides insights into the NYAG's expectations around breach investigations and response.

The case arose from Zoetop's 2018 discovery that user credentials for 39 million account holders had been compromised. According to the AG's Assurance of Discontinuance, the user passwords were hashed using encryption software that was "known at the time" to be insecure. Upon learning of the compromise, Zoetop engaged a forensic investigator, who determined that not only were user credentials stolen, but also that customer payment information had been compromised at the point of purchase. Following discovery of the data breach, Zoetop made written notification of the breach to its customers and notified the AG at the same time. As has become increasingly common following notification, the AG launched an inquiry into the Zoetop data breach. The AG expressed concern with several of Zoetop's incident response-related actions. These included:

- Failing to reset the credentials of all of impacted users, and instead only resetting credentials of those users who placed an order and thereby had their payment information compromised;
- Failing to automatically force password resets for users, and instead having users reset their credentials themselves;

- Communicating in the FAQs issued with notification that "impacted individuals" were being contacted, when in reality only those users who had placed an order were notified (and not all users whose credentials were compromised);
- Communicating to impacted individuals that their credit card numbers were not impacted, when its investigation showed the opposite; and
- Failing to give its PCI investigators access to the impacted systems.

As part of the settlement, Zoetop has agreed to pay $1.9 million and to implement a comprehensive information security program that addresses the AG's stated concerns.

PUTTING IT INTO PRACTICE: This settlement is a reminder that regulators are increasing their scrutiny of organizations who suffer a data breach. That scrutiny may include not just whether the company's security measures were sufficient, but also if it properly investigated the incident and accurately notified consumers about the nature and scope of the breach. As a result, it will be important for companies to ensure their forensic investigations, incident remediation, and communications are thoughtful, comprehensive, and defensible in the context of guidance issued by both regulators and industry organizations.

Wegmans Settles With NYAG for $400,000 Over Data Incident

Posted July 14, 2022

The New York Attorney General recently announced a data security-related settlement with Wegmans Food Markets. The issue arose in April 2021 regarding a cloud-based incident. At that time a security researcher notified Wegmans that the company had an Azure cloud storage container that was unsecured. Upon investigation, the company determined that the container had been misconfigured and that three million customer records had been publicly accessible since 2018. The records included email addresses and account passwords.

Of concern for the AG, among other things, were that the passwords were salted and hashed using SHA-1 hashing, rather than PBKDF2. Similarly, the AG found concerning the fact that the company did not have an asset inventory of what it maintained in the cloud. As a result, no security assessments were conducted of its cloud-based databases. The NYAG also took issue with the company's lack of long-term logging: logs for its Azure assets were kept for only 30 days. Finally, the company kept checksums derived from customer driver's license information, something for which the NYAG did not feel the company had a "reasonable business purpose" to collect or maintain.

The NYAG argued that these practices were both deceptive and unlawful in light of the promises Wegman's made in its privacy policy. It also felt that the practices were a violation of the state's data security law. As part of the settlement, Wegmans agreed to pay $400,000. It also agreed to implement a written information security program that addresses, among other things:

1. asset management that covers cloud assets and identifies several items about the asset, including its owner, version, location, and criticality;
2. access controls for all cloud assets;
3. penetration testing that takes into account cloud assets, and includes at least one annual test of the cloud environment;
4. central logging and monitoring for cloud assets, including keeping cloud logs readily accessible for 90 days (and further stored for a year from logged activity);
5. customer password management that includes hashing algorithms and a salting policy that is at least commensurate with NIST standards and "reasonably anticipated security risks;" and
6. policies and procedures around data collection and deletion.

Wegmans agreed to have the program assessed within a year of the settlement, with a written report by the third-party assessor provided to the NYAG. It will also conduct at-least-annual reviews of the program. As part of that review it will determine if any changes are needed to better protect and secure personal data.

PUTTING IT INTO PRACTICE: This case is a reminder for companies to think not only about assets on its network, but its cloud assets, when designing a security program. Part of these efforts include clearly identifying locations that house personal information (as defined under security and breach laws) and evaluating the security practices and controls in place to protect that information. The security program elements the NYAG has asked for in this settlement signal its expectations of what constitutes a reasonable information security program.

Maryland Amends Data Security and Breach Notice Obligations

Posted June 22, 2022

Maryland recently passed two companion bills amending the state's Personal Information Protection Act. The bills modify the data breach notification requirements and scope of businesses subject to the data security requirements. The key changes are summarized below, and will go into effect October 1 of this year:

- **Expanded scope of data security requirements**: The requirement to implement and maintain "reasonable" security measures will also apply to businesses that *maintain* personal information of Maryland residents (and not just those who own or license such information).
- **Expanded definition of personal information**: The definition of genetic information has been revised and expanded. This change follows a similar update California made to its breach notification law.
- **Additional notice requirements to the Attorney General**: Additional information must now be provided in any notice to the Attorney General. This includes the number of affected Maryland individuals and a description of the breach, including when and how it occurred. It also includes steps the company has taken or plans to take relating to the security of the system, and a sample notice sent to affected individuals.
- **Impacts to Timing Requirements:** Businesses that *maintain* personal data must notify the owner of the data of a breach as soon as practicable, but within 10 (formerly 45) days of discovering or being notified of the breach. While in some cases, companies maintaining information may have shorter notification obligations by contract, this is a fairly aggressive statutorily imposed timing requirement. For businesses owning or licensing personal information whose notification is delayed because of circumstances surrounding a law enforcement investigation, notification must be made as soon as reasonably practicable, but with seven (previously 30) days after the law enforcement agency determines that notification will not impede an investigation. This is if the original 45-day period has lapsed or by the end of the original 45-day period.

PUTTING IT INTO PRACTICE: Beginning October 1, 2022 companies who suffer a breach impacting Maryland residents will want to keep in mind these changes. Namely, the expanded definition of personal information, shortened notification timelines, and content requirements for regulator notification.

FTC Weighs In On Data Breach Notification

Posted June 16, 2022

The FTC recently reminded companies that principles of fairness and the likelihood of harm may in some cases prompt breach notification. This requirement might exist even if state breach notice laws have not been triggered. The FTC emphasized at the same time the need for breach disclosures to be accurate. These comments appeared in the FTC blog, and underscore the agency's continuing trend to exercise its enforcement authority under the FTC Act in the data security and data breach context.

When discussing breach notification, of focus for the FTC were situations when disclosing information to an individual might have "mitigate[d] reasonably foreseeable harm." This stands in contrast to more explicit notification triggers under state breach notice laws. Laws that specifically define what constitutes a "breach" for which notification is necessary. Many of which, though, have exceptions to notification if no harm is likely. The FTC's commentary presents the other analytical side to these state laws' "no harm" exceptions. According to the FTC, even if notification is not legally required under state breach laws, notification may nevertheless be advisable if it might mitigate reasonably foreseeable harm. Or, if failing to disclose would increase affected parties' potential harm.

While the FTC's blog post has garnered attention in the incident response community, the legal basis for its position is not necessarily new. Indeed, the FTC has used the FTC Act for some time to deal with data breaches and data security practices. The FTC pointed to several actions it has filed under tenets of unfairness and deception (i.e., Section 5 of the FTC Act) against companies that suffered data breaches. In those cases, it argued the companies committed unfair or deceptive practices by failing to notify consumers (even if state laws did not require notification), by failing to timely notify consumers, or by issuing inaccurate or inadequate notice communications. This emphasis suggests that the FTC will be scrutinizing not only the timing of any notice made, but also whether breach notice communications contain misleading statements.

Also interesting to note is the FTC's reference to "other relevant parties" in its post. In particular, the FTC suggests companies may now need to think about communicating to more than just *individuals*. Companies may also, the FTC states, need to think about "other relevant parties"—such as third-party businesses—to enable them to mitigate possible harm.

PUTTING IT INTO PRACTICE: This post is a reminder that the FTC may closely scrutinize public statements companies make about data breaches. The FTC is signaling that it will continue to use its authority under Section 5 the FTC Act when it believes (1) notices were not "timely," (2) communications were misleading, or (3) steps have not been taken to "mitigate reasonably foreseeable harm."

Mint Gets Data Breach Claims Dismissed

Posted May 13, 2022

California federal Judge William Alsup dismissed various claims against Mint Mobile LLC based on a data breach that exposed personal information of Mint customers. Plaintiff Daniel Fraser alleged that Mint, a mobile virtual network operator using the T-Mobile network infrastructure, was hit with a data breach in June 2021. According to Fraser, the breach resulted in disclosure of his and others' personal information, including names, addresses, email addresses, phone numbers, account numbers, and passwords.

Fraser alleged that within a few days of the data breach, his phone number was ported out, or switched from one service provider to another. Fraser alleged that less than two hours after the SIM port-out, cryptocurrency drained from his ledger account. Ultimately, he alleges $466,000 in cryptocurrency was stolen from him.

Fraser's allegation that Mint had a role in helping the hacker gain control of his phone number sets this case apart from the typical data breach case. Usually, plaintiffs allege that disclosing their information in a breach resulted in later fraudulent activity or a risk of future fraud against the plaintiff. Often, plaintiffs allege no causal connection between the breach and the fraud.

Fraser alleges that Mint allowed Fraser's number to be ported out because it approved the porting out of his number. In doing so, he alleges Mint bypassed the access PIN Fraser had set up just days before to enhance the security on his account. In Fraser's theory, that would allow the hacker greater access to his accounts, such as the ability to bypass multi-factor authentication. Mint thus allegedly took steps after the breach that helped the hacker complete a fraud using the disclosed information.

Based on this series of events within just a few days of the breach or less, the Court allowed Fraser's negligence and breach of implied-in-fact contract claims past a motion to dismiss.

However, the Court dismissed Fraser's claim under California's Unfair Competition Law. The only available remedy that Fraser sought under the UCL was restitution. The Court held that restitution is unavailable in a situation like this because any stolen money went to a third-party criminal. As is common when data breaches lead to theft by the hacker, the defendant, Mint, acquired no money or other benefit from the alleged fraud. The Court similarly dismissed Fraser's request for punitive damages as to all claims.

The Court held that Fraser's federal claims required damage to a computer system. Fraser only alleged financial loss flowing from the disclosure. The Court dismissed Fraser's federal claims under the Computer Fraud and Abuse Act and Federal Communications Act.

PUTTING IT IN PRACTICE: With data breaches becoming more common, courts are becoming sophisticated at understanding the roles of the different players. Courts are also showing they will closely examine the harm alleged by the plaintiff early in a case. Companies defending against data breach claims may greatly limit the exposure early by asking a court to dismiss claims or remedies where the plaintiff's harm does not logically flow from the defendant's actions.

Arizona Expands Regulator Data Breach Notification Obligations

Posted April 11, 2022

Arizona recently amended its breach notice law to change the regulator notification requirements. Starting this summer, depending on the scope of the incident, the Arizona Department of Homeland Security will need to be notified. Specifically, as amended, if more than 1,000 Arizona individuals are notified of a breach, then notification must be made to the three largest consumer reporting agencies, the Arizona attorney general *and the Arizona Department of Homeland Security*. Previously, only the consumer reporting agencies and Arizona AG needed to be notified if that threshold was met. This notification should be made within 45 days after the determination that there has been a breach. Arizona joins New York as being one of the few states that require notification to multiple state regulatory agencies.

PUTTING IT INTO PRACTICE: Beginning July 22, 2022, companies who suffer a breach impacting more than 1,000 Arizona residents will need to notify the Arizona Department of Homeland Security (in addition to other agencies). This amendment joins the minor change in Indiana that we wrote about previously, which will also go into effect in July.

Indiana Breach Notification Law, Amended, Changed Effective July 1, 2022

Posted April 5, 2022

Indiana has made a minor amendment to its data breach notification law. Starting July 1, companies who are obligated to notify under the law must do so (to affected individuals and the Indiana Attorney General) without unreasonable delay, but *no later* than 45 days after discovery of the breach. This changes the current time frame, which is "without unreasonable delay." Indiana joins many other states that impose a specific timing requirement, in particular no later than 45 days after determining there has been a breach. For example, Alabama, Maryland, Ohio, and Wisconsin (among several others) all require notice to individuals no later than 45 days from discovery.

PUTTING IT INTO PRACTICE: Beginning July 1, 2022, companies who suffer a breach impacting Indiana residents will want to keep in mind this notification timing change.

DATA SECURITY

FTC Action Against Drizly and CEO Provides Insight Into Its Security Expectations

Posted November 3, 2022

The FTC recently took action against the online alcohol marketplace company Drizly and its CEO for alleged security failures. The case arose from a 2018 data breach which was caused – according to the FTC – by poor security measures stemming from the company's alleged failure to devote sufficient resources or attention to data security.

According to the FTC, Drizly stored a variety of personal information in its production database. Included in that information were 2.5 million consumers' passwords hashed using bcrypt encryption, which as the FTC stated was "widely considered insecure." The FTC also indicated in its complaint that the company had not hired anyone to run its information security program. In the context of these findings, the FTC took issue with Drizly's privacy policy which stated, conversely, that "All information we collect is securely stored within our database, and we use standard, industry-wide, commercially reasonable security practices such as 128-bit encryption, firewalls and SSL (Secure Socket Layers)."

As the FTC complaint contends, the security problems began when Drizly hosted a coding competition. As part of the competition, it gave one of its executives access to its GitHub platform, which contained not only source code to support the company site, but also credentials to its production database. After the competition ended, those credentials were not revoked, even though they were meant to be temporary, and the executive ultimately left the company. The credentials were stolen in an unrelated breach and used by the threat actor to access the production database and exfiltrate the consumers' information. Drizly did not discover the exfiltration, and instead learned only through media reports that customers' accounts were being sold on dark web forums. According to the FTC, the company conducted a post-breach analysis which determined that the incident occurred because the company did not have in place a formal security program or hygiene practice.

The FTC alleged in the complaint that Drizly's lack of sufficient security practices coupled with the statements in its privacy policy were both unfair and deceptive in violation of the FTC Act. Among other things, the FTC pointed to the fact that another employee's access to the production database was compromised in a similar fashion on GitHub, which resulted in a threat actor using Drizly's servers to mine cryptocurrency.

The FTC said that Drizly could have likely prevented the 2020 breach by requiring regular review of access permissions, multifactor authentication for all employees with access to code repositories, and scanning of code repositories for unsecured credentials. The FTC order was directed against both the company and its CEO, a co-founder and active in all parts of its management. (One commissioner disagreed with finding him personally responsible.) If the order is made final by the FTC, Drizly and the CEO will be required to:

- Destroy unnecessary consumer personal information;
- Publicly post a retention schedule for personal information;
- Limit the future collection of personal information;
- Implement a comprehensive data security program that includes:
  - multi-factor authentication for databases with consumer data; vulnerability testing of the network and applications every four months; penetration testing the business's network and applications every twelve months; and
- Conduct biennial security assessments for the next twenty years

Putting it into practice: This case highlights several of the FTC's expectations around a company's security measures. These include having someone in charge of information security, having a formal information security program, utilizing multi-factor authentication, and taking action on any

recommendations or remedial areas identified in a post-breach analysis. This case is also a reminder that here, as in many other cases, an FTC consent decree may be issued not just against the company, but its directors or owners as well.

NYDFS's $4.5 Million EyeMed Cyber Settlement Reminder To Industry

Posted November 1, 2022

In a recent settlement with the New York Department of Financial Services, EyeMed Vision Care LLC agreed to pay a $4.5 million penalty and undertake remedial measures to increase its cybersecurity. This includes undertaking an action plan based on a comprehensive risk assessment, subject to the review and approval of NYFSD.

The case stemmed from an October 2020 incident. At that time, a threat actor gained access to an EyeMed email account used by nine employees through a likely phishing attack. The threat actor was then able to view consumer nonpublic information in the email account. NYDFS alleged that EyeMed did not conduct required risk assessments, failed to implement multifactor authentication, and did not have appropriate access controls in place.

The settlement focused on EyeMed's security practices and its failure to conduct required cybersecurity risk assessments as required by the NYDFS Cybersecurity Regulation.

PUTTING IT INTO PRACTICE: This is a reminder for covered entities that the NYDFS Cybersecurity Regulations require companies to conduct periodic risk assessments of information systems and nonpublic information stored on company networks.

White House Aims for Spring 2023 Rollout of Internet of Things Labeling Program

Posted October 28, 2022

The White House recently hosted a group of industry and government partners to discuss the development and implementation of an Internet of Things (IoT) labeling program. This program would develop a common label to help consumers easily recognize which devices meet the highest cybersecurity standards to protect against vulnerabilities.

This program is born out of a requirement in Executive Order 14028, *Improving the Nation's Cybersecurity*, which tasked NIST with developing pilot programs to help educate the public on the security capabilities and vulnerabilities of IoT devices. NIST released guidance for the pilot programs earlier this year that discussed recommendations for an internet of things labeling program (discussed here).

Modeled after the Energy Star labeling program, the IoT labeling program seeks to create an internationally recognized label that will help consumers make informed choices about the security of an Internet-enabled device. While the program is still in development, the label likely will include information about whether the product complies with U.S. government and international security standards; the amount of information collected on consumers; and whether data is encrypted. Because the nature of cybersecurity is fluid, the label will also contain a barcode that consumers can scan to receive the most up-to-date information about the security of that device.

The White House expects to rollout this voluntary labeling program in Spring 2023. The program will start with the most common and most vulnerable devices, to include internet routers and home cameras.

PUTTING IT INTO PRACTICE: IoT device companies should continue monitoring updates to the IoT labeling program and seek to ensure devices are developed with security standards in mind.

CISA Seeking Input on Cyber Incident Reporting for Critical Infrastructure

Posted September 26, 2022

The Cybersecurity and Infrastructure Security Agency (CISA) is seeking input on various aspects of proposed incident reporting regulations under the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (discussed here). CISA issued a Request for Information (RFI) and has scheduled a number of listening sessions across the country. Written comments may be submitted until November 14, 2022.

CISA is particularly interested in input from owners and operators of critical infrastructure entities on the potential impact of the proposed requirements. CISA has provided a non-exhaustive list of topics related to the rulemaking, but of note are the following:

- The definition of "covered entity" including the number of entities, either overall or for a specific industry or sector
- The meaning of "covered cyber incident" and "substantial cyber incident" and in particular how to better align these definitions with other federal incident reporting requirements
- What constitutes a "reasonable belief" that a covered cyber incident has occurred
- The meaning of "ransom payment" and "ransomware attack," and when the timeline for reporting a ransom payment should begin
- Input about information preservation after an incident, including methods, cost, and duration
- The role of third-party entities in submitting covered cyber incident or ransomware reports

Putting it Into Practice: The RFI outlines key terms and considerations relevant to critical infrastructure and provides insight on CISA's general approach to incident response, which may serve as the basis for future requirements applicable to other sectors. This comment period is an opportunity for companies to influence the scope and impact of the final rule. Comments may be submitted through November 14, 2022 at https://www.regulations.gov/document/CISA-2022-0010-0002.

Privacy and Cybersecurity Training Addressing Regulatory Concerns

Posted July 12, 2022

As we pass the half-way mark of 2022, many are reflecting on their privacy compliance progress. One area that seems to be a constant battle is training. How much is needed? What kind of training? What are expectations from regulators around training?

Many privacy and security laws require some form of employee training. Under CCPA, for example, organizations need to train individuals who handle consumer inquiries. Most comprehensive privacy laws (like GDPR) expect training to be a part of ensuring privacy compliance, as do regulators who enforce unfair and deceptive trade practice principles. Canada's privacy law (PIPEDA) requires general privacy training. Under industry-specific laws (GLBA and HIPAA) and certain state insurance law regulations, training is also contemplated. Training has also been recommended as an important compliance step by regulators like the Department of Labor, SEC, OFAC, NYAG, NYDFS, and others.

Training is required under many security laws as well. For example, state security laws (Massachusetts, New York and Oregon) mandate training. In Kansas, having a training protocol, along with other measures, can serve as an affirmative defense in the event of a breach. Industry standards, like NIST and ISO, require a clear training strategy and that role/risk-based training be provided to employees. Finally, in the aftermath of a breach, regulators often point to lack of training (or lack of alleged *effective* training) in assessing fines – or make training part of a settlement decree. (See recent NYAG and FTC settlements).

In the face of these legal imperatives, how can companies most effectively implement a training program? One that can show regulators measurable results and address their concerns? Especially in light of some common, practical, refrains?: "the training is too long;" "the training is too boring, I didn't pay attention;" or the related "I'm too busy, I did the training while I was multitasking." Borrowing from the education field, here are ideas to consider when designing privacy and cybersecurity training:

1. **Make it appropriate**: Training should be substantively relevant to the audience, and the right people and groups need to be trained. These include those who collect and use personal information, as well as those whose activities with respect to that information could put the company at risk. Typically most individuals will need some level of training, but what training it is depends on who they are.
2. **Make the training interactive**: People learn best when they are engaged. It may be harder to develop, but an interactive session will result in more learning than putting people in a room or online lecture for the same amount of time.
3. **Keep it short!**: The people you are training are busy. This is one more "extra" in their day. Think series of "60 second ad spots," and deliver training about one key topic rather than trying to get everything covered in one go.
4. **Know your audience**: Each constituency in your organization is unique. They have their own culture, communication styles, and needs. Think through not just the appropriate substance for your audience, but also how they learns best. What will make the content you need to communicate most digestible for the group?: Group exercises? "Gamification?"
5. **Be planful**: The first four steps will be difficult to implement if you jump in without a plan. Deciding both who to train and *how* to do so effectively requires thoughtful consideration. Spending planning time can make the difference between successful training outcomes and mediocre ones. Another important piece of any plan is prioritizing. Where are the greatest risks? Who are the people whose actions could result in the largest exposure to the company? Tying the planning into an organization's overall goals can make a big difference. Demonstrate how effective training can and will support the organization's goals. Finally, think about measurements when designing your training. How will you measure behavior changes rather than just measuring numbers of people who attend the training? If we want fewer "click throughs" on phishing campaigns, look at click-throughs both before and after the training to demonstrate its effectiveness.

PUTTING IT INTO PRACTICE: With about six months remaining in the year, now is a good time to revisit training efforts. Do you have a comprehensive plan that addresses both statutory requirements as well as regulator expectations? These steps may help putting in place a practical program that addresses your highest areas of risk.

UK ICO and NCSC Issue Caution About Making Ransomware Payments

Posted July 11, 2022

In a recent letter to the UK law society, the UK Information Commissioner's Office and the National Cyber Security Centre have provided lawyers with advice about ransomware payments. The two agencies cautioned lawyers that such payments would not help "protect" the data, mitigate the risk to individuals, or result in a lower ICO penalty in the event of a regulatory investigation. Instead, they stated in a release that accompanied the letter, lawyers "should not advise clients to pay ransomware demands should they fall victim to a cyber-attack."

The agencies reminded lawyers that paying ransoms may instead incentivize threat actors, could impact sanction regimes, and further will not guarantee the decryption of data. This caution about sanctions echoes similar guidance from the US Department of Treasury from late last year. The concerns about ransoms generally echoes advice from the New York State Department of Financial Services.

In this letter, the agencies reminded entities what steps *could* help mitigate risk. These include taking steps to fully understand what has occurred, "learn[ing] from it," and showing that the entity has followed NCSC guidance. Additionally, mitigation includes working with the NCSC "where appropriate." The agencies point to the ICO's ransomware guide, which recommends treating exfiltrated personally identifiable information as "breached" even if a ransom has been paid to avoid its publication.

PUTTING IT INTO PRACTICE: Navigating a ransomware incident can be thorny. This letter is a reminder that paying the ransom will not solve all. When faced with a ransomware demand, take into account these cautions as well as those from other agencies regarding sanctions/prohibitions on ransom payments to criminal organizations. Companies will also still need to make assessments of whether there has been a breach of personal information and address potential resulting notification obligations.

Updated Timeline for DoD's Cybersecurity Certification Program

Posted June 23, 2022

The Department of Defense recently provided some clarity on the timeline for implementation of its Cybersecurity Maturity Model Certification (CMMC) program. The DoD now expects to complete documentation to submit to the Office of Management and Budget for its rulemaking process by July 2022. And, it plans to issue interim final rules by March 2023. If DoD sticks to this new timeline, the CMMC requirements could begin appearing in solicitations for government contracts as early as May 2023 (60 days after the rules are published).

DoD plans to roll out the CMMC requirements in solicitations under a "phased approach." During phase one, when the CMMC requirement first starts appearing in solicitations, all offerors will be required to conduct a self-assessment and provide a positive affirmation of compliance. This stands in contrast to having a third-party certification, which will eventually be required for some contractors under CMMC. In phase two, solicitations will require either self-assessments or third-party certifications. Which approach is required depends on the type of information involved, and the required certification level. The timing of phase two is still to be determined.

DoD also has confirmed that the third-party CMMC certification will be good for three years once the certification is issued (while not required until phase 2, contractors may choose to secure certification early), but contractors will be required to provide an annual affirmation confirming compliance. The third-party certification is for those associated with critical programs and contracts involving information critical to national security. Self-assessments required for contractors not handling information critical to national security will need to be performed on an annual basis. The assessment will need to be accompanied by an associated affirmation by a senior company official.

PUTTING IT INTO PRACTICE: It seems the time finally has come for DoD contractors and suppliers to prepare their information systems for a CMMC assessment, if they have not already. Now is time for DoD contractors to consider (1) comprehensive self-assessments, (2) appropriate remediation, and (3) updating any reported cybersecurity scores to ensure they reflect the current posture of the system.

Cybersecurity Act Signed Into Law Creates New Reporting Obligations

Posted March 29, 2022

President Biden recently signed into law the Cyber Incident Reporting for Critical Infrastructure Act of 2022 as a part of a larger omnibus appropriations bill. The new law sets out mandatory reporting requirements for critical infrastructure entities in the event of certain cyber incidents and ransomware payments. Under the Act, once implementing regulations are issued (which are not expected this year) covered entities will be subject to two new reporting requirements:

- Covered entities must report covered cyber incidents *no later than 72 hours* after the covered entity reasonably believes that an incident has occurred.
- Covered entities that make ransom payments as a result of a ransomware attack against critical infrastructure must report the payment *no later than 24 hours* after payment has been made.

While the general reporting timeframes are clear, the questions of who is impacted by this Act, what incidents must be reported, and what the reporting process requires are decidedly less clear. The Cybersecurity and Infrastructure Security Agency (CISA) will be issuing rules addressing those points. A proposed rule is to be issued within 24 months, and the Director of CISA is to issue a final rule within 18 months of issuance of the proposed rule. As part of the rulemaking, CISA will further define the scope of critical infrastructure entities that are covered. It is hoped that the rulemaking will also include a more clear description of what constitutes a substantial cyber incident. The requirements will not go into effect until CISA issues its rules.

The Act outlines strict enforcement mechanisms to ensure compliance with the Act. If CISA suspects a covered entity has not submitted a required report, CISA will ask the entity to disclose an incident. If the entity does not respond within 72 hours, CISA can subpoena the entity for more information. Failure to comply with the subpoena can result in civil penalties and/or suspension and debarment from federal contracting.

PUTTING IT INTO PRACTICE: Reporting requirements will not be effective immediately, but companies that generally operate in critical infrastructure sectors should review the Act and proposed rulemaking when it is released to determine if they will be subject to the reporting requirements.

Keeping Both Eyes on Cybersecurity

Posted March 22, 2022

The New York State Attorney General's finding that EyeMed Vision Care LLC had failed to protect customer data in violation of the NY SHIELD Act provides insights for companies on how to protect information. New York's SHIELD Act applies, as we have written previously, to any organization owning or licensing the information of a NYS resident, not just organizations located in New York. It requires companies to take reasonable administrative, technical, and physical safeguards to protect collected personal information.

The underlying incident occurred when an attacker gained access to an EyeMed email address for a week, and used it to send 2000 phishing emails to EyeMed clients. During that time, the attacker accessed and had the ability to exfiltrate emails and attachments with customer information from as far back as 2014. EyeMed retained counsel, engaged a reputable forensic cybersecurity firm to assist with their investigation, and offered impacted individuals credit monitoring, fraud consultation, and identify theft restoration.

While the attorney general did not comment on EyeMed's incident response process, the office felt that the company's prior actions -or lack thereof- helped lead to the incident. Of particular concern were the following elements:

- Lack of multi-factor authentication on the compromised web-facing email account.
- Insufficient password management requirements on the account that contain large volumes of customer information (character length only a minimum of eight; six login attempts were allowed before locking the user account).
- Account logs only were available for 90 days.
- Emails stored that had customer information from as far back as 2014.

As a result of the investigation, EyeMed was required to update its internal processes to address these concerns. EyeMed also agreed to pay a $600,000 fine.

PUTTING IT INTO PRACTICE: In keeping with other guidance from New York, the EyeMed settlement shows that the New York AG has very specific expectations of companies' data security measures. These include password strength, logging capabilities, and data storage minimization.

NIST Releases New Guidance on Software Security and Cybersecurity Consumer Labeling Programs

Posted March 14, 2022

NIST recently released several key deliverables relating to cybersecurity. These focus on secure software development and new consumer labeling programs as contemplated by President Biden's Executive Order 14028, which seeks to implement multiple new practices to improve the Nation's cybersecurity.

Software Supply Chain Deliverables:

The security of the software supply chain is of great importance following multiple far-reaching cyber attacks in recent years. To help software developers mitigate the risk of vulnerabilities, NIST released a final version of its Secure Software Development Framework (SSDF) (available here: SP 800-218, Secure Software Development Framework (SSDF)). The SSDF is organized into four groups of high-level practices and tasks:

- Prepare the Organization
- Protect the Software
- Produce Well-Secured Software
- Respond to Vulnerabilities

NIST also published guidance for software acquirers on how to secure proper attestation that a developer has followed required security practices as called for by the Executive Order. The guidance document focuses on best practices for federal agency procurement of software and includes examples of what should be required in a conformance statement. Generally, the government may accept first-party attestation unless a risk-based approach determines second or third-party attestation is required. New federal regulations are expected this year that will memorialize the recommendations in government contracts and subcontracts.

Consumer Labeling Deliverables:

NIST also released two final deliverables addressing recommendations for cybersecurity labeling programs for consumer software and consumer internet of things (IoT) devices. The impetus behind the programs is President Biden's Executive Order, which aims to better educate the public on cybersecurity practices and the security capabilities of products. At present, these programs are meant to be voluntary and are in the very early stages of development. NIST acknowledges that implementation of the programs will require a scheme owner to guide and own the programs.

NIST's documents outline general desired outcomes for a labeling scheme, including three key considerations:

- Baseline Product Criteria
- Labeling Considerations (Single Binary Label)
- Conformity Criteria and Assessment

NIST recommends that labeling be based on baseline product criteria rather than set standards. For software, NIST outlines 15 baseline product criteria ranging from implementation of secure development processes to documenting information regarding software integrity and provenance. For IoT, NIST recommends 10 baseline product criteria

to include extensive documentation of the development lifecycle of an IoT product with a focus on cybersecurity considerations and the origin of product components.

For labeling considerations, NIST recommends a "binary label" that would easily signal to non-expert users that a product has met a baseline standard. Finally, NIST believes that a single conformity assessment approach would not achieve desired objectives and recommends that a scheme owner specifically tailor the assessments to the recommended product.

PUTTING IT INTO PRACTICE: Software producers should familiarize themselves with the SSDF and NIST documents as best practices for development of secure software, while government contractors in this space will want to pay particular attention and adopt NIST's guidance in anticipation of new regulations. Companies that provide IoT devices should stay abreast of developments for consumer labeling and seek to ensure devices are developed with security standards in mind.

NIST Seeks Comments on Cybersecurity Framework Refresh

Posted March 10, 2022

The National Institute of Standards and Technology (NIST) is seeking comments to improve its Cybersecurity Framework, "Framework for Improving Critical Infrastructure Cybersecurity" (Request for Information available here). The Cybersecurity Framework is a key document providing organizations with standards, guidelines, and best practices to manage cybersecurity risk. With many changes to the cybersecurity landscape since the last update to the Cyber Framework in 2018, NIST hopes to address new threats, capabilities, technologies, and resources. Comments are due by April 25, 2022.

In particular, NIST is seeking guidance on whether it should integrate supply chain-related cybersecurity guidance into the Cyber Framework or create a new cyber-related supply chain framework. In addition, NIST seeks public feedback on the following key categories:

- **Functionality of the Current Cyber Framework:** How are organizations using the Framework? What areas need improvement? Should NIST consider structural changes to the Framework? What challenges have organizations had in adopting or using the Framework? What are features of the Framework that can be added, modified, or removed?
- **Alignment with other Resources:** What other NIST and non-NIST resources should the Cyber Framework align with to make the tools more compatible and effective? Examples include: the Privacy Framework, Secure Software Development Framework, Risk Management Framework, Workforce Framework for Cybersecurity, and the Internet of Things Baseline.
- **Integrating the Cyber Supply Chain:** How should the Cyber Framework address supply chain related cybersecurity needs and risks? What practices are organizations using to manage these risks? How should NIST's cyber supply-chain public private partnership, NIICS, be aligned and integrated with the Cyber Framework? Should NIST develop a dedicated framework addressing cybersecurity supply chain risk management?

The comment period closes on **April 25, 2022**, and information on submitting comments can be found here.

PUTTING IT INTO PRACTICE: The NIST Cyber Framework is an important cyber threat management tool for companies looking to develop and secure their data security programs. This comment period is a key opportunity for organizations to improve the Framework and provide important feedback to ensure the Framework reflects actual experience and practice.

NYDFS Issues Cybersecurity Guidance in Response to Events in Ukraine

Posted March 9, 2022

In light of Russia's recent military actions in Ukraine, the New York Department of Financial Services issued guidance on its cybersecurity and virtual currency regulations. The Department is specifically concerned about heightened risk for Russia's cyberattacks against Ukraine, which could in turn lead to retaliatory attacks against U.S. critical infrastructure due to U.S. sanctions against Russia.

The Department clarified that regulated entities should comply with U.S. sanctions on Russia, but should take measures to mitigate potential security risks. The following includes some recommendations to mitigate increased cyber threats:

- Review cybersecurity programs with a particular eye on security hygiene measures, such as multi-factor authentication;
- Review, update and test incident response and business continuity planning;
- Implement practices not already in place in the Department's June 2021 Ransomware Guidance;
- Conduct regular penetration testing to check ability to restore backups; and
- Provide additional cybersecurity awareness trainings and reminders for employees within the organization.

PUTTING IT INTO PRACTICE: Current world events serve as a reminder for why it is important for organizations to prioritize their cybersecurity programs and ensure that they take mitigation efforts to prevent the devastating effects of cyber-attacks.

White House Focuses on Improving the Cybersecurity of National Security Systems

Posted February 15, 2022

President Biden recently signed a National Security Memorandum on cybersecurity. This memorandum was required by an earlier executive order, which we previously have discussed here. The new memorandum (NSM) requires certain network cybersecurity measures for any government information system that is used for highly sensitive national security purposes. The requirements go into effect on a rolling basis over the next 6 months.

Systems covered include those used for intelligence activities, command and control of military forces, or weapons systems (dubbed, "National Security Systems" or "NSS"). Requirements will include use of multifactor authentication, encryption, cloud technologies, and endpoint detection services. Notably, the NSM:

1. requires agencies to identify their National Security Systems and report cyber incidents to the National Security Agency (NSA) (the agency tasked with responsibilities over NSS);
2. authorizes the NSA to create Binding Operational Directives requiring agencies to take specific actions against known or suspected cybersecurity threats and vulnerabilities; and
3. requires agencies to secure cross domain solutions (*i.e.*, tools that transfer data between classified and unclassified systems).

The NSM also outlines how the cybersecurity requirements will be implemented.

PUTTING IT INTO PRACTICE: At this point, the NSM is directed only at requirements for agencies (rather than contractors or vendors). But, as we've seen in the past, once agencies have new policies and processes in place, these requirements are likely to impact or flow-down to contractors that support National Security Systems.

Colorado AG Issues Guidance on Data Security Best Practices

Posted February 14, 2022

The Colorado AG recently issued guidance on practices companies should consider to safeguard consumer data. This guidance was issued in response to companies asking what "reasonable" security means. While noting that the standard is a flexible one and calls for case-by-case determinations, the AG highlighted activities it will weigh when making a decision on whether companies are acting reasonably to safeguard information.

Specifically, the AG noted a few practices as critical when determining whether a company is acting reasonably to safeguard information. These include identifying and managing data (including proper retention practices). The AG also noted having and implementing a written information security policy and incident response plan. The CO AG also placed importance on ensuring that vendors have proper security measures in place.

Altogether, nine practices were highlighted. These include advising companies to:

1. Inventory types of data collected and establish systems to store and manage data.
2. Develop a written information security policy.
3. Adopt a written data incident response plan.
4. Manage vendors' security.
5. Train employees to prevent and respond to cybersecurity incidents.
6. Follow the Department of Law's ransomware guidance
7. Notify affected individuals and the Colorado AG of a breach, as required under law.
8. Protect affected individuals of a data breach from identity theft and harm.
9. Review and update security policies regularly.

This guidance comes in light of the upcoming Colorado Privacy Act (CPA), which we previously covered here. The CO AG also announced rulemaking for the CPA to begin soon, with the adoption of final rules expected by early next year.

PUTTING IT INTO PRACTICE: The CO AG's advice signals the growing expectations of the steps companies should take to protect information. This follows the trend of other state AG's issuing cybersecurity guidance. For example, the New York AG recently issued information on how to protect against credential stuffing attacks.

NYAG Issues Credential Stuffing Guidance

Posted January 26, 2022

The New York AG recently issued information about steps companies can take to protect against credential stuffing attacks, and how to handle them if they occur. The guidance makes up a majority of a larger AG report on credential stuffing.

"Credential stuffing" attackers flood a website with automated login attempts using previously-stolen credentials. These attacks are on the rise, and the amount of activity involved in them can be staggering. One restaurant chain contacted by the AG was the victim of at least 271 million login attempts over a 17-month period. Another suffered at least 40 million in just two months.

Expressing concern over the increase in these attacks, the NYAG lays out four categories of suggestions. They are "lessons learned" from a broader investigation by the Office to identify safeguards that might be effective in protecting

against credential stuffing. These steps are useful for companies to review and serve as a signal of what the NYAG might expect of companies who have suffered an incident. While not all of these steps, the NYAG recognizes, would be appropriate in all circumstances evaluating which would work best can be helpful. They are:

- **Defense**: The NYAG recommends appropriate detection software, as well as CAPTCHA systems to validate logins (recognizing that these are not perfect). Other steps include multifactor authentication, firewalls, and password-less authentication (using an authenticator app or one time code in lieu of a password).
- **Detection**: Monitoring for potential attacks should, it indicated, include automated measures with human oversight. Other detection safeguards are analyzing customer fraud reports and notifying customers of unusual or significant account activity. It also recommends that companies use third-party tools to monitor possible compromises.
- **Preventing Fraud and Customer Data Misuse**: In situations where online payment is involved, the NYAG recommends using re-authentication at the time of purchase. Special care should also be taken when gift cards are accepted, like limiting access to the cards' serial numbers. In payment situations, third-party monitoring tools can be an added defense. Another suggested strategy is anticipating and mitigating attempts at social engineering. And, testing the effectiveness of these strategies through simulations or tabletop exercises.
- **Incident Response**: In the hopefully unlikely event that a credential stuffing attack is successful, and threat actors gain access to accounts, the NYAG indicates that it expects companies will have incident response plans that address "processes for responding to credential stuffing attacks." In its guidance, the NYAG indicates some steps it thinks companies should be taking during the process that are unique to credential stuffing. This includes figuring out if customer accounts were accessed or reasonably likely to have been accessed, swiftly blocking such access (if it has occurred), and giving customers clear notice that *inter alia* tells them which accounts were accessed and when. When appropriate, the report suggests notification may be appropriate before an investigation is over.

PUTTING IT INTO PRACTICE: The NYAG's advice signals its expectations of companies in terms of steps they should take to protect against a credential stuffing attack. We expect more targeted guidance like this as threat actors continue to refine their techniques around specific types of attacks.

EMPLOYEE PRIVACY

Poultry Processors with Department of Justice Over Wage Information Exchanges

Posted September 28, 2022

This summer the US Department of Justice settled with three poultry processors, Cargill Meat Solutions Corp., Sanderson Farms, Inc., and Wayne Farms, LLC. (*U.S. v. Cargill Meat Solutions Corp. et al*, 1:22-cv-01821 (D. Md. 2022)). The antitrust case focused on "long-running conspiracy to exchange information about wages and benefits for poultry processing plant workers and collaborate with their competitors on compensation decisions."

The eyepopping $85 million settlement captured headlines, but this case is more than a cautionary tale about unlawful wage fixing.

Cargill serves as a reminder and a warning for all employers about how to use compensation research or other analyses of employee data. In this case, the processors allegedly shared confidential employee wage and benefit information to make industry-wide decisions about compensation for their workers. They also, according to the DOJ, engaged consulting firms to collect and circulate disaggregated identifiable data, including employee wage information.

While it is common and legal to conduct market research and benchmark compensation, disclosure of employee data could create risk for the employer under a variety of privacy laws. These might include allegations that the information

is being used deceptively or unfairly, actionable under unfair and deceptive trade practice laws. Or, it could result in alleged violations under newer state comprehensive privacy laws. For example, California's CCPA require employers to provide notice to employees at the time of data collection. That notice needs to explain the reason for collection of the data and the scope of use. State privacy laws prohibit employers from collecting data for one stated purpose and using it for another. For example, collecting personal data to process payroll and then sharing it with a third party for industry-wide compensation research.

PUTTING IT INTO PRACTICE: ***Cargill*** **serves as a reminder for employers to properly train their HR team on privacy law requirements and ensuring that privacy notices are an accurate and up-to-date reflection of current practices.**

CCPA May Soon Apply to Employee and B2B Information

Posted August 29, 2022

Companies subject to California's Consumer Privacy Act (CCPA) may soon need to figure out how to scale their privacy compliance programs to include employee and B2B information. The current exemptions that exist for most of the law's requirements to this type of information are set to expire January 1, 2023.

While earlier this year, the California Assembly and Senate introduced several bills that would extend the duration of the current exemptions in CCPA, the window for those bills to pass is quickly narrowing. Two of the bills included AB2871, which proposes to extend the exemptions indefinitely and AB2891, which would extend the exemptions until 2026. According to California's legislative calendar, May 27 was the deadline for bills to be passed out of the house of origin and August 31 is the last day for each house to pass bills. The last day for the governor to sign or veto bills passed by the legislature is September 30. According to the bills' history on the legislative website, neither seems to have passed out of committee or the Assembly (or had any other movement since March).

PUTTING IT INTO PRACTICE: With the clock ticking and no movement on either bill, companies should begin thinking about what it would mean to expand current CCPA compliance efforts to employee and B2B information. In particular, companies will want to consider how rights requests would be handled and what potential exceptions to requests could apply.

Silver Lining in New York City? New Requirements For Using A.I. in Employment Decisions

Posted January 25, 2022

Artificial Intelligence is here to stay and New York City has enacted legal guidelines for employers who use it. NYC's Automated Employment Decision Tools (AEDT) law will, effective January 1, 2023, set new standards for employers using AI tools in making employment decisions.

While it is likely the AEDT will lead to an uptick in litigation, it provides some much needed clarity for AI developers and auditors. It also provides guidance to employers who want to use AI to help eliminate workplace bias. Under the AEDT, NYC employers who use AI must implement the following processes or face civil penalties:

1. Provide notice to applicants and employees of: (a) the use of A.I. in the assessment for hire or promotion; (b) the job qualifications and characteristics assessed by the A.I. tool; and (c) the data that will be collected.
2. The A.I. used to make employment decisions must: (a) clear a "bias audit;" and (b) a summary of the bias audit results must be publicly available. The bias audit must be conducted by a third-party auditor and designed to ensure that A.I. used for employment decision-making does not make biased decisions that violate antidiscrimination laws.

A silver lining? The AEDT may provide -much needed- guidance for AI developers, auditors, and employers by setting standards for AI used to make employment decisions. Also, it is anticipated that the AEDT will provide compliant employers ammunition to defend against legal challenges to their use of AI and related discrimination claims.

PUTTING IT INTO PRACTICE: NYC Employers have until January 1, 2023 to implement audited AI, and prepare or revise existing applicant and employee data collection and privacy notices. Employers who use AI, or intend to, will want to take steps now to prepare for compliance.

EU PRIVACY

EU Regulators to Take Closer Look at DPO Position

Posted September 26, 2022

The EDPB recently announced its second topic for coordinated enforcement. At a national level, data protection authorities in the EU will be looking into the position of the data protection officer. The results of these national actions are analyzed and bundled, generating deeper insights into a particular topic. Last year, the EDPB had selected the use of cloud-based services by the public sector for its first coordinated enforcement action. So, this second topic will be of more relevance to a wider set of organizations. Given that the report on the outcome of the 2022 coordinated action is expected to be adopted before the end of the year, companies can expect a report on the DPO position sometime in 2023.

PUTTING IT INTO PRACTICE: Companies subject to GDPR, whether US-based or operating in the EU, are reminded of the requirement to appoint a DPO where certain thresholds are met under Article 37. There are many factors to consider when selecting an individual for this position, including whether the individual may have a conflict of interest and the relevant expertise. The EDPB's guidelines provide some insights on these points. The Berlin Commissioner recently issued at 525,000 euro fine to a company for violation of the DPO requirements, signaling that this topic may be of increasing interest to EU regulators.

Deadlines for EU and UK Standard Contractual Clauses Approaching

Posted September 14, 2022

Companies transferring personal data out of the EU or UK are reminded of key deadlines approaching for the contracts that govern these transfers. When the European Commission adopted the new Standard Contractual Clauses (SCCs) in 2021, it set a deadline of December 27, 2022 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.

Post-Brexit, the new EU SCCs are not a valid transfer mechanism under the UK GDPR. In February of this year, the UK ICO adopted an international data transfer addendum to the EU SCCs (the UK Addendum) and a standalone international data transfer agreement (IDTA). As of September 21, 2022, all new agreements that govern the transfer of personal data out of the UK must use either the UK Addendum alongside the new EU SCCs, or the IDTA. Existing agreements for transfers are valid until March 21, 2024. At that time, any existing agreements must be replaced with either the IDTA or the UK Addendum.

PUTTING IT INTO PRACTICE: Companies should inventory all data transfers out of the EU and UK and access the status of the data transfer clauses in those contracts. In some instances, companies may find that some vendors have unilaterally updated agreements for data transfers. Nonetheless, companies will want to note which agreements have been updated or not, and take steps to update the ones that are not. Both controllers and processors of personal data should look to update all form agreements to account for these requirements.

Interactive Advertising Bureau of Europe Fined by Belgian DPA for GDPR Violation

Posted February 24, 2022

The Belgian Data Protection Authority (APD) recently released a draft decision imposing a €250,000 fine ($285,000) on the provider of a consent mechanism that operates within a real-time ad bidding program. The ad bidding program, OpenRTB, allows advertisers to place online ads through an automated online auction of available ad space. Thousands of advertisers can bid on space in real time, through a fairly complex process involving many different entities (a schematic of the process was included by the ADP in its decision on page 9). The case first arose in 2019, and after several interim decisions the ADP has now held in this draft decision, among other things, a two month deadline for IAB Europe to present a remediation plan to the ADP. The case was one with cross-Europe impact, and thus the ADP's decision has been sent to its European counterparts for feedback.

The subject matter of the case was IAB Europe's "Transparency and Consent Framework" (TCF). TCF was designed to provide consumers control over the targeted ads they are served through the OpenRTB process. Under TCF, the first time a user visits a website with targeted ads served through OpenRTB, the user sees a pop-up that asks for consent. This includes asking if information can be shared with third parties, and consent for ad tech vendors' processing of information. The IAB then stores and shares these consent preferences with companies that participate in their program.

The APD ruled that IAB Europe's Transparency and Consent Framework did not meet the lawfulness, transparency, and accountability provisions of the GDPR. The ADP found, among other things, that users didn't truly understand what they were agreeing to. Thus, that the consent was not clear. Providing clear consent was the responsibility of IAB Europe, the ADP held, since it was the "controller" of the information. (That finding, of being the "controller" is something IAB Europe has disagreed with.) Included in the sanctions imposed on IAB Europe was strict vetting of companies participating in the program to make sure that they complied with GDPR. The APD decision gives IAB Europe two months to present an action plan to remedy the violations and bring TCF into compliance with GDPR. IAB Europe has since stressed that TCF has not been prohibited, but that it will need "additional functionality." The European data protection authorities to whom the draft has been sent have until early March to provide their input.

PUTTING IT INTO PRACTICE: We anticipate that the TCF program will be changing soon. While we wait, publishers and vendors who rely on the TCF may need to "adapt" their use of TCF (as noted by IAB Europe). IAB Europe has provided a list of FAQs for those companies who rely on TCF which may be useful, and we will continue to monitor for developments.

CNIL Recommends Using US Analytics Tools Only for Anonymous Statistical Data

Posted February 22, 2022

Following a similar case from Austria, the French data protection authority recently concluded that certain use of cookies placed by US data analytics tools violated GDPR. The case came before the CNIL as the result of a complaint filed by "None of Your Business," the non-governmental organization created by Max Schrems.

The complaint argued, and the CNIL agreed, that because of the way Google Analytics was implemented, there were not sufficient supplemental protection measures in place when transferring personal data to the US. Although Google had adopted additional measures, the CNIL concluded these measures could not prevent US intelligence services from accessing the personal data and are therefore insufficient. The website operator in question has one month to comply. Supplemental measures may be needed if a company is relying on standard contractual clauses as a basis for transferring personal data to the US. The EDPB has provided direction on what those measures might look like.

Following the earlier Austrian decision, Google indicated that to address the EDPB's direction on "supplemental security measures" it had several security features that companies could put in place when configuring Google Analytics. They also disagreed with the EU DPAs conclusions that US law enforcement would likely gain access to EU individuals' information. This French decision suggests that other EU DPAs may also disagree with Google's current position.

PUTTING IT INTO PRACTICE: The CNIL recommends that companies use Google Analytics with anonymous data, thus avoiding the transfer of personal information to the US (and taking the activity outside the scope of GDPR). CNIL has also indicated that it will be providing more direction on how to use these tools when transferring personal data to the US and directed companies to its September 2021 recommendations regarding use of cookies. We will continue to monitor developments here.

FINANCIAL PRIVACY

CFPB Sues Payment Platform Over Dark Patterns

Posted October 27, 2022

On October 18, the CFPB sued a software company for utilizing their online payment platform to enroll unknowing consumers into annual subscriptions through deceptive acts and "dark pattern" techniques in violation of the CFPA and EFTA. Among other things, the complaint alleges that the company encouraged consumers to unknowingly enroll in free trials and converted the free trials into annual subscriptions through a "negative option" renewal policy (our sister blog covered "negative option" marketing in a previous post here). During this process, the company allegedly collected consumers' registration information and consumer payments data (e.g., credit or debit card number) so that it could transmit the consumer payments data through its payments systems.

CFPB's complaint alleges that during that registration and payment process, after the consumer has entered their payment information, the software company inserts a webpage with a button labeled "accept," which enrolls consumers in their annual subscription, a discount membership club. However, the complaint alleges that many consumers click on the accept button, believing it is related to accepting the charges for the event, and erroneously enroll in the annual subscription.

According to a statement by CFPB Director Rohit Chopra, the Bureau is "closely watching whether financial services firms are deploying digital dark patterns," and is "looking at a range of ways to reduce unwanted junk fees." He also added that the CFPB is "working to ensure our payments system is working safely and fairly" and that it "will continue to look at how payment platforms extract data and fees from their users."

PUTTING IT INTO PRACTICE: This suit illustrates the CFPB's continued efforts to monitor and eliminate the utilization of digital dark patterns. As evidenced, third party vendors and payment platforms should refrain from using deceptive acts and dark patterns to take advantage of consumers.

CFPB: Safeguard Consumer Data or Face Liabilty

Posted August 23, 2022

The CFPB recently published a circular clarifying liability under consumer financial protection law for financial companies that fail to safeguard consumer data. The circular describes how firms may be violating the CFPA's prohibition on unfair acts or practices with respect to the handling of consumer data by not implementing adequate measures to protect against data security incidents. According to the CFPB. in the event of large scale, customer-base-wide breaches, consumers may become victims of targeted identify theft.

The CFPB outlines several data security measures and practices which, if not implemented, may increase or trigger liability:

- Multi-factor authentication that reduces the possibility of compromised user accounts and unauthorized access to sensitive customer information.

- Adequate password management to monitor for breaches where employees or others may be re-using usernames and passwords.
- Timely software updates to address known vulnerabilities once a software vendor or creator sends out a patch or announces an update.

PUTTING IT INTO PRACTICE: The measures in the circular are not new to banks and other financial institutions subject to the Gramm-Leach-Bliley Act. For companies under the CFPB's authority, in particular, it's worth noting that the agency continues to use its enforcement authority to set new standards for finance companies – this time for insufficient data protection or information security (our sister blog discussed a similar trend in previous blog posts here and here). To help minimize the risk of an unfairness violation, financial companies and their vendors should ensure that they implement and routinely test robust security measures.

US, UK Collaborate on Prize Challenges for Privacy-Enhancing Technologies

Posted June 24, 2022

On June 13, US and UK governments announced that they are developing prize challenges focused on advancing the maturity of privacy-enhancing technologies (PETs) to combat financial crime. The announcements highlight that up to $2 trillion of cross-border money laundering takes place each year. The White House explained that PETs could address financial crime through maturing technologies, which allows machine learning models to be trained on high quality datasets, without the data leaving safe environments. PETs also facilitate privacy-preserving financial information sharing and collaborative analytics; allowing suspicious types of behavior to be identified without compromising the privacy of individuals, or requiring the transfer of data between institutions or across borders.

The prize challenges will allow innovators to develop state-of-the-art privacy-preserving solutions to help combat barriers to the wider use of these technologies without the uncertainty of potential regulatory implications. Innovators will be able to engage with regulators, including the U.K.'s Financial Conduct Authority and Information Commissioner's Office, and the U.S. Financial Crimes Enforcement Network (FinCEN). Challenge solutions will be showcased in the second Summit for Democracy, to be convened by President Joe Biden, in early 2023.

PUTTING IT INTO PRACTICE: PETs present an important opportunity to harness the power of data in a manner that protects privacy and intellectual property, enabling cross-border and cross-sector collaboration to solve shared challenges.

Senate Banking Committee Sends Letter to Yellen on Collection, Use of Consumer Data

Posted June 21, 2022

On June 7, Sen. Sherrod Brown (D-OH), Chair of the Senate Committee on Banking, Housing, and Urban Affairs, sent a letter to Treasury Secretary Janet Yellen to request a review by the Financial Stability Oversight Council of financial institutions' consumer data activities and their potential threat to U.S. financial stability and security. The letter raised concerns that this information may be sold to third-party purchasers or data brokers who compile it with personal data collected from other sources often associated with advertising and exploited for other uses. The Committee also raised concerns that such data could be used for nefarious purposes including "glean[ing] consumers' tolerance for price hikes, or using certain people's spending patterns to target them for blackmail or ransomware."

PUTTING IT INTO PRACTICE: Consumer data activities will surely be a large focus of Wall Street oversight hearings slated for September where a number of large and regional banks will testify before the Committee. As Capitol Hill spotlights these issues, companies should use this as a reminder to conduct data inventories to assess whether they collect or disclose data sets that are subject to any federal and state regulations.

Kentucky and Maryland Enact Insurance Data Security Laws

Posted May 27, 2022

In April, Kentucky (HB 474) and Maryland (SB 207) adopted insurance data security legislation based on the National Association of Insurance Commissioners (NAIC) model law. A total of 15 states have adopted the NAIC Model Law. We previously discussed the requirements of the model law in our insurance certifications round-up, including its recent adoption by other states. Among other things, the model law further calls for insurers to quickly report and investigate data breaches and certify their compliance efforts annually with security provisions.

Maryland's law takes effect on October 1, 2022 and Kentucky's law goes into effect on January 1, 2023. Both states have a one-year grace period with respect to the requirement to establish a written information security program and a two-year grace period for compliance with relevant service provider oversight requirements.

PUTTING IT INTO PRACTICE: As more states look to adopt the model law, insurers should evaluate their in-house security programs, and monitor developments in states that have yet to pass similar laws.

On the Clock: Cyber Incidents Notification Deadline Approaching for Banks

Posted April 19, 2022

The May 1 change to banks' cyber-notification process is fast approaching. As we wrote previously the OCC, FDIC, and Federal Reserve Board implemented a final rule under which banks and their service providers must notify their primary federal regulators within 36 hours of certain incidents. A notification incident that triggers this requirement is defined as a computer security incident that materially disrupts a banking organization's operations or lines of business. Thus not all incidents will meet these levels. For those that do, banks will need to be prepared. Part of that is having the right points of contact, which include:

- **OCC:** BankNet home page; BankNet Help Desk: Email: BankNet@occ.treas.gov; Phone: (800) 641-5925.
- **FDIC:** FDIC case managers of FDIC-supervised banks or if unavailable, by email at incident@fdic.gov.
- **Federal Reserve:** Contact by email incident@frb.gov or telephone (866) 364-0096.

PUTTING IT INTO PRACTICE: Before May 1, banks will want to make sure they have processes in place to identify and address "notification incidents." Part of the process updates can be adding the correct points of contact to their standing incident plans.

FTC Fines Lead Generation Company $1.5M Citing Misuse of Consumer Financial Data

Posted January 24, 2022

A California-based lead generation company recently settled with the FTC for $1.5 million over alleged privacy violations. The FTC argued that the company deceptively acquired consumer personal information and improperly shared this information with various entities under the guise of connecting consumers with lenders. Information in question included Social Security numbers and bank account information.

As covered in our sister blog, according to the complaint, the company operates hundreds of websites encouraging consumers to complete online loan applications. It represented that it would send those applications *only* to a "trusted network of lenders." The company made many representations about the limits of its sharing. Despite these promises, the FTC alleged, the company sold consumers' information to non-lender marketers, debit card sellers, debt negotiation and credit repair services. This sharing constituted deception under Section 5 of the FTC Act.

The company also failed to impose use restrictions on the information sold and, in many instances, was not aware of the purposes for which companies were purchasing the consumers' information. These acts constituted unfair

practices under Section 5. The FTC's complaint also alleged that the company unlawfully obtained and resold the credit scores of consumers in violation of the Fair Credit Reporting Act.

PUTTING IT INTO PRACTICE: This case highlights the FTC's ongoing focus on ensuring companies are following their stated practices, especially when it involves sharing sensitive information with third parties.

CFPB's Latest Orders Place Data Practices Front and Center for 2022

Posted January 5, 2022

Last month, the CFPB utilized its market monitoring authority to issue a series of orders to five companies offering "buy now, pay later" credit. Buy now, pay later, or BNPL, is a deferred payment option that allows consumers to split a purchase into smaller installments, typically four or less, often with a down payment of 25 percent due at checkout.

As we detail in our sister blog here, the CFPB is seeking information on the risks and benefits of these "fast-growing" products over concerns about, among other things, data harvesting and data monetization in a consumer credit market already quickly changing with technology. The CFPB provided to the public an example of the order issued to these companies. The order has 20 requests for information and data on several topics. Two key areas are discussed below.

Data Harvesting: The CFPB seeks data that the companies collect and retain as a result of BNPL product usage, the type of data that is generated from BNPL product usage, and the purpose associated with harvesting different data fields. The information sought relates to "Direct Product Data" and "Indirect Product Data" and the kinds of data that the companies generate from this data. "Direct Product Data" means data collected (and maintained) as a result of consumer's use of BNPL. "Indirect Product Data" is data that is both (1) generated, at least in part from Direct BNPL Data, and (2) about individual users of BNPL.

Data Monetization: The CFPB is also seeking information about how BNPL use data or data generated from BNPL data is used in connection with developing, selling, or marketing BNPL products or other products or services. The CFPB is also looking to understand third-party data sharing and related revenues, and use of BNPL use data or data generated from BNPL use data to sell advertising or targeted offers.

PUTTING IT INTO PRACTICE: While this is the CFPB's first salvo directed at BNPL companies, all businesses should take this action as a prompt to conduct data inventories to assess whether they collect or disclose data sets that are subject to any federal and state regulations. As part of the action items for 2022, companies would be well served to also thoroughly analyze who is receiving their data and how the relationship is characterized, including for online marketing and analytics purposes.

HEALTHCARE PRIVACY

FTC and Other Regulators Continue to Signal Interest in Mobile Health Apps

Posted December 8, 2022

The FTC is closing out 2022 with additional guidance for mobile health app developers signaling its continued interest in this industry. Since 2021, we have seen several steps from the agency demonstrating a focus on companies that collect health information but may not be a covered entity or business associate under HIPAA. This includes publishing additional resources, releasing commentary broadly interpreting the FTC's Health Breach Notification Rule, and enforcement activity. Most recently, the FTC and other key regulators updated its "Mobile Health App Interactive Tool".

Companies may use this tool to evaluate whether their mobile health app falls triggers HIPAA, the FTC Act, the Food Drug and Cosmetic Act (FD&C Act), the 21st Century Cures Act and ONC Information Blocking Regulations, the FTC's Health Breach Notification Rule, and COPPA. Previously, the tool largely focused on applicability of HIPAA, the FTC Act, and the FD&C Act. This resource, which has existed for several years, includes new questions and considerations. The questions posed in the tool also contemplate more specific examples and use cases than before.

PUTTING IT INTO PRACTICE: Companies collecting health information are reminded of the myriad of laws (both federal and state) that may apply. The updated mobile health interactive tool can be used by organizations as an initial starting point in evaluating potential laws. Given emerging new laws (like the Information Blocking Regulations) and the broad interpretation of existing laws (like the FTC Health Breach Notification Rule) now is a good time for companies to re-access whether they are complying with all relevant laws. These additional resources also signal that the FTC is likely to have increased expectations of companies in the forthcoming year. Companies are also reminded of forthcoming state comprehensive privacy laws – several of which introduce concepts around the collecting of "sensitive" information. Both California and Virginia's laws, coming into effect January 1, 2023, have requirements for collecting sensitive (or health) information if no exceptions apply.

FTC Continues to Signal Interest in Digital Health Industry, Publishing Updated Resources

Posted March 15, 2022

The FTC recently published two new resources for complying with the Health Breach Notification Rule. The Rule requires vendors of personal health records (PHR), PHR-related entities and service providers to these entities, to notify consumers and the FTC (and, in some cases, the media) in the event of a breach of unsecured identifiable health information. The guidance reaffirms and adds further clarity to the Agency's broad interpretation of the Rule released in its policy statement last fall.

The shorter guidance largely provides a high level overview of the Rule. The second, lengthier guidance provides more detail about applicability of the rule, what triggers notification, and notification requirements in the event of a breach. It also provides answers to questions asked about the Rule. This new guidance confirms the FTC's position that breaches are not limited to just cybersecurity intrusions. It also includes incidents of unauthorized access, including sharing of covered information without authorization. A settlement from last year with a popular fertility tracking app demonstrates how broadly the FTC may interpret such "sharing." The guidance also clarifies that the Rule preempts contradictory state breach notification laws. But, it does not preempt state laws that impose additional, non-contradictory breach notification requirements.

PUTTING IT INTO PRACTICE: Health and wellness apps and wearables that sit outside of HIPAA are reminded of other requirements they may have from the FTC. This includes considerations under unfair and deceptive trade practice laws (Section 5) as well as the Health Breach Notification Rule. In light of the broad interpretation of "breach" under this Rule, companies should consider auditing all instances of "sharing" of health information. Companies in this space are also reminded of potential obligations under upcoming state privacy laws (California, Colorado, and Virginia).

States Catch Health Care Entities Taking the Bait in Phishing Attacks

Posted February 25, 2022

The State Attorneys General in New York and New Jersey recently settled with four companies over alleged HIPAA noncompliance following phishing attacks. The New Jersey settlements were brought against three NJ-based cancer care providers after a phishing attack on several employees' email accounts. That attack resulted in the unauthorized access of the PHI of 105,200 patients. Although the providers had implemented safeguards, the NJAG concluded that those measures were insufficient to protect against reasonably anticipated threats. In particular, the NJAG was concerned that an accurate and thorough risk assessment had not been conducted, nor was there sufficient employee training. As part of the settlement, the providers agreed to pay $425,000.

The NYAG announced a similar enforcement recently following a phishing attack of an employee email account that compromised the PHI of approximately 2.1 million individuals. That action resulted in a $600,000 settlement with a provider of vision benefits that the NYAG determined had failed to implement sufficient security measures. In particular, the NYAG was concerned that the provider did not have multifactor authentication for the affected e-mail account or sufficient password management protocols. Also of concern was the lack of email account logging, which made investigations difficult.

PUTTING IT INTO PRACTICE: These cases illustrate that state attorneys general are using HIPAA, along with other state laws, as tools in their data breach investigation arsenal. Companies will want to take heed of these cases, as well as advice coming directly from state AGs (such as the NY recommendations we described recently). Measures to keep in mind include MFA, logging, HIPAA risk analyses, and appropriate workforce training.

Digital Health Trends and Privacy; What to Watch in 2022

Posted February 4, 2022

The digital health sector has been rapidly growing, and the demand is not expected to diminish. Those in the industry will want to keep in mind some key legal concerns in the coming year, which we outline in this recent article. Privacy and cybersecurity features among these, and include more than just HIPAA concerns. There is an ever-growing patchwork of state and federal privacy laws that are being applied to the industry. At the same time, cyber threat actors are finding ways to attack even the most prepared companies in the digital health space.

PUTTING IT INTO PRACTICE: Our recent article outlines risks companies may face in 2022, and can serve as a helpful tool as companies prepare their privacy and compliance programs for the coming months.

US GENERAL PRIVACY LAWS

New Draft Regulations for Colorado's Privacy Law

Posted December 28, 2022

The Colorado Attorney General recently released the second set of draft regulations to the Colorado Privacy Act (CPA). In this draft, the AG is seeking specific input on five different topics. There are also a number of changes to the first draft – some of which will be welcomed by businesses. Companies are reminded that the CPA goes into effect July 1, 2023.

Topics for Comment

In soliciting additional comments to the revised CPA regulations, the Colorado AG is seeking specific input on: (1) clarifications to definitions; (2) use of IP addresses to verify consumer requests; (3) a universal opt-out mechanism; (4) streamlining the privacy policy requirements; and (5) bona fide loyalty programs.

Overview of Some Notable Changes

- **Definitions**. There are new and revised definitions. For example, there is a new definition for "employee" and "employment records." There is also an update to the definition of "biometric identifiers."
- **Notice**. This draft removes the requirement that privacy notices be purpose-based. Instead, the processing purpose and type of personal data processed must be linked in a way that gives consumers a meaningful understanding of how their personal data will be used. The previous draft's "purposed based" requirement

differed from requirements in other states and would have made simultaneous compliance difficult. This draft also includes further detail on the "substantive or material" changes to processing that will trigger a requirement to update privacy notices.

- **Universal Opt-out Mechanism**. The Colorado AG has moved up the date for publishing its initial list of approved opt-out providers from April 2024 to January 2024. Under this draft, businesses would have six months from the date an opt-out signal/provider is recognized by the AG to begin complying with that new signal or provider.
- **Security Measures**. There are more detail about the obligations to safeguard personal data. For example, organizations will be required to consider "[a]pplicable industry standards and frameworks" when identifying reasonable and appropriate safeguards.
- **Consent**. The original draft regulations introduced the concept that businesses might have to refresh consumer consent on regular intervals but largely left to a business' discretion what that interval should be. The new draft regulations now provide that consents must be refreshed when the consumer has not interacted with the controller in the last 12 months, and (i) the controller is processing sensitive personal information or (ii) is processing personal data for a secondary data use that involves profiling for a decision that could have a significant effect on the consumer. The draft includes a safe harbor of sorts to the extent consumers have the ability to update their own opt-out preferences at any time, then there is no need to refresh consent.
- **Data Protection Assessment Requirements.** The most recent changes reduce the substance of what must be in data protection assessments.

Stakeholders have until January 18, 2023 to submit comments to this draft. A rulemaking hearing is set for February 1, 2023. It is anticipated that the final draft will be published in advance of when the law takes effect in July 2023.

PUTTING IT INTO PRACTICE: Companies working now to make updates for the forthcoming changes in California and Virginia on January 1 may want to consider what aspects are also addressing Colorado requirements.

How To Handle CPRA Regulations Delay

Posted December 21, 2022

As many are aware, the CPRA regulations are currently in draft status and may continue in that state until April, despite the law's January 1 effective date. This could result in regulations being in final form after the July 1 date that the California Privacy Protection Agency (CPPPA) has signaled that it will begin enforcement. Last week, during a Dec. 16 CPPA board meeting, the agency's executive director indicated that the final rules will likely be released at the end of January. Although there will then be a comment period, the director indicated that the agency does not currently anticipate making further revisions to the draft regulations.

As anticipated, then, under the revised timeline from the CPPA, the final regulations would take effect in approximately April 2023, three months before enforcement of those same regulations will begin. The agency has not indicated any planned delay to the July enforcement time frame, even though the law gives it the discretion to do so. Given the law's upcoming effective date companies should move forward with implementation, following the current draft regulations. While there may be some minor modifications in January, companies can take heart that the CPPA doesn't currently anticipate them being significant.

During the same meeting, the CPPA signaled that it is moving forward with additional rulemaking on risk assessments, cybersecurity audits, and automatic decision making. Draft questions for seeking public comments were introduced, which questions will be finalized at a later meeting.

PUTTING IT INTO PRACTICE: This most recent news from the CPPA should not impact companies' current implementation activities. At this stage, companies should continue implementing the regulations as currently drafted and accept the risk that more revisions could occur.

UK Reprimands Companies For Failing to Keep Up with Access Requests

Posted October 26, 2022

The ICO, Britain's privacy authority, recently issued reprimands to seven organizations citing multiple failures of the organizations to respond to data subject access requests either within the statutory time frame or at all. Recognized as one of the fundamental rights under numerous data protection laws, data or subject access requests ("DSARs") provide a mechanism by which a consumer can request that an organization explain what personal information it has about that consumer, and how such information is used and shared. This requirement exists under UK GDPR, mirroring the GDPR requirement.

Organizations generally have thirty to forty-five days to respond to a DSAR. That time period may be extended under certain circumstances. The ICO has increased its focus on DSAR violations. One of the cited organizations, Virgin Media, received over 9500 SARs over a six-month period in 2021, but according to the ICO, failed to respond to 14% of them during the statutory timeframe.

The ICO emphasized its continuing expectation that DSARs be handled appropriately and in a timely fashion in order to "encourage[s] public trust and confidence and ensure[s] organizations stay on the right side of the law."

PUTTING IT INTO PRACTICE: These cases are a good reminder to process DSARs in a timely manner, as those with access request rights will be expanding in the near future. For those entities who receive significant numbers of requests, having a streamlined process in place will help review and respond to requests.

IAB Steps In State Signal Morass

Posted October 25, 2022

Companies who participate in the AdTech and digital advertising eco-system are very familiar with the Interactive Advertising Bureau and its form advertiser agreements. Those agreements can help streamline negotiations, presenting the parties with, essentially, a pre-negotiated approach to common issues. When CCPA was passed, IAB updated its form to address that law and address consumer notice and consent. With the upcoming laws in California, Colorado, Connecticut, Utah and Vermont, the document is now outdated.

The IAB has thus updated its Multi-State Privacy Agreement (MSPA) and proposed what it is calling "US State Signals." Signatories to the MSPA will need to respect those signals. The signals are intended to be used in conjunction with the IAB's Global Privacy Platform (GPP), a protocol that is intended to support consumer rights within the AdTech infrastructure. The two allow users' preferences to be communicated between advertisers, publishers and vendors. There are separate signals for each state, and cover sale, sharing, sensitive data, and other items as may be required under the relevant laws. These updates are timely as California, Colorado and Connecticut all require following "universal opt-out signals" and the IAB process might be a tool for respecting those signals. (For more about the status of state opt-out signals see our earlier article.

IAB is accepting comments to its draft US State Signals and update to the Multi-State Privacy Agreement until October 27.

PUTTING IT INTO PRACTICE: As a reminder, the requirement for following universal opt-out signals is required first in California (2023), then in Colorado (July 2024), and finally Connecticut (January 2025). Until then, we anticipate seeing various technological approaches proposed for respecting consumers' choices. AdTech companies will want to keep in mind that of the IAB, especially if they are asked to sign the MSPA.

Comparing and Contrasting the Opt Out Preference Signal Across States

Posted October 24, 2022

The talk of "opt-out preference signals" or global privacy controls (GPC) has been increasing as companies dig into the forthcoming requirements under US "comprehensive" privacy laws. What is an opt-out preference signal? An "opt-out preference signal" also known colloquially as "GPC," is a signal sent by a platform or technology on behalf of a consumer that communicates the consumer's choice to opt out of sale or sharing. Below, we summarize how each of the states treats this requirement.

- **California**. While the current version of CCPA does not statutorily require business to recognize opt-out preference signals, the regulations do contemplate such a thing. The current regulations state that companies must honor GPC as a valid opt-out request. However, CPRA (which amends CCPA and comes into effect January 1, 2023) does address GPC in the statute and more specifically in the regulations. Under the current draft version of the regulations, even where a business posts a "Do Not Sell My Personal Information" link, it *must* still process opt-out preference signals. 11 CCR 7025(e). The regulations should be consulted for more specifics around the requirements for implementing this mechanism.
- **Colorado**. Colorado's law similarly contemplates a universal opt-out mechanism. From July 1, 2023 (when the law goes into effect), until July 1, 2024, companies *may*, but are not required to, recognize the mechanism as a way for consumers to opt out of targeted advertising or sales. By July 1, 2024, companies will be required to honor this mechanism. Part 5 of the recently published regulations provide more technical details about implementing this requirement.
- **Connecticut**. There is also universal opt-out mechanism requirement in Connecticut's law. This law, which goes into effect July 1, 2023, allows companies to delay compliance with the opt-out mechanism obligations until January 1, 2025. By that date, companies will need to allow consumers to opt out of targeted advertising or sales of their data via the mechanism. Interestingly, the statute says that the mechanism should be as consistent as possible with any other similar platform, technology or mechanism required by any federal or state law or regulation." The requirements in Connecticut for this obligation are otherwise brief compared what is outlined in California and Colorado's regulations.
- **Utah and Virginia**. The *current* draft of these states do not seem to contemplate any obligation to honor a universal opt-out mechanism or signal. That said, presumably both laws could be amended to add such a requirement in the future.

PUTTING IT INTO PRACTICE: As companies look to third party tools and technologies to implement the opt-out mechanism requirement, California and Colorado's obligations should be closely reviewed. The earliest timeline for implementing will be for California consumers (January 1, 2023). Given that regulations are not currently contemplated in Connecticut, companies may choose to look to California and Colorado for guidance on how to implement this obligation there.

State Comprehensive Privacy Laws: Status of the Regulations

Posted October 20, 2022

With 2023 quickly approaching, many are spending this final quarter preparing for the five US state "comprehensive" privacy laws. Some of these contemplate clarifying regulations with technical and operational requirements. Requirements that will impact preparation activities.

Earlier this year we provided steps companies can take to get prepared in the absence of full clarity. The hope was that regulatory clarity would have been issued by now. Since it has not, many find themselves needing to prioritize or reshuffle their plans. As we get closer to January 1, keeping track of status can help. Below we thus summarize the current status of regulations (if any) across the states:

1. **California**. California released a first draft of regulations in June of this year (along with an Initial Statement of Reasons). Over 1,000 pages of written comments were submitted during the comment period. On October 17, 2022 the CPPA issued modified proposed regulations and explanations for the changes. The timeline for finalizing these regulations remains unclear. It is important to note that these are still draft and partial regulations. That said, given the complexity of these regulations, companies will need to use them in their evaluation of what steps to take in the coming weeks. This is particularly true for those with "do not sell or share" obligations.
2. **Colorado**. Colorado recently published its first draft of proposed regulations. The Office of the Attorney General will hold a public hearing on February 1, 2023. Once the hearing ends, the public can no longer offer comments on the proposed rules unless they are altered in a way that requires the process to begin again. Following the hearing on the proposed rules, the Office has 180 days to file adopted rules with the Secretary of State for publication in the Colorado Register. Adopted rules go into effect twenty days after publication or on such later date as is stated in the rules.
3. **Connecticut**. The statute does not appear to confer any express rulemaking authority. However, it does contemplate that a joint standing committee of the General Assembly be convened by September 1, 2022 to study certain matters and issue a report on its finding and recommendations by January 1, 2023. Currently, there is no publicly available update on the status of this committee's efforts.
4. **Utah**. While by statute the Attorney General and Consumer Protection Division are to report on the effectiveness of the enforcement provisions and data protected and not protected by the law, the statute does not appear to confer express rulemaking authority.
5. **Virginia**. The statute does not appear to expressly confer any rulemaking authority and non are anticipated to be promulgated. In April 2022, Virginia passed three fairly minor amendments to the law (change on rights to delete, added political organizations to the definition of excluded nonprofits, and repealed the VCDPA consumer privacy fund, remitting payments instead to a preexisting state fund).

PUTTING IT INTO PRACTICE: The time frame and status above should help as companies continue to work on their compliance activities with these US state "comprehensive" laws. The California regulations can be used now, keeping in mind that they are not yet final. Companies striving towards a singular approach and date for compliance will also want to keep in mind Colorado's draft regulations.

FTC Announces Proposed Rulemaking On Privacy and Data Security

Posted August 22, 2022

The FTC recently announced an ambitious Advance Notice of Proposed Rulemaking (ANPR) broadly aimed at a host of privacy and data security issues. This is the first step by the agency to explore using its Section 18 rulemaking authority under the FTC Act to issue a broad consumer privacy-focused trade regulation rule. The ANPR poses 95 questions and various topics, ranging from collection of information from children, to consent, data security, biometrics, artificial intelligence, and automated decision-making. The ANPR is focused on the impact to consumers and as workers or employees in a business capacity.

In its overview, the FTC points to the rise in privacy and security regulation at the international and state levels, suggesting a need for a more comprehensive approach at the federal level. The Agency also noted limitations in its own regulatory parameters, citing limits to its ability to issue remedies. Because the agency generally lacks authority to seek monetary remedies for initial violations of the FTC Act, the Commission believes that enforcement of the FTC Act alone may not be enough to protect consumers. As a result, the Commission views rules that establish privacy and data security requirements as arguably providing the FTC the authority to seek financial penalties for first-time violations and thereby driving compliance.

Section 18 of the FTC Act authorizes the FTC to issue trade regulation rules that define with specificity acts or practices that are unfair or deceptive (known as "Mag Moss Rulemaking"). Under Section 18, the agency must show

that the unfair or deceptive acts or practices in question are prevalent. This determination can be made only if the FTC has previously "issued cease and desist orders regarding such acts or practices," or if it has any other information that indicates a widespread pattern of unfair or deceptive acts or practices. That said, the FTC's stated purpose for the ANPR is to generate a public record about prevalent commercial surveillance practices or lax data security practices that are unfair or deceptive. The Commission concedes that the comments might not ultimately result in the promulgation of new rules, but that the comments will inform the Commission's enforcement work and may inform reform by Congress or other policymakers.

PUTTING IT INTO PRACTICE: While it is too soon to say whether this process will result in any substantive rules (Mag Moss rulemaking is a lengthy process taking several years if successful), the ANPR is nonetheless informative. The questions posed in the ANPR provide clues on the FTC's perspective on certain activities and potential enforcement priorities. Comments to the ANPR must be received 60 days after publication of the notice in the federal register. The FTC will also be holding a public forum on September 8, 2022. Comments can be submitted online or by paper. Other guidelines for submitting comments can be found in the ANPR.

Preparing for US State Privacy Law Compliance: The Six Month Mark

Posted July 25, 2022

With six months before the first of the new US state general privacy laws go into effect, there are several steps companies can take now to begin to prepare. Unfortunately there are some parts of compliance that will be impacted by regulations that have either not been drafted, or if drafted, remain unfinalized. What, then, can companies do now? Familiarizing themselves with the types of requirements and beginning to address and develop mechanics for those requirements is a good start. Fortunately for most, these will not be new, as they are conceptually covered by CCPA, GDPR, or both.

As a reminder, and as we have written previously, the Virginia privacy law and modifications to the California law go into effect January 1, 2023. The Connecticut and Colorado laws go into effect July 1, 2023, and the Utah law December 31, 2023. In putting together your plan, it is helpful to think about the impact that these laws have on the lifecycle of data collection and use. Namely, what impact they have on (1) notice, (2) consent, (3) vendor management, and (4) rights provisions. We have provided thoughts below organized by the order which an entity might want to think about these areas:

- **Rights Provisions**: This is perhaps the area that will require the heaviest lift for companies. The laws expand the current California requirements to provide individuals with the ability to access and delete their information. They also add concepts of data portability and (for all but Utah) the ability to have information corrected.
- **Vendor Management**: The new laws more closely mirror the GDPR in requiring certain contractual provisions when engaging third parties to "process" information on your company's behalf. Now is a good time to conduct an audit of any such third parties and gather existing contractual terms. Contracts with those entities can be evaluated against what will be required under the upcoming laws.
- **Consent and Opt-Outs**: Companies already have obligations to obtain consent in certain circumstances under various existing privacy laws (TCPA or COPPA for example) and to give individuals the ability to opt-out (CCPA and CAN-SPAM, for example). The upcoming laws add to the matrix by requiring consent for processing sensitive information in some states (Colorado, Connecticut, and Virginia), though an opt-out for the same information in others (California and Utah), and an opt-out of profiling. All states include a right to opt-out of "sale." Companies can thus think about the extent to which they process sensitive information (which includes biometric and precise geolocation data) or engage in selling or profiling. The laws also introduce into law an opt-out of targeted advertising (already interpreted by the FTC as required to avoid allegations of unfairness and deception under Section 5 of the FTC Act).
- **Notice**: While notice is what consumer's see first, modifications to notice will likely be last on companies' roadmaps. As your organization begins to think about notice updates, things to assess now include whether you

will offer rights (access, deletion, correction, etc.) to individuals in all locations, or only in those locations that legally require it.

The regulations for each of these laws should (hopefully) clarify many implementation points. However, only California has released draft regulations (and Connecticut has sought pre-rulemaking input), but those have not yet been finalized.

PUTTING IT INTO PRACTICE: With six months left before the first of the US state privacy laws go into effect, now is a good time to begin thinking about how your organization will address compliance. Sheppard Mullin has put together this compendium with copies of all of the laws (as well as GDPR), which should serve as a helpful resource.

What Should We Do About the Draft CPRA Regulations?: Contracts

Posted June 29, 2022

In this third post of our ongoing series, we examine key takeaways for companies in light of the recently released draft CPRA regulations. Today's focus is on contractual requirements. (Visit here for information about collection and notice under the draft regulations, and here for information about choice.)

The contractual requirements in the draft regulations do not mirror the statute and add entirely new obligations. For example, the draft regulations prescribe a new, five-day time period in which a service provider, contractor, or third party must notify the business if they determine they can no longer comply with the CPRA's requirements. The draft regulations also require contracts with service providers to identify the specific business purposes and services for which personal information will be processed and prohibit generic descriptions of such purposes, such as referencing the entire contract generally.

The draft regulations state that failure to meet the prescriptive requirements means that the recipient is not a service provider or contractor under the CCPA. This means that any such transfer would be deemed a "share" subject to the right to opt out of sharing. Businesses must also conduct due diligence on service providers, contractors, and third parties to take advantage of the CPRA statute's liability shield for compliance failures of the service provider, etc. without the business's knowledge.

PUTTING IT INTO PRACTICE: While the draft regulations may undergo many updates between now and CPRA's January 1, 2023 effective date, there are certain things companies can do today. This includes analyzing these new requirements for contracts and analyzing existing service provider relationships to identify possible gaps.

What Should We Do About the Draft CPRA Regulations?: Choice

Posted June 28, 2022

In this second post in our ongoing series, we examine key takeaways for companies in light of the recently released draft CPRA regulations. Today's focus is on issues surrounding consumer choice:

- **Dark patterns**. Businesses are provided a set of principles to follow in how they allow consumers to submit requests and obtain consent where required. A violation of these principles could be considered a "dark pattern" under the draft regulations and as such, would not constitute valid consent. The inclusion of "dark patterns" follows other regulators' concerns about the practice, including the FTC. (More information about dark patterns is included in this post.)

- **Opt-out links**. The draft regulations permit businesses to offer a single opt-out link instead of both a "Do Not Sell or Share My Personal Information" and a separate "Limit the Use of My Sensitive Personal Information" link. The so-called "alternative opt-out link" may be titled either "Your Privacy Choices" or "Your California Privacy Choices," and must be accompanied by a specific opt-out icon to the right or left of the link.
    - Unlike the statute, the proposed CPRA regulations arguably suggest that honoring opt-out preference signals are mandatory. This despite global opt-out signals being optional in the CPRA. As proposed, an opt-out preference signal would be sent by a platform, technology, or mechanism on behalf of a consumer. The point is to signal a consumer's choice to opt-out of the sale and sharing of personal information with all businesses they interact with online instead of making individualized requests with each business. There are no technical specifications for these signals in the draft regulations. The requirements for handling of signals is likely to be subject to much debate and receive significant commentary during the public comment period.
- **Right to limit use and disclosure of sensitive personal information**. Businesses that collect sensitive personal information must, under the draft regulations, provide consumers a right to limit such use. This may be done through an interactive form accessible via a "Limit the Use of My Sensitive Personal Information" link, an alternative opt-out link, or the privacy policy. A business has 15 days to comply with the request, including notifying service providers, contractors, and third parties. There are instances where a business may use or disclose sensitive personal information without offering a right to limit the use.

PUTTING IT INTO PRACTICE: Companies can review the draft regulations to understand expectations around consent (and how to avoid processes that could be viewed as a dark pattern). They can also begin thinking about how they will handle requirements around opt-out links and preference signals.

What Should We Do About the Draft CPRA Regulations?: Collection and Notice

Posted June 27, 2022

The California Privacy Protection Agency (CPPA) recently released the draft proposed CCPA Regulations and draft initial statement of reasons. Importantly, these are *draft* regulations that are likely to be subject to extensive public comment and modification before they become final. At the June 8 meeting, the board moved to approve the draft regulatory text to begin the formal rule making process and public comment period.

These draft regulations redline the existing CCPA regulations. Though some provisions were largely unedited, they could be modified in forthcoming updates. This includes notices regarding financial incentives, rules for consumers under the age of 16, non-discrimination practices, and requirements for verifying requests. Requirements around cybersecurity audits, risk assessments, and automated decision-making technology were *not* covered in this draft.

While the draft regulations do not address all topics on which the CPRA required the CPPA to adopt regulations, the draft does include guidance on certain topics of interest such as data processing agreements and the opt-out preference signal. In this series we examine some of the key takeaways for companies.

Our focus in today's post is on collection and notice. Under the proposed regulations, a business's collection, use, retention and sharing of personal information should be consistent with what a consumer would expect when the information was collected. Any uses that are unrelated or incompatible with the original purpose requires explicit consent from the consumer. The draft provides four illustrative examples on this point.

For privacy policies, the regulations largely incorporate the statutory content requirements, and then adds new requirements. Where more than one business controls the collection of a consumer's personal information, both the first-party business and any third-party businesses would have to provide a notice at collection. The draft provides several examples on this point.

PUTTING IT INTO PRACTICE: This draft is likely to undergo many updates during the public notice and comment period. Whether they will be finalized before the CPRA comes into effect on January 1, 2023 is not clear. In light of this uncertainty, companies would be well served to look at the key developments to begin to develop approaches for addressing compliance.

Connecticut Fifth State to Pass a Comprehensive Privacy Law

Posted May 12, 2022

Connecticut just joined California, Colorado, Utah, and Virginia in passing a comprehensive privacy law. The Connecticut Data Privacy Act (CTDPA) goes into effect July 1, 2023, the same time as Colorado's very similar law. Companies preparing for these new laws (Virginia goes into effect January 1, 2023 and Utah December 31, 2023) will want to keep in mind the following five things about this fifth general US state privacy law.

1. **Applicability**. It applies to businesses that (1) conduct business in Connecticut, or produce products or services targeted to CT residents; and (2) during the preceding calendar year either (a) controlled/processed the personal data of at least 100,000 consumers (excluding for payment transactions), or (b) controlled/processed the personal data of at least 25,000 consumers and derived more than 25% of gross revenue from the sale of personal data. A "consumer" is not an employee or individual acting in their role as an employee. Similar to other state laws, there are exemptions. The law does not apply to government entities or nonprofits or institutions in higher education. The law also exempts financial institutions subject to GLBA and entities and information subject to HIPAA.
2. **Individual Rights**. Like other states, Connecticut provides consumers with the right to access, correction, portability and deletion. Taking its cue from Virginia and Colorado, it also gives consumers the right to opt-out of processing data for targeted advertising, sales, and profiling. "Sales" is defined broadly as in California and Colorado: "monetary or other valuable consideration." This opt-out requirement will go into effect January 2025, six months after Colorado's similar requirement. As with Virginia, Colorado, and GDPR, companies must get consent to process sensitive data.
3. **Contractual Requirements**. Similar to other state laws, data controllers will need to enter into contractual agreements with processors. Those contracts must hold a processor to at least the same protections as the controller.
4. **Data Security and Governance**. Connecticut currently has a broad data security law, requiring "safeguarding" of personal information. This new law provides more detailed requirements. Companies will need to establish, implement and maintain reasonable administrative, technical and physical data security practices. Connecticut also joins California, Virginia, and Colorado in requiring controllers to conduct data protection assessments prior to engaging in data processing activities that present a heightened risk of harm to consumers. The Attorney General may request copies of these assessments.
5. **Enforcement**. Similar to the other general state privacy laws, this law does not provide for a private right of action. Enforcement rests with the Attorney General. Businesses will be given a temporary 60-day right to cure violations until December 31, 2024. Starting in 2025, the Attorney General will have discretion to determine whether to grant a cure period. Violations can result in civil penalties of up to $5,000 per violation plus actual and punitive damages, and attorneys' fees and costs.

PUTTING IT INTO PRACTICE: The passing of this law is yet another reminder of the importance of adaptive privacy programs. As 2023 approaches, companies will want to balance these laws' similarities -providing rights, contractual provisions, security obligations- with the laws' nuances.

Colorado AG Seeks Input on Key Aspects of Upcoming Privacy Act

Posted April 28, 2022

The Colorado AG's office recently released pre-rulemaking considerations for the Colorado Privacy Act (CPA). The office is seeking informal public feedback on a series of topics. While the AG listed eight specific topics for feedback, the public can offer input on any aspect of the upcoming rulemaking. The AG's office is interested in comments about the universal opt-out, the requirements around consent, and "dark patterns." The AG is also interested in circumstances triggering data protection assessments and the requirements around profiling. Questions were also posed about "offline" collection of data. Lastly, the office seeks feedback to the rules around opinion letters and about how CPA compares or contrasts to privacy laws in other jurisdictions.

PUTTING IT INTO PRACTICE: Interested stakeholders can submit comments through this form, or participate in informal listening sessions. The formal rulemaking procedures are expected to begin this fall. This will include the release of the draft regulations.

Virginia Tweaks Its Upcoming Privacy Law

Posted April 26, 2022

The Virginia privacy law going into effect January 2023 received some minor tweaks this month. In particular, provisions around deletion requests. As originally enacted, the Virginia law mirrored similar provisions in California and Europe, giving individuals the ability to ask for their information to be deleted. As amended, if information that the individual asks to be deleted was obtained "from a source other than the consumer" then the business can treat that deletion request as a request to opt out of targeted advertising, sale, and profiling. The business can also delete the information.

PUTTING IT INTO PRACTICE: This amendment is a reminder for companies that the California and European concept of "rights requests" will soon be extended to individuals in Virginia, Utah and Colorado. While the processes are similar, there are nuances that are worth examining prior to the 2023 implementation dates.

The Beehive State Joins the State Privacy Law Hive: Utah Privacy Law Passes

Posted March 28, 2022

Utah recently joined California, Colorado, and Virginia in passing a comprehensive privacy law. It goes into effect December 31, 2023 and shares similarities with other states' laws. Businesses may be glad to learn that Utah takes a lighter touch in some key areas.

Applicability. Like Virginia and Colorado, Utah's law applies to information about consumers, not employee or B2B information. It applies to businesses that (1) conduct business in Utah or produce products or services targeted to Utah residents, (2) have annual revenues of $25 million or more, and (3) either (a) process personal data of 100,000 or more Utah residents, *or* (b) derive more than 50 percent of their gross revenue "from the sale of personal data and [control or process] the personal data of 25,000 or more Utah consumers." That the law includes both a financial and volume threshold is unique. As a result, the law may apply to fewer businesses than those that are, or will be, subject to other state laws. Similar to other states, Utah provides for a number of exceptions. For example, the law does not apply to government entities, nonprofits, and HIPAA-covered entities and business associates. It also does not apply to financial institutions subject to the Gramm-Leach-Bliley Act.

Individual Rights. Like other US laws and GDPR, Utah consumers will have certain rights under this law. This includes a right to access and deletion. It also includes a right to portability. There is no right to correction (as exists in the other state laws). The law also contemplates a right to opt out of "sale" and "targeted advertising." Utah's law follows Virginia's more narrow definition of "sale" rather than California's broader definition. In Utah, a sale is limited to the

exchange of personal data for monetary consideration. Further, the law does not consider disclosures of personal information to third parties a sale if the purpose is consistent with the consumer's reasonable expectations. Utah allows collection of "sensitive data" if consumers are given notice and the right to opt *out* of such collection. This differs from Colorado and Virginia, that require opt-in consent.

Contractual Requirements. Like other general privacy laws, Utah requires a contract with entities engaged to "process" information on the company's behalf. That contract should outline the nature and purpose of processing, that information processed remain confidential, and that subcontractors enter into an agreement with similar obligations.

Governance requirements. Unlike California, Virginia, and Colorado, Utah does not require companies to conduct and document data protection impact assessments. The law also does *not* contemplate any cybersecurity audits or risk assessments.

Enforcement. In line with the other laws, Utah does not provide for a private right of action. The law will be enforced by the Utah Attorney General. There is a 30-day cure period for alleged violations. The AG may recover actual damages to the consumer, and a penalty up to $7,500 for each violation.

PUTTING IT INTO PRACTICE: Companies operating in the US now have four comprehensive state privacy laws to keep on their radar for 2023. These are in addition to the myriad (and changing) state privacy laws that govern specific activities and types of information (biometric laws, telephone marketing laws, and more). The continued passage of these laws is a reminder of the importance of having a nimble privacy program that can readily adapt to the changing legislative landscape.

In First CCPA "Opinion", California AG Clarifies Scope of Access Requests

Posted March 24, 2022

The California AG recently issued an opinion interpreting the scope of information that should be provided to consumers in an access request. In responding to access requests, companies must provide a list of all personal information that it has about that consumer. The AG opinion clarifies that *inferences* a company draws from personal information should be included in such a response.

The CCPA defines inferences as the "derivation of information, data, assumption, or conclusions from facts, evidence, or another source of information or data." For example, if a consumer indicates that they pay homeowner taxes, a company would likely conclude that the consumer is a homeowner. Or, if a consumer purchases an "I voted" shirt a company may conclude that the consumer is a likely voter. The AG provides a two-step test to help determine what information is an inference. First, is the information derived from personal information? If yes, and the company can use this information to create a profile about the consumer, or to predict a characteristic, then that information is an inference. Companies are not required to disclose the inputs or algorithms that form the inferences. Notably, the AG stated that even if the underlying information is exempt from disclosure (for example, the original data was not personal information since it was publicly available), the inference of this information will be subject to an access request.

PUTTING IT INTO PRACTICE: Businesses subject to the CCPA (and the forthcoming CPRA) should revisit their individual rights request policies and procedures. Specifically, to verify that inferences are being included when responding to an access request.

California AG Takes Aim At Customer Loyalty Programs

Posted February 23, 2022

Did your business receive a letter from the California Attorney General's office about your loyalty program? You are not alone. The California AG celebrated Data Privacy Day last month by announcing that his office had conducted an "investigative sweep" of business operating loyalty programs in California. His office then sent out notices of non-compliance to several loyalty program operators.

In general, loyalty programs give customers who enroll incentives, rewards or discounts. The business then tracks the products purchased or the dollars spent by each program member. The California Consumer Protection Act (CCPA) requires that programs that provide "financial incentives" (i.e., promotions, discounts, and deals in exchange for personal information) must provide a notice of financial incentive. More about CCPA requirements and applicability can be found here.

The AG non-compliance notices, however, seem to focus more on the CCPA notice requirement. According to the Data Privacy Day press release, the California Attorney General intends to take action against businesses that fail to clearly inform consumers about how the business will use their data: "I urge all businesses in California to take note and be transparent about how you're using your customer's data. My office continues to fight to protect consumer privacy, and we will enforce the law."

PUTTING IT INTO PRACTICE: This news shows that the California AG is going to be focusing on loyalty programs, and companies would be well served to review their disclosures and practices against the CCPA requirements.

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

"The fantastic advances in the field of electronic communication constitute a greater danger to the privacy of the individual."

—Earl Warren

2022 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

David Poell
Partner
dpoell@sheppardmullin.com
312.499.6349

Wynter Deagle
Partner
wdeagle@sheppardmullin.com
858.720.8947

Kari Rollins
Partner
krollins@sheppardmullin.com
212.634.3077

Morgan Forsey
Partner
mforsey@sheppardmullin.com
415.774.3254

Moorari Shah
Partner
mshah@sheppardmullin.com
714.424.8264

Rachel Tarko Hudson
Partner
rhudson@sheppardmullin.com
415.774.2999

Sara Shanti
Partner
sshanti@sheppardmullin.com
312.499.6358

Snehal Desai
Associate
sdesai@sheppardmullin.com
415.774.2960

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

James Fazio
Special Counsel
jfazio@sheppardmullin.com
858.720.7418

Jarrod Brodsky
Associate
jbrodsky@sheppardmullin.com
202.747.1901

Anne-Marie Dao
Associate
adao@sheppardmullin.com
858.720.8963

Charles Glover
Associate
cglover@sheppardmullin.com
212.896.0679

Julia Kadish
Associate
jkadish@sheppardmullin.com
312.499.63340

Elfin Noce
Associate
enoce@sheppardmullin.com
202.747.2196

Alyssa Paddock
Associate
apaddock@sheppardmullin.com
212.896.0692

Nikole Snyder
Associate
nsnyder@sheppardmullin.com
202.747.3218

Alyssa Sones
Associate
asones@sheppardmullin.com
424.288.5305

Brittany Walter
Associate
bwalter@sheppardmullin.com
858.876.3525

Lauren Weiss
Associate
laweiss@sheppardmullin.com
202.747.2678

SheppardMullin

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

www.sheppardmullin.com