GIBSON DUNN

U.S. Cybersecurity and Data Privacy Outlook and Review – 2023

Client Alert | January 30, 2023

I. Introduction In this tenth edition of Gibson Dunn's US Cybersecurity and Data Privacy Outlook and Review, we provide an overview of some of the most significant developments in cybersecurity and data privacy in the United States in 2022 and look ahead to trends for 2023. In addition to the privacy and cybersecurity challenges that were and continue to be wrought by the COVID-19 pandemic, 2022 was shaped by volatile geopolitics. Russia's invasion of Ukraine ushered in a new era of cyberwarfare and exacerbated the already-precarious threat landscape. In addition, there was a spate of new privacy and cyber laws and regulations due in large part to new technologies and the increased attention on protective privacy and cyber hygiene. There was also a substantial uptick in regulatory scrutiny and enforcement, as well as civil and criminal litigation, which further amplified the focus and urgency of privacy and cybersecurity issues. Although the full impact of these developments is yet to be realized, one thing is clear: the challenges and opportunities are extraordinary, far reaching, and unprecedented. This Review places these and other 2022 developments in broader context. We proceed by addressing: (1) the regulation of privacy and data security, other legislative developments, enforcement actions by federal and state authorities, and new regulatory guidance; (2) trends in civil litigation around data privacy and security in areas including data breach, digital, telecommunications, and biometric information privacy laws; and (3) trends related to data innovations and governmental data collection. We refer to companies by generic descriptors in the body of the alert; for further details, please see the endnotes. For information on developments outside the United States—which are relevant to domestic and international companies alike—please see Gibson Dunn's International Cybersecurity and Data Privacy Outlook and Review.

Related People

Cassandra L. Gaedt-Sheckter

Svetlana S. Gans

Amanda M. Aycock

Ryan T. Bergsieker

Abbey A. Barrera

Matt Buongiorno

Terry Wong

Ruby B. Lang

Sarah Scharf

Jennifer Katz

Brendan Krimsky

I. Introduction

II. Regulation of Privacy and Data Security

A. Legislation

1. State Legislation and Related Regulations

a. Comprehensive State Privacy Laws

i. California ii. Virginia iii. Colorado iv. Connecticut v. Utah vi. Practical Implications of State Privacy Laws on AdTech Ecosystem

b. Other State Privacy Laws

i. California Age-Appropriate Design Code Act ii. California's Confidentiality of Medical Information Act iii. New York Department of Financial Services' Proposed Amendments to Part 500 Cybersecurity Rules and New Guidance Related to Cryptocurrencies

2. Federal Legislation

B. Enforcement and Guidance

1. Federal Trade Commission

a. FTC Organization Updates b. Algorithmic Bias and Artificial Intelligence c. Commercial Surveillance and Data Security i. April 2022 Speech by FTC Chair Khan ii. Rulemaking on Commercial Surveillance and Data Security d. FTC's Approach to Data Security e. Notable FTC Enforcement Actions f. Financial Privacy g. Children's and Teens' Privacy h. Dark Patterns

2. Consumer Financial Protection Bureau

a. Regulation of Nonbank Entities b. Artificial Intelligence and Algorithmic Bias c. Data Harvesting and Contribution d. Personal Financial Data Rights Rulemaking e. Data Security

3. Securities and Exchange Commission

a. Regulation b. Enforcement

4. Department of Health and Human Services and HIPAA

a. Rulemaking on HIPAA Compliance and Data Breaches b. Telehealth and Data Security Guidance c. Reproductive and Sexual Health Data d. HHS Enforcement Actions

5. Other Federal Agencies

a. Department of Homeland Security b. Department of Justice c. Department of Energy d. Joint Agency Actions Regarding Banking Cybersecurity e. Department of Commerce AI Initiative

6. State Agencies

a. National Association of Attorneys General b. State AGs' Reaction to *Dobbs* c. State AG Letter on National Consumer Privacy Laws d. Dark Patterns e. Other State AG Actions f. New York Department of Financial Services

III. Civil Litigation Regarding Privacy and Data Security

A. Data Breach Litigation

1. Standing Implications of *TransUnion v. Ramirez* 2. Potential Increase in Trials and Derivative Lawsuits 3. Major Settlements 4. Rise in State and Federal Legislation

B. Computer Fraud and Abuse Act Litigation

C. Telephone Consumer Protection Act Litigation

D. State Law Litigation

1. California Consumer Privacy Act Litigation

a. Potential Anchoring Effect of CCPA Statutory Damages b. Requirements for Adequately Stating a CCPA Claim c. Broadening the Scope of a "Data Breach" d. CCPA Violations Under the UCL e. CCPA as a Shield for Immunity to Substantive Claims Litigation f. The CCPA in Discovery Disputes g. Supplementing Time for the CCPA's 30-Day Notice Requirement h. Guidance on Reasonable Security Measures in Connection with the CCPA i. Staying CCPA Litigation Due to Other, First-Filed Litigation Arising from the Same Data Breach 2. Illinois Biometric Information Privacy Act Litigation 3. Texas Biometric Privacy Law Litigation

E. Other Noteworthy Litigation

IV. Trends Related To Data Innovations and Governmental Data Collection

V. Conclusion

II. Regulation of Privacy and Data Security Since 2018, five states have enacted comprehensive data privacy legislation. Two of these laws passed in 2021, and two—Utah and Connecticut—passed in 2022. An additional 27 state legislatures considered comprehensive consumer privacy bills this past year, but have yet to enact them. Another notable legislative development in 2022 was the significant progress towards passing a bipartisan federal privacy bill, the American Data Privacy and Protection Act ("ADPPA"). While the future of the ADPPA is uncertain, this bill has provided a useful framework that will likely pave the way for future attempts at enacting a federal privacy law. We detail these recent legislative initiatives below. **A. Legislation 1. State Legislation and Related Regulations a. Comprehensive State Privacy Laws** To date, five states – California, Colorado, Connecticut, Virginia, and Utah – have enacted comprehensive data privacy legislation. California was the first state to enact such legislation in 2018 with the California Consumer Privacy Act ("CCPA"), and before another state could enact legislation, enacted a second law in 2020, the California Privacy Rights Act ("CPRA"). California was followed by other states, as seen in the table below. These state privacy laws are generally similar, but there are notable differences that we discuss in this section.

Law	Enacted Date	Effective Date
California Consumer Privacy Act (CCPA)	June 28, 2018	January 1, 2020
California Privacy Rights Act (CPRA)	November 3, 2020	January 1, 2023
Virginia Consumer Data Protection Act (VCDPA)	March 2, 2021	January 1, 2023
Colorado Privacy Act (CPA)	July 7, 2021	July 1, 2023
Connecticut Data Privacy Act (CTDPA)	May 10, 2022	July 1, 2023
Utah Consumer Privacy Act (UCPA)	March 24, 2022	December 31, 2023

Last year, an additional 27 state legislatures considered comprehensive consumer privacy bills, which largely align with Virginia's, Colorado's, and Connecticut's laws (California and Utah have some unique features), and would have provided consumers with the right to access, correct, and delete their personal information, the right to data portability, the right to opt out of the sale of their personal information, as well as the use of their personal information for targeted advertising and profiling, and the right not to be discriminated against for exercising these rights. However, some of the proposed bills follow Utah's more business-friendly approach (e.g., the Ohio Personal Privacy Act and Pennsylvania's H.B. 1126), while others are more similar to the CPRA (which we discuss in more detail below). Still others go even further – for example, the New Jersey Disclosure and Accountability Transparency Act would prohibit the processing or collection of any personal information without *affirmative consent* from the consumer.[1] For 2023, at least nine states have already introduced comprehensive privacy bills, generally consistent with prior legislative efforts. Oregon is a notable addition, with a bill resulting from a working group organized by the state Attorney General which includes a private right of action. Five states also currently have legislation to increase protections for children's data, including some following the lead of California's Age Appropriate Design Code Act. And at least seven states are considering bills addressing particular subsets of data, such as collection and use of biometric data or health data and third-party data brokers. **i. California** The CCPA was signed into law by Governor Jerry Brown in June 2018, and took effect on January 1, 2020. On August 24, 2022, California Attorney General Rob Bonta announced the first settlement of a CCPA enforcement action, which included $1.2 million monetary relief, and equitable relief, as discussed in more detail in Section ?II.B.6 below. The CCPA has continued to evolve over the past year. The CPRA, which went into effect on January 1, 2023, represents the most significant change to date. Passed as a ballot initiative (Proposition 24) in November 2020, the CPRA amends and builds upon the CCPA. Accordingly, the CPRA includes several key changes to the CCPA, the most

significant of which have been detailed in prior Gibson Dunn alerts.[2] 2022 saw companies scrambling to become compliant with the CPRA, even when the regulations were—once again—not finalized by the time the law took effect. California Consumer Privacy Act ("CCPA") The CCPA applies to any for-profit organization that collects California consumers' personal information, does business in California, and satisfies one of the following thresholds:

- has annual gross revenues in excess of $25 million;
- buys, receives for its commercial purposes, sells, or shares for commercial purposes the personal information of 50,000 or more California consumers, households, or devices, annually; or
- derives 50 percent or more of its annual revenues from selling California consumers' personal information.[3]

Notably, the CCPA is the only comprehensive state privacy law that applies to entities based on revenue alone (the first criterion above). Other states generally require that the business processes the data of a threshold number of state consumers in order for the law to apply, *and* those thresholds are generally higher (typically 100,000). The CCPA is also the only state law that applies solely because a business is deriving a certain percentage of its revenue from selling consumers' personal information (the third criterion above). Other states' laws generally apply only if the business processes a threshold number of state consumers' data (typically 25,000) *and* derives revenue from selling personal information. The CCPA grants privacy rights to California consumers, imposes duties on businesses that meet the thresholds described above, and is enforced through both administrative enforcement and a limited private right of action for consumers whose nonencrypted and nonredacted data was breached as a result of a business's violation of these aforementioned duties. We discuss CCPA-related private litigation in more detail in Section ?II.B.6 below. The CCPA has served as an example for other states when enacting comprehensive privacy legislation. Specifically, the CCPA grants consumers the following rights, which other states have consistently incorporated into their laws:

- right to access personal information that a business has collected about them;[4]
- right to data portability;[5]
- right to delete personal information that a business has collected about them;[6]
- right to opt out of the sale of their personal information;[7] and
- right to not be discriminated against for exercising these rights.[8]

California Privacy Rights Act ("CPRA") As mentioned above, the CPRA amends and builds upon the CCPA. A change worth mentioning is the applicability thresholds, which align more closely with other states' laws that followed. The CPRA increases the CCPA's processing threshold from 50,000 to 100,000 consumers or households, eliminates the consideration of "devices" from this number, and removes information that the business receives for its commercial purposes, but does not buy, sell or share from the calculation.[9] This change will reduce the law's applicability to smaller businesses. On the other hand, the CPRA expands the threshold for the percentage derived from selling personal information to also include revenue derived from "sharing" personal information.[10] Businesses that meet the revised applicability thresholds should be aware that the CPRA imposes additional obligations on them, and they need to come into compliance now, if they have not already. The CPRA expands upon the CCPA by: granting consumers new rights (i.e., the right to limit the use of their sensitive personal information, the right to correct their personal information, the right to data minimization, and a broader right to opt out of the "sale" *or "sharing"* of personal information, which the CPRA defines as sharing for cross-context behavioral advertising, whether or not for monetary or other valuable consideration); and by imposing requirements and restrictions on businesses, including new storage limitation requirements, restrictions on automated decision-making, and audit requirements. The CPRA also sunsetted the CCPA's

exemptions for personal information obtained from employees and job applicants in the context of employment as well as certain personal information obtained in business-to-business ("B2B") transactions. Furthermore, the CPRA provides consumers with rights relating to their personal information collected on or after January 1, 2022, despite its January 1, 2023 effective date. The CPRA also establishes a new, first-of-its-kind, enforcement agency – the California Privacy Protection Agency ("CPPA") – which is set to begin enforcement on July 1, 2023. Importantly, the CPRA makes the CCPA's 30-day cure period discretionary, seemingly intending to allow the CPPA authority to find a violation absent any notice and cure period.[11] In making a decision to provide time to cure, the CPPA may consider whether the business intended to violate the CPRA and voluntary efforts taken to cure the alleged violation prior to being notified by the CPPA, making such efforts important absent strict compliance.[12] Although the CPPA is expected to have primary responsibility for enforcing the CPRA, the CPPA's enforcement authority will be co-extensive with the California Attorney General, and consumers have a limited private right of action. The CPPA is tasked with handling administrative enforcement (i.e. bring administrative proceedings),[13] while the Attorney General will continue to handle civil enforcement (i.e. bringing an action in a civil court action).[14] The CPPA may impose administrative fines and the Attorney General may impose civil penalties, in each case of up to $2,500 per violation or $7,500 per intentional violation or violation involving a minor's protected personal information.[15] The CPPA is also tasked with implementing the CPRA through regulations,[16] and rulemaking authority was officially transferred in April 2022.[17] Proposed regulations were initially released on July 8, 2022. For additional information about the proposed regulations, please see our previous client alert, which highlights what we believe to be some of the most interesting and potentially impactful draft regulations. Further modifications were released in response to public comments on November 3, 2022.[18] Comments on the proposed modifications were accepted until November 21, 2022, and the rulemaking process is ongoing. These modifications clarify that businesses must treat opt-out preference signals as a valid request to opt-out of the sale and sharing of personal information for "any consumer profile associated with that browser or device, including pseudonymous profiles," in addition to the browser or device itself.[19] The revisions also clarify that if a business received an opt-out preference signal that conflicts with the consumer's participation in the business's financial incentive program and does not ask the consumer to affirm their intent with regard to the financial incentive program, the business must still process the opt-out preference signal as a valid request to opt-out of the sale and sharing of the consumer's personal information.[20] The CPPA also further expounded the already lengthy section on dark patterns, adding a sentence indicating that "a business's intent to design the user interface to subvert or impair user choice weighs heavily in favor of establishing a dark pattern."[21] The soonest we expect to receive finalized rules is April 2023. Notably, the most recent draft of the regulations explicitly allows the CPPA to take into account the delay in issuing regulations when deciding whether to pursue investigations of alleged violations of the CPRA.[22] Although the regulations are subject to change, they still provide helpful guidance for businesses that can be implemented now.

ii. Virginia The VCDPA,[23] which was signed into law in March 2021 and went into effect on January 1, 2023, enumerates a number of similar rights for Virginia consumers, as discussed in our prior client alert. Virginia was the second state to enact comprehensive privacy legislation, following California. However, the VCDPA differs from the CCPA/CPRA in several notable ways, and Colorado, Connecticut, and Utah have declined to follow some of the CCPA's/CPRA's provisions in favor of the VCDPA's. The VCDPA applies to all for-profit organizations that "conduct business in [Virginia] or produce products or services that are targeted to residents of [Virginia]" and either:

- during a calendar year, control, or process the data of at least 100,000 Virginia consumers; or
- derive more than 50% of their gross revenue from the sale of personal data *and* control or process the data of at least 25,000 Virginia consumers.[24]

Unlike California's laws, the VCDPA does not contain a revenue-only based threshold,

and Colorado, Connecticut, and Utah have followed suit. Therefore, even large businesses will not be subject to such state laws unless they process the personal information of a certain number of residents. Also, the term "consumer" as defined in the VCDPA does not include any person "acting in a commercial or employment context"[25]—another departure from the CPRA (in light of the sunsetted exemptions) that Colorado, Connecticut, and Utah have followed. Thus, applicability of the other laws is more narrow. That said, the VCDPA, like the CPRA, grants Virginia consumers the right to access, correct, and delete their personal data, the right to data portability, and the right to opt out of the sale of their personal data (but limits the definition of "sale" to the exchange of personal data for "*monetary*" (as opposed to "valuable") consideration by the controller to a third party, and explicitly does not include transfers to affiliates and processors).[26] While the CPRA provides Californians with the right to opt out of the sharing of their personal information for the purpose of cross-context behavioral advertising, the VCDPA goes a step further and grants Virginians the right to opt-out of *any* processing of their personal data for the purpose of targeted advertising.[27] The VCDPA also provides Virginians with the right to opt out of any processing of personal data for the purposes of profiling in furtherance of decisions that produce legal or similarly significant effects.[28] Additionally, the VCDPA requires that controllers obtain consent before processing a consumer's sensitive data, defined as including "[p]ersonal data revealing racial or ethnic origin, religious beliefs, mental or physical health diagnosis, sexual orientation, or citizenship or immigration status"; genetic or biometric data processed for the purpose of uniquely identifying a natural person; the personal data collected from a known child; and precise geolocation data (as defined by the VCDPA).[29] The definition of "sensitive data" under the VCDPA is narrower than the equivalent "sensitive personal information" under the CPRA. The VCDPA also grants consumers the right to appeal a controller's refusal of a consumer request through a novel "conspicuously available" appeal process to be established by the controller.[30] Within 60 days of receiving an appeal, a controller must inform the consumer in writing of its response to the appeal, including a written explanation of the reasons for the decision.[31] If a controller denies the appeal, it must also provide the consumer with an "online mechanism, if available, or other method" through which the consumer can submit a complaint to the Virginia Attorney General.[32] The VCDPA also contains GDPR-like requirements. Namely, the VCDPA requires controllers to conduct "data protection assessments" to evaluate the risks associated with processing activities that pose a heightened risk, such as processing personal data for purposes of targeted advertising or profiling, and the controller-processor relationship must be governed by a data processing agreement.[33] In April 2022, Virginia Governor Glenn Youngkin signed into law three amendments to the VCDPA. One amendment provided that data controllers that have obtained personal data from a source other than the consumer will be deemed to be in compliance with a consumer's request to delete if they opt the consumer out of the processing of such personal data, allowing businesses to avoid potentially technically infeasible requirements to delete data, so long as they no longer use it for any purpose.[34] Another changed the definition of "nonprofit organization" to include political organizations, thus exempting such entities from the VCDPA.[35] Because the VCDPA does not allow the Attorney General to promulgate regulations, these amendments finalized the VCDPA's text ahead of its January 1, 2023 effective date, and the law is now in full effect. Enforcement of the VCDPA is entrusted to the Virginia Attorney General and subject to a 30-day cure period.[36] The Attorney General may seek injunctive relief and damages for up to $7,500 for each violation, as well as "reasonable expenses incurred in investigating and preparing the case, including attorney fees."[37] Notably, the VCDPA, unlike the CCPA/CPRA, does not grant consumers a private right of action.[38] **iii. Colorado** As discussed in a prior client alert, the CPA was enacted on July 7, 2021 and will go into effect on July 1, 2023.[39] The CPA largely follows Virginia's model. The CPA applies to any legal entity that "[c]onducts business in Colorado or produces or delivers commercial products or services that are intentionally targeted to residents of Colorado" and that:

- during a calendar year, controls, or processes the personal data of 100,000 or more Colorado consumers, or

- both derives revenue or receives discounts from selling personal data *and* processes or controls the personal data of 25,000 or more Colorado consumers.[40]

Notably, like the VCDPA (and unlike the CPRA), the statute does not include a standalone revenue threshold for determining applicability. Also of note, the CPA applies to nonprofit organizations that meet these thresholds, whereas other states' privacy laws exempt nonprofit organizations. Like the VCDPA and unlike the CPRA, the CPA does not apply to employee or B2B data. The CPA will grant Colorado consumers the right to access, correct, and delete their personal data held by entities within the scope of the law, as well as the right to data portability.[41] Following Virginia's model, it will also give Colorado consumers the right to opt out of the processing of their personal data for (a) targeted advertising, (b) sale of their personal data, and (c) certain profiling.[42] The CPA, like the CPRA, adopts a broad definition of "sale" of personal data to mean "the exchange of personal data for *monetary or other valuable* consideration by a controller to a third party."[43] However, the CPA contains some broader exemptions from the definition of "sale" than the CPRA, including for the transfer of personal data to an affiliate or to a processor or when a consumer discloses personal data by using the controller to interact with a third party or makes personal data publicly available.[44] The CPA permits consumers to communicate this opt out through technological means, such as a browser or device setting.[45] By July 1, 2024, consumers must be allowed to opt out of the sale of their data or its use for targeted advertising through a "user-selected universal opt-out mechanism."[46] Additionally, the CPA, like the VCDPA, requires businesses to obtain opt-in consent before processing consumers' sensitive data,[47] which includes children's data, genetic or biometric data, and data that could reveal race, ethnicity, religious beliefs, sexual orientation, sex life, mental or physical health conditions, or citizenship status.[48] Finally, the CPA follows Virginia's lead in requiring controllers to establish an internal appeals process for consumers when the controller does not take action on their request.[49] Like its California and Virginia counterparts, the CPA also obligates covered entities to practice data minimization and implement technical safeguards.[50] The CPA, like the VCDPA and CPRA, requires in-scope entities to conduct "data protection assessments" to evaluate the risks associated with certain processing activities that pose a heightened risk.[51] The CPA, like the VCDPA, also requires controllers and processors to contractually define their relationship.[52] The CPA permits the Colorado Attorney General to promulgate rules for the purpose of carrying out the CPA. The Colorado Attorney General's office initially published draft rules on September 30, 2022, and subsequently published revised draft rules on December 21, 2022 in response to public input gathered at several stakeholder meetings.[53] Significantly, the December revisions remove the requirement that privacy notices be centered around business purposes (rather than the categories of personal information collected), which would have conflicted with California's notice requirements and made interoperability across states difficult. The draft rules require that controllers notify consumers of "substantive or material changes" to their privacy notices. The draft rules clarify that where the CPA requires consumer consent, controllers will need to obtain such consent before January 1, 2024 in order to continue processing data collected prior to July 1, 2023. The draft rules also add a new requirement that controllers must obtain consent in order to process "sensitive data inferences[,]" which are defined as "inferences made by a [c]ontroller based on [p]ersonal [d]ata, alone or in combination with other data, which indicate an individual's racial or ethnic origin; religious beliefs; mental or physical health condition or diagnosis; sex life or sexual orientation; or citizenship or citizenship status"; provided, that controllers may process sensitive data inferences from consumers over the age of thirteen without consent if (1) the processing purposes are obvious, and (2) such inferences are deleted within 24 hours, (3) not transferred, sold, or shared with any processor, affiliates, or third parties, and (4) not processed for any purpose other than the express purpose disclosed to the consumer. Additionally, the draft rules clarify the CPA's purpose specification and secondary use provisions, and include a requirement that controllers must obtain consent before processing personal data for purposes that are not "reasonably necessary to or compatible with specified [p]rocessing purpose(s)." The draft rules also require controllers create and enforce retention schedules, including setting specific time limits for the

erasure of personal data and annually reviewing and deleting data that is no longer necessary. Comments on the draft rules will be accepted until February 1, 2023, when the Colorado Attorney General's office will hold a public rulemaking hearing (though, to be considered at the hearing, comments should have been submitted by January 18, 2023). The CPA limits enforcement to the Colorado Attorney General and state district attorneys, subject to a 60-day cure period for any alleged violation until January 1, 2025 (in contrast to the 30-day cure period under the VCDPA and the CPRA's discretionary cure period).[54] The Attorney General and district attorneys may enforce the CPA by seeking injunctive relief or civil penalties. A violation of the CPA constitutes a deceptive trade practice for purposes of the Colorado Consumer Protection Act, with violations punishable by civil penalties of up to $20,000 per violation (with a "violation" measured per consumer and per transaction).[55] The CPA's maximum penalty per violation is notably higher than that of other states' laws. **iv. Connecticut** The CTDPA,[56] which was enacted on May 10, 2022, largely follows Virginia's and Colorado's model, with very few departures of significance. The details of the CTDPA are also discussed in a prior client alert. The CTDPA will take effect at the same time as the CPA, on July 1, 2023, six months after the CPRA and VCDPA, and six months before Utah's law will take effect on December 31, 2023. The CTDPA applies to persons that conduct business in Connecticut or produce products or services that are targeted to residents of the state, and that control or process the personal data of a particular number of residents during the preceding calendar year, namely either:

- 100,000 or more Connecticut consumers, excluding consumers whose personal data is controlled or processed solely for the purpose of completing a payment transaction; or
- 25,000 or more Connecticut consumers, where the business derives more than 25% of its gross revenue from the sale of personal data.[57]

Connecticut is the only state law to explicitly carve out payment transaction data from its applicability threshold; this provision was added to alleviate concerns of restaurants, small convenience stores, and similar businesses that process the personal information of many customers for the sole purpose of completing a transaction. Like the VCDPA and CPA, and unlike the CPRA, the CTDPA defines "consumer" to exclude individuals "acting in a commercial or employment context."[58] Like its predecessors, the CTDPA will grant Colorado consumers the right to access, correct, and delete their personal data, as well as the right to data portability.[59] The CTDPA allows consumers to opt out of the processing of their personal data for purposes of (a) targeted advertising, (b) the sale of personal data, and (c) profiling in furtherance of solely automated decisions that produce similarly significant effects, following the Virginia and Connecticut models.[60] And, the CTDPA defines "sale" broadly—similar to California's CPRA and Colorado's CPA—to include "the exchange of personal data for *monetary or other valuable* consideration."[61] By January 1, 2025, data controllers must allow Connecticut consumers to exercise their opt-out right through an opt-out preference signal.[62] Unlike California, which expects its CPPA to opine on what an opt-out signal might be and how it might work, and Colorado, which expects its Attorney General to define the technical requirements of such a mechanism, Connecticut's provision is largely undefined, encouraging the market to create signals, bringing with it the potential for confusion as to what signals must be followed. The CTDPA, like Virginia's and Colorado's laws, also prohibits processing a consumer's sensitive data without consent, and requires data controllers to provide a mechanism for revoking consent that is "at least as easy as" the mechanism by which the consumer provided consent.[63] It also requires data controllers to practice data minimization and purpose limitation, implement technical safeguards, conduct data protection assessments, and enter into contracts with their processors.[64] Finally, the CTDPA follows Virginia's and Colorado's lead in requiring controllers to establish a conspicuously available internal appeals process for consumers when the controller does not take action on their request.[65] Notably, Connecticut does not include a private right of action in its law – the CTDPA limits enforcement to the Connecticut Attorney General.[66] Until December 31, 2024, enforcement actions will be subject to a 60-day cure period; thereafter, the Attorney

General may, but is not required to, provide an opportunity to correct an alleged violation.[67] A violation of the CTDPA will constitute an unfair trade practice,[68] which carries civil penalties of up to $5,000 per violation for willful offenses.[69] **v. Utah** Utah's comprehensive privacy law, unlike the other states' laws, only applies to companies that meet both a revenue threshold *and* a processing threshold. By contrast, California's law applies to companies that meet either a revenue threshold *or* a processing threshold, whereas Virginia's, Colorado's, and Connecticut's laws only contain processing thresholds. Like Virginia, Colorado, and Connecticut, Utah exempts employee and B2B data from the UCPA's scope by defining "consumer" to exclude individuals acting in "an employment or commercial context."[70] While Utah's law is similar to Virginia's, Colorado's and Connecticut's laws, it has a few differences that may make the law easier for businesses to follow. The UCPA does not provide consumers the right to opt out of the use of their personal information for profiling. Moreover, out of the five states with enacted comprehensive privacy legislation, Utah is the only state that does not grant consumers a right to correct inaccuracies in their personal data. The UCPA also does not require in-scope businesses to perform data protection assessments or require businesses to set up a mechanism for consumers to appeal a business's decision regarding the consumer's request to exercise any of their personal data rights. Utah's law also makes it easier to charge a fee when responding to consumer requests. Specifically, businesses may charge a reasonable fee when responding to consumer requests to exercise their personal data rights in California only if those requests are "manifestly unfounded or excessive[,]"[71] in Virginia only if those requests are "manifestly unfounded, excessive, or repetitive[,]"[72] and in Colorado only if a second request is made in a 12-month period.[73] By contrast, Utah allows businesses to charge a reasonable fee in those situations as well as when the business "reasonably believes the primary purpose in submitting the request was something other than exercising a right" or is harassing, disruptive, or poses an undue burden on the controller.[74] While Utah's Division of Consumer Protection can investigate potential violations, Utah's law limits enforcement to the Attorney General, subject to a 30-day cure period.[75] If the Attorney General does bring such an action, they may recover statutory damages of up to $7,500 per violation or actual damages.[76] See Appendix A for a Comprehensive State Privacy Laws Comparison Chart. **vi. Practical Implications of State Privacy Laws on AdTech Ecosystem** State privacy laws will have a particular impact for companies operating in the AdTech space. AdTech, or "advertising technology," encompasses software and tools that agencies, brands, publishers, and platforms use to target, deliver, and measure the success of ad campaigns. In practice, the AdTech ecosystem typically involves businesses leveraging products from AdTech companies and publishers to serve targeted ads to consumers as part of digital marketing campaigns. The ability to target ads to particular consumers relies heavily on the use of personal information or inferences derived therefrom. Accordingly, as the foregoing state privacy laws go into effect this year, businesses engaged in the transfer or processing of personal data for targeted ads may need to reassess their practices and provide opt-out mechanisms to remain compliant with applicable privacy laws. In particular, the CPRA requires businesses to offer consumers the ability to opt-out of the "sharing"[77] of their personal information to third parties for "cross context behavioral advertising" (which the CPRA defines as the targeting of ads to a consumer based on the consumer's personal information obtained from services other than the business in which the consumer intentionally interacts).[78] In addition, Virginia's, Colorado's, Connecticut's, and Utah's laws each require businesses to offer consumers the ability to opt out of the processing of their personal data for targeted ads.[79] Despite the minor differences in verbiage, in practice, businesses can offer consumers the ability to opt out of the "sharing" of personal information for "cross-context behavioral advertising" in California, as well as the right to opt out of "targeted advertising" to consumers in Virginia, Colorado, Utah, and Connecticut, by using the same opt-out mechanism. Notably, the privacy laws in California, Colorado, and Connecticut will also require companies to recognize and respect "universal opt-out signals"—signals that are sent to the business' website by a consumer's browser or control to communicate the individual has chosen to opt out of the sale, sharing, or use of their personal data for targeted advertising.[80] For any company engaging in targeted ads that is subject to these laws, it is important to ensure that the opt-out mechanism offered complies with the

specific requirements in the applicable state privacy law. As discussed above, California expects its CPPA to opine on what an opt-out signal might be and how it might work and Colorado expects its Attorney General to define the technical requirements of such a mechanism. By contrast, Connecticut's provision is largely undefined, encouraging the market to create signals, bringing with it the potential for confusion as to what signals must be followed. To assess whether these laws apply, businesses will need to conduct data mapping to understand data flows, data combinations, and who is processing what data, and for what purposes. **b. Other State Privacy Laws i. California Age-Appropriate Design Code Act** The California Age-Appropriate Design Code Act ("CAADCA"),[81] which is aimed at protecting the wellbeing, data, and privacy of children under the age of eighteen using online platforms, was signed into law by Governor Gavin Newsom on September 15, 2022 and will take effect on July 1, 2024. The CAADCA applies to businesses that provide any online service, product or feature "likely to be accessed by children" under the age of eighteen, and defines "likely to be accessed by children" to mean that it is reasonable to expect that the online service, product, or feature would be accessed by children under the age of eighteen, based on certain enumerated indicators.[82] The CAADCA requires businesses within its scope to comply with certain requirements, including to configure default privacy settings to offer a high level of privacy[83] and to use "clear language suited to the age of children likely to access that online service, product, or feature" in their policies.[84] The CAADCA also prohibits such businesses from profiling children or collecting, selling, sharing, or retaining children's personal information unless necessary to provide the online service, product, or feature unless the business can demonstrate that doing so is in the best interest of children.[85] The CAADCA requires a purpose limitation and further prohibits using children's personal information "in a way that the business knows, or has reason to know, is materially detrimental to the physical health, mental health, or well-being of a child."[86] The CAADCA also prohibits using dark patterns to lead or encourage children to provide personal information, forego privacy protections, or to take any action that the business knows (or has reason to know) is materially detrimental to the child's physical or mental health or well-being.[87] The CAADCA also requires that businesses within its scope complete a data protection impact assessment ("DPIA") before any new online services, products, or features that are likely to be accessed by children are offered to the public, maintain documentation of the assessment for as long as the online service, product, or feature is likely to be accessed by children, and biennially review the assessment.[88] Additionally, the business must document any "risk of material detriment to children" identified by any such DPIA and create a timed plan to mitigate or eliminate such risks before the online service, product, or feature is accessed by children.[89] Enforcement of the CAADCA is tasked to the California Attorney General, who may seek an injunction or civil penalty up to $2,500 per affected child for each negligent violation and $7,500 per affected child for each intentional violation, subject to a 90-day cure period if the business has conducted DPIAs in material compliance with the CAADCA's requirements.[90] The CAADCA is explicit that it does not provide a private right of action.[91] **ii. California's Confidentiality of Medical Information Act** On September 28, 2022, Governor Newsom signed into law Assembly Bill No. 2089,[92] which amends California's Confidentiality of Medical Information Act ("CMIA"). Specifically, AB 2089 clarifies that any business that offers a "mental health digital service" to a consumer "for the purpose of allowing the individual to manage the individual's information, or for the diagnosis, treatment, or management of a medical condition of the individual" is considered a "provider of health care" and therefore subject to the CMIA.[93] AB 2089 defines "mental health digital service" as "a mobile-based application or internet website that collects mental health application information from a consumer, markets itself as facilitating mental health services to a consumer, and uses the information to facilitate mental health services to a consumer."[94] AB 2089 also amended the definition of "medical information" to include "mental health application information[,]" which is defined as "information related to a consumer's inferred or diagnosed mental health or substance use disorder . . . collected by a mental health digital service."[95] Together, these changes expand the scope of the CMIA and strengthen protections for mental health information collected by a mental health digital service. **iii. New York Department of Financial Services' Proposed Amendments to Part 500 Cybersecurity Rules and New Guidance Related to**

Cryptocurrencies The New York State Department of Financial Services ("DFS") has also been active in the cybersecurity space, primarily through promulgation and enforcement of its Part 500 Cybersecurity Rules, which are becoming a floor that other agencies are looking to as a model regulation. As discussed in more depth in our recent client alert, DFS recently announced proposed amendments to these rules, which would increase cybersecurity oversight expectations for senior leaders, heighten technology requirements, expand the set of events covered under the mandatory 72-hour notification requirements, introduce a new 24-hour reporting requirement for ransom payments and a 30-day submission of defenses, introduce significant new requirements for business continuity and disaster recovery, and heighten annual certification and assessment requirements, among other changes.[96] Separately, DFS also issued new guidance related to cryptocurrencies, requiring virtual currency entities to monitor crypto transactions and maintain information about their customers.[97] **2. Federal Legislation**

1. **American Data Privacy and Protection Act**

While federal consumer privacy legislation has been a topic of conversation for decades, the ADPPA, introduced in 2022, marked the most successful attempt at enacting such a law. Although this bill ultimately met its end when Congress adjourned in January 2023, it provided meaningful insight and laid the groundwork for future federal data privacy laws. On June 3, 2022, leaders in the U.S. House and Senate released a discussion draft of the comprehensive federal data privacy and data security bill, the ADPPA. On June 21, the ADPPA was introduced in the House; on June 23, 2022, it passed the House Subcommittee on Consumer Protection and Commerce; and on July 20, 2022, the House Committee on Energy and Commerce voted 53-2 to advance the ADPPA to the full House.[98] Although former House Speaker Nancy Pelosi did not bring the bill to a vote on the House floor, the ADPPA advanced further than any prior bill attempting to enact comprehensive federal privacy legislation. The bill's substantial progress can be attributed to the significant bipartisan support it received when first introduced, demonstrating the widespread interest in comprehensive federal privacy legislation. The ADPPA defined "covered entity" to include "any entity or any person . . . that alone or jointly with others determines the purposes and means of collecting, processing, or transferring covered data and . . . is subject to the Federal Trade Commission Act" in addition to common carriers and nonprofit organizations.[99] With the exception of Colorado's CPA, the ADPPA's scope was notably broader than most enacted comprehensive state privacy laws, which exempt nonprofit organizations. Hallmarks of the ADPPA included a "duty of loyalty," requiring covered entities to: engage in "data minimization"; limit the collection, processing, and transferring of certain covered data to instances where there is a permissible purpose; and adopt "privacy by design" principles.[100] This was in stark contrast with the current consent-based privacy regime. Under the ADPPA, data minimization required covered entities to limit the collection, processing, or transfer of covered data to "what is reasonably necessary and proportionate" to the delineated purposes.[101] The ADPPA's duty of loyalty required covered entities to obtain "affirmative express consent" from data subjects before collecting, processing, or transferring certain personal information.[102] Finally, "privacy by design" principles required that covered entities "establish, implement, and maintain reasonable policies, practices, and procedures regarding the collection, processing, and transfer of covered data" that account for certain considerations.[103] These requirements were similar to the CPRA's data minimization and privacy by design requirements and were more prescriptive than the data minimization and privacy by design provisions outlined in the GDPR, the first regulation to implement these principles. While the GDPR offers general guidelines to ensure data minimization and privacy by design, the ADPPA outlined specific considerations covered entities should weigh along with requirements, particularly in the context of privacy by design. The ADPPA also sought to regulate how covered entities design and employ "algorithms," a term the ADPPA defined as including machine learning, artificial intelligence, and other computational processing techniques.[104] Specifically, the ADPPA stated that covered entities could not "collect, process, or transfer covered data in a manner that discriminates in or otherwise makes unavailable the equal enjoyment of goods or services on the basis of race, color, religion, national origin, sex, or

disability."[105] Furthermore, the ADPPA required "large data holders" that use algorithms to conduct "algorithm impact assessments" to evaluate how the algorithms employed by the entity use data and what outputs they produce.[106] These assessments were required to be submitted for evaluation with the FTC.[107] Federal enforcement of the ADPPA was to be left largely to the FTC, which was to be granted rulemaking authority under the Administrative Procedure Act.[108] The bill called for the creation of a "Bureau of Privacy" within the FTC to help enforce violations of the ADPPA, as well as an "Office of Business Mentorship" for covered entities to provide covered entities with guidance and education on compliance.[109] Violations of the ADPPA were to be treated as "unfair or deceptive act[s] or practice[s]" under the FTC Act.[110] The ADPPA also granted state attorneys general and states' chief consumer protection officers, or states' consumer protection agencies with expertise in data protection, the ability to bring federal civil actions to enforce the ADPPA.[111] Although the ADPPA provided for a private right of action, that provision was only to have gone into effect four years after the law's enactment.[112] This delayed private right of action was to include a requirement that potential plaintiffs notify either the FTC or their state attorney general prior to bringing suit, and those agencies would then have the discretion to intervene in such action within sixty days.[113] With entities concerned about the burden and cost of class action lawsuits, the private right of action was a sticking point for the ADPPA. Preemption was one of the most contentious aspects of the bill and was largely responsible for the end of the ADPPA's movement through the legislative process. The ADPPA explicitly preempted most state privacy legislation, including under the five comprehensive privacy statutes in California, Virginia, Colorado, Utah, and Connecticut.[114] However, both the Illinois Biometric Information Privacy Act and the Illinois Genetic Information Privacy Act would have enjoyed express preservation under the ADPPA, ensuring that they would not have been preempted.[115] Stakeholders were concerned that the ADPPA's preemption of state privacy laws would ultimately weaken protections for consumers.[116] Echoing the concerns of California lawmakers, consumers, and the California Privacy Protection Agency,[117] former Speaker Pelosi released a statement in September noting that the ADPPA "does not guarantee the same essential consumer protections as California's existing privacy laws."[118] This skepticism from former Speaker Pelosi and other lawmakers ultimately led to the waning of the ADPPA's initial support. Senator Maria Cantwell (D-Wash.), Chair of the Senate Committee on Commerce, Science, and Transportation, citing concerns about the ADPPA's enforcement loopholes and preemption, stated in June that she would not support the bill in its current form.[119] Senator Cantwell also expressed concerns with the four-year delay in the ADPPA's private right of action, indicating that she would prefer a bill that allows consumers to file suit "on day one."[120] Although it was ultimately not enacted, the ADPPA and its progress demonstrated the enormous support for a federal comprehensive privacy law in the United States and provides important context for future potential efforts to enact one. **B. Enforcement and Guidance** In 2022, several different governmental regulators were active players in enforcement and regulatory efforts related to data privacy and cybersecurity, including efforts related to regulation of artificial intelligence, commercial surveillance, financial privacy, children's and teens' privacy, and dark patterns, among others. **1. Federal Trade Commission** The Federal Trade Commission ("FTC") was a particularly active player in the regulation and enforcement of data privacy and cybersecurity in 2022. The Commission took a number of significant steps toward addressing issues related to algorithmic bias and artificial intelligence, commercial surveillance, data security, consent interfaces and dark patterns, advertising technology, and children's privacy, among others. In this section, we discuss actions the FTC took in furtherance of several of these key areas over the past year. **a. FTC Organization Updates** There were notable updates in the FTC organization in 2022. First, ending the stalemate between two Democratic and two Republican Commissioners, on May 11, 2022, Vice President Kamala Harris broke the 50-50 Senate tie to confirm Alvaro Bedoya. The FTC is headed by five Commissioners each serving a seven-year term, and no more than three Commissioners can be of the same political party. The addition of Commissioner Bedoya established the first Democratic majority at the FTC since Commissioner Rohit Chopra left the agency to lead the Consumer Financial Protection Bureau in October 2021, and is seen as a booster as Chair Lina Khan seeks to accomplish her ambitious

agency agenda. Commissioner Bedoya hails from the Center on Privacy and Technology at the Georgetown University Law Center, where he served as the founding director and a professor. At Georgetown, Commissioner Bedoya specialized in digital privacy issues, including on the intersection of privacy and civil rights, biometric software, "algorithmic discrimination," children's privacy, and data aggregation. In October 2022, Commissioner Noah Phillips, nominated by President Trump in 2018, left the FTC to return to private practice, creating a vacancy on the five-member Commission. Commissioner Phillips, together with fellow Republican Commissioner Christine Wilson (who remains a Commissioner), had questioned the direction of the Commission on a variety of issues. President Joe Biden has yet to select Phillips' successor, but is expected to defer to Senate Minority Leader Mitch McConnell to recommend a Republican candidate per tradition. The FTC lost and added several key technology and data privacy personnel in the last year. Departures include Erie Meyer (Chief Technologist), Maneesha Mithal (Associate Director of Division of Privacy and Identity Protection), and Kristin Cohen (also formerly Associate Director of Division of Privacy and Identity Protection). Additions include Olivier Sylvain (Senior Advisor on Technology to the Chair) and Stephanie Nguyen (Chief Technology Officer and expert in human-computer interaction).[121] **b. Algorithmic Bias and Artificial Intelligence** The FTC has long expressed concern about the use of artificial intelligence ("AI") and algorithms, namely that companies rely on algorithms built on incomplete or biased data sets, resulting in allegedly discriminatory practices.[122] The FTC heightened its messaging on AI and algorithmic issues in 2021, when it published a blog post warning companies that if they did not hold themselves accountable for the performance of their algorithms, the FTC would do it for them.[123] The FTC asserted its enforcement authority under three laws important to algorithm and AI regulation. First, the FTC stated that it could take action against allegedly discriminatory algorithms under Section 5 of the Federal Trade Commission Act ("FTC Act"), which prohibits unfair or deceptive acts or practices in or affecting commerce.[124] Second, the FTC cited the Fair Credit Reporting Act ("FCRA"), which prohibits certain uses of algorithms to deny employment, insurance and other benefits.[125] Finally, the FTC pointed to Equal Credit Opportunity Act ("ECOA"), which bans algorithms that introduce credit discrimination based on race, color, religion, or other protected characteristics.[126] Congress has also sparked interest in the same issues, which culminated in its 2021 directive that the FTC "study and report on whether and how artificial intelligence (AI) 'may be used to identify, remove, or take any other appropriate action necessary to address' a wide variety of specified 'online harms.'"[127] In its report, the FTC shared its concerns that algorithms and AI may be "inaccurate, biased, and discriminatory by design."[128] The report highlights three main concerns regarding the use of AI tools and how algorithms may cause more harm than they solve.

- First, the FTC stressed that algorithms and AI tools may have inherent design flaws and inaccuracies, specifically with "unrepresentative datasets, faulty classifications, failure to identify new phenomena, and lack of context and meaning."[129]
- Second, the FTC worried that AI tools are biased and will result in discriminatory outcomes. The FTC has warned that it will intervene if an algorithm results in an unfair practice, which the FTC argued includes discriminatory outcomes.[130]
- Third, the FTC considered the relationship between algorithms and commercial surveillance.[131] The FTC stated that AI tools may incentivize and enable invasive forms of surveillance and data extraction practices.

On October 19, 2022, the FTC announced its first lawsuit in which alleged discrimination was brought as a stand-alone violation of FTC Section 5. The action, in which the FTC asserted that an automotive group charged Black and Latino consumers higher fees and financing costs, could signal greater Section 5 enforcement against algorithmic discrimination in the future.[132] Notably, while the FTC has regulated AI tools and algorithms in the past, it has only done so in relation to data collection, and has yet to enforce against a company's allegedly biased or discriminatory algorithms under Section 5 of the FTC Act.[133] **c. Commercial Surveillance and Data Security i. April 2022**

Speech by FTC Chair Khan On April 11, 2022, Chair Lina Khan spoke at the International Association of Privacy Professionals ("IAPP") Global Privacy Summit. During her speech, Chair Khan spoke of the increased integration of data technologies into consumers' lives and the FTC's concern about increased data privacy risks to consumers.[134] She made clear that the FTC plans to continue using Section 5 of the FTC Act and "other statutory authorities" to "take swift and bold action."[135] Chair Khan discussed three ways that the FTC plans to approach data practices:

- First, Chair Khan stated that the FTC intends to focus on dominant firms and intermediaries that cause widespread harm. Chair Khan said that the FTC's main focus will be on firms whose actions may facilitate unlawful conduct "on a massive scale."[136]
- Second, Chair Khan shared that the FTC plans to take an interdisciplinary approach and consider how data collection and commercial surveillance intersect. Chair Khan noted that the FTC will rely on lawyers, economists, and technologists and shared that the FTC already increased the number of data scientists, engineers, user design experts, and AI researchers on its staff.[137]
- Third, Chair Khan stated that the FTC will implement "effective" remedies that "fully cure the underlying harm," which may include depriving lawbreakers of the "fruits of their misconduct."[138] She explained that remedies may include deleting ill-gotten data and destroying any derivative algorithms. This statement appears consistent with the FTC's past practices of ordering companies that allegedly engaged in improper data collection to delete their datasets and algorithms.[139]

Chair Khan also suggested ways that the FTC may "update" its approach regarding data privacy and surveillance. During the speech, she shared that the FTC was considering rulemaking to address commercial surveillance due to indications that the current frameworks addressing unlawful surveillance conduct are outdated and insufficient.[140] Chair Khan explained that she did not believe data protection should be limited to procedural protections but should include more substantive limits. At the end of her speech, she called on Congress to enact more expansive privacy legislation.[141] **ii. Rulemaking on Commercial Surveillance and Data Security** Indeed, a few months after Chair Khan's IAPP speech, the FTC initiated an Advance Notice of Proposed Rulemaking ("ANPRM") on commercial surveillance and data security.[142] The ANPRM signaled the FTC's desire to address a broad range of potential consumer harms through data asymmetry between companies and consumers, and is the first in a series of steps by the FTC that, if completed, could lead to the adoption of the first sweeping nationwide privacy regulation. The FTC sought public comment and responses to 95 separate questions related to a variety of topics related to "consumer surveillance" and "lax data security practices."[143] The FTC defined "commercial surveillance" as the "collection, aggregation, analysis, retention, transfer, or monetization of consumer data and the direct derivatives of that information," and "data security" as "breach risk mitigation, data management and retention, data minimization, and breach notification and disclosure practices."[144] Notably, the ANPRM sought information regarding the prevalence of algorithmic error, discrimination based on protected categories facilitated by algorithmic decision-making systems, and how the FTC should address algorithmic discrimination through the use of proxies.[145] The FTC hosted a virtual public forum on September 8, 2022 to solicit feedback regarding the ANPRM.[146] The FTC received over 11,000 comments before the public comment period closed on November 21, 2022. The FTC is reviewing comments and considering next steps.[147] The ANPRM will remain an important area to watch in 2023, particularly given the ADPPA's stalled progress in advance of the 118th Congress. **d. FTC's Approach to Data Security** On December 14, 2022, the FTC held a virtual Open Meeting on cybersecurity. During the Open Meeting, the Deputy Chief Technologist of the FTC, Alex Gaynor, discussed several key takeaways from FTC recent data security cases and other cyber best practices and outlined four key modern security practices that the Commission considers best practices. The Deputy Chief Technologist stated these best practices should be implemented across the board, which may suggest the agency is looking to impose these best practices as requirements,

in conjunction with its corporate surveillance ANRPM. Deputy Chief Technologist Gaynor noted that the FTC's recent orders have emphasized the use of "modern technologies to address costs" relating to data security. He identified four "modern security practices" that the FTC deems essential as highlighted in recent FTC orders over the past year, which include multifactor authentication ("MFA"), phishing resistant form of MFA for employees, encryption and authentication of all connections within company system, and compliance with data retention schedules. Adding to Deputy Chief Technologist Gaynor's presentation, Chair Khan and Commissioners highlighted accountability and administrability, as well as data minimization, as key principles behind data security orders. **e. Notable FTC Enforcement Actions** Chair Lina Khan's statement that the FTC would consider new and "effective" remedies is consistent with FTC enforcement actions in 2022.[148] Proposed and final remedies in at least four FTC enforcement actions went beyond civil penalties and included mandated security programs and, in one case, data and algorithm disgorgement. The FTC also continued to increase its collaboration with the Department of Justice's ("DOJ") Consumer Protection Branch, which litigates actions involving civil penalties on behalf of the FTC and thus has become a more frequent partner for the agency as it more frequently seeks civil penalties from defendants. Discussed below are a few of the FTC's most progressive and consequential enforcement measures of 2022.

- ***Diet and Fitness Services Company***. In March, the DOJ's Consumer Protection Branch filed a complaint on behalf of the FTC against a fitness company and its subsidiary in which it alleged the companies violated the Children's Online Privacy Protection Act ("COPPA") by collecting the personal information of children as young as eight who used the subsidiary's app to track their weight, physical activity, and food intake. The complaint alleged that the companies violated COPPA by collecting this information without providing notice to parents and retaining the information indefinitely, only deleting it when requested by a parent. The companies agreed to pay a $1.5 million civil penalty and to delete all illegally collected data, in addition to destroying any algorithm derived from the collected data.[149]
- ***Large Social Media Platform***. In March 2011, a social media company had entered into an administrative consent decree with the FTC for alleged failure to implement reasonable safeguards to prevent unauthorized access of users' personal information. Based on allegations that the company was found to have violated the consent decree, the company entered into an amended settlement with the FTC and agreed to a stipulated court order with DOJ's Consumer Protection Branch under which it agreed to pay a civil penalty of $150 million.[150] The complaint filed by the Consumer Protection Branch on behalf of the FTC alleges that the company violated the consent decree by collecting customers' phone numbers for the stated purpose of multifactor authentication and security but exploiting it to target advertisements to users.[151] As part of the new settlement, the company is required to notify users about its improper use of users' personal data and the FTC enforcement action, offer multifactor authentication options that do not require users to provide phone numbers, and implement enhanced privacy and information security programs.[152] The company is also required to obtain privacy and security assessments by an independent third party approved by the FTC, and report privacy or security incidents to the FTC within 30 days.[153] This latest settlement comes at a moment where the company is under increased scrutiny from consumer advocates and Congress. On November 17, 2022, a group of U.S. Senators wrote a letter to Chair Khan, urging the agency to investigate the company's recent changes to its verification system for potential violations of the consent decree.[154]
- ***Online Retail Platform***. On June 23, 2022, the FTC settled claims against an online retailing platform that it had lax security practices which allowed data thieves to access personal information about millions of users. As a result of the settlement, the company must (1) pay $500,000 in redress; (2) send notices to consumers about the data breach and settlement; (3) replace its current

authentication methods with multifactor authentication methods; (4) implement and maintain an Information Security Program which includes third-party security assessments; and (5) provide a redacted version of its third-party security assessments to the public.[155]

- ***Online Alcohol Marketplace***. On October 24, 2022, the FTC issued a complaint and order regarding allegations that an online alcohol marketplace company and its CEO committed certain security failures which led to a data breach exposing certain customer information.[156] The FTC placed particular emphasis on the fact that the company and its CEO were aware of the security problems two years before the breach and failed to mitigate the issues.[157] The order requires the company to (1) destroy any unnecessary personal data it collected; (2) in the future, collect only data necessary to conduct its business; and (3) implement a comprehensive information security program including security training, controls on who can access personal data, and mandatory multifactor authentication.[158] Most notably, the order also applies to the CEO, requiring him to implement an information security program at any company he moves to which collects consumer information from more than 25,000 individuals.[159]
- ***Mobile App Attribution and Analytics Company***. On August 29, 2022, the FTC filed a complaint against a mobile app attribution and mobile app analytics company, after the company itself sought a preemptive declaratory judgment that its data collection practices did not violate Section 5 of the FTC Act.[160] The complaint alleged that the company collected and sold geolocation data that could reveal consumers' visits to houses of worship, reproductive health facilities, and addiction recovery centers, among other sensitive information. The company allegedly gathered data from hundreds of millions of personal devices and sold data samples from tens of millions of these devices on publicly accessible online marketplaces.[161] In a press release, the FTC argued that the data, such as precise coordinates and a unique mobile device number, could be combined with other information, like a home address, to reveal a user's identity.[162] The FTC is seeking a permanent injunction to block further collection and sale of the identifying data by the company.[163]
- ***Education Technology Company***. On October 31, 2022, the FTC issued a complaint and order regarding numerous security breaches that led to the misappropriation of personal information of approximately 40 million consumers.[164] The FTC alleged that the named education technology company failed to take reasonable cybersecurity measures to protect the data of its users. For example, the FTC alleged that the company failed to implement two-factor authentication and failed to implement adequate encryption of sensitive customer information.[165] As a result of the violations, the company will be required to revamp its cybersecurity program as well as detail and limit its data collection, provide consumer access to data, and implement multifactor authentication.[166]
- ***Video Game Developer***. On December 19, 2022, the FTC and DOJ's Consumer Protection Branch reached the largest-ever settlement with a video game development company, under which the company agreed to pay $520 million for alleged violations of COPPA.[167] The settled complaint alleged that, despite its alleged awareness that many children played its battle royale combat game, the company proceeded to collect personal data from children without first obtaining parental consent.[168] The company also allegedly enabled default settings matching children and teens with strangers for game play, exposing them to harm.[169] Finally, the complaint also alleged the company used dark patterns to trick users into making purchases, charge account holders without their authorization, and block access to purchased content.[170] In addition to monetary penalties, the settlement requires the company "to adopt strong privacy default settings for children and teens, ensuring that voice and text communications are turned off by default."[171]

f. Financial Privacy The FTC approved changes to the Safeguards Rule in October

2021, which included more specific criteria for the safeguards financial institutions must implement as part of their information security programs. Although many provisions of the Rule went into effect 30 days after the publication of the Rule in the Federal Register, certain sections of the Rule were set to go into effect on December 9, 2022. These sections included requirements that required financial institutions to:

- designate a qualified individual to oversee their information security program;
- develop a written risk assessment;
- limit and monitor who can access sensitive customer information;
- encrypt all sensitive information;
- train security personnel;
- develop an incident response plan;
- periodically assess the security practices of service providers; and
- implement multifactor authentication or another method with equivalent protection for any individual accessing customer information.

On November 15, 2022, however, the FTC issued a press release announcing a six-month extension of the deadline for financial institutions to comply with the new provisions in the Safeguards Rule that were to become effective in December 2022. The FTC granted the extension due to reports from businesses that personnel shortages and supply chain issues would delay the necessary improvements to security systems and procedures. The new deadline for complying with certain sections is June 9, 2023.[172] **g. Children's and Teens' Privacy** During the pandemic, and as more children and families rely on technology, the FTC became increasingly focused on regulating children's data privacy through COPPA. In the last decade, the FTC has amended and expanded COPPA in an attempt to regulate the collection of kid's information online.[173] COPPA imposes requirements on operators of websites or online services regarding the collection of personal information from children under the age of 13. In a December 2021 blog post, the FTC warned that COPPA is not limited to sites and apps "directed to children," but may include companies that are not "consumer-facing."[174] The FTC stated that it will apply COPPA to sites or online services that have "actual knowledge that [they are] collecting personal information from users of another Web site or online service directed to children."[175] The deadline for comments on the COPPA rule elapsed on December 11, 2022, although the FTC's review is still ongoing.[176] The FTC's enforcement efforts through COPPA correspond with its larger goal of prioritizing investigations into violations impacting vulnerable communities. As discussed above, in the first part of 2022, the FTC settled with a weight-watching company and its subsidiary in a COPPA enforcement (*see* discussion at Section ?II.B.1.e above). The FTC also released a policy statement on May 19, 2022 (the "May Statement"), speaking to COPPA compliance and the use of education technology (also known as "Ed Tech").[177] In the May Statement, the FTC restated its intention to enforce "meaningful substantive limitations on operators' ability to collect, use, and retain children's data, and requirements to keep that data secure."[178] The May Statement set out four particular areas:

- Mandatory Collection of Data:

The FTC stated it will pay particular attention to whether companies conditioned participation on a child disclosing more information than is reasonably necessary.[179]

- Use Prohibitions:

The FTC warned COPPA-covered companies that they are strictly limited in how they can use personal information collected from children. The FTC cautioned that companies could only use the child's personal information to provide the requested online education service and that the information could not be used for any unrelated commercial

purpose.[180]

- Retention Prohibitions:

The FTC reminded companies that they could not retain personal information for longer than was reasonably necessary to fulfill the purpose for which the information was collected.[181]

- Security Requirements:

The FTC stated that COPPA requires companies to have procedures to maintain the confidentiality, security, and integrity of personal information from children.[182] The FTC further noted that it will take the position that a company is in violation of COPPA's security provisions if the company fails to take reasonable security precautions, regardless of whether an actual breach occurs.[183] In a separate post, the FTC suggested that companies provide a "non-neutral age gate" for their sites or apps, ensure that parents receive notice of the collection of their children's data, and securely and diligently destroy data when it is no longer reasonably necessary to maintain.[184] The FTC is accepting comments on a petition filed by the Center for Digital Democracy, Fairplay and other groups, asking the agency to promulgate a rule banning particular "engagement-optimizing" features targeted at minors.[185] In an Advanced Notice of Proposed Rulemaking published on August 22, 2022, the agency also asked whether commercial surveillance practices harm children and teenagers.[186] **h. Dark Patterns** On September 15, 2022, the FTC, pursuant to a request by Congress, released a report (the "Report") discussing sophisticated design practices known as "dark patterns," which can trick or manipulate consumers into buying products or services or giving up their privacy.[187] More specifically, the Report warned that certain practices may obscure consumers' data privacy choices and thus be considered dark patterns. The Report lists: (1) not allowing consumers to definitively reject data collection or use; (2) repeatedly prompting consumers to select settings they wish to avoid; (3) presenting confusing toggle settings leading consumers to make unintended privacy choices; (4) purposely obscuring consumers' privacy choices and making them difficult to access; (5) highlighting a choice that results in more information collection, while greying out the option that enables consumers to limit such practices; or (6) including default settings that maximize data collection and sharing.[188] The Report references a 2017 settlement as a "clear example."[189] The FTC had alleged that the company, a smart TV manufacturer, enabled a default setting titled "Smart Inactivity," which in effect enabled the company to collect and share consumers' television viewing activity with third parties without making it clear that it was doing so.[190] The FTC alleged that by keeping the name of the default setting vague, the company effectively removed consumers' ability to make an informed choice about their data sharing.[191] The Report warns entities employing dark patterns that the FTC will continue to take action where these practices violate the FTC Act or other statutes and regulations enforced by the FTC (e.g., the Restore Online Shoppers Confidence Act, the Telemarketing Sales Rule, the Truth in Lending Act, the Controlling the Assault of Non-Solicited Pornography and Marketing Act, the COPPA, and the Equal Credit Opportunity Act). Particularly with the backdrop of the FTC's proposed rulemaking on commercial surveillance and data security, the Report signals that the FTC will continue to take action to ensure that the notice and choices presented to consumers regarding their data are clear, easily understandable, and accessible. As evidenced by its recent enforcement actions, dark pattern activity has been a focus area of FTC enforcement.[192] **2. Consumer Financial Protection Bureau** It was a busy year for the Consumer Financial Protection Bureau ("CFPB"), with 2022 highlighting a significant expansion of the CFPB's supervisory reach and underscoring the its authority in data privacy, security, and consumer protection. As discussed below, in the first half of 2022, the CFPB signaled its intent to regulate both banking and nonbanking companies. The CFPB also continues to be interested in how AI is used in the financial services industry. In the latter half of 2022, the CFPB issued a long-awaited rulemaking on data access and portability, and reminded regulated entities about its increasing focus on potential misuse and abuse of personal financial data. **a. Regulation of Nonbank Entities** In April 2022, the CFPB announced

that it intends to invoke a largely unused legal provision of the Dodd-Frank Wall Street Reform and Consumer Protection Act of 2010 ("Dodd-Frank Act") to supervise nonbank financial companies, such as fintech and digital assets firms, that purportedly pose risk to consumers.[193] As discussed in Gibson Dunn's prior alert, the CFPB has generally used the Dodd-Frank Act to supervise only banks and credit unions.[194] However, the CFPB claimed in April that nonbank entities are subject to its supervision if the CFPB has "reasonable cause that the entity's activities pose risks to consumers."[195] The CFPB stated that reasonable cause can be based on complaints collected by the CFPB, whistleblower complaints, judicial opinions and administrative decisions, state and federal partners, or news reports. The CFPB warned nonbank companies to be prepared to respond to CFPB notices regarding unfair, deceptive, or abusive acts or practices, or practices that the CFPB believes violate federal consumer financial law.[196] In November 2022, the CFPB finalized changes to its nonbank supervision procedural rule.[197] The following month, the CFPB also proposed another rule, which would requiring nonbank entities to register with the agency if they are subject to any local, state or federal court order or regulatory enforcement orders.[198] **b. Artificial Intelligence and Algorithmic Bias** The CFPB made clear that it is paying particular attention to companies' use of AI, specifically algorithms. The CFPB cautioned that using algorithms based on biased or incomplete datasets may target highly specific demographics and violate federal consumer financial protection laws. In a February 2022 press release, CFPB Director Rohit Chopra stated that "[i]t is tempting to think that machines crunching numbers can take bias out of the equation, but they can't."[199] In 2023, the CFPB intends to regulate the use of algorithms and AI in the following ways:

- Equal Credit Opportunity Act

The Equal Credit Opportunity Act ("ECOA") prohibits discrimination in any aspect of a credit transaction. In a circular published on May 26, 2022, the CFPB asserted that the ECOA requires creditors that use complex algorithms in any part of the credit decision-making process to provide specific and accurate reasons for any adverse decisions, regardless of the level of complication or the opaqueness of the algorithms.[200] The CFPB defined an adverse action to include denying an application, terminating an existing credit account, making unfavorable changes to the terms of an existing account, and refusing to increase a credit limit.[201] In the circular, the CFPB warned companies that they "are not absolved of their legal responsibility when they let a black-box model make lending decisions" and that "[t]here is no exception for violating the law because a creditor is using technology that has not been adequately designed, tested, or understood."[202] The FTC is also responsible for ECOA enforcement and education regarding most non-bank financial service providers. In its annual summary of its ECOA enforcement activities to the CFPB, the FTC highlighted its expertise enforcing laws important to developers and users of AI, including the ECOA.[203] The FTC noted its experience with respect to big data analytics and machine learning, AI, and predictive analytics, and referred to its recent guidance on AI and algorithms, cautioning businesses to hold themselves accountable and use AI truthfully, fairly, and equitably.[204]

- Consumer Financial Protection Act

In a blog published on March 16, the CFPB stated its mandate to address and eliminate unfair practices that allegedly run afoul of the Consumer Financial Protection Act ("CFPA").[205] The CFPA prohibits unfair, deceptive, and abusive acts or practices in connection with a consumer financial product or service. In its blog, the CFPB focused on machine learning models and their alleged potential for biased outcomes. The CFPB shared its plans to regulate models that allegedly cause discriminatory harm in the financial markets, and announced changes to its examination guidelines in its "broad efforts to identify and address unfair acts and practices[.]"[206] According to the CFPB, the new guidelines encourage examiners to review any policies and practices that exclude individuals from products or services in an unfairly discriminatory manner. The CFPB stated that the new guidelines would expand the CFPB's authority to include allegedly unfair practices that are traditionally outside the scope of the ECOA.[207] On August 10,

the CFPB took action against a fintech company that used a faulty algorithm that wrongfully depleted checking accounts which led to overdraft penalties for customers. The CFPB found that the company violated the CFPA by engaging in deceptive acts or practices, required the company to pay redress to its harmed customers, and fined the company $2.7 million for its actions.[208]

- Housing Valuations

In a February 2022 article, the CFPB raised concerns regarding the use of computer models and AI to determine home valuations.[209] According to the CFPB, a home valuation is one of the most important steps in the mortgage process and inaccurate valuations put consumers at risk. The CFPB is "particularly concerned that without proper safeguards, flawed versions of [automated valuation models] could digitally redline certain neighborhoods . . . and perpetuate historical lending, wealth, and home value disparities."[210] The CFPB shared that it intends to work with its federal partners to require random sample testing and model review to ensure a high level of confidence in estimates produced by automated valuation models and algorithms. **c. Data Harvesting and Contribution** In 2022, the CFPB continued to express concerns about how companies collect, use, and share data with third parties, such as data brokers, and across product lines. The CFPB focused on a few areas where data harvesting is of particular concern:

- Algorithmic Bias

In a May press release, the CFPB raised concerns about the amount of data harvesting conducted on Americans.[211] The CFPB stated that the high quantity of data harvested gives firms the ability to know detailed information about customers before they ever interact with them. The CFPB reflected that firms use detailed datasets developed from data harvesting to run algorithms for a broad range of commercial uses.[212] Like the FTC, the CFPB worried that algorithms based on incomplete or biased datasets would harm consumers. The CFPB stated its intent to closely examine companies' automated decision-making models for potentially discriminatory outcomes, as well as the data inputs used to train and develop the models.[213] At a National Association of Attorneys General Capital Forum in December 2022, FTC Chair Khan and CFPB Director Chopra served as panelists and addressed state AGs on a number of pressing priorities, including privacy. Both panelists continued to express concerns about collection and use of data, including algorithms and automated decision-making.[214]

- Behavioral Targeting

With the growth of online commerce and electronic payment services, Director Chopra identified a particular interest of the CFPB in Big Tech companies and how they allegedly "exploit their payment platforms."[215] Director Chopra said that tech companies that seek to profit from behavioral targeting, such as targeted advertising and marketing, benefit from data related to consumer purchasing behavior. While the CFPB has studied Chinese tech giants in the past, in the last months of 2021, the CFPB included domestic tech companies in its investigations and requested data harvesting information from several large U.S. companies.[216] On August 10, the CFPB also issued an interpretive rule reminding digital marketing providers for financial firms that they must comply with federal consumer financial protection law.[217] The CFPB emphasized that digital marketers acting as service providers can be held liable under the CFPA for committing unfair, deceptive, or abusive acts or practices as well as other consumer financial protection violations.[218]

- Credit Cards and "Buy Now, Pay Later" Loans

The CFPB's concerns relate not only to data harvesting but also to data contribution and suppression. In a May 2022 blog post, the CFPB explained that companies that fail to share complete and accurate data with credit reporting companies may impact

consumers' ability to access credit at the most competitive rates.[219] The CFPB shared its concern that credit card companies are unfairly impacting consumers' credit scores by suppressing actual monthly payment amount information. The CFPB stated that it sent letters to major U.S. banks requesting information about their data sharing practices.[220] In September 2022, the CFPB also published a report with insights on the growth of the Buy Now, Pay Later ("BNPL") industry, whereby BNPL lenders offer to divide a total purchase into several equal payments, with the first due at checkout.[221] The report highlighted several areas of risk of consumer harm, including data harvesting and monetization. Specifically, the report noted the shift toward proprietary app usage, allowing BNPL lenders to harvest and monetize consumer data by building digital profiles of users' shopping preferences and behavior.[222] Director Chopra stated that the CFPB "will be working to ensure that borrowers have similar protections, regardless of whether they use a credit card or a [BNPL] loan."[223] **d. Personal Financial Data Rights Rulemaking** On October 27, 2022, the CFPB announced that it is in the process of writing a regulation to implement Section 1033 of the Dodd-Frank Act, which authorizes the CFPB to prescribe rules under which consumers may access information about themselves from their financial service providers.[224] Section 1033 requires the CFPB to balance a number of different priorities — including data privacy, consumer choice, and information security — in accordance with the process established by Congress in the Small Business Regulatory Enforcement Fairness Act ("SBREFA"). The CFPB released an outline that provides proposals and alternatives under consideration for the proposed data rights rulemaking.[225] According to Director Chopra, the rulemaking "has the potential to jumpstart competition, giving Americans new options for financial products"[226] and "explor[es] safeguards to prevent excessive control or monopolization by one, or even a handful of, firms."[227] The CFPB plans to publish a report on input received through the SBREFA process in the first quarter of 2023, issue the proposed rule later in 2023, and finalize and implement the rule in 2024.[228] The CFPB's approach to consumer data here is novel, and once adopted, the rule will significantly impact banks and fintech companies in the consumer financial data sharing industry. **e. Data Security** In the second half of 2022, the CFPB reminded companies that it is a data security regulator. In August, the CFPB confirmed in a circular that financial companies may violate federal consumer financial protection law when they fail to safeguard consumer data.[229] The published circular provided examples where the failure to implement certain data security measures might increase the risk that a firm's conduct triggers liability under the CFPA.[230] These measures include multi-factor authentication, adequate password management, and timely software updates. More recently, the CFPB published a new bulletin analyzing rise in crypto-asset complaints.[231] The bulletin identified several common risk themes, including hacks by malicious actors. **3. Securities and Exchange Commission** In 2022, the Securities and Exchange Commission ("SEC") emphasized the importance of transparency in cybersecurity risks and incidents. This goal of increased transparency was evident in the SEC's proposed rules in February and March, which would impose stricter cybersecurity disclosure and reporting requirements. Subsequently, the SEC announced that it would double the size of its Crypto Assets and Cyber Unit, which was followed by several enforcement actions by this unit. The increase in enforcement resources, in combination with the likely promulgation of final cybersecurity rules, signal that this will likely be an area of heightened enforcement activity for the SEC in 2023. **a. Regulation**

- February 2022 Proposed Rules for Registered Investment Advisers, Registered Investment Companies, and Business Development Companies

On February 9, 2022, the SEC proposed cybersecurity rules for registered investment advisers, registered investment companies, and business development companies.[232] The key requirements of the proposed rules are policies and procedures, reporting, disclosures, and recordkeeping. The rules would require advisers and funds to implement new "policies and procedures reasonably designed to address cybersecurity risks."[233] The SEC specifies that these policies and procedures should cover risk assessments, user security and access, protection of information, threat and vulnerability management, and incident response and recovery.[234] Investors and funds would be required to review

their policies and procedures at least annually and to provide the SEC with a written report of the review.[235] The new rules would also mandate reporting "significant cybersecurity incidents" to the SEC, including those on behalf of a fund or private fund client, and to disclose cybersecurity risks and incidents to clients and prospective clients.[236] This information about cybersecurity incidents and risks should also factor into risk disclosures in fund registration statements under the proposed rule.[237] Finally, the proposed rules impose new recordkeeping requirements for records related to cybersecurity risk management, cyber incidents, and policies and procedures.[238] Commissioner Peirce released a dissenting statement.[239] She explained that although she is in favor of establishing a cybersecurity reporting system, she would advocate for a public-private partnership system rather than the traditional regulation-examination-enforcement regime. In the SEC's rulemaking agenda, which was recently published by the Office of Information and Regulatory Affairs,[240] the agency indicated that it will take final action on the proposed rule in April of 2023.[241]

- March 2022 Proposed Rules for Public Companies

On March 9, 2022, as reported in detail in Gibson Dunn's prior client alert, the SEC proposed new cybersecurity disclosure rules for public companies. These rules would require (i) current reporting of material cybersecurity incidents and (ii) periodic reporting of material updates to cybersecurity incidents, risk management, strategy, governance, and expertise.[242] Reporting Material Cybersecurity Incidents The proposed rules would require disclosure of any "material cybersecurity incident" within four business days of the determination that the company has experienced a "material cybersecurity incident."[243] The SEC will not permit reporting delays, even in the case of an ongoing investigation.[244] The required disclosure includes: (1) when the incident was discovered and whether it is ongoing; (2) a description of the nature and scope of the incident; (3) whether data was accessed, altered, stolen, or used for any unauthorized purpose; (4) the incident's effect on operations; and (5) whether the company has remediated or is remediating.[245] Periodic Reporting Requirements The proposed rules would also require periodic reporting of material updates to cybersecurity incidents, as well as the company's cybersecurity risk management, strategy, governance, and expertise.

- Material Updates to Cybersecurity Incidents: Companies would be required to disclose any material changes to information required to be disclosed pursuant to proposed Item 1.05 of Form 8-K in the company's Form 10-Q or Form 10-K for the covered period in which the material change occurred.[246] Item 106(d) would also require companies to disclose when previously undisclosed individually immaterial cybersecurity incidents became material in the aggregate.[247]
- Risk Management and Strategy: Companies would be required to disclose their policies and procedures, as relevant to identifying and managing cybersecurity risks and threats.
- Governance: The proposed Item 106(c) of Regulation S-K would require companies to disclose the role of the board of directors and management in cybersecurity governance.
- Board of Directors' Cybersecurity Expertise: Under proposed Item 407(j) of Regulation S-K, companies would be required to annually disclose any cybersecurity expertise of their directors.
- Foreign Private Issuers: Comparable changes to require similar disclosures on an annual basis on Form 20-F.[248]

Commissioner Peirce again dissented. She generally objected to her colleagues' approach as going beyond the SEC's limited role by effectively setting forth expectations for what cybersecurity programs should look like.[249] She also voiced a specific objection to the lack of a cyber incident reporting delay, in particular, in cases where there is cooperation with law enforcement. The agency plans to take final action on this proposed rule in April 2023.[250]

- Anticipated 2023 Rules

In addition to likely finalizing the cyber rules from February and March 2022, we anticipate that additional data privacy and security rules are forthcoming. In a January 2022 speech, SEC Chair Gary Gensler suggested that "customer and client data privacy and personal information" is the "next arena."[251] He noted that "there may be opportunities to modernize and expand" Regulation S-P, which was adopted more than two decades ago and requires companies to implement policies and procedures for the protection of customer records and information.[252] He mentioned that he had asked SEC staff for recommendations on certain related issues, and thus, a data privacy-oriented rule may be issued in 2023. Gensler revisited the possibility of new rules related to modernizing Regulation S-P in his remarks to the Financial and Banking Information Infrastructure Committee and the Financial Services Sector Coordination Council in April. He noted that new rules would likely "require breach notifications when a customer's information is accessed without authorization."[253] In these remarks, Gensler also stated that the agency is considering additional cybersecurity rules. First, Gensler mentioned the possibility of issuing rules similar to the February 2022 proposed rules, but for broker-dealers. Second, he discussed updating Regulation Systems Compliance and Integrity ("SCI") to cover a broader range of entities and strengthening it to "shore up the cyber hygiene" of covered entities.[254] Finally, Gensler indicated that the SEC was considering how it can further address cybersecurity risks that come from service providers in the financial sector. The SEC's rulemaking agenda signals that at least some of Gensler's plans may take shape in the form of proposed rules early as April of 2023. The agency previewed that it is considering proposing rules "to address registrant cybersecurity risk and related disclosures, amendments to Regulation S-P and Regulation SCI, and other enhancements related to the cybersecurity and resiliency of certain Commission registrants."[255] **b. Enforcement** In addition to the proposed rules, the SEC signaled its intent to regulate companies through enforcement by nearly doubling the size of its Crypto Assets and Cyber Unit (formerly known as the Cyber Unit).[256] This expansion will better equip the SEC to police wrongdoing in crypto markets and to identify cybersecurity disclosure and control issues.[257] Since this announcement, the unit has been highly active in investigating and charging crypto-related issues.[258] The SEC has taken on some of the bigger industry players in the last year. In February, the SEC fined a crypto lending company $100 million based on registration failures.[259] Later, in October, the SEC settled charges against Kim Kardashian for $1.26 million after she publicly endorsed tokens without disclosing the $250,000 she received in exchange for the promotion.[260] The SEC wrapped up 2022 with much publicized charges against the former CEO and co-founder of a major cryptocurrency exchange and hedge fund for violations of the anti-fraud provisions of the Securities Act of 1933 and the Securities Exchange Act of 1934.[261] These charges were brought in parallel with the U.S. Attorney's Office for the Southern District of New York and the Commodities Futures Trading Commission and were quickly followed by charges against two other former leaders at the companies, who are cooperating with the investigation.[262] Much of the SEC's crypto agenda going forward will hinge on the outcome in the SEC's lawsuit against another cryptocurrency company for allegedly selling unregistered securities. The SEC and that cryptocurrency company submitted the final reply briefs for summary judgment in December 2022, which will potentially answer the question of whether one of the company's tokens is a security.[263] As of the time of this report, no court date had been set for oral argument on the motions or for trial. In addition to the numerous crypto enforcement actions, the FTC has announced a few actions related to data privacy and security. In late July, the SEC charged certain financial institutions with violations of the SEC's Identity Theft Red Flags Rule or Regulation S-ID, based on deficiencies in their identity theft prevention programs.[264] They agreed to pay penalties of $1.2 million, $925,000, and $425,000, respectively, and to cease and desist from future violations of Regulation S-ID.[265] Shortly thereafter, in August, the SEC announced that it had filed charges against three individuals who allegedly tipped and traded information about a credit reporting agency's 2017 data breach in advance of the public announcement of the breach.[266] Then, in September, the SEC announced charges against and a settlement with a different financial institution. The SEC alleged that the institution failed to protect the personal

identifying information of 15 million consumers over a five-year period, and without admitting or denying these allegations, it consented to the SEC's order finding that the firm violated certain rules under Regulation S-P and agreed to pay a $35 million fine.[267] Once the final cybersecurity rules are implemented, likely in 2023, we expect to see additional enforcement in this area. **4. Department of Health and Human Services and HIPAA a. Rulemaking on HIPAA Compliance and Data Breaches** The Department of Health and Human Services ("HHS") embarked on rulemaking in November 2022 to relax administrative hurdles around patient substance abuse records, as required by the Coronavirus Aid, Relief, and Economic Security Act ("CARES" Act).[268] The proposal would harmonize regulations related to patient substance abuse records that differ from the privacy and data-breach requirements of the Health Insurance Portability and Accountability Act ("HIPAA") and its related regulations.[269] Most notably, the notice explains that the proposed rule would (1) make it easier for providers to share substance abuse records with other providers by requiring only single patient consent, and (2) give HHS enforcement authority over violations of the substance-abuse regulations.[270] HHS Secretary Xavier Becerra explained that the rule would both improve care coordination among providers and strengthen privacy protections so patients can seek treatment without worrying that their substance abuse records will be improperly disclosed.[271] Separately, HHS's Office of Civil Rights ("OCR") is considering whether to conduct new cybersecurity rulemaking, as it published a request for information ("RFI") in April 2022 under the Health Information Technology for Economic and Clinical Health Act of 2009 ("HITECH" Act).[272] OCR asked for feedback on whether it should consider recognized cybersecurity measures when assessing fines and other remedies for data breaches, as well as whether it should consider distributing any penalties it receives to the individuals' whose protected health information ("PHI") was compromised. [273] The RFI comes as data breaches involving unsecured PHI are on the rise, according to a U.S. Government Accountability Office ("GAO") report.[274] Now that the comment period has closed, OCR is weighing whether to issue future guidance or rulemaking on this issue.[275] **b. Telehealth and Data Security Guidance** Three years into the coronavirus pandemic, HHS has yet to signal that it is preparing to transition to a post-pandemic world. Due to the pandemic, rules on telehealth services were relaxed to provide more flexibility amidst the declared "Public Health Emergency" ("PHE").[276] However, HHS has continued to extend the emergency status, which keeps in place its pandemic-era enforcement discretion surrounding telehealth that would expire alongside the PHE.[277] At the time of publishing this Review, the Biden Administration has continued to extend the PHE but has signaled it may want to end it in the spring.[278] Meanwhile, HHS has explained that some telehealth practices can continue even after the end of the eventual end of the PHE, publishing guidance in June 2022 to clarify how covered entities may continue to provide telehealth services.[279] HHS noted that the HIPAA Privacy Rule does not apply to audio-only telehealth over a standard landline, but there are compliance considerations when data is transmitted electronically, such as through voice over internet protocol ("VoIP") or on smartphone applications.[280] The increasing use of technology for remote access of health-related information continues to be an administration priority. For example, in June 2022, the White House convened government officials to discuss cybersecurity threats in the health-care space.[281] And in guidance issued in December 2022, OCR reminded covered entities and their vendors that HIPAA rules related to privacy and disclosure apply to technologies used to track a user's interactions with an app or website if the data collected includes protected health information.[282] **c. Reproductive and Sexual Health Data** Another recent focus of HHS has been educating the public and addressing concerns with state law enforcement access to health-care data, particularly as it relates to sexual and reproductive health. Following Texas Governor Greg Abbott's order for Texas officials to open child abuse investigations concerning transgender children receiving gender-affirming care,[283] including with guidance that clarified that HIPAA prohibits the disclosure of gender affirming care in most situations, among other recommendations.[284] But a federal district court in Texas later vacated that guidance—although it did not mention HIPAA—because it found that government officials "appear to misstate the law and do not detail what went into their decision-making."[285] Following the Supreme Court's June 2022 ruling in *Dobbs v. Jackson Women's Health Org.*, which reversed *Roe v. Wade* (1973) and ended federal protection for abortion

access,[286] HHS also issued guidance clarifying the protections regarding reproductive-health data and educating the public on the limits of those protections, such as the limitations on disclosing PHI to law enforcement.[287] More actions may be forthcoming as OCR Director Melanie Fontes Rainer[288] said in the wake of the ruling that "all options are on the table" as OCR considers additional ways to respond to *Dobbs*.[289] **d. HHS Enforcement Actions** OCR has continued to enforce the HIPAA Privacy Rule through actions targeting medical-records access, PHI security, and data breaches. These efforts include OCR's continued push to bring cases under its HIPAA Right of Access Initiative to encourage compliance with the HIPAA Privacy Rule's provision giving individuals the right to access their health records. For example, OCR announced in July 2022 that it had resolved eleven investigations involving such access,[290] and another three in September 2022, bringing the total number of cases under the initiative to 41.[291] These enforcement actions resulted in settlements that ranged from $3,500 to $240,000 and were brought against entities varying in size from local one-office practices to a regional health-care providers operating 17 different hospitals.[292] OCR has also settled several cases involving improper disclosure and disposal of PHI. In August 2022, a dermatology practice agreed to pay more than $300,000 for putting empty specimen containers that had labels with patient information in the garbage bin in the practice's parking lot, an alleged violation of the HIPAA Privacy Rule's requirements to safeguard the privacy of patient information.[293] In March 2022, OCR also settled with a dental practice that used patients' names and addresses in campaign literature for the dentist's Alabama state senate campaign.[294] OCR also settled with several dental practices throughout the year that disclosed PHI in response to online reviews of their dental practices.[295] Further, in July 2022, OCR announced a settlement with a state university's health sciences department following a data breach where a hacker gained access to an university web server containing electronic PHI of 279,865 individuals. The university agree to pay $875,000 for not implementing proper security measures, conducting an appropriate investigation, or timely notifying HHS of the breach.[296] OCR intends these enforcement actions to serve as cautionary tales for others. OCR Director Fontes Rainer warned after a recent settlement, "OCR is sending a clear message to regulated entities that they must appropriately safeguard patients' protected health information. We take complaints about potential HIPAA violations seriously, no matter how large or small the organization."[297]

5. Other Federal Agencies **a. Department of Homeland Security** The Department of Homeland Security ("DHS") continued the cybersecurity "sprints" initiative it launched in 2021, with international cybersecurity as the designated focus for the first quarter of 2022.[298] The international cybersecurity sprint included efforts to strengthen collaboration and cooperation with law enforcement partners around the world, build domestic and international capacity to defend against cyberattacks, and combat transnational cybercrimes. In February 2022, pursuant to President Biden's Executive Order on Improving the Nation's Cybersecurity, DHS established the Cyber Safety Review Board ("CSRB"), a public-private advisory board tasked with reviewing and assessing "significant cybersecurity events so that government, industry, and the broader security community can better protect [the] nation's networks and infrastructure."[299] The unique public-private composition of the CSRB reflects the Biden Administration's acknowledgment that much of the U.S.'s critical infrastructure is owned and operated by the private sector, and thus has a crucial role in preventing and addressing cybersecurity threats. In its inaugural year, the CSRB issued its first report on a major cybersecurity incident and launched a review of a second incident. In July 2022, the CSRB released a report addressing the Apache Log4j vulnerabilities discovered in late 2021; Log4j, a widely used logging framework among Java developers, had vulnerabilities that enabled cyberattackers to execute malicious code or extract data. The report made 19 recommendations for industry and government entities to prevent and respond more effectively to future incidents.[300] In December 2022, the CSRB announced its review of the prolific international hacker group Lapsus$, which has reportedly targeted major corporations and government agencies around the world in extortion attacks since 2021.[301] As required by the Cyber Incident Reporting for Critical Infrastructure Act of 2022 ("CIRCIA"),[302] DHS's Cybersecurity and Infrastructure Security Agency ("CISA") published a Notice of Proposed Rulemaking in September 2022 regarding CIRCIA's new reporting requirements for cyber incidents and ransom payments.[303] CISA sought public

feedback on a range of topics, including which entities are covered by the requirements, the types of substantial cyber incidents that CIRCIA covers, data preservation, and the manner, timing, and form of reports. CISA subsequently hosted a series of public listening sessions from September through November 2022 to receive input on the forthcoming proposed regulations.[304] The CISA Cybersecurity Advisory Committee also reserved a portion of its quarterly meeting held in December 2022 for public comment.[305] Under the CIRCIA, the final rule must be issued by March 2024 (within 18 months of the Notice of Proposed Rulemaking).[306] Further analysis of the CIRCIA and ongoing considerations was reported in detail in Gibson Dunn's recent alert on the act.[307] **b. Department of Justice** The DOJ continued to enhance and expand its capacity to prevent and respond to malicious cyber activity, including through the work of the Civil Cyber-Fraud Initiative ("CCFI") and the Ransomware and Digital Extortion Task Force. The DOJ also adapted its enforcement priorities in light of the Biden Administration's focus on preventing corruption. The CCFI, launched by Deputy Attorney General Monaco in 2021, demonstrates the DOJ's willingness to deploy civil enforcement tools to prevent cybersecurity-related fraud.[308] The initiative seeks to "hold accountable entities or individuals that put U.S. information or systems at risk by knowingly providing deficient cybersecurity products or services, knowingly misrepresenting their cybersecurity practices or protocols, or knowingly violating obligations to monitor and report cybersecurity incidents and breaches."[309] The CCFI plans to utilize the False Claims Act, including its whistleblower provision, to pursue cybersecurity fraud by government contractors and grantees.[310] In March 2022, the DOJ reached its first settlement under this initiative—for $930,000—in a case involving a medical services contractor who allegedly failed to securely store medical records as required in contracts with the Air Force and State Department.[311] In the second settlement under this initiative, a defense contractor agreed to pay $9 million to resolve allegations that it made misrepresentations regarding its compliance with cybersecurity requirements outlined in federal contracts.[312] The DOJ is poised to continue this trend of pursuing enforcement actions against companies that have received federal funds and failed to adhere to cybersecurity standards to protect and secure data. In 2021, the Biden Administration declared that the government's fight against corruption was a core national security interest.[313] Curbing illicit finance was designated as a pillar of the U.S.'s anti-corruption program.[314] Given this focus, the DOJ will likely increase its enforcement efforts in the coming years on foreign bribery, the illicit use and laundering of cryptocurrency, and ransomware and digital extortion, among other areas. In response to the global proliferation of ransomware attacks on companies and government entities, as well as the increased scope of damage caused by such attacks, the Biden Administration created the Ransomware and Digital Extortion Task Force within the DOJ.[315] In addition to actively investigating hundreds of ransomware variants and ransomware groups, over the past year, the DOJ has successfully recovered portions of ransom payments made in high-profile attacks by domestic and foreign hackers.[316] In May 2022, the DOJ clarified its priorities for prosecutions under the Computer Fraud and Abuse Act ("CFAA"). The DOJ formally recognized non-prosecution of ethical security hackers hired to identify system vulnerabilities (commonly referred to as "white hat" hackers) who are conducting "good faith security research" which includes "accessing a computer solely for purposes of good-faith testing, investigation, and/or correction of a security flaw or vulnerability."[317] The DOJ also clarified that it will not seek to charge a number of other hypothetical CFAA violations, such as using a pseudonym on a social networking site that prohibits them, checking sports scores or paying bills online while at work, or embellishing online dating profiles contrary to the site's terms of service.[318] Under this new policy, the DOJ intends to focus its resources on cases where a defendant was either not authorized at all to access a computer, or was authorized to access part of a computer but knowingly accessed a part of the computer to which the authorized access did not extend.[319] Although the DOJ is unlikely to target private companies for enforcement in cyberattacks, companies should be prepared to face increased pressure to report cyberattacks, share information, and take swift and appropriate action to prevent these attacks. **c. Department of Energy** In June 2022, the Department of Energy ("DOE") released its National Cyber-Informed Engineering Strategy, which provides a framework to protect the nation's energy infrastructure by incorporating cybersecurity measures into the engineering and design stage of grid development.[320] The DOE

guidance emphasizes building cybersecurity measures into infrastructure early in the design lifecycle, instead of attempting expensive, potentially less-effective aftermarket bolt-on efforts.[321] The strategy also focuses on reducing disruptions of critical energy infrastructure even if a cyberattack is successful.[322] The DOE released a report and recommendations on the cybersecurity of distributed energy resources ("DER"), such as distributed solar, wind, and other clean energy technologies.[323] The study found that while a cyberattack on DER systems would likely have a negligible impact on grid reliability, as the use of DER systems rapidly grows and evolves, cybersecurity must be taken into consideration. The report makes policy recommendations for decisionmakers and provides strategies for DER operators and electric power entities to make the nation's power grids more secure. **d. Joint Agency Actions Regarding Banking Cybersecurity** The Office of the Comptroller of the Currency ("OCC"), the Federal Reserve System, and the Federal Deposit Insurance Corporation ("FDIC") issued a joint rule for banking organizations and bank service providers regarding computer-security incident notifications.[324] The application of the rule varies slightly depending on the regulating agency.[325] The rule requires organizations to report cyber incidents to its primary federal regulator within 36 hours of determining a notification incident occurred, and to inform affected customers of an incident in certain situations.[326] At the recommendation of the Government Accountability Office, the Treasury Department's Federal Insurance Office ("FIO") and the DHS's CISA are conducting a joint assessment of whether there should be a federal insurance response to catastrophic cyber incidents, and potential structures for a federal insurance response.[327] The agencies issued a request for comments in September 2022 to gather public input on a range of topics, including what cyber incidents could have a catastrophic effect on critical infrastructure, how to measure the financial impact of catastrophic cyber incidents, which types of cyber incidents should warrant a federal insurance response, and how to structure a federal insurance response for catastrophic cyber incidents.[328] The FIO and CISA will report the results of its joint assessment to Congress in order to inform deliberations on the merits of a federal insurance response to catastrophic cyber incidents.[329] **e. Department of Commerce AI Initiative** The U.S. Department of Commerce announced the appointment of 27 committee members who were nominated by the public to the National Artificial Intelligence Advisory Committee ("NAIAC") in April 2022.[330] The NAIAC's role is to ensure the U.S. "leads the world in the ethical development and adoption of AI, provides inclusive employment and education opportunities for the American public, and protects civil rights and civil liberties in our digital age."[331] The NAIAC will advise President Biden on AI-related issues, including bias, security of data, the use of AI for security or law enforcement, and whether AI use is consistent with privacy rights, civil rights, civil liberties, and disability rights.[332] The NAIAC held open meetings in May and October 2022 to discuss topics such as the competitiveness of U.S. AI, the science around AI, the potential use of AI for workforce training and government operations, oversight of AI systems, and the adequacy of addressing societal issues with AI.[333] The NAIAC is required to submit a report with its findings and recommendations to President Biden and Congress after its first year, and to submit subsequent reports no less than every three years.[334] **6. State Agencies** State privacy enforcers wielded their considerable authority with decisiveness and creativity in 2022, capping the year with the largest multistate privacy settlement in United States history. **a. National Association of Attorneys General** The National Association of Attorneys General ("NAAG") launched the Center for Cyber and Technology to help state attorneys general "in understanding technical aspects of emerging and evolving technologies, conducting cybercrime investigations and prosecutions, and ensuring secure and resilient public and private sector networks and infrastructure."[335] The Center will also work to form strategic partnerships with government agencies, nonprofits, and private sector entities to focus on cyber-related issues.[336] On December 12, 2022, the NAAG sent a letter to the Federal Communications Commission ("FCC") on behalf of 51 state and territory attorneys general expressing their support for more stringent protections against robotexts, citing a slew of consumer complaints concerning unwanted text messages.[337] The NAAG also sent a letter signed by 41 state attorneys general to the FCC commending the agency's commitment to stopping robocalls.[338] Most of the signing states have committed to information sharing agreements with the FCC to combat robocalls, and those states that

have yet to enter any agreements have signaled a good faith effort to do so.[339] **b. State AGs' Reaction to *Dobbs*** Just as the Supreme Court's June 2022 ruling in *Dobbs v. Jackson Women's Health Org.* set off a flurry of activity at HHS in regards to protecting health and reproductive data, several states have also reacted swiftly in response to the decision. A coalition of 22 state attorneys general issued a statement committing to use the full force of the law to support those seeking abortions.[340] Conversely, other states have embraced the Court's ruling.[341] State attorneys general have pressured technology companies in different directions. For example, the California Attorney General issued a statement warning companies of the consequences for failing to protect reproductive health information, emphasizing the heightened security and confidentiality obligations associated with the California Confidentiality of Medical Information Act.[342] He also sponsored a first-in-the-nation law, passed by the California State Legislature, that prohibits technology companies from responding to out-of-state search warrants for private reproductive health data.[343] On the other side of the spectrum, a coalition of 17 Republican state attorneys general wrote to another large tech company to threaten legal action if it suppresses anti-abortion pregnancy centers in response to political pressure.[344] **c. State AG Letter on National Consumer Privacy Laws** On July 19, 2022, a coalition of ten state attorneys general, led by California Attorney General Rob Bonta, wrote Congress to demand that any national consumer privacy law not preempt state legislation, urging that a national law should set a floor, not a ceiling, for privacy regulation.[345] The states cited HIPAA as a model for its provision giving states concurrent enforcement authority and only preempting "contrary" state laws.[346] The letter cited the need to adapt to a fast-paced, rapidly changing industry with appropriate regulation to protect consumer privacy rights.[347] **d. Dark Patterns** State agencies have shared the FTC's and Congress' concern over "dark patterns." For example, the New York Attorney General's Office secured $2.6 million in disgorged profits from an online travel company for use of deceptive online advertising including the use of "dark patterns," or "nefarious tactics . . . used to manipulate and trick consumers into buying goods or services."[348] Overstating user control of privacy settings can also potentially constitute a "dark pattern," and can lead to regulatory action. On November 14, 2022, a coalition of 40 state attorneys general reported a $394 million settlement with a major tech company for allegedly misrepresenting the level of user control over location history collection.[349] It is the largest multistate settlement in history, and requires the company to be more transparent to users about its location tracking practices.[350] In addition to the multistate suit, the company defended against similar allegations in several other state actions. As reported in Section I.A of our 2021 annual review, the Arizona Attorney General filed a complaint focused on misconduct in its collection of location data.[351] In October 2022, the technology company settled with Arizona for $85 million.[352] And in January 2022, the District of Columbia, which did not join the previous settlement, brought a separate lawsuit against the same large tech company, again for allegedly manipulating users with "dark patterns" to track and collect their location history.[353] According to the complaint, the company allegedly misled users to believe that they could protect their location privacy by changing their account and device settings; however, it was extremely difficult to limit location tracking.[354] Attorneys General of Texas, Washington, and Indiana also have pending lawsuits on similar issue.[355] All investigation and proceedings originated from an AP story revealing the company's location tracking practices.[356] **e. Other State AG Actions** Large tech companies have become the targets of data privacy-related lawsuits and investigations from attorneys general on both sides of the aisle, who have asserted legal theories ranging from deceptive practices to unauthorized collection of biometric data. The Texas, California, and New York attorneys general have been particularly active. This February, Texas Attorney General Ken Paxton launched a suit against a large social media company under Texas' Capture or Use of Biometric Identifier Act alleging illegal capture and use of biometric data retrieved from uploaded photos and videos.[357] Paxton is also bringing data privacy-related lawsuits under Texas' Deceptive Trade Practices Act; for instance, in May of 2022, he amended a suit against a large tech company to allege that its web browser's "Incognito Mode" falsely implies to consumers that their data is not being tracked.[358] California Attorney General Rob Bonta is also targeting businesses that have loyalty programs that may violate the California Consumer Privacy Act.[359] Further analysis of California's enforcement policies related to customer

loyalty programs can be found in Gibson Dunn's prior alert.[360] This spring, the California Attorney General's office released an opinion paper indicating that, under the California Consumer Privacy Act, a consumer's right know information a business has collected on that consumer includes internal inferences or "characteristic[s] deduced about a consumer."[361] On August 24, 2022, Bonta announced the first settlement under the CCPA, resolving allegations against a large retailer of beauty products that it failed to disclose it was selling consumers' personal information and that it neglected to process requests to opt out of data sales.[362] The retailer agreed to $1.2 million in penalties and to provide streamlined procedures for opting out of the sale of personal information, including a requirement to honor user-enabled global privacy controls.[363] Bonta emphasized he is "committed to the robust enforcement of California's groundbreaking data privacy law."[364] The New York Attorney General's Office often sets the tone for attorneys general across the country, increasingly bringing high-profile actions alongside federal regulators, as covered in more detail in Gibson Dunn's recent alert.[365] The New York Attorney General stated that internet-related issues were the number one source of consumer complaints to the office in 2021, and the area is a key focus for enforcement actions.[366] New York Attorney General Letitia James kicked off 2022 by announcing that an investigation into credential stuffing resulted in 17 affected companies taking steps to protect consumers.[367] Her office announced a $600,000 settlement with a medical company following a data breach at the company that allegedly compromised 2.1 million customers' information.[368] Another data breach settlement was entered with a grocery retailer, requiring $400,000 in penalties along with protective measures, based on allegations that the company exposed the sensitive information of more than 3 million customers, including over 830,000 New Yorkers.[369] The New York Attorney General's office was also part of an agreement along with 45 other states to settle with a major cruise line company for $1.25 million after a 2019 data breach at the company allegedly compromised the information of 180,000 employees and customers.[370] **f. New York Department of Financial Services** The New York State DFS has also been active in enforcing of its Part 500 Cybersecurity Rules, effective beginning in 2019. For example, the same major cruise line company referenced above was subject to a $5 million penalty—separate from the one imposed by the New York Attorney General, discussed above—from DFS for violating its Cybersecurity Regulation for failing to timely report its 2019 and 2021 data breaches, and for failing to implement Multi-Factor Authentication and adequate cybersecurity training, all of which rendered improper its cybersecurity compliance certifications.[371] In step with enforcement of its cybersecurity rules, DFS has been at the vanguard of regulation of virtual currencies. In August 2022, DFS announced another settlement, a $30 million penalty against a young cryptocurrency exchange based on allegations that the company was not compliant with cybersecurity and transaction monitoring requirements and improperly certified its compliance with the DFS regulations, including the Part 500 Cybersecurity Rules.[372] **III. Civil Litigation Regarding Privacy and Data Security A. Data Breach Litigation** Cybercrimes targeting consumer data are increasingly pervasive according the Identity Theft Resource Center ("ITRC") which compiles statistical information on data breaches. The ITRC reported that 2021 featured almost 2,000 data breaches, a record-breaking number and a more than 68% increase over 2020 and 23% increase over the previous record reached in 2017.[373] Nearly 50% of data breach victims in 2022 were affected by breaches at just two companies, with 23 million consumers affected when a major telecommunications company suffered a data breach and 69 million consumers affected when a virtual game site was hacked.[374] These trends signify that the business community will continue to contend with increasingly aggressive attacks by cybercriminals and litigation by affected consumers and shareholders while simultaneously grappling with the evolving legal landscape surrounding data security. **1. Standing Implications of *TransUnion v. Ramirez*** Data breach litigation often takes the form of federal class actions due to the number of affected consumers, and the uniform administration of federal rather than state class actions under the Class Action Fairness Act. Data breach litigants pursuing claims against data custodians in federal court are subject to the standing requirements of Article III of the U.S. Constitution. In 2021, the U.S. Supreme Court decided *TransUnion v. Ramirez*, a landmark decision increasing the burden on plaintiffs to demonstrate standing in actions for money damages brought in federal court.[375] The Court held that the risk of future harm was insufficient to

establish the concrete injury required for standing under Article III, especially where the plaintiff was unaware of the risk of future harm.[376] This decision has the potential to seriously affect plaintiffs whose data has been breached but not yet misused. Prior to the Supreme Court's decision in *TransUnion*, circuit courts had differing interpretations on whether the increased risk of future harm resulting from a data breach was sufficient to constitute a "concrete and particularized and actual or imminent" harm as required to establish Article III standing.[377] For example, the Second Circuit held that plaintiffs were not foreclosed from establishing standing based on a future risk of identity theft, and laid out three non-exhaustive factors to evaluate that risk.[378] In that same year, the Eleventh Circuit declined to extend standing to a class of data breach plaintiffs based on an increased risk of future harm resulting from a data breach.[379] The Supreme Court in *TransUnion* attempted to resolve the circuit split; however, divergent approaches to the issue of standing persist. In the wake of the *TransUnion* decision, some courts have chosen to interpret the Supreme Court's reasoning expansively and confer standing even when data has yet to be misused. For example, the Third Circuit in *Clemens v. ExecuPharm*, found standing for a data breach plaintiff whose data had not yet been misused, when "the exposure to the risk of future harm itself cause[d] a *separate* concrete harm" such as psychological or emotional harm or spending money on mitigation measures.[380] Other courts have relied on the Court's language in *TransUnion*, which identified "intrusion on seclusion" as an intangible harm sufficient to serve as a basis for standing.[381] In similar cases, other courts have taken different approaches in applying *TransUnion*. In *Cooper v. Bonobos Inc.*, the court declined to confer standing on a data breach plaintiff because the risk of identity theft was too remote to constitute an injury in fact.[382] Based on the varying interpretations and uncertainty surrounding interpretations of *TransUnion*, it is clear that courts will continue to grapple with its application and how to assess standing for data breach litigants whose data has not yet been misused but are at a higher risk of harm. **2. Potential Increase in Trials and Derivative Lawsuits** Litigation surrounding data breaches rarely goes to trial, but the Missouri district court case *Hiscox Ins. Co. v. Warden Grier* did just that, resulting in a multi-day trial in which the jury ruled for the defense.[383] The action was brought by an insurance company claiming (1) breach of contract; (2) breach of implied contract; (3) breach of fiduciary duty; and (4) negligence, after a hacker gained access to consumer data on the servers of the defendant law firm retained by the insurance company.[384] Like many data breach cases, the plaintiff relied largely on a common law cause of action, which in this case was negligence.[385] While public perception of data breaches tends to favor plaintiffs, this case serves as a reminder that careful defendants can still convince a jury that they acted appropriately under the circumstances. Whether this will embolden future defendants to consider taking similar cases to trial rather than settling with plaintiffs remains to be seen. In the last few years there has also been an uptick in derivative lawsuits from prior data breach cases. Many of these cases, like *Reiter v. Fairbanks*, rely on alleged breaches of oversight duties by company directors.[386] Results in these derivative suits are mixed, but where plaintiffs do recover, payouts can be quite high. As data breaches continue to become more common, derivative cases against directors can be expected to become more common as well. **3. Major Settlements** There have been significant settlements in 2022 that reflect the financial ramifications that modern data breaches can bring. A large financial institution agreed to a $60 million settlement regarding a data breach that compromised the data of around 15 million customers.[387] This payment is in addition to the $60 million civil penalty imposed by the OCC in 2020 related to the same events.[388] After a 2017 data breach that exposed the information of 147 million individuals, a major credit reporting bureau finalized a settlement in January of 2022 that included up to $425 million to assist victims of the breach.[389] In September of 2022, another large financial institution reached a $190 million settlement stemming from a cyber incident in 2019 in which about 140,000 Social Security numbers and 80,000 bank account numbers were exposed.[390] On the government side, the U.S. Office of Personnel Management reached a $63 million settlement agreement after information on federal government employees and contractors was compromised.[391] Class action suits like these reaffirm the need for appropriate data security measures. **4. Rise in State and Federal Legislation** As discussed in more detail in Section ?II.A.1 above, new comprehensive state data privacy legislation has become increasingly common, promising to bring fundamental changes to data breach litigation.

Enacted state data privacy legislation aims to give consumers added control over their data and how it used and stored and expands the avenues by which consumers can pursue claims against data custodians in the event of data breaches. There are currently active data privacy bills in committee in states across the country, including Illinois, Michigan, Massachusetts, New Jersey, New York, Ohio, D.C., Rhode Island, and Pennsylvania.[392] As additional state data privacy legislation is considered across the country, the legal landscape surrounding data privacy will continue to transform. As discussed below, the CCPA and BIPA grant consumers a limited private right of action for data breaches, creating an additional front for data custodians to litigate in the event of a data breach. Similarly, the ADPPA also sought to create a private right of action for litigants at the federal level. Other states have enacted data privacy laws without creating a private right of action for consumers. For example, the VCDPA is enforced solely by the Virginia Attorney General.[393] The enacted and upcoming changes to data privacy laws will significantly impact data breach litigation in a multitude of ways. The lack of a unified approach to data privacy laws amongst the states leads to complexity and uncertainty and makes careful consideration of new emerging legislation important. **B. Computer Fraud and Abuse Act Litigation** The Computer Fraud and Abuse Act generally makes it unlawful to "intentionally access a computer without authorization" or to "exceed[] authorized access."[394] In recent years, several high-profile court decisions have limited the CFAA's scope. As a result, relatively commonplace online activity—like mere breaches of a website's terms of service or routine data scraping—are now unlikely to violate the CFAA. In 2022, these decisions also prompted the DOJ to narrow its CFAA enforcement policies, as previously described in this Review. On June 3, 2021, the U.S. Supreme Court issued its much-anticipated opinion in *Van Buren v. United States*, holding that the CFAA's "exceeds authorized access" clause does not extend to circumstances where an individual has legitimate access but uses that access for a "prohibited purpose."[395] In *Van Buren*, a police officer improperly accepted a $5,000 payment to run a license plate search in a law enforcement computer database.[396] The officer was legitimately authorized to use the database for law enforcement purposes, but department policy forbade him from using the database for any other reason, including the license plate search at issue.[397] The Eleventh Circuit upheld the officer's criminal conviction, but the Supreme Court reversed, resolving a circuit split on the CFAA's scope.[398] The Court held that "an individual 'exceeds authorized access' when he accesses a computer with authorization but then obtains information located in *particular areas* of the computer—such as files, folders, or databases—that are off limits to him."[399] Therefore, the Court reasoned, the officer "did not 'exceed authorized access' to the database" because he was legitimately permitted to access it, even though he ultimately used it for an improper purpose.[400] Following *Van Buren*, on April 18, 2022, the Ninth Circuit decided *hiQ Labs, Inc. v. LinkedIn*.[401] This was the second Ninth Circuit decision in *hiQ* because, ten months earlier, the Supreme Court had granted certiorari in the case, vacating and remanding it back to the Ninth Circuit for reconsideration based on *Van Buren*.[402] In *hiQ*, a professional networking platform had tried to block a data analytics company from scraping data from its publicly available pages in violation of the platform's terms of use.[403] In May 2017, the professional networking platform sent the data analytics company a cease-and-desist letter, which prompted the data analytics company to file a complaint for injunctive and declaratory relief to continue its data scraping operations.[404] The district court granted the request for a preliminary injunction and the professional networking platform appealed.[405] The Ninth Circuit held the district court did not abuse its discretion by granting the preliminary injunction because the data analytics company was likely to succeed on its claim that the CFAA does not bar data scraping in this context.[406] The court reasoned the CFAA's "prohibition on unauthorized access is properly understood to apply only to private information—information delineated as private through use of a permission requirement of some sort."[407] Thus, "[i]t is likely that when a computer network generally permits public access to its data, a user's accessing that publicly available data will not constitute access without authorization under the CFAA."[408] The case's outcome was therefore consistent with longstanding Ninth Circuit authority that violating the "terms of use of a website—without more—cannot establish liability under the CFAA."[409] Of course, the outcome of *hiQ* does not mean that breaching a website's terms of use leaves website operators without recourse—state

contract and tort law may still provide avenues for relief.[410] Indeed, in December 2022, after six years of litigation, the parties in *hiQ* filed a consent judgment that required the data analytics company to pay $500,000 and permanently enjoined it from breaching the professional networking platform's terms, including scraping data, among other matters.[411] The court subsequently entered that judgment.[412] District courts around the country have also continued to grapple with the CFAA's outer bounds. We highlight two cases from 2022 of particular interest. ***Ryanair DAC v. Booking Holdings Inc.*** In October 2022, a Delaware federal district court held that an airline had sufficiently stated CFAA claims against various online travel booking companies, which had allegedly accessed non-public sections of the airline's website by creating user accounts and bypassing certain technological restrictions.[413] Interpreting *Van Buren*, the court held that the "operative question" in CFAA cases under Section 1030(a)(2) "is whether a technological or code-based limitation exists to prevent access to a computer by those who do not have proper authorization."[414] Because the airline had restricted access to the data at issue only to authenticated users—and because the airline had instituted other technological measures to block would-be data scrapers—the defendants had plausibly breached the CFAA when they accessed that data.[415] The court also credited the plaintiff's allegations that its terms of use prohibited data scraping—which by itself would not be sufficient to establish liability under the CFAA—distinguishing the case from *hiQ* on the basis that the data at issue here was not entirely "accessible to the public."[416] ***United States v. Thompson***. In March 2022, a Washington federal district court held the government had sufficiently stated CFAA claims against an alleged computer hacker. The hacker allegedly had (1) "created proxy scanners that allowed her to identify [] servers with misconfigured web application firewalls"; (2) sent certain commands to those servers that automatically returned security credentials to them; (3) accessed those servers using the security credentials; (4) copied data to them; and (5) set up "cryptocurrency mining operations" on them for her benefit.[417] The court rejected the defendant's argument that she had authorized access to the servers as a matter of law because the servers were configured to provide her with valid security credentials.[418] At the same time, the court seemed potentially swayed by the defendant's claim that the servers' misconfiguration rendered the information residing on them equivalent to information on a "public-facing web page"—somewhat redolent of the allegations in *hiQ*.[419] The court noted that the "question of whether accessing a server that is not meant to be public (unlike a public facing website) but nonetheless lacks protective authentication requirements constitutes acting 'without authorization' under the CFAA therefore exists in a gray area."[420] The court ultimately held the jury should resolve that question in the context of this case.[421] On May 19, 2022, the DOJ also announced adjustments to its CFAA enforcement policies, aligning the policies with *Van Buren* and *hiQ*.[422] The DOJ has now committed not to prosecute "without authorization" claims unless: "(1) the defendant was not authorized to access the protected computer under any circumstances by any person or entity with the authority to grant such authorization; (2) the defendant knew of the facts that made the defendant's access without authorization; and (3) prosecution would serve the [DOJ]'s goals for CFAA enforcement."[423] Similarly, the DOJ will not prosecute "exceeds authorized access" claims premised solely on violations of "a contract, agreement, or policy, with the narrow exception of contracts, agreements, or policies that entirely prohibit defendants from accessing particular files, databases, folders, or user accounts on a computer in all circumstances."[424] In other words, the DOJ will not prosecute mere violations of contractual access restrictions or terms of service established by Internet service providers or publicly-available web services, as was the case in *hiQ*.[425] Thus, "exceeding authorized access" prosecutions will be confined to circumstances where: "(1) a protected computer is divided into areas . . . (2) that division is established in a computational sense . . . (3) a defendant is authorized to access some areas, but unconditionally prohibited from accessing other areas of the computer; (4) the defendant accessed an area of the computer to which his authorized access did not extend; (5) the defendant knew of the facts that made his access unauthorized; and (6) prosecution would serve the [DOJ]'s goals for CFAA Enforcement" (as described in the policy statement).[426] In discussing those policy goals, the DOJ offered guidance for government attorneys to consider when determining whether to pursue CFAA prosecutions. This guidance pronounced that government attorneys should decline to

prosecute security researchers that access an organization's networks "solely for purposes of good-faith testing, investigation, and/or correction of a security flaw or vulnerability, where such activity is carried out in a manner designed to avoid any harm to individuals or the public."[427] Notably, the DOJ clarified that, across all prosecutions, prosecutors must be ready to prove a particular mental state: "that the defendant was aware of the facts that made the defendant's access unauthorized at the time of the defendant's conduct," and "not merely that the defendant subsequently misused information or services that he was authorized to obtain from the computer at the time he obtained it."[428] **C. Telephone Consumer Protection Act Litigation** Civil litigation under the Telephone Consumer Protection Act ("TCPA") has continued to present pivotal questions brought by changing technology over the past year. Specifically, courts have been deliberating issues related to calling systems and the devices on which calls are received in the aftermath of a landmark Supreme Court decision in 2021, which clarified and restricted the definition of an automatic telephone dialing system ("ATDS").[429] On April 1, 2021, in a TCPA action brought against a major social media platform, the Supreme Court held that the adverbial phrase "using a random or sequential number generator" in the statutory definition of ATDS modifies both the words "store" and "produce" as used in the statute.[430] Accordingly, the Court held that a device is an ATDS under the TCPA only if it can store telephone numbers using a random or sequential number generator, or produce telephone numbers using a random or sequential number generator.[431] This reversed the Ninth Circuit's broad interpretation of the term that included any device capable of storing and automatically dialing numbers.[432] Following the Supreme Court's guidance, many courts have raised the threshold of TCPA challenges even higher.[433] Most prominently, in *Panzarella v. Navient Solutions, Inc.*, the Third Circuit held that to allege a TCPA violation under §227(b)(1)(A)(iii), it is not enough to show that the dialing system satisfies the narrow definition of ATDS in accordance with the Supreme Court's holding.[434] Litigants must also show that the challenged call actually employed ATDS's capacity to use a random or sequential number generator.[435] This has made it more difficult for claims focused on the use of an ATDS to succeed. However, plaintiffs have begun pivoting toward bringing TCPA claims that do not center around the use of an ATDS. For example, a number of suits have been brought alleging the use of "an artificial or prerecorded voice," which also violates the TCPA under Section 227(b)(1)(A).[436] Violations of the TCPA can result in penalties as high as $500 per violation, and damages can be increased up to three times that amount if the court finds that the violation was willful or knowing.[437] Each year, thousands of TCPA claims are brought to the courts. However, the number of claims dropped by nearly 50% from 2020 to 2021, potentially reflecting the limitations on plaintiffs' ability to bring successful claims under the TCPA.[438] Yet claims continue to be brought under the TCPA under new theories that do not require proving the use of an ATDS under the new, narrower, definition. In the California federal district court case, *Tracy Eggleston v. Reward Zone*, the plaintiff argued that all text messages should be considered pre-recorded calls under the TCPA, and should therefore not require an ATDS to constitute a violation.[439] While this argument was dismissed by the court, this case demonstrates one of the many ways plaintiffs have sought to sidestep the new limitations courts have imposed on TCPA claims. This case also raises important questions about the TCPA's applicability to modern technology, like text messaging. This concern was also raised by Supreme Court Justice Clarence Thomas who questioned the established practice of considering text messages to be calls under the TCPA during oral arguments in the 2021 landmark case, asking "at what point do we say this statute is an ill fit for current technology?"[440] The uncertainty surrounding the TCPA's relevance in the face of technological advancement remains, leaving room for challenges to the application and interpretation of the law. State governments have also taken legislative steps in response to the narrow definition of ATDS. For example, Florida passed the Florida Telephone Solicitation Act ("FTSA")[441] in amendment of the Florida Telemarketing Act, which covers any "automated system for the selection or dialing of telephone numbers."[442] The newly enacted Oklahoma Telephone Solicitation Act also employs the same language.[443] Litigants have wasted no time testing the FTSA, which survived a constitutional challenge in *Turizo v. Subway Franchisee Advertising Fund Trust*, a case involving claims that the FTSA violated the Supremacy Clause, Dormant Commerce

Clause, First Amendment, and Due Process Clause of the Fifth Amendment.[444] While this case survived a motion to dismiss on constitutional grounds, there is likely to be more litigation around the constitutionality of state laws that attempt to emulate the TCPA. Along with the limitations on TCPA claims imposed by the Supreme Court decision, requirements for bringing TCPA claims involving the Do Not Call Registry ("DNC Registry") have also increased. In *Rambough v. Smith Agency*, an Iowa federal district court held that in order to bring a claim that a phone number was illegally used because of its status on the DNC Registry, the plaintiff must be the individual that registered the number.[445] In this case, the court dismissed the plaintiff's challenge because she failed to allege that "she registered her telephone number on the do-not-call-registry."[446] Even though the number was on the DNC Registry, the court ruled that the plaintiff should have re-registered the number herself in order to ensure protection under the law.[447] The court ultimately dismissed the case with prejudice, signaling that at least some courts will impose a more stringent requirement for TCPA claims involving the wrongful use of phone numbers on the DNC Registry.[448] While courts have a shown a desire to restrict the TCPA, that trend is not universal. In the New York district court case *Rose v. New TSI Holdings*, the court strayed from prior precedent in its decision regarding a fairly basic TCPA claim involving a cellphone number on the DNC Registry.[449] The court ruled that the plaintiff's claim that the number "was a personal number that [the plaintiff] did not use for business purposes and that [] has been listed on the DNC Registry since 2004" was sufficient for the plaintiff's TCPA claim to survive a motion to dismiss.[450] This was a notable relaxation of the usual requirement at the motion to dismiss stage that plaintiffs show factual evidence that the number is for "residential use." In fact, there has been disagreement over whether cell phones can fall under the umbrella of "residential telephones" at all.[451] More litigation on this issue should be expected in the near future.

D. State Law Litigation

1. California Consumer Privacy Act Litigation In addition to those regulatory actions discussed above, the CCPA includes a private right of action, allowing consumers, individually and as a class, to pursue civil litigation when their personal information falls subject to "unauthorized access and exfiltration, theft, or disclosure as a result of the business's violation of the duty to implement and maintain reasonable security procedures and practices."[452] The CCPA provides for the greater of either statutory damages—between $100 and $750 per consumer per incident—or actual damages, plus injunctive or declaratory relief, and any other relief a court deems appropriate.[453] These remedial provisions contribute to the seminal trend of companies facing continually increasing costs to settle data protection violations.

a. Potential Anchoring Effect of CCPA Statutory Damages The CCPA's provision of either actual damages or statutory damages of $100 to $750 per consumer per incident has the potential to frame the discussion of settlement terms. Such a potential anchoring effect appears reflected in at least one recent settlement. ***Automobile Manufacturers and Marketing Vendor***. Residents of California and Florida, car owners and lessees, filed class actions alleging that the failure of auto manufacturers and a marketing vendor to adequately secure and safeguard data allowed hackers to steal the personal information and sensitive personal information—there meaning driver's license numbers, Social Security numbers, payment card numbers, bank account or routing numbers, dates of birth, and/or tax identification numbers—of 3.3 million individuals.[454] The plaintiffs asserted causes of action for negligence, breach of implied contract, violation of the CCPA, violation of California's Unfair Competition Law ("UCL"), and breach of contract.[455] In an order dated December 13, 2022, the court preliminarily approved a settlement between the parties.[456] The settlement's terms appear to reflect the potential anchoring effect of the CCPA's statutory damages provision.[457] Under the settlement, California residents whose sensitive personal information was affected would receive $350 cash payments; consumers outside California, whose sensitive personal information was affected, would receive $80; and those in the U.S. whose non-sensitive personal information was affected would receive $20.[458] The total settlement fund would be in the amount of $3,500,000, with $5,000 representative incentive awards for each of four representative plaintiffs, $1,050,000 in attorney's fees, and up to $50,000 in litigation costs.[459]

b. Requirements for Adequately Stating a CCPA Claim A few recent decisions this past year provide further insight into how courts continue to give shape to the contours of the CCPA. The below cases address questions regarding the extent to

which plaintiffs must plead supporting facts to adequately allege a claim under the CCPA, and who may bring claims of CCPA violations. ***Waste Disposal Company***. Plaintiffs, current and former employees of a waste disposal company, brought suit after the company suffered a data breach.[460] A consolidated amended complaint asserted various claims on behalf of a putative nationwide class, and violations of the CCPA, the California UCL, and other California statutes on behalf of a subclass of California plaintiffs.[461] The court granted the waste disposal company's motion to dismiss the plaintiffs' CCPA claim, as well as all other claims. In reaching its decision, the court reasoned that the complaint failed to plausibly allege that the company violated its "duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information."[462] The court similarly held that plaintiffs' assertions that the company failed to cure purported violations of the CCPA or to change security practices were fatally conclusory, lacking allegations regarding any notice of cure, and did not explain what violations needed remediation.[463] Regarding plaintiffs' argument that the company failed to remedy its CCPA violations because their data remained exposed and susceptible to exploitation, the court reasoned that "the CCPA does not require businesses that have experienced a data breach to place consumers in the same position they would have been absent a breach. It just requires them to remedy any 'violation' of their 'duty to implement and maintain reasonable security procedures and practices.'"[464] The court found plaintiffs did not allege that the company failed to remedy violations of that duty.[465] Notably, the court also raised *sua sponte*, without deciding the issue, that employee plaintiffs might not fall within the CCPA's purview because they might not qualify as "consumers" under the CCPA.[466] The court also noted, but likewise found unnecessary to decide, that plaintiffs may have an obligation to plead compliance with the CCPA's 30-day notice requirement.[467] The plaintiffs' appeal of the dismissal of their complaint remains pending before the Second Circuit.[468] **c. Broadening the Scope of a "Data Breach"** As discussed in the ninth edition of Gibson Dunn's United States Cybersecurity and Data Privacy Outlook Review,[469] various consumers have filed suits seeking relief for CCPA violations and have sought to expand the limited basis for the CCPA's private right of action by incorporating claims alleged under the CCPA in data breach actions. Courts have responded by continuing to emphasize the limited scope of the private right of action. ***Retailers and Loss Prevention Service Provider***. This class action before the Central District of California named retailers and a loss prevention service provider as defendants and was previously covered in this Review's ninth edition.[470] There we noted that plaintiffs' allegations were based on the defendants' voluntary sharing of consumer information with a third-party loss prevention service provider that generated customer risk scores. We return here with an update that the court granted in part defendants' motion to dismiss, dismissing with prejudice most of plaintiffs' claims, including the claim under the CCPA.[471] The court in this decision addressed plaintiffs' CCPA claims and the narrowness of the private right of action in three parts.[472] First, the court agreed with defendants that the CCPA was not retroactive in effect—i.e., plaintiffs who allegedly attempted returns or exchanges before the operative date of the CCPA were required to have those claims dismissed because the CCPA (1) was not yet in effect and (2) lacked an express retroactivity provision as necessary to apply retroactively.[473] Second, the court held that the CCPA's private right of action is clearly limited to claims brought under Section 1798.150(a), and accordingly dismissed with prejudice the plaintiffs' CCPA claims under Sections 1798.100(b), 110(c), and 115(d). Finally, the court addressed the plaintiffs' CCPA claim under Section 1798.150(a). The court held that under Section 1798.150(a) a plaintiff is required to show that the theft of "nonencrypted and nonredacted personal information" resulted from "*the business's violation of the duty to implement and maintain reasonable security procedures and practices* appropriate to the nature of the information to protect the personal information."[474] The court found that the sale of the plaintiffs' non-anonymized data was "a business decision to combat retail fraud," not the result of the defendant violating the duty to implement reasonable security measures, and thus no violation of the statute was alleged.[475] The court also held that the out-of-state plaintiffs' claims lacked standing because the CCPA does not apply to non-California residents.[476] **d. CCPA Violations Under the UCL** As we reported in the ninth edition of this Review, California's UCL—like the CCPA—provides a private right of action for consumers.[477] Under the UCL, the

private right is to enjoin and seek restitution for a business act or practice that is "unlawful," "unfair," or "fraudulent."[478] Violations of other statutes can serve as the "unlawful" predicate for a UCL claim. However, the CCPA's text and legislative history prohibit consumers from using CCPA violations as a predicate for a cause of action under a separate statute, seemingly precluding the CCPA from constituting grounds for liability under the UCL.[479] Nevertheless, private litigants have continued to test this prohibition on such use of the CCPA, as in the following example: ***Loan Servicing Company***. On April 21, 2022, a class action was filed in California Superior Court against a loan servicing company.[480] In their complaint, the plaintiffs alleged that the defendant failed to implement reasonable security measures in violation of the CCPA, resulting in a data breach of the class's personal information.[481] The plaintiffs sought actual damages, equitable and declaratory relief, and other relief deemed appropriate by the court.[482] In an example of how plaintiffs are further incorporating the CCPA into data breach actions, the plaintiffs also claimed that the loan servicing company committed "unlawful" business practices within the meaning of the UCL by failing to implement appropriate data security that complied with the CCPA.[483] The plaintiffs further asserted that the defendant violated the UCL by engaging in "unfair" business practices contrary to public policies reflected in the CCPA.[484] The loan servicing company removed the complaint to the U.S. District Court for the Southern District of California.[485] On May 9, 2022, the Southern District of California granted a joint motion to transfer venue to the Southern District of Florida.[486] As of this writing, the case has been electronically transferred to but not docketed in the Southern District of Florida. **e. CCPA as a Shield for Immunity to Substantive Claims Litigation** Over the past year, parties in several actions have attempted to wield the CCPA as a shield, whether as a source of immunity or otherwise, to protect themselves from claims under substantive law. In particular, while courts have continued to find that the scope of liability under the CCPA remains limited, some courts nonetheless have found also that the law does not provide defendants with particular affirmative defenses in certain circumstances. ***People Search Website***. On November 19, 2021, plaintiffs brought a class action suit against the operator of a website that aggregates and makes available individuals' public information from both online and offline sources, alleging violations of the UCL, as well as California's, Indiana's, and Ohio's right of publicity and appropriation of name or likeness statutes.[487] Notably, whereas plaintiffs alleged no violation of the CCPA, defendant moved to dismiss the complaint contending that, among other arguments, the CCPA granted immunity from plaintiffs' UCL claim because the CCPA expressly allows the use of publicly available information.[488] On April 19, 2022, the court denied the motion and specifically rejected this argument, holding that the CCPA only "exempt[s] publicly available data from special *notification* and *disclosure* rules that the statute imposes on companies that collect Californians' data," and that the CCPA did not nullify plaintiffs' privacy torts or California UCL claims.[489] On July 8, 2022, the court denied a motion to certify an interlocutory appeal,[490] and on September 13, 2022, the case was referred to private alternative dispute resolution.[491] On January 18, 2023, the plaintiffs and defendant people search website filed a joint statement of discovery dispute concerning the scope of social media posts that the plaintiffs would be required to produce.[492] The plaintiffs had agreed to produce social media posts visible to all members of the public, whereas the people search website sought production also of social media posts that were visible only to plaintiffs' social media "friends."[493] The plaintiffs contended that the people search website misunderstood their legal theory that they suffered injury by violations of state laws prohibiting the use of personal information for commercial purposes.[494] On January 25, 2023, the court resolved the dispute by denying the people search website's request.[495] The court found it unclear how the many years of non-public social media posts were proportional to the needs of the case or relevant to resolving the issues.[496] The court further found that the people search website's theory that the posts were necessary to show that the plaintiffs lacked privacy rights in that information seemed tenuous.[497] According to the most recent publicly available information on the docket, the parties are scheduled to mediate on March 7, 2023,[498] with the plaintiffs' motion for class certification due February 10, 2023, the defendants' opposition due March 24, 2023, and the hearing on the motion set for May 10, 2023.[499] **f. The CCPA in Discovery Disputes** The CCPA has played a role in recent discovery disputes. A number of litigants

have sought to leverage the CCPA as a defense in a range of conflicts in discovery—from sanctions motions to objections to discovery requests. These efforts, however, have generally been less than successful. Additionally, information generated pursuant to the CCPA has become a target of discovery: the CCPA and its August 2020 implementing regulations require businesses that collect personal information for incentive programs to estimate the "value [provided] to the business" by the consumer's data, considering factors specified in the regulations.[500] ***Workforce Automation Company***. On September 29, 2022, the U.S. District Court for the Northern District of Ohio issued discovery spoliation sanctions against a workforce automation company and its founder—in the form of a mandatory adverse-inference instruction to the jury.[501] The court rejected as not credible the defendants' claim that the data destruction that occurred when the founder both deleted previously exported Slack data and changed Slack data retention settings from unlimited to seven days resulted from a misunderstanding of their obligations under the CCPA and International Standard of Operation Compliance ("ISO").[502] The court found that the founder admittedly changed the retention settings and deleted the previously exported data shortly after becoming aware of the likelihood of litigation a month before receiving a litigation hold letter.[503] The court further found that the company then failed to revert to unlimited Slack data retention for almost a year after receiving the litigation hold's request to preserve all data relevant to the litigation.[504] The timing of the data destruction, coupled with the persistent refusal to retain Slack data indefinitely, led the court to find the defendants' claims of a misunderstanding of CCPA and ISO compliance obligations not credible.[505] Rather, the court noted the defendants' failure—despite plaintiffs' requests—to produce any evidence to support their claim that the seven-day retention policy was instituted to comply with the CCPA and ISO.[506] ***Law Firm***. Similarly, litigants have been unsuccessful in arguing that the CCPA creates a privacy right or a privilege that shields disclosure during discovery.[507] In one such litigation, a defendant law office objected to a request for production of documents on the basis that the discovery would invade protected privacy interests established by California privacy statutes, including the CCPA.[508] The court sided with plaintiffs, agreeing that the privacy objection lacked merit because, at the outset, the California Constitution, the CCPA, and other California privacy statutes were not applicable in the federal discovery proceeding.[509] Rather, the court reasoned, even if the state constitution and statutes created a privilege—which the court declined to decide, "only federal law on privilege applies in cases, such as this one, involving federal question jurisdiction."[510] **g. Supplementing Time for the CCPA's 30-Day Notice Requirement** The CCPA's statutory scheme notably requires that a "consumer provide[] a business 30 days' written notice identifying the specific provisions of [the CCPA] the consumer alleges have been or are being violated."[511] A recent decision upheld defendants' argument that this requirement is one that a plaintiff must meet prior to initiating a CCPA claim and that a plaintiff "cannot supplement the time between the notice and the initiation of the lawsuit by amending [the] complaint."[512] ***Health Care Company***. On June 29, 2020, plaintiffs brought a putative class action against a health care company after a breach of the company's computer systems resulted in the personal information and protected health information of employees, contractors, and health care benefit plan participates being stolen.[513] On June 1, 2022, the court granted in part and denied in part defendant's motion to dismiss a second amended consolidated class action complaint, dismissing with prejudice a California plaintiff's allegation that the health care company violated the CCPA by providing inadequate data security and failing to prevent the data breach.[514] The court noted that it had previously dismissed the CCPA claim (without prejudice) in September 2021 because the plaintiff failed to allege out-of-pocket damages, did not seek statutory damages, failed to comply with the CCPA's 30-day notice requirement, and failed to allege how data security measures were inadequate.[515] In its motion to dismiss the second amended complaint, the defendant healthcare company contended that the California plaintiff still failed to allege compliance with the CCPA's 30-day notice requirement.[516] The court agreed and rejected the plaintiff's argument that notice was timely because over 30 days had elapsed between the notice and the filing of the second amended complaint.[517] Pointing out that courts have held that pre-suit notice requirements aim to permit a defendant to cure the defect outside court, the court found that the CCPA's requirement serves the same end and allowing a plaintiff to supplement

the time between serving the notice and initiating the lawsuit by filing an amended complaint would defeat the notice requirement's purpose.[518] Further, in this case, the plaintiff had served notice just three days before initially filing the CCPA claim; the court therefore dismissed the claim with prejudice.[519] **h. Guidance on Reasonable Security Measures in Connection with the CCPA** A few CCPA decisions this past year have suggested some guidance on what courts might find would be reasonable data security measures and what potential defendants can do to implement reasonable data security procedures and avoid liability under the CCPA. ***Insurance Broker Companies***. After suffering a cybersecurity attack in 2020, insurance brokers were named defendants in putative class actions brought by former employees and clients who asserted injuries under common law, data notification statutes, and consumer protection statutes, including the CCPA.[520] On September 28, 2022, the court notably held that plaintiffs adequately alleged that defendants failed to implement reasonable data security measures, as required by the CCPA, and held that plaintiffs sufficiently identified those measures that defendants assertedly failed to implement in alleging that:

> (1) the United States government recommends certain measures that organizations can take to prevent and detect ransomware attacks, including awareness and training programs, spam filters, firewalls, anti-virus and anti-malware programs; and (2) Defendants failed to implement "one or more of the above measures to prevent ransomware attacks."[521]

The U.S. District Court for the Northern District of Illinois agreed with defendants, stating that it "strains plausibility to assume that Defendants caused increased spam to those Plaintiffs who do not allege that their contact information was accessed via the Data Breach."[522] However, the court held that plaintiffs did plausibly assert that the breach caused other kinds of harm such as "'lost time,' anxiety, and increased concerns for the loss of the privacy as a result of the Data Breach."[523] The court did agree with defendants that one of the complaint's CCPA claims was deficient for omitting allegations regarding a plaintiff's personal experience with the data breach, but as both parties acknowledged this was done inadvertently, the court permitted the plaintiff to amend and permitted the other CCPA claim to proceed.[524] ***Fintech Company***. A fintech company agreed to pay up to $20 million to provide compensation and credit monitoring to thousands of customers who claimed their accounts were hacked in order to settle a putative class action alleging that the company failed to take sufficient steps to prevent unauthorized access to users' accounts, thereby committing common law negligence, breach of contract, violation of the CCPA, UCL, and other California statutes.[525] The lawsuit alleged that the company failed to maintain industry-standard security measures that plaintiffs claimed could have prevented third parties from accessing approximately 40,000 customer accounts.[526] The fintech company filed two motions to dismiss, each granted in part and denied in part.[527] Plaintiffs' motion for approval of the settlement portrayed a "major question of law" in those motions as to "whether Plaintiffs' CCPA claim could survive despite [the company's] contention that no data breach of its computer systems had occurred."[528] Specifically, the fintech company challenged "whether the CCPA applies where a defendant's own computer network was not subject to a security breach."[529] The U.S. District Court for the Northern District of California found the CCPA claim to be adequately pleaded.[530] The parties proceeded to discovery in which over 11,000 pages of documents were produced regarding the fintech company's security and business practices during the period before the parties turned to mediation in March 2022, eventually reaching a settlement in principle on May 4, 2022.[531] Plaintiffs acknowledged that given the fintech company's conduct in the case, it would have been reasonable to assume that any award for statutory damages under the CCPA would be towards the lower end of the $100 to $750 range.[532] As part of the settlement, the company agreed to implement "improved policies and procedures to prevent unauthorized access to customer accounts," including "supplemental two-factor authentication; screening for, and prompting users to update, potentially compromised passwords; proactive monitoring of account takeovers; customer awareness campaigns that provide information and tools for better cybersecurity hygiene; and real-time voice support."[533] These new procedures would need to be instituted for at least 18 months.[534] As further

part of the settlement, the company would pay class members up to $260 each, as well as provide two years' worth of credit monitoring and identity theft protections services estimated to be worth approximately $19.5 million.[535] **i. Staying CCPA Litigation Due to Other, First-Filed Litigation Arising from the Same Data Breach *Insurance Companies***. On May 26, 2022, the U.S. District Court for the Southern District of California resolved defendant insurance company entities' motion to transfer a putative data breach class action to the Eastern District of New York—where other class actions arising from the same data breach were already pending—by staying the Southern District of California action until the Eastern District of New York litigation concluded.[536] In late April and early May 2021, after the insurance company entities announced the data breach, five putative class action lawsuits were filed by plaintiffs in three different district courts: three in the Eastern District of New York, one in the District of Maryland, and one in the Southern District of California.[537] Plaintiffs transferred or consented to transfer the other actions to be heard by the same judge in the Eastern District of New York, but plaintiffs in the Southern District of California opposed defendants' motion for such transfer.[538] To resolve the disputed motion, the Southern District of California court applied the three-factor first-to-file rule, which permits a district court to transfer, stay, or dismiss an action when a complaint regarding the same parties and issues has already been filed in another district.[539] Applying the rule's namesake first factor, the district court found the Eastern District of New York action had been filed first.[540] Regarding the second factor, the similarity of parties, the court observed that the Eastern District of New York's actions proposed nationwide classes, and the Southern District of California proposed a California class, "making the classes duplicative."[541] Regarding the third factor, similarity of issues, the court agreed with the plaintiffs that the other four actions asserted no California state law claims, but noted each raised breach or invasion of privacy claims under New York State law or the Driver's Privacy Protection Act.[542] Rather, the court found persuasive, and adopted, the reasoning of a June 2021 Central District of California CCPA decision that addressed a parallel data breach action filed in Nevada with Nevada state-law claims[543]: "Because '[t]his factor does not require total uniformity of claims but rather focuses on the underlying factual allegations,' . . . the core theory is what drives the analysis."[544] The Southern District of California court found that because all five actions implicated how the data breach occurred, the measures in place at the time, and the insurance companies' response, they would be "duplicative litigation" posing a risk of disparate judgments to which the first-to-file rule would apply.[545] The court then determined to exercise its discretion to stay the case pending resolution of the Eastern District of New York actions to conserve judicial resources and promote efficiency.[546] **2. Illinois Biometric Information Privacy Act Litigation** The Illinois Biometric Information Privacy Act ("BIPA"), passed into law in 2008, was the first statute governing the regulation, collection, use, and handling of biometric data by private entities. With BIPA, Illinois has become the leading state for litigation alleging violations of biometric data privacy. BIPA regulates private entities that collect or are in possession of "biometric identifier[s]," which are defined by the Act to include "a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry," while excluding writing, physical descriptions of a person, or photographs.[547] Biometric information is defined broadly to include "any information . . . based on an individual's biometric identifier used to identify an individual."[548] The Act prohibits for-profit transactions of biometric data by the collectors of that data, which likely disincentivizes the collection of biometric data by private entities,[549] unless the source of the biometric data consents to the sharing of their data.[550] BIPA creates an expansive private right of action. In its 2019 decision, *Rosenbach v. Six Flags Entertainment Corp.*, the Illinois Supreme Court held that "a person need not have sustained actual damage beyond violation of his or her rights under [BIPA] in order to bring an action under it."[551] This "no actual damages" holding was affirmed by the Illinois Supreme Court's 2022 decision, *McDonald v. Symphony Bronzeville Park, LLC*, where the Court held that the Illinois Workers' Compensation Act, which provides the exclusive means for an employee to recover from an employer for work-related injuries, does not preempt BIPA.[552] *McDonald* removed a key defense for businesses that utilize employees' biometric information, so businesses that deal with such information should be careful to follow BIPA precisely, or risk liquidated damages—$1,000 per violation and $5,000 for willful or reckless violations—as well as

attorneys' fees and other litigation costs.[553] Even so, there are limitations to BIPA's private right of action. In *Walton v. Roosevelt University*, the Appellate Court of Illinois held that a labor union member's claim against his employer for collection of his biometric handprint as a means of clocking in and out of work was preempted by the federal Labor Management Relations Act.[554] The Court determined that the claim was preempted because Walton's collective bargaining agreement clearly indicated that the employer's timekeeping procedures was a topic for negotiation.[555] Despite this preemption, 2022 has seen a swathe of BIPA-related litigation in the U.S. For example, private plaintiffs have used BIPA to bring claims against a software company that provides automated proctoring tools for exams,[556] and against a company allegedly collecting sales workers' biometric data by scanning their facial geometry.[557] Additionally, prominent technology companies have faced a rise in BIPA-related litigation. In February 2020, plaintiffs—comprised of users whose pictures had allegedly been scanned by a social media company in connection with its "Tag Suggestions" program—and the company reached a $650 million settlement relating to its alleged collection of users' biometric data without their consent, in violation of BIPA.[558] Illinois plaintiffs have also recently reached a $35 million settlement with a photo-sharing social media company for allegedly violating BIPA by purportedly failing to obtain consent to collect app users' facial scans, or to transfer them to third parties.[559] Litigation is also currently pending against a large software company for its alleged collection of facial biometric data,[560] against Clearview AI—a facial recognition software company—for its collection of consumer data;[561] and against a jewelry company for its virtual try-on tool, which allegedly captures users' facial geometry.[562] In each of these proposed class action lawsuits, plaintiffs alleged that private companies failed to obtain informed, written consent to the collection of their biometric data; disclosed and disseminated that information without consent; and violated BIPA's disclosure and retention requirements. Companies should be careful about collecting information—such as facial scans, facial geometry data, voiceprints, and wellness data—and the nature of any consumer notice provided and consent obtained. That notice and consent should also include provisions regarding the sharing of biometric data, especially in instances where a third-party Application Programming Interface ("API") is being used to process that biometric data. Finally, companies should develop comprehensive data retention policies and schedules for destroying biometric data, which must be done "when the initial purpose for collecting or obtaining such identifiers or information has been satisfied within 3 years of the individual's last interaction with the private entity, whichever occurs first."[563] **3. Texas Biometric Privacy Law Litigation** Illinois is not the only state where litigation and investigations have been launched related to the collection and use of individuals' biometric features. In Texas, the Texas Capture and Use of Biometric Identifier Act ("CUBI") regulates private entities that capture "biometric identifiers" for commercial purposes.[564] The Act defines "biometric identifiers" as "a retina or iris scan, fingerprint, voiceprint, or record of hand or face geometry," and makes it illegal to capture "a biometric identifier of an individual for a commercial purpose unless the person" provides informed consent for such capture.[565] The Act prohibits the sale, lease, or disclosure of biometric identifiers except in certain situations, and places an affirmative duty on the capturer to handle biometric identifiers with "reasonable care" and to destroy the biometric identifier after a reasonable amount of time no later than a year after the date the reason for the collection expires.[566] A notable difference between CUBI and other similar state biometric privacy laws (like Illinois's BIPA) is that CUBI does not create a private right of action, but rather empowers only the Attorney General to bring civil claims against a party for violations of the Act.[567] Like BIPA, CUBI provides for steep statutory damages—up to $25,000 for each violation.[568] There is not yet any meaningful precedent or case law discussing or construing CUBI. Attorney General Ken Paxton brought the first suit under CUBI against a large social media company in February 2022, alleging that the company's collection of "facial geometries" in connection with its facial recognition and tagging feature that it deprecated in November 2021 violated the Act, in addition to bringing claims under Texas' Deceptive Trade Practices Act.[569] The suit's CUBI claims argue that the company's "tagging" system, which prompted users on the platform to "tag" other individuals in photos and later in videos when the software detected a face, allegedly trained the software to associate a particular facial geometry with an individual without that individual's consent or knowledge.[570] In late October, 2022, the State filed a

similar action against another large tech company for alleged violations of CUBI.[571] Specifically, the suit alleges that the company impermissibly captured voiceprints and facial geometries of users through certain services it offers, and that the company used these biometric identifiers for their own commercial benefit.[572] Significantly, these two cases are the first actions brought under CUBI since it was enacted in 2009. Though there are similarities between CUBI and other equivalent state law—for example, the definitions of "biometric identifier" in CUBI and BIPA are essentially identical—there are differences as well, such as BIPA's more stringent requirements for obtaining informed consent[573] and the absence of a private right of action under CUBI.[574] With states like Texas beginning to enforce data privacy laws—though perhaps with different underlying motivations than other states—it is clear that companies can expect to face increasing enforcement actions and associated costs regarding these data privacy laws across the country. **E. Other Noteworthy Litigation *Anti-Wiretapping Statutes, Session Replay Litigation and Express Prior Customer Consent***. 2022 has seen a deluge of lawsuits, including consumer class actions, brought under federal and state anti-wiretapping statutes. These statutes were initially intended to prevent surreptitious recording of or eavesdropping on phone calls without the consent of everyone involved, but have evolved to cover other forms of electronic and digital communications as technology has evolved. The suits allege that businesses and their software providers are violating state anti-wiretapping statutes and invading consumers' privacy rights through various technologies, including pixel tools, software development kits ("SDKs"), and "session replay" technologies—essentially a tool that allows businesses and their session replay service providers to analyze visitors' interactions with their public-facing website or mobile/web application to understand and optimize user experience—without obtaining sufficient and valid consent. Nearly all 50 U.S. states have some form of anti-wiretapping statute; however, 13 states require "two-party" (or "all-party") consent (three of these 13 states have some instances, however, where one party consent is applicable).[575] This arguably means that companies are required to inform all parties who are part of a conversation that they are being recorded and further obtain their consent to the recording. Litigation in this area has thus far been most prominent in California, Pennsylvania, and Florida—all three of which are two-party consent states. Plaintiffs generally allege in these lawsuits that a customer's interactions with a business's website or app is a "communication" between the customer and the business, which is being "recorded" and "intercepted" by the business and the third-party pixel, SDK, or session replay service provider—essentially a form of wiretapping.[576] An unpublished Ninth Circuit decision in May 2022 spurred a wave of session replay lawsuits, especially in California.[577] In *Javier v. Assurance IQ LLC*, the plaintiff alleged that the defendant—an insurance platform—violated Section 631 of the California Invasion of Privacy Act ("CIPA") by employing session replay technology to track or record the plaintiff's "communication" on its websites.[578] Notably, Section 631 does not actually mention "track" or "record"; instead, it penalizes anyone "who reads, or attempts to read, or to learn the contents" of a communication "without the consent of all parties to the communication".[579] The Ninth Circuit not only held that a plaintiff could base a CIPA claim on session replay software, which several district courts had previously rejected, but also found that CIPA prohibits companies from recording communications without first informing all parties of the recording.[580] This can be interpreted as creating an additional compliance obligation for businesses by reversing the trial court's ruling that retroactive consent is valid.[581] That is, website operators may now have to obtain express prior consent from California users for their use of session replay technology under CIPA. This decision has opened the door to dozens of new wiretapping cases filed in California under CIPA, including ones targeting businesses' use of the "live chat" feature, or chatbots—artificial intelligence technology that can answer customer questions directly or narrow down the customer's issues before connecting them with a live customer service representative.[582] In August 2022, the Third Circuit joined the Ninth Circuit in reversing a trial court's dismissal of a session replay case.[583] In *Popa v. Harriet Carter Gifts, Inc.*, the Third Circuit ruled that the transfer of consumer data from a business's website to service providers is considered "interception" under Pennsylvania's Wiretapping and Electronic Surveillance Control Act ("WESCA").[584] Previously, before the Pennsylvania General Assembly's 2012 revisions to WESCA modified the definition of "intercept,"[585] Pennsylvania courts applied a "direct

party" exception to WESCA, finding that a party who directly receives a communication does not "intercept" it.[586] *Popa* also raised the issue of jurisdiction in session replay cases, finding that "interception" occurs where a third party routes a communication to its own servers (even if the servers are out of state); in other words, at the location of the plaintiff's browser, situated in Pennsylvania. Predictably, multiple class actions have followed on the heels of this decision, each alleging that companies violated WESCA by tracking the plaintiffs' activities on retailers' websites. While the Eleventh Circuit has not ruled on any session replay cases, and most of the session replay software cases brought in federal district courts in Florida have been dismissed for failure to state a claim,[587] one Middle District of Florida case denied the defendant's motion to dismiss by finding that the plaintiff successfully distinguished the complaint's allegations from previously dismissed session replay cases.[588] There, the plaintiff alleged that the live chat function on a storage company's website, which was recorded by the company, violated the Florida Security of Communications Act ("FSCA") and the "[d]efendant's use of session replay software during [plaintiff's] visit to its website recorded more than just her non-substantive browsing movements." The court found that the plaintiff "sufficiently demonstrated how her claim's involvement of live chat communications distinguishes it from the other session replay software cases recently dismissed by courts in Florida."[589] However, the court added that the determination of whether the FSCA applied to a website's recording of its live chats is more appropriately addressed at the summary judgment stage.[590] ***Grant of Certiorari – Section 230***. Section 230 of the Communications Decency Act ("Section 230") has long protected "interactive computer service[s]" from liability where they are treated as the publisher or speaker of third-party content.[591] Historically, it has provided online platforms with broad immunity against liability if a third-party—typically a user—posts illegal content, with limited exceptions. In October 2022, the U.S. Supreme Court agreed to hear two related cases that would explore the scope of Section 230 in the anti-terrorism context and have the potential of redefining the broad immunity granted by Section 230.[592] In both cases, the plaintiffs argued that the technology companies should be held liable when they provided online social media platforms for ISIS that launched attacks resulting in the death of their relatives.[593] According to the plaintiffs, ISIS used those platforms to recruit members, plan attacks, issue terrorist threats, and intimidate civilian populations, often with little or no interference and sometimes with active promotion by the platform's algorithms.[594] A major barrier to plaintiffs' claims was Section 230.[595] On appeal, the Ninth Circuit decided the two cases in a single opinion, but reached drastically different conclusions. In the first case related to a series of attacks launched by ISIS in Paris, the Ninth Circuit found that Section 230 barred most of the plaintiffs' claims.[596] In the second case resulted from ISIS's attack in Istanbul, the Ninth Circuit reversed lower court's dismissal because it determined that the social media companies were indeed aware their role in ISIS's terrorism scheme, and did not reach to discuss the implication of Section 230.[597] Therefore, in the first petition for certiorari, relatives of the terrorist attack victims argued that Section 230 could not immunize interactive computer services when their algorithms make targeted recommendations of extremist content, because by making recommendations they are no longer merely "publishing" third-party contents."[598] In the second petition, the platform providers countered that they were not liable for "aiding and abetting" ISIS in violation of the Antiterrorism Act simply because "their undisputed efforts to detect and prevent terrorists from using their widely available services allegedly could have been more meaningful or aggressive."[599] The granting of certiorari marked the first time the U.S. Supreme Court has taken the opportunity to scrutinize the scope of Section 230. Regardless the outcome of the cases, the Supreme Court's decision would leave a profound impact of the Section 230 community, especially in the contexts of algorithmic immunity and the Antiterrorism Act. However, the Supreme Court's decision in the above two cases may still leave open a larger question of Section 230 immunity. In two other cases, there is a circuit split over the issue of whether recommending content through an algorithm could constitute developing content,[600] and there is no expectation that the certiorari would be granted. Florida and Texas enacted similar legislation that prohibited social media platforms from taking certain moderation actions against political candidates. The Eleventh Circuit overruled the Florida law in May of this year, (1) rejecting the Attorney General's argument that social media platforms was a "common carrier" rather

than an “interactive computer service” and (2) finding that Florida unconstitutionally sought to proclaim platforms as “common carriers” and strip them of First Amendment protections.[601] By contrast, the Fifth Circuit upheld the analogous Texas law in September this year, holding that (1) platforms were common carriers since algorithmic recommendations did not constitute “editorial discretion” as required under Section 230 and (2) the Texas law did not violate the First Amendment since there was no “intimate connection” between user content and moderation by platforms that “exercise virtually no editorial control or judgment.”[602] ***Cryptocurrency – Investigation and Litigation following Cyberattacks.*** One day after it filed for bankruptcy in November, a cryptocurrency exchange platform stated that “unauthorized access” to a large amount of assets it managed had occurred.[603] The DOJ has reportedly launched a criminal investigation into the stolen assets worth more than $370 billion, an investigation that is separate from the fraud charges brought against the co-founder of the cryptocurrency company.[604] This incident highlights the importance of guarding against and properly responding to cyberattacks for the cryptocurrency industry. **IV. Trends Related To Data Innovations and Governmental Data Collection** This decade continued with further advancements in the AI space and Metaverse, with the concepts of augmented reality (“AR”) and virtual reality (“VR”) garnering commercial and public attention. In the digital assets space, drastic crypto-asset fluctuations, alleged misleading representations, and account takeovers also drew regulatory concerns and legal uncertainties. And as companies and data transfers expand globally, entities on both sides of the Atlantic are eagerly anticipating a replacement for the EU/US Privacy Shield, which was invalidated in 2020 by Schrems II. Accordingly, this section on New Trends and Data Innovations discusses privacy implications of developments with the Metaverse, key regulatory developments in the AI space, proposed policy approaches for digital assets, as well as cross-border collaboration efforts regarding personal data transfers. ***Developments in the Metaverse—Privacy Law Implications*** The Metaverse is a virtual environment that serves as an interface for immersive interactions amongst its users and visitors through AR, VR, and avatars. The processing of data across the Metaverse is quite extensive and often involves personal data, which, coupled with the novelty of the ecosystem, raises unique privacy concerns. At the outset, a key feature of the Metaverse is interoperability, as it aims to provide users with a seamless experience, allowing digital identities to transport themselves amongst different environments, even if the environments are hosted by different platforms.[605] In the absence of a global privacy framework, one threshold matter is determining the jurisdiction or governing law covering a given interaction or entity in the Metaverse—for instance, whether governing law should be based on the location of the underlying user or entity, of the entity hosting the Metaverse platform, or of the property/place of the interaction within the Metaverse itself. For example, the California Privacy Rights Act protects California residents. However, the entity hosting the platform may not know the location of the underlying user, device, or entity, or have the ability to determine this without collection of additional personal data—which may conflict with current practices, raise security concerns, or jeopardize anonymity in the Metaverse. Indeed, it is unclear from a jurisdictional perspective the extent to which liability and compliance with US state and federal consumer protection laws, global privacy regimes, and other laws applicable to Metaverse interactions should be assigned, prioritized, and resolved. As noted, the collection and use of personal data in the Metaverse to develop immersive and personalized experiences can be quite extensive. For example, for users to experience a more accurate version of their respective avatars (which are digital representations of users), Metaverse platforms may leverage a wide array of personal data to develop the avatars – from personal identifiers, characteristics and inferences, to body language, traits, facial geometry and eye movements. To the extent this data (or even the actions of one’s digital avatar) is not de-identified and can be reasonably traced back to the underlying user, it would constitute personal data subject to various privacy regimes. Further, data elements such as facial geometry likely constitute biometric data, which is generally considered to be sensitive personal data and raises additional privacy requirements. For example, the Illinois Biometric Privacy Information Act (which was discussed in detail in Section ?III.D.2), requires, *inter alia*, companies to provide notice and obtain consent from users prior to the collection of their biometric data. As entities continue to collect more data in the Metaverse from users across the world, it may prove

difficult to surface, track, and monitor these prominent notices, implement the appropriate consent mechanisms and archive responses, and determine the proper purposes, legal bases, and levels of protection applicable for certain categories of personal data across regions. The Metaverse is also not immune from cybersecurity concerns involving the unauthorized access or acquisition of one's personally identifiable information—which may prove difficult to track in the Metaverse given the increasing sophistication of the threat landscape, absence of centralized regulatory oversight in the ecosystem, and a general lack of understanding as to how virtual environments process, store, and protect personal data. Separately, the issue of children's privacy—long a focus of legislators and regulators—may raise additional challenges in the Metaverse. Notably, age verification and tracking parental consent, navigating the manner and stages at which notice and parental consent may be required for children in the Metaverse (e.g., prior to purchases, certain interactions, or data collections), implementing heightened privacy controls, and determining whether and how to impose parental locks on Metaverse content or environments, are all important considerations for companies when developing Metaverse offerings. These challenges are exacerbated with the jurisdictional issues outlined above and the passage of new children's privacy laws such as the California Age-Appropriate Design Code Act (which was discussed in detail in Section ?II.A.1.b.i). ***AI Developments***. Over the past year there have been numerous developments in the AI space that have far-reaching implications across industries and jurisdictions, in addition to increasing enforcement by the FTC and CFPB. Additional background is available in our Artificial Intelligence and Automated Systems 2022 Legal Review. ***New York City's Automated Employment Decision Tools Law.*** New York City enacted its Automated Employment Decision Tools ("AEDT") law, which will be enforced starting April 15, 2023. The law—which is similar to those enacted at the state level by Illinois and Maryland—regulates AI-driven tools in connection with employment processes, such as in hiring and promotion processes.[606] In particular, the law requires employers and employment agencies in New York City to comply with various requirements when using AEDT in their hiring and promotion processes. AEDT is broadly defined as "any computational process, derived from machine learning, statistical modeling, data analytics, or artificial intelligence, that is used to substantially assist or replace discretionary decision making for making employment decisions that impact natural persons."[607] Under proposed guidance, employers will be required to complete an independent bias audit of the tool, provide a publicly available summary regarding the audit and distribution date of the tool, give notice to New York City-resident job candidates and employees that the tool has been used, and make available information about the source and type of data collected by the tool and employer's data retention policy (with certain limitations).[608] Employers should consider these requirements, assess whether any AEDTs are in use by business and HR teams, review their practices regarding automated tools and data retention, and work internally and with third-party vendors to ensure compliance. ***White House Office of Science and Technology Policy Published the Blueprint for an AI Bill of Rights: Making Automated Systems Work for the American People.*** The White House's Office of Science and Technology issued its Blueprint for an AI Bill of Rights, signaling increased interest in AI issues and AI-related guidance and principles.[609] The Bill of Rights focuses on equitable access to the use of AI systems and on best practices that encourage transparency and trust in automated systems and decisions. In particular, the proposed Bill of Rights focuses on five principles considered central to safeguarding the public, including: (1) the development of safe and effective systems that require extensive testing prior to deployment; (2) implementation of algorithmic discrimination protections such that the public does not face discrimination based on any type of legally protected classification; (3) built-in protections for data collection allowing users to control how their personal data is used; notice requirements that sufficiently let users know when AI is in use; and (4) the option for users to reject the use of AI and choose a human alternative where this is possible.[610] While this Blueprint does not have legal force without Congressional legislation or agency-led rulemaking, it outlines a priority for the Biden Administration where we can expect further developments. Accordingly, companies may consider reviewing their AI practices and implementing regular auditing to ensure that their existing systems align with these principles. ***Digital Assets***. As the digital assets industry grows, so do concerns over protecting the participants, their assets, and the overall

security of the eco-system. Account takeover attacks have proliferated in recent times, rising 131% in the first half of 2022, when compared to the same period in 2021.[611] Digital assets have become a critical part of the financial infrastructure, as they get further integrated into the global payment systems. On March 9, 2022, President Biden issued an executive order entitled “Ensuring Responsible Development of Digital Assets” outlining the administration’s general views towards regulatory treatment of digital assets.[612] While the order does not contain a specific regulatory proposal, it helps clarify that the U.S. has endorsed development of the digital assets ecosystem, especially given nations’ divergent approach to the issue. Below are key highlights from the executive order:

- The executive order has identified a number of risk areas involving digital assets that may implicate multiple participants in the digital assets ecosystem, including exchanges, intermediaries, and companies that accept digital assets as a payment mechanism. Some of the risk areas highlighted are privacy, cybersecurity, systemic risk, illicit finance, sanctions evasion and climate.
- In terms of further action, the executive order calls for multiple government agencies, including the Treasury, the Attorney General, the Director of Office of Science and Technology Policy to further research and submit reports to the President for consideration.
- Importantly, the executive order also outlines the policy approach towards development of a central bank digital currency (“CBDC”). The order endorses CBDC as having the potential to support low-cost transactions, particularly for cross-border transfers, and emphasizes ensuring interoperability with other central bank digital currencies issued by other monetary authorities.
- Notably absent from the executive order is any discussion on tax information reporting provisions under the existing HR 3684, the Infrastructure Investment and Jobs Act, that mandates reporting obligations with respect to cryptocurrencies.

Further to the executive order, on September 16, 2022[613] the White House announced that nine reports, including those authored by the Treasury, Department of Commerce, Department of Justice, and the Office of Science and Technology Policy, were submitted to the President.[614] As announced in the press release, the reports recommended that agencies support private-sector research in this arena, while also suggesting risk mitigating measures such as tightened law enforcement and creation of cryptocurrency mining standards. The Biden-Harris administration accordingly announced that: (i) the federal agencies themselves would encourage adoption of instant payment systems, (ii) the administration would consider recommendations for a framework to cover non-banking payment providers, (iii) regulators such as the FTC and the SEC would aggressively undertake monitoring and/or enforcement, (iv) Treasury and regulators to collaborate with private U.S. firms on sharing of best practices, (v) agencies are encouraged to issue rules for risk mitigation in the digital asset space. The press release also announced that the President would evaluate whether legislative action is to be proposed for amendment of Bank Secrecy Act and other laws prohibiting unlicensed money transfers, in order to expressly cover digital asset service providers and/or to increase penalties.[615] The Department of Justice also made public its September 16, 2022 report discussing the ways in which digital asset technologies are exploited, and emphasizing the launch of Digital Asset Coordinators Network, a network comprised of 150 federal prosecutors tasked with providing specialist expertise on digital asset crimes.[616] The Treasury’s Financial Stability Oversight Council likewise released its report on October 3, 2022, recommending enactment of legislation designed to enable federal financial regulators to regulate the spot market for crypto-assets that are not securities; extend supervision to affiliates of crypto-asset entities; and study vertical integration by crypto-companies, amongst other measures.[617] In summary, the March 2022 executive order has set in motion actions from multiple agencies, thereby paving the way for future regulatory and enforcement actions, as well as influencing the development of the digital assets industry. On January 3, 2023, Board of Governors of the Federal Reserve System, the Federal Deposit Insurance Corporation, and the Office of the Comptroller of the Currency released

a joint statement assessing crypto-assets issued or stored on public or decentralized networks to be risky activities and indicated their intent to carefully supervise banking organizations' proposals to engage in such activities.[618] On January 12, 2023, the House Financial Services Committee announced the formation of a subcommittee on Digital Assets, Financial Technology and Inclusion, with the aim to lay down the rules of the road amongst the federal regulators and identifying best practices and fostering inclusion with respect to the digital asset ecosystem.[619] ***New District Court Decision Provides Useful Guidance on Application of Trademark Law to NFTs:*** Executive actions and potential legislative intervention are one part of the equation that would shape the regulation of, and accordingly influence the development of, the digital assets industry, especially on a macro-level. Judicial resolution of disputes involving different types of digital assets form the other part of the equation and would serve to provide specific guidance on application of regulations to the digital assets industry. For example, in *Hermès International, et al. v. Mason Rothschild*,[620] District Judge Jed S. Rakoff of the Southern District of New York denied a motion to dismiss the trademark infringement dispute involving non-fungible tokens ("NFTs'"). An artist had created NFTs called "MetaBirkins." The NFT was a digital image of a large design house's handbag depicted as if made of fur. The design house sued, but the artist argued that the NFT was protected expression under *Rogers v. Grimaldi*,[621] which had held that the use of a famous trademark for artistic work is not infringement if the name is "minimally artistically relevant" to the product, and does not "explicitly mislead" as to content, authorship, sponsorship, or endorsement. Judge Rakoff declined to rule at the motion to dismiss stage whether the MetaBirkin label qualified as minimally artistically relevant, as the *Rogers* case requires to protect a defendant.[622] The court acknowledged that the threshold for artistic relevance under the *Rogers* case is "low," but also observed that design house had alleged the artist did not intended artistic expression because he had told the press about his efforts to "create that same kind of illusion that [the design house's bag] has in real life as a digital commodity."[623] And regardless of whether the MetaBirkin label qualified as artistically relevant, Judge Rakoff held that the design house had adequately alleged that the MetaBirkin label was explicitly misleading, which was sufficient to state a claim that the *Rogers* test does not protect the individual's conduct. Accordingly, the court denied the motion to dismiss.[624] Judge Rakoff later denied the parties' motions for summary judgment, and the case is set for trial.[625] ***Government Data Collection***. ***New EU/U.S. Data Privacy Framework—Executive Order and Next Steps.*** On October 7, 2022, President Biden issued an executive order listing steps to implement the U.S.'s commitments under the EU-US data privacy framework.[626] The order was issued in response to the Court of Justice of the European Union's invalidation of the EU/US Privacy Shield, which created significant legal uncertainty for companies transferring personal data to and from the US to the EU. In particular, the executive order:

- Directs that the U.S.'s intelligence activities be conducted with privacy and civil liberties safeguards—including for a legitimate purpose and proportionately to such purpose—and requires oversight to the process.
- Calls on intelligence organizations to update their policies and procedures, and seeks to create a two-tiered mechanism for redress of complaints from qualifying EU individuals on collection of personal information in contravention of applicable U.S. law.[627]
- Directs the U.S. Attorney General to issue regulations for creation of a Data Protection Review Court ("DPRC"), which would function as the second level of review in the two tiered mechanism discussed above. Accordingly on October 7, 2022, regulations were issued for the DPRC.[628]

The executive order and the regulation from the Attorney General triggered further actions from the EU side, in terms of proposing an adequacy decision, subject to European Parliament's scrutiny.[629] Under Article 45 of the Regulation (EU) 2016/679, a transfer of personal data from the EU to another country is permitted without specific authorization after the European Commission has determined that such country affords an "adequate" level of data protection.[630] On December 13, 2022, the European Commission issued a

draft adequacy decision, noting that the U.S.' new framework, once adopted, would provide comparable privacy safeguards.[631] It is to be noted that the December 13, 2022 decision is still a draft, and has to be adopted by a committee comprising of EU states' representatives and is subject to European Parliament's scrutiny. Once adopted, the updated privacy framework, would enable transfer of personal data to participating U.S. companies (who join the privacy framework and commit to privacy regulations such as deletion of personal data after completion of purpose, extension of protection despite third party sharing) without specific authorizations.[632] ***CLOUD Act Updates***. The Clarifying Lawful Overseas Use of Data Act ("CLOUD Act"), enacted in 2018, enables the U.S. to enter into executive agreements with other countries that fulfil criteria such as availability of "substantive and procedural protections for privacy and civil liberties" by the foreign government, procedural safeguards to minimize data sourcing of U.S. persons.[633] As noted by the Department of Justice, a CLOUD Act agreement can be utilized to remove restrictions under each country's domestic laws, when a qualifying data request is issued by the counterparty to the agreement.[634] Recently, in October 2022, the U.S. and UK entered into a Data Access Agreement pursuant to the CLOUD Act, the first of its kind.[635] Hence, both U.S. and U.K. are to ensure that their domestic laws permit service providers to comply with orders for data production issued by the other country.[636] However, the agreement sets out certain requirements before the orders issued by either party can seek the benefit of the agreement, including that orders must be for investigation/prosecution of "serious crimes" and must not intentionally target persons in the other country.[637] The U.S. and UK have each selected designated authorities to implement the access agreement. For the U.S., that agency is the DOJ's Office of International Affairs; and for the UK, it is the Investigatory Powers Unit of the UK Home Office.[638] The U.S. has also announced negotiations of an agreement under the CLOUD Act with Canada,[639] which, once adopted, could provide an expedited path for data requests bypassing the existing mutual legal assistance process. The U.S. had also signed a data access agreement in December 2021 with Australia, [640] whereunder each nation has undertaken to ensure that its domestic laws permit service providers to comply with data request orders issued in accordance with the agreement. **V. Conclusion** As with recent years, data privacy and cybersecurity law and policy has evolved substantially over the course of 2022 in an effort to keep up with the unrelenting pace of technological developments and applications. Further, challenges to privacy and cybersecurity arose from global events such as the ongoing COVID-19 pandemic and the launch of Russia's invasion of Ukraine. As a similar, rapid rate-of-change is expected to continue over the year ahead, 2023 will undoubtedly bring novel and more sophisticated developments in law and technology as various stakeholders—companies, governments, and the general public—react to unpredictable challenges and opportunities. In particular, we will see continued aggressive regulatory actions in numerous areas. We will continue tracking these important issues in the year ahead. **Appendix A Comprehensive State Privacy Laws – Comparison Chart**

	CCPA	**CPRA**	**VCDPA**	**CPA**
Effective Date	Jan. 1, 2020	Jan. 1, 2023	Jan. 1, 2023	July 1, 20
Applicability Thresholds	For-profit businesses that **do business in California** and: 1. Have a gross annual revenue of over **$25 million**; 2. Buy, receive, or sell the personal information of **50,000 or more** California residents, households, or devices; or 3. Derive **50% or more of their annual**	For-profit businesses that **do business in California** and: 4. Have a gross annual revenue of over **$25 million** in the preceding calendar year; 5. Buy, sell, or share the personal information of **100,000 or more** California residents or households; or 6. Derive **50% or more of their annual revenue** from selling or sharing California residents' personal information.	Persons that **conduct business in Virginia** or produce products or services that are **targeted to residents of Virginia** and that annually control or process personal data of at least: 1. **100,000** Virginia residents; or 2. **25,000** Virginia residents and **derive over 50% of gross revenue** from the sale of personal data.	Any legal ent **conducts busi Colorado** or pro delivers comr products or se **intentionally ta residents of C** and annually co processes pers of: 1. **100,000** o Colorado reside **25,000** or more residents and **revenue or re discounts** fron

	revenue from selling California residents' personal information.				personal d
Exemption for B2B Data	?	?		?	?
Exemption for Employee Data	?	?		?	?
Exemption for Non-Profits	?	?		?	?
Penalties	$2,500 per violation $7,500 per intentional violation	$2,500 per violation $7,500 per intentional violation or violation involving a minor's protected information		$7,500 per violation plus "reasonable expenses incurred in investigating and preparing the case, including attorney fees"	$20,000 per v
Private Right of Action	?	?		?	?
Cure Period	30 days	Discretionary		30 days	60 days u Jan. 1, 20
				Consumer Rights	
Right to Access	?	?		?	?
Right to Data Portability	?	?		?	?
Right to Delete	?	?		?	?
Right to Correct	?	?		?	?
Right to Opt Out of Sale	?	?		?	?
Right to Opt Out of Sharing for Targeted Advertising	?	?* For cross-context behavioral advertising		? Implied	? Implied
Right to Opt Out of Processing for Targeted Advertising	?	?		?	?
Right to Opt Out of Processing for Profiling	?	?		?	?
Right to Opt In or Out of Processing of Sensitive Information	?	? Opt Out		? Opt In	? Opt In
Right to Non-discrimination	?	?		?	?
				Businesses' Obligations	
Respond to Opt-Out Signal Preferences	?	?		?	? By July 1, 2
Data Minimization	?	?		?	?
Purpose Limitation	?	?		?	?* Purpose Spec
Implement Technical Safeguards	?	?		?	?
Conduct Data Protection Assessments When Processing Poses a Heightened Risk	?	?		?	?
Enter into Data	?*	?		?	?

Processing Agreements with Processors	Required to qualify as a "service provider" relationship				
Respond to Consumer Requests	?	?		?	?
Establish Internal Appeals Process for Consumer Requests	?	?		?	?

_____ [1] New Jersey Disclosure and Accountability Transparency Act ("NJ DaTA"), A.B. 505, 2022-23 Sess. §§ (3)(a)(1), (4)(a) (N.J. 2022). [2] *See*, *e.g.*, *Insights on New California Privacy Law Draft Regulations*, Gibson Dunn (June 15, 2022), *available at* https://www.gibsondunn.com/insights-on-new-california-privacy-law-draft-regulations/; *U.S. Cybersecurity and Data Privacy Outlook and Review – 2021*, § (I)(C)(1)(i)(b), Gibson Dunn (Jan. 28, 2021), *available at* https://www.gibsondunn.com/us-cybersecurity-and-data-privacy-outlook-and-review-2021/; *The Potential Impact of the Upcoming Voter Initiative, the California Privacy Rights Act*, Gibson Dunn (Sept. 29, 2020), *available at* https://www.gibsondunn.com/potential-impact-of-the-upcoming-voter-initiative-the-california-privacy-rights-act/; *As California Consumer Privacy Act Enforcement Commences, a Tougher New Data Privacy Law Will Go Before California Votes in November*, Gibson Dunn (July 1, 2020), *available at* https://www.gibsondunn.com/as-california-consumer-privacy-act-enforcement-commences-a-tougher-new-data-privacy-law-will-go-before-california-voters-in-november/. [3] Cal. Civ. Code § 1798.140(c)(1). [4] Cal. Civ. Code § 1798.110. [5] Cal. Civ. Code § 1798.100(d). [6] Cal. Civ. Code § 1798.105. [7] Cal. Civ. Code § 1798.120. [8] Cal. Civ. Code § 1798.125(a)(1). [9] *Compare* Cal Civ. Code § 1798.140(c)(1)(B) [prior CCPA text], *with* Cal. Civ. Code §§ 1798.140(d)(1)(B) [as modified by CPRA]. [10] *Compare* Cal. Civ. Code § 1798.140(c)(1)(C) [prior CCPA text], *with* Cal. Civ. Code § 1798.140(d)(1)(C) [as modified by CPRA]. [11] Cal. Civ. Code. § 1798.199.45(a). [12] Cal. Civ. Code. § 1798.199.45(a). [13] Cal. Civ. Code §§ 1798.155(a), 1798.199.10(a), 1798.199.40(a). [14] Cal. Civ. Code § 1798.199.90(a). [15] Cal. Civ. Code §§ 1798.155(a), 1798.199.90(a). [16] Cal Civ. Code. §1798.199.10(a). [17] Cal. Priv. Prot. Agency, News & Announcements, *CPPA Releases Notice of Proposed Regulatory Action Implementing New Consumer Privacy Law* (July 8, 2022) *available at* https://cppa.ca.gov/announcements/. [18] California Privacy Protection Agency, *California Consumer Privacy Act Regulations*, *available at* https://cppa.ca.gov/regulations/consumer_privacy_act.html. [19] Draft Regulations § 7025(c)(1). [20] Draft Regulations § 7025(c)(4). [21] Draft Regulations § 7004(c). [22] Draft Regulations § 7302(b). [23] Virginia Consumer Data Protection Act ("VCDPA"), S.B. 1392, 2021 Sess. (Va. 2021) (to be codified in Va. Code tit. 59.1 §§ 59.1-571 to 581). [24] VCDPA, §§ 59.1-572(A)-(B). [25] VCDPA, § 59.1-571. [26] VCDPA, §§ 59.1-573(A)(1)-(5), 59.1-571. [27] VCDPA, § 59.1-573(A)(5). [28] VCDPA, § 59.1-573(A)(5). [29] VCDPA, §§ 59.1-571, 59.1-574(A)(5). [30] VCDPA, § 59.1-573(C). [31] VCDPA, § 59.1-573(C). [32] VCDPA, § 59.1-573(C). [33] VCDPA, §§ 59.1-575(B), 59.1-576(A)-(B). [34] H 381, 2022 Gen. Assemb., Reg. Sess. (Va. 2022). [35] S 534, 2022 Gen. Assemb., Reg. Sess. (Va. 2022). [36] VCDPA, §§ 59.1-579(A)-(B), 59.1-580(A). [37] VCDPA, §§ 59.1-580(B)-(C). [38]VCDPA, § 59.1-579(C). [39] Colorado Privacy Act ("CPA"), S.B. 21-190, 73rd Gen. Assemb., Reg. Sess. (Colo. 2021) (to be codified in Colo. Rev. Stat. Title 6). [40] CPA, § 6-1-1304(I). [41] CPA, §§ 6-1-1302(c)(II)(A), 6-1-1306(1)(b)-(e). [42] CPA, § 6-1-1306(1)(a). [43] CPA, § 6-1-1303(23)(a) (emphasis added). [44] CPA, § 6-1-1303(23)(b). [45] CPA, § 6-1-1306(1)(a)(II). [46] CPA, § 6-1-1306(1)(a)(IV)(B). [47] CPA, § 6-1-1308(7). [48] CPA, § 6-1-1303(24). [49] CPA, § 6-1-1306(3)(a). [50] *See generally* CPA, §§ 6-1-1305(2)(b), 6-1-1308(3). [51] CPA, §§ 6-1-1309(1), (3). [52] CPA, § 6-1-1305(3)-(5). [53] Colo. Dep't of Law, Proposed Colorado Privacy Act Rules, to be codified at 4 Colo. Code Regs. § 904-3, *available at* https://coag.gov/app/uploads/2022/12/CPA_Version-2-Proposed-Draft-Regulations-12.21.2022.pdf. [54] CPA, §§ 6-1-1311(1)(a), (d). [55] CPA, § 6-1-1311(1)(c); *see also* Colo. Rev. Stat. § 6-1-112(1)(a). [56] Connecticut Data Privacy Act ("CTDPA"), S.B. 6, 2022, Gen. Assemb., Reg. Sess. (Conn. 2022). [57] CTDPA, § 2. [58] CTDPA, §

1(7). [59] CTDPA, §§ 4(a)(1)-(4). [60] CTDPA, § 4(a)(5). [61] CTDPA, § 1(26). [62] CTDPA, § 6(e)(1)(A)(ii). [63] CTDPA, § 6(a)(6). [64] CTDPA, §§ 6(a)(1)-(3), 7(b), 8. [65] CTDPA, § 4(d). [66] CTDPA, § 11(a). [67] CTDPA, §§ 11(b)-(c). [68] CTDPA, § 11(e). [69] Conn. Gen. Stat. § 42-110o. [70] UCPA, § 13-61-101(10)(b). [71] Cal. Civ. Code § 1798.145(h)(3). [72] VCDPA, § 59.1-573(B)(3). [73] CPA, § 6-1-1306(2)(c). [74] UCPA, §§ 13-61-203(4)(b)(i)(B)-(C). [75] UCPA, §§ 13-61-305, 13-61-401, 13-61-402(1)-(2), 13-61-402(3)(a)-(c). [76] UCPA, § 13-61-402(3)(d). [77] Cal. Civ. Code § 1798.140(ah), *available at* https://www.caprivacy.org/cpra-text/. [78] Cal. Civ. Code § 1798.140(k), *available at* https://www.caprivacy.org/cpra-text/. [79] "Targeted Advertising" is defined similarly under each state privacy law. *See* § (25)(a), Colorado Privacy Act, *available at* https://leg.colorado.gov/sites/default/files/2021a_190_signed.pdf. *See also* § 59.1-571, Virginia Consumer Data Protection Act, *available at* https://law.lis.virginia.gov/vacodefull/title59.1/chapter53/. *See also* § 34(a), 13-61-101, Utah Consumer Privacy Act, *available at* https://le.utah.gov/~2022/bills/static/SB0227.html. *See also* § 1(28), Connecticut SB6, *available at* https://www.cga.ct.gov/2022/ACT/PA/PDF/2022PA-00015-R00SB-00006-PA.PDF. [80] *See* CPRA Draft Regulations § 7025(a), *available at* https://cppa.ca.gov/meetings/materials/20221021_22_item3_modtext.pdf; *see also* § 6-1-1306 (1)(a)(IV)(A), Colorado Privacy Act. *See also* § 6 (e)(B), Connecticut SB6. [81] Cal. Civ. Code §§ 1798.99.28-.40. [82] Cal. Civ. Code § 1798.99.30(b)(4). [83] Cal. Civ. Code § 1798.99.31(a)(6). [84] Cal. Civ. Code § 1798.99.31(a)(7). [85] Cal. Civ. Code §§ 1798.99.31(b)(2)-(3). [86] Cal. Civ. Code §§ 1798.99.31(b)(1), (4). [87] Cal. Civ. Code § 1798.99.31(b)(7). [88] Cal. Civ. Code § 1798.88.31(a)(1)(A). [89] Cal. Civ. Code § 1798.88.31(a)(2). [90] Cal. Civ. Code § 1798.99.35. [91] Cal. Civ. Code § 1798.99.35(d). [92] A.B. No. 2089, 2021-22 Leg. Sess. (Cal. 2022) (to be codified at Cal Civ. Code 56.05, 56.06, 56.251). [93] *Id.* [94] *Id.* [95] *Id.* [96] N.Y. Dep't Fin. Servs., *Proposed Second Amendment to 23 NYCRR 500* (Nov. 9, 2022), *available at* https://www.dfs.ny.gov/system/files/documents/2022/10/rp23a2_text_20221109_0.pdf. [97] Press Release, N.Y. Dep't Fin. Servs., *DFS Superintendent Adrienne A. Harris Issues New Guidance To Prevent and Manage Suspicious Activities in the Virtual Currency Industry: New York State-Regulated Virtual Currency Entities Encouraged To Adopt Blockchain Analytics Tools as a Best Practice* (Apr. 28, 2022), *available at* https://www.dfs.ny.gov/reports_and_publications/press_releases/pr202204281. [98] Actions - H.R. 8152 - 117th Congress (2021-2022): American Data Privacy and Protection Act, H.R. 8152, 117th Cong. (2022), http://www.congress.gov/. [99] American Data Privacy and Protection Act ("ADPPA"), H.R. 8152, 117th Cong. § 2(9)(A) (2022). [100] *Id.* at §§ 101(a), 102(a). [101] *Id.* at § 101(a). [102] *Id.* at § 102(a). [103] *Id.* at § 103(a). [104] *Id.* at § 2(2). [105] *Id.* at § 207(a)(1). [106] *Id.* at § 207(c)(1). [107] *Id.* at § 207(c)(3)(C). [108] *Id.* at §§ 401, 207(c)(5). [109] *Id.* at § 401(a)-(b). [110] *Id.* at § 401(a)(1). [111] *Id.* at § 402(a). [112] *Id.* at § 403(a). [113] *Id.* at § 403(a)(3)(A). [114] *Id.* at § 404(b)(1). [115] *Id.* at § 404(b)(2)(L). [116] Letter from Rob Bonta, California Attorney General, et al., to Congress (July 19, 2022), *available at* https://oag.ca.gov/system/files/attachments/press-docs/Letter%20to%20Congress%20re%20Federal%20Privacy.pdf. [117] Letter from Ashkan Soltani, Executive Director of the California Privacy Protection Agency, to Nancy Pelosi, Speaker of the United States House of Representatives, and Kevin McCarthy, Minority Leader of the United States House of Representatives, *H.R. 8152, The American Data Privacy and Protection Act – Oppose* (Aug 15, 2022), *available at* https://cppa.ca.gov/pdf/hr8152_oppose.pdf. [118] Press Release, Congresswoman Nancy Pelosi, *Pelosi Statement on Federal Data Privacy Legislation* (Sep. 1, 2022), *available at* https://pelosi.house.gov/news/press-releases/pelosi-statement-on-federal-data-privacy-legislation. [119] Christiano Lima, *Top Senate Democrat Casts Doubt on Prospect of Major Data Privacy Bill*, Wash. Post (June 22, 2022, 5:53 PM), *available at* https://www.washingtonpost.com/technology/2022/06/22/privacy-bill-maria-cantwell-congress/. [120] Rebecca Kern, *Bipartisan draft bill breaks stalemate on federal data privacy negotiations*, Politico (June 3, 2022, 1:17 PM), *available at* https://www.politico.com/news/2022/06/03/bipartisan-draft-bill-breaks-stalemate-on-federal-privacy-bill-negotiations-00037092. [121] *See* Press Release, Federal Trade Commission, *FTC Chair Lina M. Khan Announces New Appointments in Agency*

Leadership Positions (Nov. 19, 2021), *available at* https://www.ftc.gov/news-events/news/press-releases/2021/11/ftc-chair-lina-m-khan-announces-new-appointments-agency-leadership-positions; Press Release, Federal Trade Commission, *Federal Trade Commission Chair Lina M. Khan Appoints New Chief Technology Officer and Public Affairs Director* (Oct. 3, 2022), *available at* https://www.ftc.gov/news-events/news/press-releases/2022/10/federal-trade-commission-chair-lina-m-khan-appoints-new-chief-technology-officer-public-affairs. [122] *See, e.g.,* Andrew Smith, *Using Artificial Intelligence and Algorithms*, Federal Trade Commission (Apr. 8, 2020), *available at* https://www.ftc.gov/business-guidance/blog/2020/04/using-artificial-intelligence-and-algorithms; Report, *Big Data: A tool for inclusion or exclusion?*, Federal Trade Commission (Jan. 2016), *available at* https://www.ftc.gov/system/files/documents/reports/big-data-tool-inclusion-or-exclusion-understanding-issues/160106big-data-rpt.pdf. [123] Elisa Jillson, *Aiming for Truth, Fairness, and Equity in Your Company's Use of AI*, Federal Trade Commission (Apr. 19, 2021), *available at* https://www.ftc.gov/news-events/blogs/business-blog/2021/04/aiming-truth-fairness-equity-your-companys-use-ai. [124] *Id.* [125] *Id.* [126] *Id.* [127] Report to Congress, Federal Trade Commission, *Combatting Online Harms Through Innovation* (June 16, 2022), *available at* https://www.ftc.gov/system/files/ftc_gov/pdf/Combatting%20Online%20Harms%20Through%20Innovation%3B%20Federal%20Trade%20Commission%20Report%20to%20Congress.pdf. [128] Press Release, Federal Trade Commission, *FTC Report Warns About Using Artificial Intelligence to Combat Online Problems* (June 16, 2022), *available at* https://www.ftc.gov/news-events/news/press-releases/2022/06/ftc-report-warns-about-using-artificial-intelligence-combat-online-problems. [129] *Id.* [130] *Id.* [131] *Id.* [132] Press Release, Federal Trade Commission, *Federal Trade Commission Takes Action Against Passport Automotive Group for Illegally Charging Junk Fees and Discriminating Against Black and Latino Customers* (Oct. 18, 2022), *available at* https://www.ftc.gov/news-events/news/press-releases/2022/10/federal-trade-commission-takes-action-against-passport-automotive-group-illegally-charging-junk-fees. [133] Press Release, Federal Trade Commission, *FTC Finalizes Settlement with Photo App Developer Related to Misuse of Facial Recognition Technology* (May 7, 2021), *available at* https://www.ftc.gov/news-events/news/press-releases/2021/05/ftc-finalizes-settlement-photo-app-developer-related-misuse-facial-recognition-technology. [134] Lina M. Khan, Chair, Federal Trade Commission, *Remarks of Chair Lina M. Khan As Prepared for Delivery IAPP Global Privacy Summit 2022* (Apr. 11, 2022), *available at* https://www.ftc.gov/system/files/ftc_gov/pdf/Remarks%20of%20Chair%20Lina%20M.%20Khan%20at%20IAPP%20Global%20Privacy%20Summit%202022%20-%20Final%20Version.pdf. [135] *Id.* [136] *Id*. [137] *Id.* [138] *Id.* [139] *Id*. [140] *Id.* [141] *Id*. [142] Trade Regulation Rule on Commercial Surveillance and Data Security, 87 Fed. Reg. 51273 (published Aug. 22, 2022), *available at* https://www.federalregister.gov/documents/2022/08/22/2022-17752/trade-regulation-rule-on-commercial-surveillance-and-data-security. [143] *Id*. [144] *Id*. [145] *Id*. [146] Events Announcement, Federal Trade Commission, *Commercial Surveillance and Data Security Public Forum* (Sept. 8, 2022), *available at* https://www.ftc.gov/news-events/events/2022/09/commercial-surveillance-data-security-anpr-public-forum. [147] *Id.* [148] Lina M. Khan, Chair, Federal Trade Commission, Remarks of Chair Lina M. Khan As Prepared for Delivery IAPP Global Privacy Summit 2022 (Apr. 11, 2022), *available at* https://www.ftc.gov/system/files/ftc_gov/pdf/Remarks%20of%20Chair%20Lina%20M.%20Khan%20at%20IAPP%20Global%20Privacy%20Summit%202022%20-%20Final%20Version.pdf. [149] Complaint, *U.S. v. Kurbo, Inc. and WW International, Inc*., FTC Docket No. 22-CV-946 (Feb. 16, 2022). [150] Press Release, Federal Trade Commission, *FTC Charges Twitter with Deceptively Using Account Security Data to Sell Targeted Ads* (May 25, 2022), *available*

at https://www.ftc.gov/news-events/news/press-releases/2022/05/ftc-charges-twitter-deceptively-using-account-security-data-sell-targeted-ads. [151] *Id.* [152] *Id.* [153] *Id.* [154] Richard Blumenthal et al., *Letter to FTC Chair Lina Khan* (Nov. 17, 2022), *available at* https://www.blumenthal.senate.gov/imo/media/doc/111722ftctwitterletter.pdf. [155] Press Release, Federal Trade Commission, *FTC Finalizes Action Against CafePress for Covering Up Data Breach, Lax Security* (June 24, 2022), *available at* https://www.ftc.gov/news-events/news/press-releases/2022/06/ftc-finalizes-action-against-cafepress-covering-data-breach-lax-security-0. [156] Press Release, Federal Trade Commission, *FTC Takes Action Against Drizly and its CEO James Cory Rellas for Security Failures that Exposed Data of 2.5 Million Consumers* (Oct. 24, 2022), *available at* https://www.ftc.gov/news-events/news/press-releases/2022/10/ftc-takes-action-against-drizly-its-ceo-james-cory-rellas-security-failures-exposed-data-25-million. [157] *Id.* [158] *Id.* [159] *Id.* [160] Charles Manning, *Open Letter from Kochava CEO* (Sep. 1, 2022), *available at* https://www.kochava.com/open-letter-from-kochava-ceo/. [161] Complaint, *FTC v. Kochava, Inc*., FTC Docket No. 22-CV-377 (Aug. 29, 2022), *available at* https://www.ftc.gov/system/files/ftc_gov/pdf/1.%20Complaint.pdf. [162] Press Release, Federal Trade Commission, *FTC Sues Kochava for Selling Data that Tracks People at Reproductive Health Clinics, Places of Worship, and Other Sensitive Locations* (Aug. 29, 2022), *available at* https://www.ftc.gov/news-events/news/press-releases/2022/08/ftc-sues-kochava-selling-data-tracks-people-reproductive-health-clinics-places-worship-other. [163] Complaint, *FTC v. Kochava, Inc*., FTC Docket No. 22-CV-377, at 11 (Aug. 29, 2022), *available at* https://www.ftc.gov/system/files/ftc_gov/pdf/1.%20Complaint.pdf. [164] Press Release, Federal Trade Commission, *Multiple Data Breaches Suggest Ed Tech Company Chegg Didn't Do its Homework, Alleges FTC* (Oct. 31, 2022), *available at* https://www.ftc.gov/business-guidance/blog/2022/10/multiple-data-breaches-suggest-ed-tech-company-chegg-didnt-do-its-homework-alleges-ftc. [165] *Id.* [166] Press Release, Federal Trade Commission, *FTC Brings Action Against Ed Tech Provider Chegg for Careless Security that Exposed Personal Data of Millions of Customers* (Oct. 31, 2022), *available at* https://www.ftc.gov/news-events/news/press-releases/2022/10/ftc-brings-action-against-ed-tech-provider-chegg-careless-security-exposed-personal-data-millions. [167] Press Release, Federal Trade Commission, *Fortnite Video Game Maker Epic Games to Pay More Than Half a Billion Dollars over FTC Allegations of Privacy Violations and Unwanted Charges* (Dec. 19, 2022), available at https://www.ftc.gov/news-events/news/press-releases/2022/12/fortnite-video-game-maker-epic-games-pay-more-half-billion-dollars-over-ftc-allegations. [168] *Id.* [169] *Id.* [170] *Id.* [171] *Id.* [172] Press Release, Federal Trade Commission, *FTC Extends Deadline by Six Months for Compliance with Some Changes to Financial Data Security Rule* (Nov. 15, 2022), *available at* https://www.ftc.gov/news-events/news/press-releases/2022/11/ftc-extends-deadline-six-months-compliance-some-changes-financial-data-security-rule. [173] Lesley Fair, *FTC to Ed Tech: Protecting kid's privacy is your responsibility*, Federal Trade Commission (May 19, 2022), *available at* https://www.ftc.gov/business-guidance/blog/2022/05/ftc-ed-tech-protecting-kids-privacy-your-responsibility. [174] Lesley Fair, *Where in the world is…? FTC challenges stealthy geolocation tracking and COPPA violations*, Federal Trade Commission (Dec. 15, 2021), *available at* https://www.ftc.gov/business-guidance/blog/2021/12/where-world-ftc-challenges-stealthy-geolocation-tracking-coppa-violations. [175] *Id.* [176] Press Release, Federal Trade Commission, *FTC Extends Deadline for Comments on COPPA Rule until December 11* (Dec. 9, 2022), *available at* https://www.ftc.gov/news-events/news/press-releases/2019/12/ftc-extends-deadline-comments-coppa-rule-until-december-11. [177] Lesley Fair, *FTC to Ed Tech: Protecting kid's privacy is your responsibility*, Federal Trade Commission (May 19, 2022), *available at* https://www.ftc.gov/business-guidance/blog/2022/05/ftc-ed-tech-protecting-kids-privacy-your-responsibility. [178] *Id.* [179] *Id.* [180] *Id.* [181] *Id.* [182] *Id.* [183] Lina M. Khan, Chair, Federal Trade Commission, Remarks of Commission Chair Lina Khan at the FTC Open Commission Meeting (May 19, 2022), *available at* https://www.ftc.gov/system/files/ftc_gov/pdf/Transcript-Open-Commission-Meeting-

May-19-2022.pdf. [184] Lesley Fair, *When it comes to health data, comply with COPPA—no kidding*, Federal Trade Commission (Mar. 4, 2022), *available at* https://www.ftc.gov/business-guidance/blog/2022/03/when-it-comes-health-data-comply-coppa-no-kidding. [185] Petition for Rulemaking of the Center for Digital Democracy, Fairplay, 87 Fed. Reg. 74056 (published Dec. 2, 2022), *available at* https://www.federalregister.gov/documents/2022/12/02/2022-26254/petition-for-rulemaking-of-the-center-for-digital-democracy-fairplay-et-al. [186] Trade Regulation Rule on Commercial Surveillance and Data Security, 87 Fed. Reg. 51273 (published Aug. 22, 2022), *available at* https://www.federalregister.gov/documents/2022/08/22/2022-17752/trade-regulation-rule-on-commercial-surveillance-and-data-security. [187] Staff Report, FTC, *Bringing Dark Patterns to Light* (Sept. 15, 2022), https://www.ftc.gov/system/files/ftc_gov/pdf/P214800%20Dark%20Patterns%20Report%209.14.2022%20-%20FINAL.pdf. [188] *Id*. [189] *Id.* at 18. [190] *FTC v. VIZIO, Inc. and VIZIO Inscape Servs., LLC*, (D.N.J.); FTC Press Release, *Vizio to Pay $2.2 Million to FTC, State of New Jersey to Settle Charges It Collected Viewing Histories on 11 Million Smart Televisions Without Users' Consent* (Feb. 6, 2017), *available at* https://www.ftc.gov/news-events/press-releases/2017/02/vizio-pay-22-million-ftcstate-new-jersey-settle-charges-it. [191] *Id*. [192] Press Release, Federal Trade Commission, *Fortnite Video Game Maker Epic Games to Pay More Than Half a Billion Dollars over FTC Allegations of Privacy Violations and Unwanted Charges* (Dec. 19, 2022), *available at* https://www.ftc.gov/news-events/news/press-releases/2022/12/fortnite-video-game-maker-epic-games-pay-more-half-billion-dollars-over-ftc-allegations; Press Release, Federal Trade Commission, *FTC Action Against Vonage Results in $100 Million to Customers Trapped by Illegal Dark Patterns and Junk Fees When Trying to Cancel Service* (Nov. 3, 2022), *available at* https://www.ftc.gov/news-events/news/press-releases/2022/11/ftc-action-against-vonage-results-100-million-customers-trapped-illegal-dark-patterns-junk-fees-when-trying-cancel-service. [193] Press Release, CFPB, *CFPB Invokes Dormant Authority to Examine Nonbank Companies Posing Risks to Consumers* (Apr. 25, 2022), *available at* https://www.consumerfinance.gov/about-us/newsroom/cfpb-invokes-dormant-authority-to-examine-nonbank-companies-posing-risks-to-consumers/. [194] *CFPB Invokes Dormant Dodd-Frank Authority to Regulate Nonbank Financial Companies*, Gibson Dunn (May 5, 2022) *available at* https://www.gibsondunn.com/cfpb-invokes-dormant-dodd-frank-authority-to-regulate-nonbank-financial-companies/. [195] Press Release, CFPB, *CFPB Invokes Dormant Authority to Examine Nonbank Companies Posing Risks to Consumers* (Apr. 25, 2022), *available at* https://www.consumerfinance.gov/about-us/newsroom/cfpb-invokes-dormant-authority-to-examine-nonbank-companies-posing-risks-to-consumers/. [196] *Id.* [197] Press Release, CFPB, *The CFPB Finalizes Rule to Increase Transparency Regarding Key Nonbank Supervision Tool* (Nov. 10, 2022), https://www.consumerfinance.gov/about-us/blog/the-cfpb-finalizes-rule-to-increase-transparency-regarding-key-nonbank-supervision-tool/. [198] CFPB, *Proposed Rule: Registry of Nonbank Covered Persons Subject to Certain Agency and Court Orders*, Docket No. CFPB-2022-0080 (Dec. 12, 2022), *available at* https://files.consumerfinance.gov/f/documents/cfpb_proposed-rule__registry-of-nonbank-covered-persons_2022.pdf. [199] Press Release, CFPB, *Consumer Financial Protection Bureau Outlines Options to Prevent Algorithmic Bias in Home Valuations* (Feb. 23, 2022), *available at* https://www.consumerfinance.gov/about-us/newsroom/cfpb-outlines-options-to-prevent-algorithmic-bias-in-home-valuations/. [200] CFPB, Circular 2022-03, *Adverse Action Notification Requirements in Connection with Credit Decisions Based on Complex Algorithms* (2022), *available at* https://www.consumerfinance.gov/compliance/circulars/circular-2022-03-adverse-action-notification-requirements-in-connection-with-credit-decisions-based-on-complex-algorithms/. [201] *Id.* [202] Press Release, CFPB, *CFPB Acts to Protect the Public from Black-Box Credit Models Using Complex Algorithms* (May 26, 2022), *available at* https://www.consumerfinance.gov/about-us/newsroom/cfpb-acts-to-protect-the-public-from-black-box-credit-models-using-complex-algorithms/. [203] Press Release, FTC, *FTC Staff*

Provides Annual Letter to CFPB on 2021 Equal Credit Opportunity Act Activities (Feb. 23, 2022), *available at* https://www.ftc.gov/news-events/news/press-releases/2022/02/ftc-staff-provides-annual-letter-cfpb-2021-equal-credit-opportunity-act-activities. [204] FTC, *FTC Enforcement Activities under the ECOA and Regulation B in 2021: Report to the CFPB* (Feb. 23, 2022), *available at* https://www.ftc.gov/system/files/ftc_gov/pdf/p154802cfpbecoareport2021.pdf. [205] Eric Halperin & Lorelei Salas, *Cracking Down on Discrimination in the Financial Sector*, CFPB Blog (Mar. 16, 2022), *available at* https://www.consumerfinance.gov/about-us/blog/cracking-down-on-discrimination-in-the-financial-sector/. [206] *Id.* [207] *Id.* [208] Press Release, CFPB, *CFPB Takes Action Against Hello Digit for Lying to Consumers About Its Automated Savings Algorithm* (Aug. 10, 2022), *available at* https://www.consumerfinance.gov/about-us/newsroom/cfpb-takes-action-against-hello-digit-for-lying-to-consumers-about-its-automated-savings-algorithm/. [209] Press Release, CFPB, *Consumer Financial Protection Bureau Outlines Options to Prevent Algorithmic Bias in Home Valuations* (Feb. 23, 2022), *available at* https://www.consumerfinance.gov/about-us/newsroom/cfpb-outlines-options-to-prevent-algorithmic-bias-in-home-valuations/. [210] *Id*. [211] Press Release, CFPB, *CFPB Acts to Protect the Public from Black-Box Credit Models Using Complex Algorithms* (May 26, 2022), *available at* https://www.consumerfinance.gov/about-us/newsroom/cfpb-acts-to-protect-the-public-from-black-box-credit-models-using-complex-algorithms/. [212] *Id.* [213] *Id.* [214] Paul Singer, Abigail Stempson & Beth Chun, *Statements to the State AGs: CFPB and FTC Priorities for 2023*, Kelley Drye (Dec. 9, 2022), https://www.adlawaccess.com/2022/12/articles/statements-to-the-state-ags-cfpb-and-ftc-priorities-for-2023/. [215] Rohit Chopra, *Statement Regarding the CFPB's Inquiry into Big Tech Payment Platforms*, CFPB (Oct. 21, 2021), https://www.consumerfinance.gov/about-us/newsroom/statement-regarding-the-cfpbs-inquiry-into-big-tech-payment-platforms/. [216] *Id.* [217] Press Release, CFPB, *CFPB Warns that Digital Marketing Providers Must Comply with Federal Consumer Finance Protections* (Aug. 10, 2022), *available at* https://www.consumerfinance.gov/about-us/newsroom/cfpb-warns-that-digital-marketing-providers-must-comply-with-federal-consumer-finance-protections/. [218] *Id.* [219] John McNamara, *CFPB Tells Credit Card CEOs: Practice of Suppressing Payment Data Has Potential for Consumer Harm*, CFPB Blog (May 25, 2022), https://www.consumerfinance.gov/about-us/blog/cfpb-tells-credit-card-ceos-practice-of-suppressing-payment-data-has-potential-for-consumer-harm/. [220] *Id.* [221] CFPB, *Buy Now, Pay Later: Market Trends and Consumer Impacts* (Sept. 2022), *available at* https://files.consumerfinance.gov/f/documents/cfpb_buy-now-pay-later-market-trends-consumer-impacts_report_2022-09.pdf. [222] Press Release, CFPB, *CFPB Study Details the Rapid Growth of "Buy Now, Pay Later" Lending* (Sept. 15, 2022), *available at* https://www.consumerfinance.gov/about-us/newsroom/cfpb-study-details-the-rapid-growth-of-buy-now-pay-later-lending/. [223] *Id.* [224] Press Release, CFPB, *CFPB Kicks Off Personal Financial Data Rights Rulemaking* (Oct. 27, 2022), *available at* https://www.consumerfinance.gov/about-us/newsroom/cfpb-kicks-off-personal-financial-data-rights-rulemaking/. [225] CFPB, *Small Business Advisory Review Panel for Required Rulemaking on Personal Financial Data Rights* (Oct. 27, 2022), *available at* https://files.consumerfinance.gov/f/documents/cfpb_data-rights-rulemaking-1033-SBREFA_outline_2022-10.pdf. [226] Press Release, CFPB, *CFPB Kicks Off Personal Financial Data Rights Rulemaking* (Oct. 27, 2022), *available at* https://www.consumerfinance.gov/about-us/newsroom/cfpb-kicks-off-personal-financial-data-rights-rulemaking/. [227] Press Release, *Director Chopra's Prepared Remarks at Money 20/20*, CFPB (Oct. 25, 2022), *available at* https://www.consumerfinance.gov/about-us/newsroom/director-chopra-prepared-remarks-at-money-20-20/. [228] *Id.* [229] CFPB, Circular 2022-04, *Insufficient Data Protection or Security for Sensitive Consumer Information* (2022), *available at* https://www.consumerfinance.gov/compliance/circulars/circular-2022-04-insufficient-data-protection-or-security-for-sensitive-consumer-information/. [230] Press Release, CFPB, *CFPB Takes Action to Protect the Public from Shoddy Data Security Practices* (Aug. 11, 2022), *available at*

https://www.consumerfinance.gov/about-us/newsroom/cfpb-takes-action-to-protect-the-public-from-shoddy-data-security-practices/. [231] CFPB, *Complaint Bulletin: An Analysis of Consumer Complaints Related to Crypto-Assets* (Nov. 2022), *available at* https://files.consumerfinance.gov/f/documents/cfpb_complaint-bulletin_crypto-assets_2022-11.pdf. [232] Press Release, SEC, *SEC Proposes Cybersecurity Risk Management Rules and Amendments for Registered Investment Advisers and Funds* (Feb. 9, 2022), *available at* https://www.sec.gov/news/press-release/2022-20. [233] Cybersecurity Risk Management for Investment Advisers, Registered Investment, 87 Fed. Reg. 13524, 13561 (proposed Mar. 9, 2022) (to be codified at 40 C.F.R. pts. 230-279). [234] *Id*. [235] *Id*. at 13576. [236] *Id*. at 13533, 13540. [237] *Id.* at 13541. [238] *Id*. at 13578-79. [239] Hester M. Peirce, *Statement by Commissioner Peirce on Proposal for Mandatory Cybersecurity Disclosures*, SEC (Feb. 9, 2022), *available at* https://www.sec.gov/news/statement/peirce-statement-cybersecurity-risk-management-020922. [240] Off. of Mgmt. and Budget, Off. of Info. & Reg. Affs., SEC Agency Rule List - Fall 2022, https://www.reginfo.gov/public/do/eAgendaMain?operation=OPERATION_GET_AGENCY_RULE_LIST&currentPub=true&agencyCode=&showStage=active&agencyCd=3235&csrf_token=719D9069A6A2307A419060DE1EA2B78FA7F312F3D9ECC0826CE5C087AC965D1D54A2056E2C7574CDC380C46931D210AF148D (last visited Jan. 26, 2023). [241] Off. of Mgmt. and Budget, Off. of Info. & Reg. Affs., *Cybersecurity Risk Governance* (3235-AN08), https://www.reginfo.gov/public/do/eAgendaViewRule?pubId=202210&RIN=3235-AN08 (last visited Jan. 26, 2023). [242] Press Release, SEC, *SEC Proposes Rules on Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure by Public Companies* (Mar. 9, 2022), *available at* https://www.sec.gov/news/press-release/2022-39. [243] Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure, Exchange Act Release, 87 Fed. Reg. 16590, 16595 (proposed Mar. 23, 2022) (to be codified at 17 C.F.R. pts. 229-249). [244] *Id*. at 16596-97. [245] *Id.* at 16595. [246] *Id.* [247] *Id.* at 16599. [248] *Id*. at 16602. [249] Hester M. Peirce, *Dissenting Statement on Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure Proposal*, SEC (Mar. 9, 2022), *available at* https://www.sec.gov/news/statement/peirce-statement-cybersecurity-030922. [250] Off. of Mgmt. and Budget, Off. of Info. & Reg. Affs., *Cybersecurity Risk Governance* (3235-AM89), https://www.reginfo.gov/public/do/eAgendaViewRule?pubId=202210&RIN=3235-AM89 (last visited Jan. 26, 2023). [251] Gary Gensler, Chair, SEC, *Remarks on Cybersecurity and Securities Laws at the Northwestern University Pritzker School of Law* (Jan. 24, 2020), *available at* https://www.sec.gov/news/speech/gensler-cybersecurity-and-securities-laws-20220124. [252] *Id*. [253] Gary Gensler, Chair, SEC, *Remarks by Chair Gensler Before the FBIIC and FSSCC* (Apr. 15, 2022), *available at* https://corpgov.law.harvard.edu/2022/04/15/remarks-by-chair-gensler-before-the-fbiic-and-fssc/. [254] *Id*. [255] Off. of Mgmt. and Budget, Off. of Info. & Reg. Affs., *Cybersecurity* (3235-AN15), https://www.reginfo.gov/public/do/eAgendaViewRule?pubId=202210&RIN=3235-AN15 (last visited Jan. 26, 2023). [256] Press Release, SEC, *SEC Nearly Doubles Size of Enforcement's Crypto Assets and Cyber Unit* (May 3, 2022), *available at* https://www.sec.gov/news/press-release/2022-78. [257] *Id.* [258] *See, e.g.*, Press Release, SEC, *SEC Seeks to Stop the Registration of Misleading Crypto Asset Offerings* (Nov. 18, 2022), *available at* https://www.sec.gov/news/press-release/2022-208 (instituting administrative proceeding against American CryptoFed DAO LLC "to determine whether a stop order should be issued to suspend the registration of the offer and sale of two crypto assets, the Ducat token and the Locke token"); Press Release, SEC, *SEC Charges Creator of Global Crypto Ponzi Scheme and Three US Promoters in Connection with $295 Million Fraud* (Nov. 4, 2022), *available at* https://www.sec.gov/news/press-release/2022-201 (filing charges against defendants allegedly involved in "fraudulent crypto Ponzi scheme" under antifraud, securities registration, and broker-dealer registration provisions of the securities laws); Press Release, SEC, *SEC Charges The Hydrogen Technology Corp. and its Former CEO for*

Market Manipulation of Crypto Asset Securities (Sept. 28, 2022), *available at* https://www.sec.gov/news/press-release/2022-175 (announcing charges against individuals and entity "for their roles in effectuating the unregistered offers and sales of crypto asset securities"); Press Release, SEC, *Sparkster to Pay $35 Million to Harmed Investor Fund for Unregistered Crypto Asset Offering* (Sept. 19, 2022), *available at* https://www.sec.gov/news/press-release/2022-167 (issuing cease-and-desist order "for the unregistered offer and sale of crypto asset securities" and charging failure to disclose compensation for promoting tokens); Press Release, SEC, *SEC Charges Eleven Individuals in $300 Million Crypto Pyramid Scheme* (Aug. 1, 2022), *available at* https://www.sec.gov/news/press-release/2022-134 (bringing charges against individuals "for their roles in creating and promoting . . . a fraudulent crypto pyramid and Ponzi scheme"); Press Release, SEC, *SEC Charges Former Coinbase Manager, Two Others in Crypto Asset Insider Trading Action* (July 21, 2022), *available at* https://www.sec.gov/news/press-release/2022-127 (charging former Coinbase product manager, his brother, and his friend for insider trading crypto assets); Press Release, SEC, *SEC Halts Fraudulent Cryptomining and Trading Scheme* (May 6, 2022), *available at* https://www.sec.gov/news/press-release/2022-81 (charging defendants with "unregistered offerings and fraudulent sales of investment plans called mining packages to thousands of investors"); Press Release, SEC, *SEC Charges NVIDIA Corporation with Inadequate Disclosures about Impact of Cryptomining* (May 6, 2022), *available at* https://www.sec.gov/news/press-release/2022-79 (announcing a settlement for $5.5 million based on "inadequate disclosures concerning the impact of cryptomining on the company's gaming business"). [259] Press Release, SEC, *BlockFi Agrees to Pay $100 Million in Penalties and Pursue Registration of its Crypto Lending Product* (Feb. 14, 2022), *available at* https://www.sec.gov/news/press-release/2022-26. [260] Press Release, SEC, *SEC Charges Kim Kardashian for Unlawfully Touting Crypto Security* (Oct. 3, 2022), *available at* https://www.sec.gov/news/press-release/2022-183. [261] Press Release, SEC, *SEC Charges Samuel Bankman-Fried with Defrauding Investors in Crypto Asset Trading Platform* FTX (Dec. 13, 2022), *available at* https://www.sec.gov/news/press-release/2022-219. [262] *Id.*; *see also* Press Release, SEC, *SEC Charges Caroline Ellison and Gary Wang with Defrauding Investors in Crypto Asset Trading Platform FTX* (Dec. 21, 2022), *available at* https://www.sec.gov/news/press-release/2022-234. [263] Jessica Corso, *SEC, Ripple Issue Final Salvos As Crypto Decision Nears*, Law360 (Dec. 5, 2022), *available at* https://www.law360.com/articles/1555098/sec-ripple-issue-final-salvos-as-crypto-decision-nears. [264] Press Release, SEC, *SEC Charges JPMorgan, UBS, and TradeStation for Deficiencies Relating to the Prevention of Customer Identity Theft* (July 27, 2022), *available at* https://www.sec.gov/news/press-release/2022-131. [265] *Id.* [266] Press Release, SEC, *SEC Charges Three Chicago-Area Residents with Insider Trading Around Equifax Data Breach Announcement* (Aug. 16, 2022), *available at* https://www.sec.gov/litigation/litreleases/2022/lr25470.htm. [267] Press Release, SEC, *Morgan Stanley Smith Barney to Pay $35 Million for Extensive Failures to Safeguard Personal Information of Millions of Customers* (Sept. 20, 2022), *available at* https://www.sec.gov/news/press-release/2022-168. [268] Press Release, Department of Health and Human Services, *HHS Proposes New Protections to Increase Care Coordination and Confidentiality for Patients With Substance Use Challenges* (Nov. 28, 2022), *available at* https://www.hhs.gov/about/news/2022/11/28/hhs-proposes-new-protections-increase-care-coordination-confidentiality-patients-substance-use-challenges.html. [269] Press Release, Department of Health and Human Services, *HHS Proposes New Protections to Increase Care Coordination and Confidentiality for Patients With Substance Use Challenges* (Nov. 28, 2022), *available at* https://www.hhs.gov/about/news/2022/11/28/hhs-proposes-new-protections-increase-care-coordination-confidentiality-patients-substance-use-challenges.html. [270] Press Release, Department of Health and Human Services, *HHS Proposes New Protections to Increase Care Coordination and Confidentiality for Patients With Substance Use Challenges* (Nov. 28, 2022), *available at* https://www.hhs.gov/about/news/2022/11/28/hhs-proposes-new-protections-increase-care-coordination-confidentiality-patients-substance-use-challenges.html. [271] Press Release,

Department of Health and Human Services, *HHS Proposes New Protections to Increase Care Coordination and Confidentiality for Patients With Substance Use Challenges* (Nov. 28, 2022), *available at* https://www.hhs.gov/about/news/2022/11/28/hhs-proposes-new-protections-increase-care-coordination-confidentiality-patients-substance-use-challenges.html. [272] Considerations for Implementing the Health Information Technology for Economic and Clinical Health (HITECH) Act, as Amended, 45 Fed. Reg. 19833 (June 6, 2022). [273] Request for Information, Considerations for Implementing the Health Information Technology for Economic and Clinical Health (HITECH) Act, as Amended, 87 Fed. Reg. 19833, 19833-34 (April 6, 2022), *available at* https://www.federalregister.gov/documents/2022/04/06/2022-07210/considerations-for-implementing-the-health-information-technology-for-economic-and-clinical-health. [274] Press Release, U.S. Government Accountability Office, *Electronic Health Information: HHS Needs to Improve Communications for Breach Reporting* (May 27, 2022), *available at* https://www.gao.gov/products/gao-22-105425. [275] Request for Information, Considerations for Implementing the Health Information Technology for Economic and Clinical Health (HITECH) Act, as Amended, 87 Fed. Reg. 19833, 19833-34 (April 6, 2022), *available at* https://www.federalregister.gov/documents/2022/04/06/2022-07210/considerations-for-implementing-the-health-information-technology-for-economic-and-clinical-health. [276] Press Release, Department of Health and Human Services, *OCR Announces Notification of Enforcement Discretion for Telehealth Remote Communications During the COVID-19 Nationwide Public Health Emergency* (Mar. 30, 2020), *available at* https://www.hhs.gov/hipaa/for-professionals/special-topics/emergency-preparedness/notification-enforcement-discretion-telehealth/index.html. [277] Department of Health and Human Services, *Guidance on How the HIPAA Rules Permit Covered Health Care Providers and Health Plans to Use Remote Communication Technologies for Audio-Only Telehealth*, *available at* https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/hipaa-audio-telehealth/index.html. [278] Adam Cancryn, *Biden team eyes end of Covid emergency declaration and shift in Covid team*, Politico (Jan. 10, 2023), *available at* https://www.politico.com/news/2023/01/10/biden-covid-public-health-emergency-extension-00077154. [279] Department of Health and Human Services, *Guidance on How the HIPAA Rules Permit Covered Health Care Providers and Health Plans to Use Remote Communication Technologies for Audio-Only Telehealth* (June 13, 2022), *available at* https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/hipaa-audio-telehealth/index.html. [280] Department of Health and Human Services, *Guidance on How the HIPAA Rules Permit Covered Health Care Providers and Health Plans to Use Remote Communication Technologies for Audio-Only Telehealth* (June 13, 2022), *available at* https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/hipaa-audio-telehealth/index.html. [281] Press Release, White House, *Readout of Healthcare Cybersecurity Executive Forum Hosted by National Cyber Director Chris Inglis* (June 16, 2022), *available at* https://www.whitehouse.gov/briefing-room/statements-releases/2022/06/16/readout-of-healthcare-cybersecurity-executive-forum-hosted-by-national-cyber-director-chris-inglis/. [282] Department of Health and Human Services, *Use of Online Tracking Technologies by HIPAA Covered Entities and Business Associates* (Dec. 1, 2022), *available at* https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/hipaa-online-tracking/index.html. [283] Press Release, Department of Health and Human Services, *Statement by HHS Secretary Xavier Becerra Reaffirming HHS Support and Protection for LGBTQI+ Children and Youth* (Mar. 2, 2022), *available at* https://www.hhs.gov/about/news/2022/03/02/statement-hhs-secretary-xavier-becerra-reaffirming-hhs-support-and-protection-for-lgbtqi-children-and-youth.html. [284] Department of Health and Human Services, *HHS Notice and Guidance on Gender Affirming Care, Civil Rights, and Patient Privacy* (March 2, 2022, and updated Oct. 1, 2022), *available at* https://www.hhs.gov/sites/default/files/hhs-ocr-notice-and-guidance-gender-affirming-care.pdf. [285] *Texas v. E.E.O.C.*, No. 2:21-CV-194-Z, 2022 WL 4835346, at *9 (N.D. Tex. Oct. 1, 2022). [286] *See Dobbs v. Jackson Women's Health Org.*, 579 U.S. ___ (2022).

[287] Department of Health and Human Services, *HIPAA Privacy Rule and Disclosures of Information Relating to Reproductive Health Care* (June 29, 2022), *available at* https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/phi-reproductive-health/index.html. [288] Press Release, Department of Health and Human Services, *HHS Announces Melanie Fontes Rainer as Director of the Office for Civil Rights* (Sept. 14, 2022), *available at* https://www.hhs.gov/about/news/2022/09/14/hhs-announces-melanie-fontes-rainer-as-director-of-the-office-for-civil-rights.html. [289] Alexandra Kelley, *The HHS's Office of Civil Rights is focusing on guidance and stakeholder coordination to enforce reproductive health data post Roe v. Wade*. Nextgov (Sept. 28, 2022), *available at* https://www.nextgov.com/analytics-data/2022/09/all-options-are-table-hhs-privacy-official-doubles-down-data-protection/377791/. [290] Press Release, Department of Health and Human Services, *Eleven Enforcement Actions Uphold Patients' Rights Under HIPAA* (July 15, 2022), *available at* https://www.hhs.gov/about/news/2022/07/15/eleven-enforcement-actions-uphold-patients-rights-under-hipaa.html. [291] Pres Release, Department of Health and Human Services, *OCR Settles Three Cases with Dental Practices for Patient Right of Access under HIPAA* (Sept. 20, 2022), *available at* https://www.hhs.gov/about/news/2022/09/20/ocr-settles-three-cases-dental-practices-patient-right-access-under-hipaa.html. [292] Press Release, Department of Health and Human Services, *Eleven Enforcement Actions Uphold Patients' Rights Under HIPAA* (July 15, 2022), *available at* https://www.hhs.gov/about/news/2022/07/15/eleven-enforcement-actions-uphold-patients-rights-under-hipaa.html. [293] Press Release, Department of Health and Human Services, OCR Settles Case Concerning Improper Disposal of Protected Health Information (Aug. 23, 2022), *available at* https://www.hhs.gov/about/news/2022/08/23/ocr-settles-case-concerning-improper-disposal-protected-health-information.html. [294] Press Release, Department of Health and Human Services, *Four HIPAA Enforcement Actions Hold Healthcare Providers Accountable With Compliance* (Mar. 28, 2022), *available at* https://www.hhs.gov/about/news/2022/03/28/four-hipaa-enforcement-actions-hold-healthcare-providers-accountable-with-compliance.html. [295] Press Release, Department of Health and Human Services, *Four HIPAA Enforcement Actions Hold Healthcare Providers Accountable With Compliance* (Mar. 28, 2022), *available at* https://www.hhs.gov/about/news/2022/03/28/four-hipaa-enforcement-actions-hold-healthcare-providers-accountable-with-compliance.html; Press Release, Department of Health and Human Services, *HHS Civil Rights Office Enters Settlement with Dental Practice Over Disclosures of Patients' Protected Health Information* (Dec. 14, 2022), *available at* https://www.hhs.gov/about/news/2022/12/14/hhs-civil-rights-office-enters-settlement-with-dental-practice-over-disclosures-of-patients-protected-health-information.html. [296] Press Release, Department of Health and Human Services, *Oklahoma State University – Center for Health Services Pays $875,000 to Settle Hacking Breach* (July 14, 2022), *available at* https://www.hhs.gov/about/news/2022/07/14/oklahoma-state-university-center-health-services-pays-875000-settle-hacking-breach.html. [297] Press Release, Department of Health and Human Services, *HHS Civil Rights Office Enters Settlement with Dental Practice Over Disclosures of Patients' Protected Health Information* (Dec. 14, 2022), *available at* https://www.hhs.gov/about/news/2022/12/14/hhs-civil-rights-office-enters-settlement-with-dental-practice-over-disclosures-of-patients-protected-health-information.html. [298] *FY22 Cybersecurity Sprints,* Department of Homeland Security (Nov. 1, 2022), *available at* https://www.dhs.gov/cybersecurity-sprints. [299]Press Release, Department of Homeland Security, *DHS Launches First-Ever Cyber Safety Review Board* (Feb. 3, 2022), *available at* https://www.dhs.gov/news/2022/02/03/dhs-launches-first-ever-cyber-safety-review-board. [300]Press Release, Department of Homeland Security, *Cyber Safety Review Board Releases Unprecedented Report of its Review into Log4j Vulnerabilities and Response* (July 14, 2022), *available at* https://www.dhs.gov/news/2022/07/14/cyber-safety-review-board-releases-report-its-

review-log4j-vulnerabilities-and; *see also Review of the December 2021 Log4j Event*, Report of the Cyber Safety Review Board (July 11, 2022), *available at* https://www.cisa.gov/sites/default/files/publications/CSRB-Report-on-Log4-July-11-2022_508.pdf. [301] Press Release, Department of Homeland Security, *Cyber Safety Review Board to Conduct Second Review on Lapsus$* (Dec. 2, 2022), *available at* https://www.dhs.gov/news/2022/12/02/cyber-safety-review-board-conduct-second-review-lapsus. [302] Cyber Incident Reporting for Critical Infrastructure Act of 2022, H.R. 2471, 116th Cong. (2022). [303] Request for Information on the Cyber Incident Reporting for Critical Infrastructure Act of 2022, 87 Fed. Reg. 55833 (published Sept. 12, 2022), *available at* https://www.federalregister.gov/documents/2022/09/12/2022-19551/request-for-information-on-the-cyber-incident-reporting-for-critical-infrastructure-act-of-2022. [304] Cyber Incident Reporting for Critical Infrastructure Act of 2022 Listening Sessions, 87 Fed. Reg. 55830 (published Sept. 12, 2022), *available at* https://www.federalregister.gov/documents/2022/09/12/2022-19550/cyber-incident-reporting-for-critical-infrastructure-act-of-2022-listening-sessions; Cyber Incident Reporting for Critical Infrastructure Act of 2022: Washington, D.C. Listening Session, 87 Fed. Reg. 60409 (published Oct. 5, 2022), *available at* https://www.federalregister.gov/documents/2022/10/05/2022-21635/cyber-incident-reporting-for-critical-infrastructure-act-of-2022-washington-dc-listening-session. [305] Notice of Cybersecurity and Infrastructure Security Agency Cybersecurity Advisory Committee Meeting, 87 Fed. Reg. 69283 (published Nov. 18, 2022), *available at* https://www.federalregister.gov/documents/2022/11/18/2022-25110/notice-of-cybersecurity-and-infrastructure-security-agency-cybersecurity-advisory-committee-meeting. [306] *Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA)*, Cybersecurity & Infrastructure Security Agency, *available at* https://www.cisa.gov/circia. [307] *Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA)*, Cybersecurity & Infrastructure Security Agency, *available at* https://www.cisa.gov/circia; *see also* Gibson Dunn's client alert on the Cyber Incident Reporting for Critical Infrastructure Act, *available at* https://www.gibsondunn.com/president-biden-signs-into-law-the-cyber-incident-reporting-for-critical-infrastructure-act-expanding-cyber-reporting-obligations-for-a-wide-range-of-public-and-private-entities/. [308] Press Release, Department of Justice, *Deputy Attorney General Lisa O. Monaco Announces New Civil Cyber-Fraud Initiative* (Oct. 6, 2021), *available at* https://www.justice.gov/opa/pr/deputy-attorney-general-lisa-o-monaco-announces-new-civil-cyber-fraud-initiative. [309] Press Release, Department of Justice, *Deputy Attorney General Lisa O. Monaco Announces New Civil Cyber-Fraud Initiative* (Oct. 6, 2021), *available at* https://www.justice.gov/opa/pr/deputy-attorney-general-lisa-o-monaco-announces-new-civil-cyber-fraud-initiative. [310] Press Release, Department of Justice, *Deputy Attorney General Lisa O. Monaco Announces New Civil Cyber-Fraud Initiative* (Oct. 6, 2021), *available at* https://www.justice.gov/opa/pr/deputy-attorney-general-lisa-o-monaco-announces-new-civil-cyber-fraud-initiative. [311] Press Release, Department of Justice, *Contractor Pays $930,000 to Settle False Claims Act Allegations Relating to Medical Services Contracts at State Department and Air Force Facilities in Iraq and Afghanistan* (Mar. 8, 2022), *available at* https://www.justice.gov/usao-edny/pr/contractor-pays-930000-settle-false-claims-act-allegations-relating-medical-services. [312] Press Release, Department of Justice, *Aerojet Rocketdyne Agrees to Pay $9 Million to Resolve False Claims Act Allegations of Cybersecurity Violations in Federal Government Contracts* (July 8, 2022), *available at* https://www.justice.gov/opa/pr/aerojet-rocketdyne-agrees-pay-9-million-resolve-false-claims-act-allegations-cybersecurity. [313] United States Strategy on Countering Corruption, The White House (Dec. 6, 2021), *available at* https://www.whitehouse.gov/wp-content/uploads/2021/12/United-States-Strategy-on-Countering-Corruption.pdf. [314] *Id.* [315] Guidance Regarding Investigations and Cases Related to Ransomware and Digital Extortion, Department of Justice Office of the Deputy Attorney General (June 3, 2021), *available*

at https://www.justice.gov/media/1144356/dl?inline=. [316] Press Release, Department of Justice, *Justice Department Seizes and Forfeits Approximately $500,000 from North Korean Ransomware Actors and their Conspirators* (July 19, 2022), *available at* https://www.justice.gov/opa/pr/justice-department-seizes-and-forfeits-approximately-500000-north-korean-ransomware-actors; Press Release, Department of Justice, *Department of Justice Seizes $2.3 Million in Cryptocurrency Paid to the Ransomware Extortionists Darkside* (June 7, 2021), *available at* https://www.justice.gov/opa/pr/department-justice-seizes-23-million-cryptocurrency-paid-ransomware-extortionists-darkside. [317] Press Release, Department of Justice, *Department of Justice Announces New Policy for Charging Cases under the Computer Fraud and Abuse Act* (May 19, 2022), *available at* https://www.justice.gov/opa/pr/department-justice-announces-new-policy-charging-cases-under-computer-fraud-and-abuse-act. [318] *Id.* [319] *Id.* [320] Press Release, Department of Energy, *DOE Releases Strategy for Building Cyber-Resilient Energy Systems* (June 15, 2022), *available at* https://www.energy.gov/articles/doe-releases-strategy-building-cyber-resilient-energy-systems [321] Department of Energy, *National Cyber-Informed Engineering Strategy* (June 15, 2022), *available at* https://www.energy.gov/articles/doe-releases-strategy-building-cyber-resilient-energy-systems; *see also* Department of Energy, *The U.S. Department of Energy's (DOE) National Cyber-Informed Engineering (CIE) Strategy Document* (June 14, 2022), *available at* https://www.energy.gov/ceser/articles/us-department-energys-doe-national-cyber-informed-engineering-cie-strategy-document. [322] Department of Energy, *National Cyber-Informed Engineering Strategy* (June 15, 2022), *available at* https://www.energy.gov/articles/doe-releases-strategy-building-cyber-resilient-energy-systems. [323] Office of Cybersecurity, Energy Security, and Emergency Response, *DOE Cybersecurity Report Provides Recommendations to Secure Distributed Clean Energy on the Nation's Electricity Grid* (Oct. 6, 2022), *available at* https://www.energy.gov/ceser/articles/doe-cybersecurity-report-provides-recommendations-secure-distributed-clean-energy. [324] Supervision and Regulation Letter, Board of Governors of the Federal Reserve System, *SR 22-4 / CA 22-3: Contact Information in Relation to Computer-Security Incident Notification Requirements* (Mar. 29, 2022), *available at* https://www.federalreserve.gov/supervisionreg/srletters/SR2204.htm. [325] Computer-Security Incident Notification Requirements for Banking Organizations and Their Bank Service Providers, 86 Fed. Reg. 66424 (published Nov. 23, 2021), *available at* https://www.federalregister.gov/documents/2021/11/23/2021-25510/computer-security-incident-notification-requirements-for-banking-organizations-and-their-bank. [326] Computer-Security Incident Notification Requirements for Banking Organizations and Their Bank Service Providers, 86 Fed. Reg. 66424 (published Nov. 23, 2021), *available at* https://www.federalregister.gov/documents/2021/11/23/2021-25510/computer-security-incident-notification-requirements-for-banking-organizations-and-their-bank. [327] Potential Federal Insurance Response to Catastrophic Cyber Incidents, 87 FR 59161 (Sept. 29, 2022). [328] *Id.* [329] Cyber Insurance: Action Needed to Assess Potential Federal Response to Catastrophic Attacks, GAO-22-104256, U.S. Government Accountability Office (June 2022), *available at* https://www.gao.gov/products/gao-22-104256. [330] Press Release, Department of Commerce, *U.S. Department of Commerce Appoints 27 Members to National AI Advisory Committee* (Apr. 14, 2022), *available at* https://www.commerce.gov/news/press-releases/2022/04/us-department-commerce-appoints-27-members-national-ai-advisory. [331] *Id.* [332] *Id.* [333] Notice of Federal Advisory Committee Open Meeting, 87 FR 23168 (Apr. 19, 2022); Notice of Federal Advisory Committee Open Meeting, 87 FR 58312 (Sept. 26, 2022). [334] National Artificial Intelligence Advisory Committee (NAIAC), *available at* https://www.ai.gov/naiac/. [335] *NAAG Center on Cyber and Technology*, National Association of Attorneys General (July 18, 2022), *available at* https://www.naag.org/naag-center-on-cyber-and-technology/. [336] Press Release, National Association of Attorneys General, *NAAG Announces Formation of Center on Cyber and Technology* (May 9, 2022), *available at* https://www.naag.org/press-releases/naag-announces-formation-of-center-on-cyber-and-technology/. [337] Press Release, National Association of Attorneys General, *51 Attorneys*

General Support FCC Proposal to Require Anti-Robotext Protections (Dec. 12, 2022), *available at* https://www.naag.org/press-rel12eases/51-attorneys-general-robotext-protection/. [338] Press Release, National Association of Attorneys General, *41 State Attorneys General Pledge to Join FCC and Other States in Combatting Robocalls* (June 2, 2022), *available at* https://www.naag.org/press-releases/41-state-attorneys-general-pledge-to-join-fcc-and-other-states-in-combatting-robocalls/. [339] NAAG Letter to FCC, National Association of Attorneys General, *Re: State Attorneys General Support FCC Efforts in Combatting Robocalls* (May 31, 2022), *available at* https://naagweb.wpenginepowered.com/wp-content/uploads/2022/06/Letter-to-FCC-re-Robocalls_FINAL.pdf. [340] Press Release, State of California Department of Justice, *Attorney General Bonta, National Coalition of Attorneys General Issue Joint Statement Reaffirming Commitment to Protecting Access to Abortion Care* (June 27, 2022), *available at* https://oag.ca.gov/news/press-releases/attorney-general-bonta-national-coalition-attorneys-general-issue-joint. [341] *See e.g.*, Press Release, Utah Office of the Attorney General, *Utah Attorney General's Office Statement on Supreme Court Abortion Ruling* (June 24, 2022), *available at* https://attorneygeneral.utah.gov/utah-attorney-generals-office-statement-on-supreme-court-abortion-ruling/; Press Release, Missouri Attorney General, *Missouri Attorney General Eric Schmitt Becomes First to Issue Opinion Following SCOTUS Opinion in Dobbs, Effectively Ending Abortion in Missouri* (June 24, 2022), *available at* https://ago.mo.gov/home/news/2022/06/24/missouri-attorney-general-eric-schmitt-becomes-first-to-issue-opinion-following-scotus-opinion-in-dobbs-effectively-ending-abortion-in-missouri. [342] Press Release, State of California Department of Justice, *Attorney General Bonta Emphasizes Health Apps' Legal Obligation to Protect Reproductive Health Information* (May 26, 2022), *available at* https://oag.ca.gov/news/press-releases/attorney-general-bonta-emphasizes-health-apps-legal-obligation-protect. [343] Press Release, State of California Department of Justice, *Attorney General Bonta Testifies at Maryland Cybersecurity Council on California's Groundbreaking Effort to Protect Digital Information on Abortion* (Sep. 22, 2022), *available at* https://oag.ca.gov/news/press-releases/attorney-general-bonta-testifies-maryland-cybersecurity-council-california%E2%80%99s. [344] Letter, Virginia Office of the Attorney General and Kentucky Office of the Attorney General, *Re: Google Must Not Discriminate Against Crisis Pregnancy Centers* (July 21, 2022), *available at* https://www.oag.state.va.us/files/StateAttorneysGeneralLettertoGoogleJuly21,2022.pdf. [345] Press Release, State of California Department of Justice, *Attorney General Bonta Leads Coalition Calling for Federal Privacy Protections that Maintain Strong State Oversight* (July 19, 2022), *available at* https://oag.ca.gov/news/press-releases/attorney-general-bonta-leads-coalition-calling-federal-privacy-protections. [346] *Id*. [347] *Id*. [348] Press Release, NY Attorney General, *Attorney General James Secures $2.6 Million From Online Travel Agency for Deceptive Marketing* (Mar. 16, 2022), *available at* https://ag.ny.gov/press-release/2022/attorney-general-james-secures-26-million-online-travel-agency-deceptive. [349] Press Release, Oregon Department of Justice, *Google: AG Rosenblum Announces Largest AG Consumer Privacy Settlement in U.S. History* (Nov. 14, 2022), *available at* https://www.doj.state.or.us/media-home/news-media-releases/largest-ag-consumer-privacy-settlement-in-u-s-history/. [350] *Id*. [351] Press Release, Arizona Attorney General, *Attorney General Mark Brnovich Files Lawsuit Against Google Over Deceptive and Unfair Location Tracking* (May 27, 2020), *available at* https://www.azag.gov/press-release/attorney-general-mark-brnovich-files-lawsuit-against-google-over-deceptive-and-unfair. [352] Press Release, *Arizona Attorney General, Attorney General Mark Brnovich Achieves Historic $85 Million Settlement with Google* (Oct. 4, 2022), *available at* https://www.azag.gov/press-release/attorney-general-mark-brnovich-achieves-historic-85-million-settlement-google. [353] Complaint, *District Of Columbia v. Google LLC*, 2022-CA-000330-B (D.C. Super. Ct. Jan. 24, 2022). [354] *Id.* at ¶¶45–94. [355] Press Release, District of Columbia Attorney General, *AG Racine Leads Bipartisan Coalition in Suing Google Over Deceptive Location Tracking Practices That Invade Users' Privacy*

(Jan. 24, 2022), *available at* https://oag.dc.gov/release/ag-racine-leads-bipartisan-coalition-suing-google. [356] Ryan Nakashima, *Google tracks your movements, like it or not*, AP News (Aug. 13, 2018), *available at* https://apnews.com/article/north-america-science-technology-business-ap-top-news-828aefab64d4411bac257a07c1af0ecb. [357] Press Release, Attorney General of Texas, *Paxton Sues Facebook for Using Unauthorized Biometric Data* (Feb. 14, 2022), *available at* https://www.texasattorneygeneral.gov/news/releases/paxton-sues-facebook-using-unauthorized-biometric-data. [358] Press Release, Attorney General of Texas, *AG Paxton Amends Google Lawsuit to Include ?"Incognito Mode" as Another Deceptive Trade Practices Act Violation* (May 19, 2022), *available at* https://www.texasattorneygeneral.gov/news/releases/ag-paxton-amends-google-lawsuit-include-incognito-mode-another-deceptive-trade-practices-act. [359]Press Release, State of California Department of Justice, *On Data Privacy Day, Attorney General Bonta Puts Businesses Operating Loyalty Programs on Notice for Violations of California Consumer Privacy Act* (Jan. 28, 2022), *available at* https://oag.ca.gov/news/press-releases/data-privacy-day-attorney-general-bonta-puts-businesses-operating-loyalty. [360] Client Alert, Gibson, Dunn & Crutcher LLP, *California AG's CCPA Enforcement Priorities Expand to Loyalty Programs* (Feb. 3, 2022), *available at* https://www.gibsondunn.com/california-ags-ccpa-enforcement-priorities-expand-to-loyalty-programs/. [361] Opinion Paper, State of California Department of Justice, *Opinion of Rob Bonta on Califronia Consumer Privacy Act Right to Know* (Mar. 10, 2022), *available at* https://oag.ca.gov/system/files/opinions/pdfs/20-303.pdf. [362] Press Release, State of California Department of Justice, *Attorney General Bonta Announces Settlement with Sephora as Part of Ongoing Enforcement of California Consumer Privacy Act* (Aug. 24, 2022), *available at* https://oag.ca.gov/news/press-releases/attorney-general-bonta-announces-settlement-sephora-part-ongoing-enforcement. [363] *Id.* [364] *Id*. [365] Client Alert, Gibson, Dunn & Crutcher LLP, *New York Attorney General's Office Fall Round-Up* (Nov. 15, 2022), *available at* https://www.gibsondunn.com/new-york-attorney-generals-office-fall-round-up-november-2022/#_ednref21. [366] Press Release, NY Attorney General, *Attorney General James Releases Top 10 Consumer Complaints of 2021* (Mar. 7, 2022), *available at* https://ag.ny.gov/press-release/2022/attorney-general-james-releases-top-10-consumer-complaints-2021. [367] Press Release, NY Attorney General, *Attorney General James Alerts 17 Companies to "Credential Stuffing" Cyberattacks Impacting More Than 1.1 Million Consumers* (Jan. 5, 2022), *available at* https://ag.ny.gov/press-release/2022/attorney-general-james-alerts-17-companies-credential-stuffing-cyberattacks. [368] Press Release, NY Attorney General, *Attorney General James Announces $600,000 Agreement with EyeMed After 2020 Data Breach* (Jan. 24, 2022), *available at* https://ag.ny.gov/press-release/2022/attorney-general-james-announces-600000-agreement-eyemed-after-2020-data-breach. [369] Press Release, NY Attorney General, *Attorney General James Secures $400,000 From Wegmans After Data Breach Exposed Consumers' Personal Information* (June 30, 2022), *available at* https://ag.ny.gov/press-release/2022/attorney-general-james-secures-400000-wegmans-after-data-breach-exposed-consumers. [370] Press Release, NY Attorney General, *Attorney General James Recovers $1.25 Million for Consumers Affected by Carnival Cruise Line's Data Breach* (June 23, 2022), *available at* https://ag.ny.gov/press-release/2022/attorney-general-james-recovers-125-million-consumers-affected-carnival-cruise. [371] Press Release, NY Department of Financial Services, *DFS Superintendent Harris Announces $5 Million Penalty On Cruise Company Carnival Corporation And Its Subsidiaries For Significant Cybersecurity Violations* (June 24, 2022), *available at* https://www.dfs.ny.gov/reports_and_publications/press_releases/pr202206241. [372] Press Release, NY Department of Financial Services, *DFS Superintendent Harris Announces $30 Million Penalty on Robinhood Crypto for Significant Anti-Money*

Laundering, Cybersecurity & Consumer Protection Violations (Aug. 21, 2022), *available at* https://www.dfs.ny.gov/reports_and_publications/press_releases/pr202208021. [373] *Identity Theft Resource Center's 2021 Annual Data Breach Report*, Identity Theft Resource Center, *available at* https://www.idtheftcenter.org/post/identity-theft-resource-center-2021-annual-data-breach-report-sets-new-record-for-number-of-compromises/ (last visited Dec. 8, 2022). [374] *Q3 2022 Data Breach Analysis*, Identity Theft Resource Center, *available at* https://www.idtheftcenter.org/publication/q3-2022-data-breach-analysis/ (last visited Dec. 8, 2022). [375] *TransUnion LLC v. Ramirez*, 141 S. Ct. 2190 (2021) (finding that plaintiffs who have not suffered concrete harm due to data breach, and instead claim they are at heightened risk of future farm, do not have standing to sue under Article III of the U.S. Constitution). [376] *Id.* at 2211. [377] *Lujan v. Defenders of Wildlife*, 504 U.S. 555, 560-61 (1992) (synthesizing U.S. Supreme Court jurisprudence on the constitutional minimum requirements for standing). [378] *McMorris v. Carlos Lopez & Assocs.*, 996 F.3d 295 (2d Cir. 2021) (finding the following factors persuasive in establishing standing based on future harms: "(1) whether the plaintiffs' data has been exposed as the result of a targeted attempt to obtain that data; (2) whether any portion of the [compromised] dataset has already been misused, even if the plaintiffs themselves have not yet experienced identity theft or fraud; and (3) whether the type of data that has been exposed is sensitive such that there is a high risk of identity theft or fraud."). [379] *Tsao v. Captiva MVP Rest. Partners, LLC*, 986 F.3d 1332 (11th Cir. 2021) (finding that breaches of existing credit card information do not amount to a "substantial risk" of harm, and reasoning that it will be difficult for a named plaintiff to plead facts sufficient to demonstrate standing where no there is no evidence that any class members' data has been misused). [380] *Clemens v. ExecuPharm Inc.*, 48 F.4th 146, 156 (3d Cir. 2022) (emphasis in original) (quoting *TransUnion LLC v. Ramirez*, 210 L. Ed. 2d 568, 141 S. Ct. 2190, 2211 (2021)). [381] *Bohnak v. Marsh & McLennan Cos.*, Inc., 580 F. Supp. 3d 21 (S.D.N.Y. 2022) (finding that certain intangible harms such as privacy related harms, have been judicially cognizable and are sufficiently concrete and analogous to the common law tort of public disclosure of private information, to confer standing on a data breach plaintiff despite there being no materialized misuse of data). [382] *Cooper v. Bonobos, Inc.*, No. 21-CV-854 (JMF), 2022 WL 170622 (S.D.N.Y. Jan. 19, 2022). [383] *Hiscox Ins. Co. Inc. et al v. Warden Grier LLP*, No. 4:20-cv-00237 (W.D. Mo.). [384] *Id.* [385] *Id.* [386] *Reiter v. Fairbanks*, No. 2021-1117 (Del. Ch. filed Jan. 11, 2020). [387] *In re Morgan Stanley Data Security Litigation*, 1:20-cv-05914-AT (S.D.N.Y). [388] News Release, Office of the Comptroller of the Currency, *OCC Assesses $60 Million Civil Money Penalty Against Morgan Stanley* (Oct. 8, 2020), *available at* https://www.occ.gov/news-issuances/news-releases/2020/nr-occ-2020-134.html. [389] Settlement Update, Federal Trade Commission, *Equifax Data Breach Settlement*, *available at* https://www.ftc.gov/enforcement/refunds/equifax-data-breach-settlement (last visited July 20, 2022). [390] Dan Avery, *Capital One $190 Million Data Breach Settlement: Today is the Last Day to Claim Money*, cnet (Sept. 30, 2022) https://www.cnet.com/personal-finance/capital-one-190-million-data-breach-settlement-today-is-deadline-to-file-claim. [391] *In re U.S. Office of Personnel Management Data Security Breach Litigation*, No. 15-1394 (ABJ) (D.D.C.). [392] 2022 Consumer Privacy Legislation, Nat'l Conf. of St. Legislatures (June 10, 2022) *available at* https://www.ncsl.org/research/telecommunications-and-information-technology/2022-consumer-privacy-legislation.aspx. [393] *Virginia Passes Comprehensive Privacy Law*, Gibson Dunn (March 8, 2021), *available at* https://www.gibsondunn.com/wp-content/uploads/2021/03/virginia-passes-comprehensive-privacy-law.pdf. [394] 18 U.S.C. § 1030(a)(2). [395] *Van Buren v. United States*, 141 S. Ct. 1648, 1654–55 (2021). [396] *Id.* at 1653. [397] *Id.* [398] *Id.* at 1653–54. [399] *Id*. at 1662 (emphasis added). [400] *Id.* [401] *hiQ Labs, Inc. v. LinkedIn Corp.*, 31 F.4th 1180 (9th Cir. 2022). [402] *LinkedIn Corp. v. hiQ Labs, Inc*., 141 S. Ct. 2752 (2021). [403] *hiQ Labs, Inc. v. LinkedIn Corp.*, 31 F.4th 1180, 1187 (9th Cir. 2022). [404] *Id.* at 1187–88. [405] *Id.* at 1188. [406] *Id.* at 1197–1201. [407] *Id.* at 1197. [408] *Id.* at 1201. [409] *Facebook, Inc. v. Power Ventures, Inc*., 844 F.3d 1058, 1067 (9th Cir. 2016). [410] *hiQ Labs, Inc. v. LinkedIn Corp.*, 31 F.4th 1180, 1201 (9th Cir. 2022). [411] *See* Stipulation and [Proposed] Consent Judgment and Permanent Injunction, *hiQ Labs, Inc. v. LinkedIn Corp*., No.

3:19-cv-00410-EMC (N.D. Cal. Dec. 6, 2022), ECF No. 405. [412] *See* Consent Judgment and Permanent Injunction, *hiQ Labs, Inc. v. LinkedIn Corp*., No. 3:19-cv-00410-EMC (N.D. Cal. Dec. 8, 2022), ECF No. 406. [413] *Ryanair DAC v. Booking Holdings Inc*., 2022 WL 13946243, at *11 (D. Del. Oct. 24, 2022). [414] *Id*. [415] *Id.*at *10–11. [416] *Id.* at *11–12. [417] *United States v. Thompson*, 2022 WL 834026, at *2 (W.D. Wash. Mar. 21, 2022), *reconsideration denied*, 2022 WL 1719221 (W.D. Wash. May 27, 2022). [418] *Id.* at *2–3. [419] *Id.* at *4. [420] *Id.* at *5. [421] *Id.* [422] Press Release, Department of Justice, *Department of Justice Announces New Policy for Charging Cases under the Computer Fraud and Abuse Act* (May 19, 2022), *available at* https://www.justice.gov/opa/press-release/file/1507126/download. [423] *Id.* at 2. [424] *Id.* at 4. [425] *Id.* [426] *Id.* at 3. [427] *Id.* at 4. [428] *Id.* at 5. [429] *Facebook, Inc. v. Duguid*, 141 S. Ct. 1163, 209 L. Ed. 2d 272 (2021). [430] *Id.* at 1173. [431] *Id.* at 1163, 1167 ("To qualify as an 'automatic telephone dialing system,' a device must have the capacity either to store a telephone number using a random or sequential generator or to produce a telephone number using a random or sequential number generator."); *see also Supreme Court Declines To Extend Telephone Consumer Protection Act's Coverage Of Automatic Telephone Dialing Systems*, Gibson Dunn (Apr. 1, 2021), *available at* https://www.gibsondunn.com/supreme-court-declines-to-extend-telephone-consumer-protection-acts-coverage-of-automatic-telephone-dialing-systems/. [432] *See Duguid v. Facebook, Inc.*, 926 F.3d 1146, 1151 (9th Cir. 2019) (citing *Marks v. Crunch San Diego, LLC*, 904 F.3d 1041 (9th Cir. 2018), and noting that "[i]n *Marks*, we clarified that the adverbial phrase 'using a random or sequential number generator' modifies only the verb 'to produce,' and not the preceding verb, 'to store'"), rev'd 141 S. Ct. 1163 209 L. Ed. 2d 272 (2021). [433] *See Barnett v. First Nat'l Bank of Omaha*, No. 3:20-CV-337-CHB, 2022 WL 2111966 (W.D. Ky. June 10, 2022); *Mina v. Red Robin Int'l, Inc.*, No. 20-CV-00612-RM-NYW, 2022 WL 2105897 (D. Colo. June 10, 2022); *Panzarella v. Navient Sols., Inc.*, No. 20-2371, 37 F.4th 867 (3d Cir. June 14, 2022); *DeMesa v. Treasure Island, LLC*, No. 218CV02007JADNJK, 2022 WL 1813858 (D. Nev. June 1, 2022); *Jiminez v. Credit One Bank, N.A.*, No. 17 CV 2844-LTS-JLC, 2022 WL 4611924 (S.D.N.Y. Sept. 30, 2022). [434] *Panzarella v. Navient Solutions, Inc.,* 37 F.4th 867, 867-68 (3rd Cir. 2022) ("This is so because a violation of section 227 (b)(1)(A)(iii) requires proof that the calls at issue be made 'using' an ATDS. The issue turns . . . on whether Navient violated the TCPA when it employed this dialing equipment to call the Panzarellas."). [435] *See Barnett v. First Nat'l Bank of Omaha*, No. 3:20-CV-337-CHB, 2022 WL 2111966 (W.D. Ky. June 10, 2022); *Mina v. Red Robin Int'l, Inc.*, No. 20-CV-00612-RM-NYW, 2022 WL 2105897 (D. Colo. June 10, 2022); *Panzarella v. Navient Sols., Inc.*, No. 20-2371, 37 F.4th 867 (3d Cir. June 14, 2022); *DeMesa v. Treasure Island, LLC*, No. 218CV02007JADNJK, 2022 WL 1813858 (D. Nev. June 1, 2022); *Jiminez v. Credit One Bank, N.A.*, No. 17 CV 2844-LTS-JLC, 2022 WL 4611924 (S.D.N.Y. Sept. 30, 2022). [436] *See, e.g.*, *Pizarro v. Quinstreet, Inc.*, No. 3:22-cv-02803-MMC, 2022 WL 3357838 (N.D. Cal. Aug. 15, 2022). [437] 47 U.S.C. § 227(b)(3). [438] *FCRA Leads the Way: WebRecon Stats For DEC 2021 & Year in Review*, WebRecon, LLC, *available at* https://webrecon.com/fcra-leads-the-way-webrecon-stats-for-dec-2021-year-in-review/ (last visited, Dec. 16, 2022). [439] *Tracy Eggleston et al. v. Reward Zone USA LLC, et al.*, No. 2:20-cv-01027-SVW-KS, 2022 WL 886094 (C.D. Cal. Jan. 28, 2022). [440] Transcript of Oral Argument at 31, *Facebook, Inc. v. Duguid*, 141 S.Ct. 1163 (2021) (No. 19-511). [441] An act relating to telephone solicitation; amending s. 501.059, F.S.; defining terms; prohibiting certain telephonic sales calls without the prior express written consent of the called party; removing provisions authorizing the use of certain automated telephone dialing systems; providing a rebuttable presumption for certain calls made to any area code in this state; providing a cause of action for aggrieved called parties; authorizing a court to increase an award for willful and knowing violations; amending s. 501.616, F.S.; prohibiting a commercial telephone seller or salesperson from using automated dialing or recorded messages to make certain commercial telephone solicitation phone calls; revising the timeframe during which a commercial telephone seller or salesperson may make commercial solicitation phone calls; prohibiting commercial telephone sellers or salespersons from making a specified number of commercial telephone solicitation phone calls to a person over a specified timeframe; prohibiting commercial telephone sellers or

salespersons from using certain technology to conceal their true identity; providing criminal penalties; reenacting s. 501.604, F.S., relating to exemptions to the Florida Telemarketing Act, to incorporate the amendment made to s. 501.616, F.S., in a reference thereto; reenacting s. 648.44(1)(c), F.S., relating to prohibitions regarding bail bond agent telephone solicitations, to incorporate the amendment made to s. 31 501.616, F.S., in a reference thereto; providing an effective date, S.B. 1120, 2021 Leg., Reg. Sess. (Fla. 2021), *available at* https://www.flsenate.gov/Session/Bill/2021/1120/BillText/er/PDF. [442] §501.059(8)(a), Fla. Stat. (2022). [443] An Act relating to telephone solicitation; creating the Telephone Solicitation Act of 2022; defining terms; prohibiting certain telephonic sales calls without the prior express written consent of the called party; prohibiting commercial telephone sellers or salespersons from using certain technology to conceal their true identity; providing a rebuttable presumption for certain calls made to any area code in this state; prohibiting a commercial telephone seller or salesperson from using automated dialing or recorded messages to make certain commercial telephone solicitation phone calls; providing the time frame during which a commercial telephone seller or salesperson may make commercial solicitation phone calls; prohibiting commercial telephone sellers or salespersons from making a specified number of commercial telephone solicitation phone calls to a person over a specified time frame; exempting certain persons; providing a cause of action for aggrieved called parties; authorizing a court to increase an award for willful and knowing violations; providing for codification; and providing an effective date, H.B. 3168, 2022 Leg., Reg. Sess. (Okla.2022), *available at* https://www.flsenate.gov/Session/Bill/2021/1120/BillText/er/PDF. [444] *Turizo v. Subway Franchisee Advertising Fund Trust Ltd.*, No. 21-CIV-61493-RAR, 2022 WL 2919260 (S.D. Fla. May 18, 2022). [445] *Rombough v. Robert D Smith Ins. Agency, Inc. et al.*, No. 22-CV-15-CJW-MAR, 2022 WL 2713278 (N.D. Iowa June 9, 2022). [446] *Id.* at *3. [447] *Id.* at *4. [448] *Id.* at *5. [449] *Rose v. New TSI Holdings, Inc.*, No. 21-CV-5519 (JPO), 2022 WL 912967 (S.D.N.Y. Mar. 28, 2022). [450] *Id.* at *4. [451] *Compare Morgan v. U.S. Xpress, Inc.*, No. 3:17-cv-00085, 2018 WL 3580775 (W.D. Va. Jul. 25, 2018) (holding that cell phones are necessarily separate from residential telephone lines); *Hunsinger v. Alpha Cash Buyers, LLC*, No. 3:21-CV-1598-D, 2022 WL 562761 (N.D. Tex. Feb. 24, 2022) (holding that DNC Registry rules can apply to cell phones). [452] Cal. Civ. Code § 1798.150(a)(1). [453] *Id.* [454] Class Action Complaint for 1. Negligence; 2. Breach of Implied Contract; 3. Violation of California's Consumer Privacy Act; 4. Violation of California's Unfair Competition Law; and 5. Breach of Contract, *Hajny v. Volkswagen Grp. of Am. Inc.*, No. C22-01841, ¶¶ 2 & n.3, 11-17 (Cal. Sup. Ct. Contra Costa Cnty. Aug. 30, 2022). [455] *Id.* ¶¶ 98-148. [456] Order After Hearing Re: Preliminary Approval of Class Action Settlement, *Service v. Volkswagen Grp. of Am., Inc.*, No. MSC22-01841 (Cal. Sup. Ct. Contra Costa Cnty. Dec. 13, 2022). *See also* Tentative Ruling, *Service v. Volkswagen Grp. of Am., Inc.*, No. C22-01841 (Cal. Sup. Ct. Contra Costa Cnty. Dec. 1, 2022), *available at* https://www.cc-courts.org/civil/TR/Department%2039%20-%20Judge%20Weil/39_120122.pdf. [457] Order After Hearing Re: Preliminary Approval of Class Action Settlement, *Service v. Volkswagen Grp. of Am., Inc.*, No. MSC22-01841, at 3 (Cal. Sup. Ct. Contra Costa Cnty. Dec. 13, 2022). [458] *Id.* [459] *Id.* [460] *In re Waste Mgmt. Data Breach Litig.*, No. 21CV6147, 2022 WL 561734, at *1 (S.D.N.Y. Feb. 24, 2022). [461] *Id.* [462] *Id.* at *6 (citing Cal. Civ. Code § 1798.150(a)(1); *Maag v. U.S. Bank, Nat'l Assoc.*, No. 21-cv-00031, 2021 WL 5605278, at *2 (S.D. Cal. Apr. 8, 2021)). [463] *Id*. [464] *Id.* [465] *Id.* [466] *Id.* at *7 n.3. [467] *Id.* [468] *See* Case Calendaring, *In re Waste Mgmt. Data Breach Litig.*, No. 22-641 (2d Cir. Dec. 9, 2022) (proposing week of March 13, 2023), ECF No. 77. [469] *California Consumer Privacy Act (CCPA) Litigation*, U.S. Cybersecurity and Data Privacy Outlook and Review – 2021 (Jan. 28, 2021), https://www.gibsondunn.com/us-cybersecurity-and-data-privacy-outlook-and-review-2021/#_Toc62718905. [470] *Id.* (discussing *Hayden v. Retail Equation, Inc.*, No. 8:20-01203 (C.D. Cal. filed July 7, 2020). [471] *Hayden v. Retail Equation, Inc.*, No. 8:20-01203, 2022 WL 2254461, at *8 (C.D. Cal. May 4, 2022). The court did permit a claim of invasion of privacy to proceed. *Id.* The court subsequently granted plaintiffs' motion for reconsideration, to instead dismiss the plaintiffs' California Unfair Competition Law ("UCL") claims for equitable relief with leave to amend. *Hayden v. Retail Equation, Inc.*, No. 8:20-01203, 2022 WL 3137446, at *4

(C.D. Cal. July 22, 2022). [472] *Hayden v. Retail Equation, Inc.*, No. 8:20-01203, 2022 WL 2254461, at *4 (C.D. Cal. May 4, 2022). [473] *Id.* (citing Cal. Civ. Code § 1798.198; Cal. Civ. Code § 3 ("[n]o part of [this Code] is retroactive, unless expressly so declared."); *Gardiner v. Walmart Inc.*, No. 20-cv-04618, 2021 WL 2520103, at *2 (N.D. Cal. March 5, 2021) (holding that a plaintiff must allege that the defendant violated "the duty to implement and maintain reasonable security procedures and practices . . . on or after January 1, 2020.")). [474] *Id.* at *5 (quoting Cal. Civ. Code § 1798(a)). [475] *Id.* [476] *Id.* [477] Cal. Bus. & Prof. Code § 17200. [478] *Id.* [479] Cal. Civ. Code § 1798.150(c); S. Judiciary Comm., AB-375, 2017-2018 Sess. (Cal. 2018). [480] Class Action Complaint for Violations of CCPA, California Unfair Competition Law, and Breach of Contract, *Rubio v. Lakeview Loan Serv'g, LLC*, No. CVRI2201604 (Cal. Super. Ct. April 21, 2022). [481] *Id.* ¶ 66. [482] *Id.* ¶ 68. [483] *Id.* ¶ 71. [484] *Id.* ¶ 73. [485] Notice of Removal, *Rubio v. Lakeview Loan Serv'g, LLC*, No. 3:22CV00603 (S.D. Cal. April 28, 2022); Notice of Filing of Notice of Removal, *Rubio v. Lakeview Loan Serv'g, LLC*, No. CVRI2201604 (Cal. Super. Ct. April 29, 2022). [486] Transfer Order, *Rubio v. Lakeview Loan Serv'g, LLC*, No. 3:22CV00603 (S.D. Cal. May 9, 2022). [487] Class Action Complaint, *Kellman v. Spokeo*, Inc., No. 3:21CV08976 (N.D. Cal. Nov. 19, 2021). [488] *Kellman v. Spokeo, Inc.*, No. 3:21-CV-08976-WHO, 2022 WL 1157500, at *12 (N.D. Cal. Apr. 19, 2022). [489] *Id.* (emphases in original). [490] Order Denying Mot. to Certify Interlocutory Appeal, *Kellman v. Spokeo*, Inc., No. 3:21-CV-08976 (N.D. Cal. July 8, 2022), ECF No. 64. [491] Minute Entry for Proceedings, *Kellman v. Spokeo*, Inc., No. 3:21-CV-08976 (N.D. Cal. Sept. 13, 2022), ECF No. 69. [492] Defendant Spokeo, Inc.'s & Plaintiffs' Joint Statement of Discovery Dispute, *Kellman v. Spokeo, Inc.*, No. 3:21-CV-08976, at 1 (N.D. Cal. Jan. 18, 2023), ECF No. 79 [493] *Id.* [494] *Id.* at 3-5. [495] Order Regarding Discovery Dispute, *Kellman v. Spokeo, Inc.*, No. 3:21-CV-08976, at 1 (N.D. Cal. Jan. 18, 2023), ECF No. 80. [496] *Id.* at 2. [497] *Id.* [498] Status Report, *Kellman v. Spokeo*, Inc., No. 3:21-CV-08976 (N.D. Cal. Sept. 13, 2022), ECF No. 71. [499] Order Extending Briefing Schedule for Class Certification, *Kellman v. Spokeo*, Inc., No. 3:21-CV-08976 (N.D. Cal. Jan. 4, 2023), ECF No. 78. [500] California Consumer Privacy Act (CCPA), Cal. Civ. Code tit. 1.81.5 § 1798.140 (c) (2018); 11 Cal. Code of Regs. § 999.337, Calculating the Value of Consumer Data (operative Aug. 14, 2020). [501] *Drips Holdings, LLC v. Teledrip, LLC*, No. 5:19-cv-2789, 2022 WL 4545233, at *3-5 (N.D. Ohio Sept. 29, 2022) (adopting in part, rejecting in part R. & R., *Drips Holdings, LLC v. Teledrip LLC*, No. 5:19-CV-02789, 2022 WL 3282676 (N.D. Ohio Apr. 5, 2022)). [502] *Id*. [503] *Id.* at *1. [504] *Id.* [505] *Id.* at *3-4. [506] *Id.* [507] *See RG Abrams Ins. v. L. Offs. of C.R. Abrams*, No. 2:21-CV-00194, 2022 WL 422824, at *11 (C.D. Cal. Jan. 19, 2022). [508] *Id.* at *9-11. [509] *Id.* at *11. [510] *Id.* (citing *United States v. Zolin*, 491 U.S. 554, 562 (1989) (citing Fed. R. Evid. 501); *Hardie v. Nat'l Collegiate Athletic Ass'n*, No. 3:13-CV-00346, 2013 WL 6121885 at *3 (S.D. Cal. Nov. 20, 2013) ("Because jurisdiction in this action is based upon a federal question, California's privacy laws are not binding on this court."); *Kalinoski v. Evans*, 377 F. Supp. 2d 136, 140–41 (D.D.C. 2005) ("The Supremacy Clause of the United States Constitution (as well as Federal Rule of Evidence 501) prevent a State from directing a federal court with regard to the evidence it may order produced in the adjudication of a federal claim.")). [511] Cal. Civ. Code § 1798.150(b). [512] *Griffey v. Magellan Health Inc.*, No. CV-20-01282-PHX-MTL, 2022 WL 1811165, at *6 (D. Ariz. June 1, 2022). [513] *Id.* at *1. [514] *Id.* at *6. [515] *Id.* [516] *Id.* [517] *Id.* [518] *Id.* [519] *Id.* [520] *In re Arthur J. Gallagher Data Breach Litig.*, No. 22-cv-137, 2022 WL 4535092, at *1 & 4 (N.D. Ill. Sept. 28, 2022). [521] *Id.* at *5 (quoting Complaint ¶¶ 62, 66). [522] *Id.* at *6. [523] *Id.* [524] *Id.* at *10-11. [525] Allison Grande, *Robinhood Inks $20M Deal To Settle Suit Over Account Hacks*, Law360 (July 6, 2022), https://www.law360.com/cybersecurity-privacy/articles/1508681/robinhood-inks-20m-deal-to-settle-suit-over-account-hacks; Pls.' Mot. Prelim. Approval of Settlement, *Mehta v. Robinhood Fin. LLC*, No. 21-CV-01013-SVK (N.D. Cal. July 1, 2022), ECF No. 61. [526] Allison Grande*, Robinhood Inks $20M Deal To Settle Suit Over Account Hacks*, Law360 (July 6, 2022), https://www.law360.com/cybersecurity-privacy/articles/1508681/robinhood-inks-20m-deal-to-settle-suit-over-account-hacks; Pls.' Mot. Prelim. Approval of Settlement, *Mehta v. Robinhood Fin. LLC*, No. 21-CV-01013-SVK, at 1 (N.D. Cal. July 1, 2022), ECF No. 61. [527] Allison Grande*, Robinhood Inks $20M Deal To Settle Suit Over Account Hacks*,

Law360 (July 6, 2022), https://www.law360.com/cybersecurity-privacy/articles/1508681/robinhood-inks-20m-deal-to-settle-suit-over-account-hacks; Pls.' Mot. Prelim. Approval of Settlement, *Mehta v. Robinhood Fin. LLC*, No. 21-CV-01013-SVK, at 3 (N.D. Cal. July 1, 2022), ECF No. 61. [528] Pls.' Mot. Prelim. Approval of Settlement, *Mehta v. Robinhood Fin. LLC*, No. 21-CV-01013-SVK, at 3 (N.D. Cal. July 1, 2022), ECF No. 61. [529] *Id.* at 14. [530] Order Granting In Part & Denying In Part Defs.' Mot. To Dismiss Pls.' Second Am. Compl., *Mehta v. Robinhood Fin. LLC*, No. 21-cv-01013-SVK (N.D. Cal. Sept. 8, 2021), ECF No. 41; Pls.' Mot. Prelim. Approval of Settlement, *Mehta v. Robinhood Fin. LLC*, No. 21-CV-01013-SVK, at 3 (N.D. Cal. July 1, 2022), ECF No. 61; Allison Grande, *Robinhood Can't Get Out Of Revamped Data Breach Suit*, Law360 (Sept. 9, 2021), https://www.law360.com/articles/1420135. [531] Allison Grande, *Robinhood Inks $20M Deal To Settle Suit Over Account Hacks*, Law360 (July 6, 2022), https://www.law360.com/cybersecurity-privacy/articles/1508681/robinhood-inks-20m-deal-to-settle-suit-over-account-hacks; Pls.' Mot. Prelim. Approval of Settlement, *Mehta v. Robinhood Fin. LLC*, No. 21-CV-01013-SVK, at 3 (N.D. Cal. July 1, 2022), ECF No. 61. [532] Pls.' Mot. Prelim. Approval of Settlement, *Mehta v. Robinhood Fin. LLC*, No. 21-CV-01013-SVK, at 20 (N.D. Cal. July 1, 2022), ECF No. 61. [533] *Id.* at 6. [534] *Id.* [535] *Id.* at 1. [536] *Vennerholm v. GEICO Cas. Co.*, No. 21-CV-806-GPC, 2022 WL 1694429, at *3 (S.D. Cal. May 26, 2022). [537] *Id.* at *1; *Brody v. Berkshire Hathaway, Inc. & GEICO*, No. CV 21-02481 (KAM) (RML) (E.D.N.Y., filed May 4, 2021), *Viscardi v. GEICO*, No. CV 21-02481 (KAM) (RML) (E.D.N.Y. filed May 6, 2021); *Connelly v. Berkshire Hathaway*, No. 8:21-CV-00152 (TDC) (E.D.N.Y. filed May 11, 2021). [538] *Vennerholm v. GEICO Cas. Co.*, No. 21-CV-806-GPC, 2022 WL 1694429, at *1 (S.D. Cal. May 26, 2022). [539] *Id.* (quoting *Pacesetter Sys., Inc. v. Medtronic, Inc.*, 678 F.2d 93, 94-95 (9th Cir. 1982) (citing *Church of Scientology of Cal. v. U.S. Dep't of Army*, 611 F.2d 738, 749 (9th Cir. 1989))). [540] *Id.* at *2. [541] *Id.* [542] *Id.* [543] *Id.* (citing *Mullinix v. US Fertility, LLC*, No. SACV 21-00409-CJC(KESx), 2021 WL 4935976 (C.D. Cal. June 8, 2021)). [544] *Id.* (quoting *Zimmer v. Domestic Corp.*, 2018 WL 1135634, at *4 (C.D. Cal. Dec. 22, 2018)). [545] *Id.* [546] *Id.* at *3. [547] Biometric Information Privacy Act ("BIPA"), 740 Ill. Comp. Stat. 14/10 (2008). [548] *Id.* [549] *Thornley v. Clearview AI, Inc.*, 984 F.3d 1241, 1247 (7th Cir. 2021). [550] *See, e.g.*, *Ronquillo v. Doctor's Associates, LLC*, 2022 WL 1016600 (N.D. Ill. 2022). [551] *Rosenbach v. Six Flags Ent. Corp.*, 129 N.E. 3d 1197, 1205 (Ill. 2019). [552] *McDonald v. Symphony Bronzeville Park, LLC*, 193 N.E.3d 1253, 1269 (Ill. 2022). [553] BIPA, 740 Ill. Comp. Stat. 14/20 (2008). [554] *Walton v. Roosevelt Univ.*, 193 N.E.3d 1276, 1279, 1282-85 (Ill. Ct. App. 2022), *appeal allowed*, 193 N.E.3d 8 (Table) (Ill. May 25, 2022). [555] *Id*. at 1282-85. [556] *Patterson v. Respondus, Inc.*, 593 F. Supp. 3d 783 (N.D. Ill. 2022), *reconsideration denied*, 2022 WL 7100547 (N.D. Ill. 2022). [557] *Wilk v. Brainshark, Inc.*, 2022 WL 4482842 (N.D. Ill.). [558] *In re Facebook Biometric Information Privacy Litig.*, 2020 WL 4818608 (N.D. Cal. 2020); *In re Facebook Biometric Information Privacy Litig.*, 2022 WL 822923 (N.D. Cal. 2022). [559] *Boone v. Snap Inc.*, 2022 WL 3328282 (N.D. Ill. 2022); *see Boone v. Snap Inc.*, No. 2022LA000708 (N.D. Ill. Nov. 22, 2022). [560] *Kashkeesh v. Microsoft Corp.*, 2022 WL 2340876 (N.D. Ill. 2022). [561] *See, e.g.*, *In re Clearview AI, Inc., Consumer Privacy Litig.*, 2022 WL 3226777 (N.D. Ill 2022). [562] Complaint, *Gielow v. Pandora Jewelry, LLC.*, No. 2022CH11181 (Ill. Cir. Ct. Nov. 15, 2022) [563] BIPA, 740 Ill. Comp. Stat 14/15 (2008). [564] Texas Capture and Use of Biometric Identifier Act ("CUBI"), Tex. Bus. & Com. § 503.001 (2017). [565] *Id.* §§ 503.001(a)–(b). [566] *Id.* § (c). [567] *Id.* § (d). [568] *Id.* [569] Press Release, Attorney General of Texas, *Paxton Sues Facebook for Using Unauthorized Biometric Data* (Feb. 14, 2022), *available at* https://www.texasattorneygeneral.gov/news/releases/paxton-sues-facebook-using-unauthorized-biometric-data. [570] *Id.* [571] Press Release, Attorney General of Texas, *Paxton Sues Google for its Unauthorized Capture and Use of Biometric Data and Violation of Texans' Privacy* (Oct. 20, 2022), *available at* https://texasattorneygeneral.gov/news/releases/paxton-sues-google-its-unauthorized-capture-and-use-biometric-data-and-violation-texans-privacy. [572] *Id.* [573] *Compare* BIPA, 740 Ill. Comp. Stat. 14/15(b) (requiring entities to inform users in writing about the capture of biometric identifiers and a written release from the user) *with* CUBI, Tex. Bus. & Com. § 503.001(b) (requiring persons only to "inform[]" users about the capture biometric

identifiers and requiring only “consent” from users). [574] *Compare* BIPA, 740 Ill. Comp. Stat. 14/20 *with* CUBI, Tex. Bus. & Com. § 503.001(d). [575] Recording Law, *All Party (Two Party) Consent States – List and Details*, *available at* https://recordinglaw.com/party-two-party-consent-states/. [576] See, e.g., *Javier v. Assurance IQ, LLC,* No. 21-16351, 2022 WL 1744107 (9th Cir. May 31, 2022); *Popa v. Harriet Carter Gifts, Inc.,* 45 F.4th 687 (3d Cir. 2022). [577] *Javier v. Assurance IQ, LLC,* No. 21-16351, 2022 WL 1744107 (9th Cir. May 31, 2022). [578] *Id.* [579] Cal. Penal Code § 631. [580] *Javier*, No. 21-16351 at *2. [581] *Javier v. Assurance IQ, LLC,* No. 20-cv-02860-JSW, 2021 WL 940319 (N.D. Cal., March 9, 2021). [582] See, e.g., Class Action Complaint, *Valenzuela v. Papa Murphy’s International, LLC et al*, No. 5:22-cv-01789 (C.D. Cal. October 11, 2022)—this proposed class action in California federal court alleges that a pizza chain violated CIPA by secretly wiretapping the private conversations of everyone who communicates via the business’s online chat feature; Class Action Complaint, *Miguel Licea v. Old Navy LLC*, No. 5:22-cv-01413 (C.D. Cal. August 10, 2022)—another proposed class action filed in federal court in California alleges that a clothing retailer surreptitiously deployed “keystroke monitoring” software to intercept, monitor, and record all communications (including keystrokes and mouse clicks) of visitors to its website; Class Action Complaint, *Annette Cody v. Columbia Sportswear Co. et al*, 8:22-cv-01654 (C.D. Cal September 7, 2022)— this digital privacy class action alleging that a sportswear retailer relied on keystroke monitoring methods to secretly record user activity has been removed from the Superior Court of California to the U.S. District Court for the central district of California; Class Action Complaint, *Esparza v. Crocs, Inc. et al*, No 3:22-cv-01842 (S.D. Cal. October 26, 2022)—this proposed class action alleges that a footwear retailer “secretly wiretaps the private conversations of everyone who communicates through the chat feature” on its website and “allows at least one third party to eavesdrop on such communications in real time and during transmission to harvest data for financial gain”; as of November 22, 2022, it has been removed from the superior court to the federal court in the southern district of California. [583] *Popa v. Harriet Carter Gifts, Inc.,* 45 F.4th 687 (3d Cir. 2022). [584] 18 Pa. Cons. Stat. Ann. § 5701-5782. [585] https://www.legis.state.pa.us/cfdocs/legis/LI/consCheck.cfm?txtType=HTM&ttl=18&div=0&chpt=57. [586] *See, e.g., Commonwealth v. Proetto,* 771 A.2d 823 (Pa. Super. Ct. 2001); *Commonwealth v. Cruttenden*, 58 A.3d 95 (Pa. 2012). [587] See, e.g., *Goldstein v. Costco Wholesale Corp.*, 559 F. Supp. 3d 1318 (S.D. Fla. Sept. 9, 2021) (dismissed); *Swiggum v. EAN Servs.*, LLC, No. 8:21-493, 2021 WL 3022735 (M.D. Fla. July 16, 2021) (dismissed). [588] *Makkinje v. Extra Space Storage, Inc.*, 8:21-cv-2234-WFJ-SPF, 2022 WL 80437 (M.D. Fla., Jan. 7, 2022). [589] *Id.* at *2. [590] *Id.* [591] 47 U.S. Code § 230. [592] *Gonzalez v. Google LLC*, 143 S. Ct. 80 (2022) (granting certiorari); *Twitter, Inc. v. Taamneh*, 143 S. Ct. 81 (2022) (granting certiorari). [593] *Gonzalez v. Google LLC*, 2 F.4th 871, 880–83 (9th Cir. 2021) (summarizing claims of Gonzalez Plaintiffs regarding Google’s responsibility in facilitating ISIS’s attacks in Paris); *id.* at 883–84 (summarizing complaint of Taamneh Plaintiffs regarding Twitter, Facebook, and Google’s role in aiding and abetting ISIS’s attack in Istanbul). [594] *Id.* [595] 47 U.S.C. § 230(c); *see also Fair Hous. Council of San Fernando Valley v. Roommates.Com, LLC*, 521 F.3d 1157, 1162 (9th Cir. 2008). [596] *Gonzalez*, 2 F.4th at 897. For other claims based on the revenue sharing theory between the technology company and ISIS that survived Section 230, they failed because the plaintiffs failed to establish the technology company’s motivation to support international terrorism. *See id.* at 899–907. [597] *Id.* at 907–10. [598] Petition of Writ of Certiorari at (i), *Gonzalez v. Google LLC*, No. 21-1333 (U.S. Apr. 4, 2022). [599] Petition of Writ of Certiorari at 14–15, *Twitter, Inc. v. Taamneh*, No. 21-1496 (U.S. May 26, 2022). [600] *NetChoice, L.L.C. v. Paxton*, 49 F.4th 439, 490 (5th Cir. 2022); *NetChoice, LLC v. Att’y Gen., Fla.*, 34 F.4th 1196, 1230 (11th Cir. 2022). [601] *NetChoice, LLC v. Att’y Gen., Fla.*, 34 F.4th 1196, 1230 (11th Cir. 2022). [602] *NetChoice, L.L.C. v. Paxton*, 49 F.4th 439, 490 (5th Cir. 2022). [603] David Yaffe-Bellany, *FTX Investigating Possible Hack Hours After Bankruptcy Filing*, N.Y. Times (Nov. 12, 2022), *available at* https://www.nytimes.com/2022/11/12/business/ftx-cryptocurrency-hack.html. [604] Ava Benny-Morrison, *US Probes How $372 Million Vanished in Hack After FTX Bankruptcy*, Bloomberg (Dec. 27, 2022), *available at* https://www.bloomberg.com/news/articles/2022-12-27/us-probes-how-372-million-

vanished-in-hack-after-ftx-bankruptcy. [605] Metaverse and Privacy, IAAP, *available at* https://iapp.org/news/a/metaverse-and-privacy-2/. [606] NYC Dep't Consumer & Worker Prot., *Notice of Public Hearing and Opportunity to Comment on Proposed Rules*, *available at* https://rules.cityofnewyork.us/wp-content/uploads/2022/09/DCWP-NOH-AEDTs-1.pdf. [607] N.Y.C., No. 1894-2020A § 20-870 (Nov. 11, 2021), *available at* https://legistar.council.nyc.gov/LegislationDetail.aspx?ID=4344524&GUID=B051915D-A9AC-451E-81F8-6596032FA3F9. [608] *Id.* [609] White House, Office for Science and Technology, *available at* https://www.whitehouse.gov/ostp/ai-bill-of-rights/. [610] *Id.* [611] *Report: Account takeover attacks spike-fraudsters aim at fintech and crypto,* Venturebeat, November 28, 2022, https://venturebeat.com/security/report-account-takeover-attacks-spike-fraudsters-take-aim-at-fintech-and-crypto/. [612] Exec. Order No. 14067, 87 FR 14143, Executive Order on Ensuring Responsible Development of Digital Assets (Mar. 9, 2022), *available at* https://www.whitehouse.gov/briefing-room/presidential-actions/2022/03/09/executive-order-on-ensuring-responsible-development-of-digital-assets/. [613] Press Release, The White House, FACT SHEET: White House Releases First-Ever Comprehensive Framework for Responsible Development of Digital Assets (Sep. 16, 2022), *available at* https://www.whitehouse.gov/briefing-room/statements-releases/2022/09/16/fact-sheet-white-house-releases-first-ever-comprehensive-framework-for-responsible-development-of-digital-assets/. [614] Press Briefings, The White House, Background Press Call by Senior Administration Officials on the First-Ever Comprehensive Framework for Responsible Development of Digital Assets (Sep. 16, 2022), *available at* https://www.whitehouse.gov/briefing-room/press-briefings/2022/09/16/background-press-call-by-senior-administration-officials-on-the-first-ever-comprehensive-framework-for-responsible-development-of-digital-assets/. [615] Press Release, The White House, *FACT SHEET: White House Releases First-Ever Comprehensive Framework for Responsible Development of Digital Assets* (Sep. 16, 2022), *available at* https://www.whitehouse.gov/briefing-room/statements-releases/2022/09/16/fact-sheet-white-house-releases-first-ever-comprehensive-framework-for-responsible-development-of-digital-assets/. [616] The U.S. Department of Justice*, Justice Department Announces Report on Digital Assets and Launches Nationwide Network* (Sep. 16, 2022), *available at* https://www.justice.gov/opa/pr/justice-department-announces-report-digital-assets-and-launches-nationwide-network. [617] Financial Stability Oversight Council, *Report on Digital Asset Financial Stability Risks and Regulation* (Oct. 3, 2022), *available at* https://home.treasury.gov/system/files/261/Fact-Sheet-Report-on-Digital-Asset-Financial-Stability-Risks-and-Regulation.pdf. [618] Joint Statement on Crypto-Asset Risks to Banking Organizations (Jan. 2023), available at https://www.fdic.gov/news/press-releases/2023/pr23002a.pdf [619] Press Release, Financial Services Committee, McHenrt Announces Financial Services Subcomittee Chairs and Jurisdiction for 118th Congress (Jan. 2023), available at https://financialservices.house.gov/news/documentsingle.aspx?DocumentID=408500 [620] *Hermès International, et al. v. Mason Rothschild,* No. 22-cv-384 (JSR), Dkt. 16 (S.D.N.Y). [621] *Rogers v. Grimaldi*, 875 F.2d 994 (2d Cir. 1989). [622] *Hermès International, et al. v. Mason Rothschild*, No. 22-cv-384 (JSR), Dkt. 50 (May 18, 2022) (memorandum order regarding motion to dismiss). [623] *Id.* [624] *Id.* [625] *Hermès International, et al. v. Mason Rothschild,* No. 22-cv-384 (JSR) Minute Entry (S.D.N.Y November 18, 2022). [626] Exec. Order 14086, 87 FR 62283, Enhancing Safeguards for United States Signals Intelligence Activities (Oct. 7, 2022), *available at* https://www.whitehouse.gov/briefing-room/presidential-actions/2022/10/07/executive-order-on-enhancing-safeguards-for-united-states-signals-intelligence-activities/. [627] *Id.* [628] Data Protection Review Court, 87 Fed. Reg. 62303 (Oct. 14, 2022) (rulemaking related to 20 C.F.R. § 201), *available at* https://www.govinfo.gov/content/pkg/FR-2022-10-14/pdf/2022-22234.pdf?utm_source=federalregister.gov&utm_medium=email&utm_campaign=subscription+mailing+list [629] Questions & Answers: EU-U.S. Data Privacy Framework, European Commission (Oct. 7, 2022), *available at* https://ec.europa.eu/commission/presscorner/detail/en/qanda_22_6045. [630] EU General Data Protection Regulation (GDPR): Regulation (EU) 2016/ 679. [631] Press Release, European Commission, *Data protection: Commission starts process to adopt*

adequacy decision for safe data flows with the US (Dec. 13, 2022), *available at* https://ec.europa.eu/commission/presscorner/detail/en/IP_22_7631. [632] *Id.* [633] 18 U.S.C. § 2523. [634] *Press Release,* U.S. Department of Justice, Promoting Public Safety, Privacy and the Rule of Law Around the World: The Purpose and Impact of the CLOUD Act (Apr. 2019), *available at* https://www.justice.gov/opa/press-release/file/1153446/download. [635] Press Release, U.S. Department of Justice, Landmark U.S.-UK Data Access Agreement Enters into Force (Oct. 3, 2022), *available at* https://www.justice.gov/opa/pr/landmark-us-uk-data-access-agreement-enters-force. [636] Article 3(1), Agreement between the Government of the United States of America and the Government of the United Kingdom of Great Britain and Northern Ireland on Access to Electronic Data for the Purpose of Countering Serious Crime, U.S.-U.K. (Oct. 3, 2022), *available at* https://www.justice.gov/criminal-oia/cloud-act-agreement-between-governments-us-united-kingdom-great-britain-and-northern. [637] *Id.* at Article 4. [638] *Press Release,* U.S. Department of Justice, Landmark U.S.-UK Data Access Agreement Enters into Force (Oct. 3, 2022), *available at* https://www.justice.gov/opa/pr/landmark-us-uk-data-access-agreement-enters-force. [638] *Press Release,* U.S. Department of Justice, United States and Canada Welcome Negotiations of a CLOUD Act Agreement (Mar. 22, 2022), *available at* https://www.justice.gov/opa/pr/united-states-and-canada-welcome-negotiations-cloud-act-agreement. [639] Press Release, U.S. Department of Justice, United States and Canada Welcome Negotiations of a CLOUD Act Agreement (Mar. 22, 2022), *available at* https://www.justice.gov/opa/pr/united-states-and-canada-welcome-negotiations-cloud-act-agreement. [640] Press Release, U.S. Department of Justice, United States and Australia Enter CLOUD Act Agreement to Facilitate Investigations of Serious Crime (Dec. 15, 2021), *available at* https://www.justice.gov/opa/pr/united-states-and-australia-enter-cloud-act-agreement-facilitate-investigations-serious-crime.

The following Gibson Dunn lawyers assisted in the preparation of this article: Alexander H. Southwell, Cassandra Gaedt-Sheckter, Svetlana S. Gans, Amanda M. Aycock, Ryan T. Bergsieker, Abbey Barrera, Snezhana Stadnik Tapia, Matt Buongiorno, Terry Wong, Ruby Lang, Jay Mitchell, Sarah Scharf, Edmund Bannister*, Jenn Katz, Eric Hornbeck, Cassarah Chu, Michael Kutz, Najatt Ajarar*, Matthew Reagan, Nicole Lee, Emma Li*, Jay Minga, Apratim Vidyarthi*, Diego Wright*, Yixian Sun*, Mashoka Maimona*, Kunal Kanodia, Ayushi Sutaria*, Stanton Burke, Justine Deitz, and Brendan Krimsky.

Gibson Dunn lawyers are available to assist in addressing any questions you may have about these developments. Please contact the Gibson Dunn lawyer with whom you usually work, the authors, or any member of the firm's Privacy, Cybersecurity & Data Innovation practice group:

United States S. Ashlie Beringer – Co-Chair, PCDI Practice, Palo Alto (+1 650-849-5327, aberinger@gibsondunn.com) Jane C. Horvath – Co-Chair, PCDI Practice, Washington, D.C. (+1 202-955-8505, jhorvath@gibsondunn.com) Alexander H. Southwell – Co-Chair, PCDI Practice, New York (+1 212-351-3981, asouthwell@gibsondunn.com) Matthew Benjamin – New York (+1 212-351-4079, mbenjamin@gibsondunn.com) Ryan T. Bergsieker – Denver (+1 303-298-5774, rbergsieker@gibsondunn.com) David P. Burns – Washington, D.C. (+1 202-887-3786, dburns@gibsondunn.com) Gustav W. Eyler – Washington, D.C. (+1 202-955-8610, geyler@gibsondunn.com) Cassandra L. Gaedt-Sheckter – Palo Alto (+1 650-849-5203, cgaedt-sheckter@gibsondunn.com) Svetlana S. Gans – Washington, D.C. (+1 202-955-8657, sgans@gibsondunn.com) Lauren R. Goldman – New York (+1 212-351-2375, lgoldman@gibsondunn.com) Stephenie Gosnell Handler – Washington, D.C. (+1 202-955-8510, shandler@gibsondunn.com) Nicola T. Hanna – Los Angeles (+1 213-229-7269, nhanna@gibsondunn.com) Howard S. Hogan – Washington, D.C. (+1 202-887-3640, hhogan@gibsondunn.com) Kristin A. Linsley – San Francisco (+1 415-393-8395, klinsley@gibsondunn.com) Vivek Mohan – Palo Alto (+1 650-849-5345, vmohan@gibsondunn.com) Karl G. Nelson – Dallas (+1 214-698-3203,

knelson@gibsondunn.com) Rosemarie T. Ring – San Francisco (+1 415-393-8247, rring@gibsondunn.com) Ashley Rogers – Dallas (+1 214-698-3316, arogers@gibsondunn.com) Eric D. Vandevelde – Los Angeles (+1 213-229-7186, evandevelde@gibsondunn.com) Benjamin B. Wagner – Palo Alto (+1 650-849-5395, bwagner@gibsondunn.com) Michael Li-Ming Wong – San Francisco/Palo Alto (+1 415-393-8333/+1 650-849-5393, mwong@gibsondunn.com) Debra Wong Yang – Los Angeles (+1 213-229-7472, dwongyang@gibsondunn.com)

Europe Ahmed Baladi – Co-Chair, PCDI Practice, Paris (+33 (0) 1 56 43 13 00, abaladi@gibsondunn.com) James A. Cox – London (+44 (0) 20 7071 4250, jacox@gibsondunn.com) Patrick Doris – London (+44 (0) 20 7071 4276, pdoris@gibsondunn.com) Kai Gesing – Munich (+49 89 189 33-180, kgesing@gibsondunn.com) Bernard Grinspan – Paris (+33 (0) 1 56 43 13 00, bgrinspan@gibsondunn.com) Joel Harrison – London (+44(0) 20 7071 4289, jharrison@gibsondunn.com) Vera Lukic – Paris (+33 (0) 1 56 43 13 00, vlukic@gibsondunn.com) Penny Madden – London (+44 (0) 20 7071 4226, pmadden@gibsondunn.com)

Asia Kelly Austin – Hong Kong (+852 2214 3788, kaustin@gibsondunn.com) Connell O'Neill – Hong Kong (+852 2214 3812, coneill@gibsondunn.com) Jai S. Pathak – Singapore (+65 6507 3683, jpathak@gibsondunn.com)

**Najatt Ajarar, Edmund Bannister, Emma Li, Yixian Sun, Ayushi Sutaria, Apratim Vidyarthi, Diego Wright, and Mashoka Maimona are recent law graduates in the New York and San Francisco offices not yet admitted to practice law.*

Related Capabilities

Privacy, Cybersecurity, and Data Innovation

Public Companies