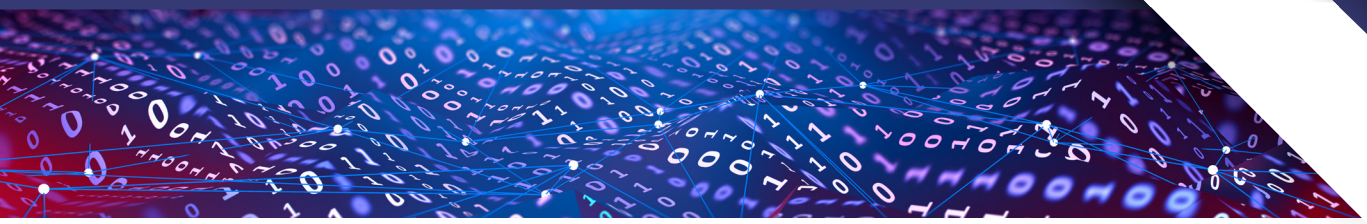
WILLKIE FARR & GALLAGHER LLP

BRUSSELS CHICAGO FRANKFURT HOUSTON LONDON LOS ANGELES MILAN NEW YORK PALO ALTO PARIS ROME SAN FRANCISCO WASHINGTON

Willkie Cybersecurity and Privacy Review: *Data Privacy Day 2022*



CONTENTS

WELCOME

Data Privacy Day is observed around the world on January 28 as a day to raise awareness of privacy and data security issues. In 2022, this task is more important than ever. There is no corner of the economy — no industry, no business, and no organization — where personal data and the laws and regulations that govern the collection, use, security, and sharing of that data do not play a critical role. Additionally, every trend line suggests that the legal, regulatory, ethical and business issues associated with privacy and data security are only going to become more complex, more material, and more important for businesses, policymakers, and regulators around the world.

For privacy and data security professionals, Data Privacy Day also serves as a useful moment to take stock of the events of the last year, and to consider the challenges and opportunities on the horizon. Today, those challenges manifest in myriad ways. For example:

- Companies in the United States ("U.S.") are working to get into compliance with new state laws that will come into effect in 2023, monitoring state legislative activity for the possibility of new privacy laws, and watching events in Washington, DC to see how regulators like the FTC and the SEC use their existing authority to move the needle on privacy and data security issues;
- Companies that do business across the Atlantic are grappling with an uncertain legal picture regarding the transfer of personal data from the European Union ("EU") to the U.S.;
- Companies of all shapes and sizes are struggling to defend against and respond to cyberattacks leveraging ransomware and other forms of malware to significantly disrupt business operations, and to ensure that their practices are compliant with new, more stringent privacy laws and cybersecurity regulations; and
- Companies that operate globally are analyzing newly enacted or proposed laws in countries like China and India, and developing compliance strategies that seek to navigate differences among the various laws.

Over the coming weeks and months, these challenges are likely to evolve — and may be replaced by new challenges. Decisions from courts and regulators, activity by legislators, and changes in technology and consumer behavior and expectations are all likely to have an impact on how we view and respond to these challenges. In the pages that follow, we share our thoughts about some of the major issues companies are likely to face over the next 12 months and discuss steps that companies can take to put themselves in the best possible position to meet those challenges and achieve their business objectives. We look forward to working with you in the coming months, and to revisiting these issues on Data Privacy Day 2023.

Daniel Alvarez
Partner
Co-Chair, Cybersecurity and Privacy Practice Group

1875 K Street, N.W.
Washington, DC 20006-1238
T 202 303 1125
F 202 303 2125

Laura Jehl
Partner
Co-Chair, Cybersecurity and Privacy Practice Group

1875 K Street, N.W.
Washington, DC 20006-1238
T 202 303 1056
F 202 303 2000

KEY ISSUES IN PRIVACY AND DATA USE

In this section, we highlight some of the key trends and issues in consumer privacy laws, and what they mean for companies moving forward. The difficult part was choosing where to focus — while we specifically highlighted issues raised by the new state privacy laws in the U.S., increased scrutiny of artificial intelligence/big data, and cross-border data transfers, there is so much more happening as consumer privacy laws and regulations around the world continue to evolve. For example:

- **FTC's New Sheriff.** President Biden's choice of Lina Khan as the newest chair of the Federal Trade Commission ("FTC") sent a clear message to industry that the FTC would be an active regulator. Chair Khan has made it clear that consumer protection in the technology space will be a significant focus of the FTC under her watch. Consumer privacy issues — potentially including both increased enforcement and new rulemakings — will likely be a major part of that focus.
- **General Data Protection Regulation ("GDPR") Enforcement Ramps Up.** By most measures, 2021 was the year in which regulators around Europe began to wield the major enforcement "sticks" in GDPR. With over $1 billion in fines levied for alleged GDPR violations in 2021 — over 500 percent more than what was levied in 2020 — the trend line is clear, and companies must consider themselves on notice.
- **Federal Privacy Legislation.** Congress continues to deliberate, and various drafts of proposed legislation continue to be circulated for feedback from stakeholders, but little real progress appears to have been made and the likelihood of passing comprehensive federal privacy legislation seems increasingly small. While most of the focus has been on differences over preemption and enforcement, recent statements by key members and their staffs suggest that there are also significant substantive differences that remain to be overcome.
- **Children's Privacy.** The Children's Online Privacy Protection Act ("COPPA") is over 20 years old, and one of the few areas where movement does seem possible is with respect to legislative efforts to update the COPPA and other children's privacy laws in the U.S. We expect to see more on this front in the coming months.
- **Biometric Privacy.** Illinois was the first state to enact a biometric privacy bill in 2008. To date, only Texas and Washington have passed broad biometric privacy laws in the same vein as that in Illinois, but numerous states, such as New York and Massachusetts, have similar laws

pending before their legislatures. Whether the biometric protections get wrapped into more comprehensive privacy bills or are rolled out as standalone laws remains to be seen, but these efforts bear watching by businesses that collect, process, or otherwise use biometric information.

- **Data Localization.** A growing number of jurisdictions are requiring companies to maintain local copies of the data they collect from individuals in the jurisdiction. But doing so might implicate broader privacy and surveillance issues that conflict with other jurisdictions' privacy laws.
- **Adtech Gets Complicated.** Use of third-party cookies and pixels on websites, once ubiquitous, is under new scrutiny on both sides of the Atlantic. New enforcement actions and judicial rulings in the EU, scrutiny of potential "sales" under the California Consumer Privacy Act ("CCPA") and the forthcoming opt-out right from targeted advertising under California Privacy Rights Act ("CPRA"), a potential rulemaking from the FTC, legislation in Congress, and development (and delays) of new technologies from Big Tech all signal major changes coming for targeted digital advertising practices.
- **China and India Join the Fray.** In 2021, China's privacy law went into effect, borrowing significantly from GDPR. In India, a proposed comprehensive privacy law is likely to be enacted and come into effect in 2022. The combination of comprehensive privacy laws in two of the largest markets in the world is likely to have a profound effect on how companies protect and use data, and whether they continue their existing business practices in those jurisdictions.

The watchwords here are uncertainty, change, and fluidity. The legal and regulatory landscape continues to be highly fluid as policymakers and regulators struggle to keep up with innovations in technology and business practices, as well as shifting consumer behaviors and demands; together, these pressures have led to significant uncertainty regarding what's next and how companies can maintain a robust compliance program in the face of constant change.

Prepping for 2023: Virginia, California, Colorado … and More?

One of the major projects that will keep privacy teams busy in 2022 is preparing for the new privacy laws coming into effect in 2023. After California voters approved the CPRA,[1] which significantly revised the CCPA,[2] legislatures in Virginia and Colorado enacted similar laws. First, on March 3, 2021, then-Governor Ralph Northam signed into law the Virginia Consumer Data Protection Act ("VCDPA").[3] Shortly thereafter, Governor Jared Polis signed into law the Colorado Privacy Act ("CPA") on July 7, 2021.[4] The VCDPA and CPRA will come into effect on January 1, 2023, and the CPA will come into effect on July 1, 2023, giving businesses the remainer of 2022 to implement necessary changes to their data collection, use, and sharing practices to bring their programs into compliance. While organizations that already have a privacy program based on the GDPR or CCPA are likely to be able to adapt their existing programs to these laws, the differences between the laws and the continued risk that additional states will follow the trend will force companies to think creatively about compliance.

[1] California Privacy Rights and Enforcement Act, available at https://oag.ca.gov/system/files/initiatives/pdfs/19-0021A1%20%28Consumer%20Privacy%20-%20Version%203%29_1.pdf.

[2] Cal. Civ. Code § 1798.100 *et seq.*

[3] Consumer Data Protection Act, SB 1392, available at https://lis.virginia.gov/cgi-bin/legp604.exe?211+ful+SB1392ES1+pdf.

[4] Colorado Privacy Act, SB 21-190, available at https://leg.colorado.gov/sites/default/files/2021a_190_signed.pdf.

CPRA, VCDPA, and CPA: Roommates or Hostile Neighbors?

The enactment of VCDPA and CPA presents particular challenges to companies because compliance work will need to happen simultaneously with similar work for CPRA. As we discussed when the CPRA first passed,[5] the CPRA is not merely an update to the CCPA. For instance, the CPRA (i) introduces the right of consumers to request the correction of their personal data; (ii) expands the "opt-out" right to require that businesses provide a means for consumers to opt out of any data sharing for targeted advertising; (iii) offers consumers the right to limit the use and disclosure of "sensitive personal information" to certain enumerated business purposes; (iv) directs service providers to assist businesses in responding to consumer rights requests; and (v) establishes the California Privacy Protection Agency, which is empowered to enforce the CPRA and promulgate regulations. These requirements will be new in California, and therefore, new to any company whose privacy practices currently are based solely on the CCPA.

VCDPA and CPA: GDPR for the United States?

Unlike CCPA and CPRA, the VCDPA and CPA import a number of concepts—including certain terms and language, like "personal data"—from the GDPR. However, in their scope and construction, they remain largely American privacy laws, with "opt-out" for collection and use of personal data (other than for "sensitive" data, to which an "opt-in" model applies). Among other things, they:

- Introduce to U.S. law the GDPR's concepts of "data controllers" and "data processors" and the attendant roles and responsibilities of each, including an affirmative duty on the part of controllers to implement appropriate data security practices;
- Require data controllers, before starting certain types of processing, to perform and document a privacy assessment—similar to GDPR's data protection impact assessment—weighing the risks, benefits, and protections possible in that processing (in the case of CPA, the data controller must make the results of the data protection assessment available to the Colorado Attorney General upon request);
- Require data controllers to be transparent about how they process data and the purposes of such processing by posting a privacy policy that provides sufficient detail about their data processing practices;
- Grant to consumers numerous rights related to their personal data when in the hands of other parties, such as the right to have their data deleted and the right to opt out of certain types of processing (e.g., targeted advertising or sales);
- Like both CPRA and GDPR (but unlike CCPA), require contracts with specific data protection provisions for data processing relationships, and impose a duty on the part of processors to assist controllers in discharging such duties as responding to consumer rights requests; and
- Apply broadly to any business that annually processes sufficiently significant volumes of the personal data of each state's residents.

Importantly, neither the VCDPA nor the CPA provides a private right of action. Enforcement of the VCDPA falls to the Commonwealth Attorney General who may bring actions against businesses for violations that seek injunctions to stop the offending activities or fines of up to $7,500 per violation. Like the CCPA and CPRA, however, VCDPA includes a 30-day cure provision. The Colorado Attorney General or District Attorneys may bring an enforcement action seeking injunctive relief or appropriate civil penalties for violations of the CPA. Unique among these laws, the CPA provides 60 days, rather than 30 days, to cure any violations.

The upcoming year is likely a precursor to a busy few years for privacy and data security legislation and policymaking in the United States. First, several states appear ready to follow Virginia, Colorado, and California in adopting comprehensive privacy regimes: there are already privacy bills in various stages of the legislative process in at least

[5] For a more in-depth summary of the CPRA, please see Willkie's client alert from Nov. 11, 2020, available here.

12 different states.[6] Many of these laws will likely be similar (for instance, the VCDPA was modeled on a bill from Washington), but as with state data breach notification laws there will probably be sufficient differences that each law will need to be examined on its own merits. Second, federal privacy legislation remains a possibility, with bills coming from both Republican and Democratic legislators. Further, regardless of whether Congress acts, federal regulatory agencies, under leadership installed by the Biden Administration, appear poised to focus their energies and authority to both enforce existing privacy requirements and adopt new ones. As a result, adaptability will remain a key component of any privacy program going forward.

[6] In addition to California, Colorado, and Virginia, privacy bills have been introduced in Alaska, Florida, Indiana, Maryland, Massachusetts, Minnesota, New Jersey, New York, North Carolina, Ohio, Pennsylvania, and Washington. *See* IAPP Tracker: US State Comprehensive Privacy Law Comparison, https://iapp.org/resources/article/us-state-privacy-legislation-tracker/ (last updated Jan. 13, 2022).

Work To Be Done

It may feel like there is plenty of time to come into compliance with the CPRA, VCDPA, and CPA, but many companies have a significant task ahead, not the least of which is actually identifying what specific steps to take. Some examples of likely workflows include:

- Data mapping/data flow review to understand what types of personal data are coming in, its sources, its purpose, its retention period, and who is responsible for that data and how those map to the VCDPA, CPA, and CPRA requirements, including identifying any "sensitive" data;
- Updating policies and procedures to ensure that employees can consistently handle consumer rights requests, data is appropriately protected, and the language in public policies and notices complies with each of the applicable laws;
- Identifying key data-sharing relationships and the contracts that govern them. In some cases, contracts may need to be renegotiated or amended; and
- Redrafting, as necessary, public-facing documents to ensure those documents contain all required disclosures and accurately reflect the company's data processing, sharing, and protection practices.

Growing Use of AI Systems Leads to Increased Scrutiny and Regulation

The last year saw significant developments with respect to Artificial Intelligence technologies ("AI Systems") and to what regulation and legislation related to the use of these technologies might look like. In analyzing guidance and proposed legislation concerning AI Systems, a few key themes emerge. Primarily, concerns about algorithmic bias have been amplified by recent social justice movements. As global businesses continue to embrace AI Systems in 2022, it is becoming an imperative for them to track regulatory changes both domestically and internationally to meet any compliance obligations.

U.S. Approach to Regulation of AI Systems Took Important Steps in 2021

Although the U.S. lacks a comprehensive federal privacy law, certain federal agencies have recently addressed AI Systems in various guidance documentation. In April 2021, the FTC

addressed potential bias in AI Systems, affirming its authority to address such issues under Section 5 of the FTC Act and the Fair Credit Reporting Act and signaling that unless businesses adopt a transparency approach, test for discriminatory outcomes, and are truthful about data use, FTC enforcement actions may result.[1] Other federal agencies, through published guidelines, have followed the FTC's model. In October 2021, for example, the Equal Employment Opportunity Commission affirmed that employers who utilize AI Systems should ensure that they comply with federal anti-discrimination laws, and announced an "initiative [that] will examine more closely how technology is fundamentally changing the way employment decisions are made … [and] aims to guide applicants, employees, employers, and technology vendors in ensuring that technologies are used fairly, consistent with federal equal employment opportunity laws."[2]

Issues regarding the fair and ethical use of AI Systems also caught the attention of Congress in 2021. In November, Representatives Maxine Waters (D-CA) and Bill Foster (D-IL) sent a letter to members of the Federal Financial Institutions Examination Council ("FFIEC") to emphasize the necessity for fair and ethical use of AI and its associated risks. It seems likely that any movement on privacy legislation from Congress in 2022 will involve some discussion of its effects on the use of AI.

At the state level, privacy laws enacted in 2021 in Colorado and Virginia will enable consumers in those states to opt out or object to the use of their personal information for, among other things, "automated decision-making." While AI Systems are not specifically addressed, these state laws, in addition to the California Privacy Rights Act, require data controllers in certain circumstances to conduct data protection impact assessments to determine whether processing risks associated with profiling may result in unfair or disparate impact on consumers. As other states consider adding their names to the list of jurisdictions with comprehensive privacy laws in 2022, we can likely expect additional requirements that will implicate the growing use of AI Systems.

EU Approach to Regulation of AI Systems

Unlike the U.S., the European Union has in GDPR a comprehensive privacy law that includes explicit guidance regarding the treatment of automated decision-making practices. Specifically, GDPR's Article 22 provides individuals in the EU with the right not to be subject to decisions based solely on automated processing which may produce legal effects for the individual. GDPR establishes many key requirements around the use of AI Systems, especially with respect to its general data minimization and purpose principles.

In addition to GDPR's requirements, regulators in the EU have proposed the draft AI Regulation ("Draft AI Regulation").[3] Released by the European Commission in April 2021, the Draft AI Regulation would require companies who use AI Systems as part of their business practices in the EU to affirmatively take steps to limit the harmful impact of AI. While AI Systems have previously been subject to guidelines from governmental entities and industry groups, the Draft AI Regulation would be the most comprehensive AI Systems law in Europe. Moreover, as currently drafted, it has sharp enforcement teeth: it would establish an EU AI board to facilitate implementation of the law, allow EU member state regulators to enforce the law, and authorize fines of *up to 6% of a company's annual worldwide turnover*.

The draft will likely be subject to a period of discussion and revision with the potential for a transition period, meaning that many specifics remain subject to change and companies will have a few years to prepare. As to the former, in November 2021, the European Parliamentary Research Service released a briefing document that summarized stakeholder input regarding the Draft AI Regulation; according to the document, stakeholder comments and proposed amendments focused on, among other things, the definition of an AI System, provisions regarding prohibited practices, and how to assess

[1] Jillson, Elisa, "Aiming for truth, fairness, and equity in your company's use of AI," Federal Trade Commission (www.ftc.gov), April 19, 2021. The FTC first issued guidance in 2020 regarding the use of AI Systems that promote fairness and equity, and directed that the use of AI tools should be "transparent, explainable, fair, and empirically sound, while fostering accountability." Smith, Andrew, "Using Artificial Intelligence and Algorithms," Federal Trade Commission (www.ftc.gov), April 8, 2020.

[2] Press Release, "EEOC Launches Initiative on Artificial Intelligence and Algorithmic Fairness," Equal Employment Opportunity Commission (www.eeoc.gov), Oct. 28, 2021.

[3] "Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts," European Commission (www.eur-lex.europa.eu), April 21, 2021.

the potential impact of AI System harms on individuals. These discussions will continue into 2022.

International Guidance Regarding AI Systems

In addition to their respective domestic initiatives, the U.S. and EU led bilateral and multilateral efforts to discuss issues around the growing use of AI Systems. In late September 2021, representatives from the U.S. and the European Union met to coordinate objectives related to the U.S.-EU Trade and Technology Council (the "Council"). Both the U.S. and the EU delegations acknowledged concerns that authoritarian regimes around the world may develop and use AI Systems to curtail human rights, suppress free speech, and enforce surveillance systems. The Council's public statements on AI Systems, issued jointly by the U.S. and EU, affirm their "willingness and intention to develop and implement trustworthy AI" and a "commitment to a human-centric approach that reinforces shared democratic values." The Council's statement notes that the responsible development of AI includes "inclusion, diversity, innovation, economic growth, and societal benefit." The U.S.-EU initiative, while emphasizing transatlantic cooperation, nevertheless highlights the different approaches of the two regulatory regimes.

In November 2021, the member states of the United Nations Educational, Scientific, and Cultural Organization ("UNESCO") adopted an agreement that "defines the common values and principles needed to ensure the healthy development of AI." The Draft Text of the Recommendations on the Ethics of Artificial Intelligence proposes similar recommendations to the Draft AI Regulation. Among other things, the UNESCO recommendations include banning the use of AI Systems for social scoring and mass surveillance, assessing the preparedness of legal and technical infrastructure, appointing an AI ethics officer or other oversight mechanism, and protecting the environment through energy and resource-efficient AI methods. The recommendations also suggest that both tech firms and governmental entities should offer more robust protection of personal data than they currently provide.

Practical Strategies for 2022 and Beyond

The increased proliferation and use of AI Systems has already resulted in an accompanying increase in regulatory scrutiny, and that trend is likely to continue. Businesses that utilize AI Systems likely should consider adopting a comprehensive governance approach that addresses both the complimentary and divergent aspects of U.S., EU, and any other applicable regulatory regimes. Although laws governing the use of AI Systems remain in flux, businesses that deploy AI need to continue to consider the ethical implications of the use of such technologies, as well as think globally and practically to best position themselves moving forward.

Cross-Border Data Transfers: Uncertainty Prevails

Since the July 2020 *Schrems II* decision by the EU's Court of Justice, which invalidated the EU-U.S. Privacy Shield program, companies around the globe have been scrambling to answer open questions and find new approaches to cross-border data transfers to provide the adequate protection necessary to comply with GDPR. In 2021, two major developments provided answers — and raised more questions. First, the European Commission ("EC") adopted new Standard Contractual Clauses ("SCCs") that more closely align with GDPR, and established a time frame for companies to transition to the new SCCs. Second, the European Data Protection Board (the "EDPB") adopted its recommendations on measures that supplement transfer tools to ensure compliance with GDPR and other EU

requirements regarding the protection of personal data (the "Recommendations"). Regulators in the EU and United Kingdom ("UK") put some questions to rest by adopting an adequacy decision for transfers between the EU and UK, but subsequent decisions from the UK's Information Commissioner's Office ("ICO") about use of the new SCCs threw another curveball into the picture. Without an agreement on the horizon between the EU and U.S. (or UK and U.S.) for a new Privacy Shield-type mechanism to facilitate data transfers, these questions — and uncertainty — will persist in 2022.

New SCCs and EDPB Recommendations — More Diligence, More Questions, More Uncertainty

With the release of the Recommendations and new SCCs, the EDPB and the EC appear to have reached what has been described as a practical compromise on the key question of risk-based data transfer assessments, which attempts to account for the likelihood that governmental authorities will seek or obtain access to transferred personal data. Both the Recommendations and the SCCs require a case-specific analysis of the law and practice of third-country destinations, or third countries through which transferred personal data may transit, with respect to the protections provided for such data. The adoption of this subjective analysis represents the greatest substantive distinction between the November 2020 draft and the Recommendations as adopted. However, the scope of review and level of documentation required to complete this analysis and demonstrate compliance with the Recommendations will be significant.

The new SCCs create substantive and procedural requirements for both data exporters and data importers. Among other things, the allocation of liability will require focused analysis by the parties to properly address risk. Data importers may seek indemnification to address changes in the allocation of liability that currently exist under contract. To the extent that terms of commercial liability conflict with the new SCCs' liability provisions (or undermine the rights of data subjects), such terms may invalidate the adequacy or legal basis of the SCCs as a transfer mechanism. The new SCCs mirror GDPR's data processing principles, and impose these requirements on data importers. These are reflected in enumerated obligations for both parties around purpose limitations, transparency, data minimization, accuracy, and storage limitations, which imply requirements to review, for instance, the information notices and consents of data subjects, data retention policies, IT and privacy policies, security measures, and the provision of more detailed instructions to processors and sub-processors.

The new SCCs expressly aim to address the concerns raised by *Schrems II*, in part by requiring data exporters and data importers to assess risks posed by the laws of third country destinations, and to account for such risks by providing specific safeguards — in particular with respect to dealing with binding requests from public authorities. Parties must assess the local laws and practices of the third country destination, and warrant that they have no reason to believe such laws or practices would prevent the data importer from fulfilling its obligations under the SCCs. The risk assessment required under the new SCCs is meant to be collaborative, and the parties may conclude there is no impediment to compliance with the SCCs based upon considerations of "relevant and documented practical experience with prior instances of requests for disclosure from public authorities, or the absence of such requests, covering a sufficiently representative timeframe."

The Recommendations set forth a specific legal analysis which is more nuanced than that required by the SCCs. The Recommendations emphasize not only the analysis of the governing legislation, but also address situations where a *known practice* suggests that non-enforcement of, or non-compliance with, such legislation may be expected. These assessments should be made in consultation with legal counsel, must include relevant internal and external operational and technical components related to the transfer, and may be based upon publicly available sources of information. Generally, where uncertainties arise in light of the application of "problematic legislation," either the transfer must be suspended or supplemental measures must be implemented. However, where the parties determine that they "have no reason to believe that relevant and problematic legislation will be applied, in practice, to [the] transferred data" in such a manner as to prevent the importer from fulfilling its obligations under

GDPR, supplemental measures beyond the SCCs may not be necessary.

Per both the SCCs and Recommendations, the data transfer risk assessment and resulting findings must be documented in a detailed report. As described in the Recommendations, this report must demonstrate through "relevant, objective, reliable, verifiable, and publicly available or otherwise accessible information" that problematic legislation, as applied in practice, will not interfere with a data importer fulfilling its obligations under GDPR Article 46. Moreover, the report must identify all actors involved in the assessment (e.g., law firms, consultants, or internal departments), the dates of the relevant checks or assessments made, and it must be kept up to date. The report should also be endorsed by the legal representative of the data exporter. The data exporter and data importer may be held liable for any decisions taken on the basis of the data transfer risk assessment report, which may be requested by competent supervisory authorities and/or judicial bodies.

Against this backdrop, decisions by various member state regulators have added further layers to the analysis. Most recently, a decision by the Austrian data protection authority raised issues regarding the *potential* for governmental authorities to access personal data pertaining to EU data subjects where such data is transferred to U.S.-based cloud service providers, despite technical measures to protect such data. Multiple member state regulators across the European Union are expected to weigh in on this issue in the coming months, potentially adding to the complexity of the situation.

Cross-Border Data Transfers: Enter the UK

Following the announcements of the new SCCs and the EDPB's recommendations, the EC announced the adoption of an adequacy decision for EU-UK data flows. Combined with the UK's decision to apply similar treatment to data flows from the UK to the EU, this appeared to simplify the legal issues around most EU-UK data flows.[1] However, the ICO in August 2021 launched a public consultation on its proposals for the International Data Transfer Agreement ("IDTA") — the UK's versions of the SCCs — and a new UK version of the transfer risk assessment. Like the SCCs, the IDTA will serve as a contract or an addendum to a contract that organizations can use when transferring personal data to jurisdictions not covered by an adequacy decision. In the meanwhile, ICO guidance suggests that companies may continue to use the *old* SCCs for any data transfers from the UK to a jurisdiction that is not subject to an adequacy decision, meaning that in some cases companies that will be sharing data between the EU, UK, and a third jurisdiction may need to have *both* the new SCCs and the old SCCs, and once the ICO's consultation is completed those agreements will need to transition from the old SCCs to the final IDTA.

1 There are some exceptions. For example, transfers for the purposes of immigration control (or data that falls within the UK immigration exemption) are restricted transfers and fall under different rules.

Moving Forward

Given developments over the last year and the likelihood (or lack thereof) of any movement on a successor regime to Privacy Shield, companies will have to further build out their GDPR compliance programs to accommodate ongoing assessment of third-country data protection laws and practices, and will need to stay flexible as they make decisions in the context of a fluid legal landscape. One thing is clear: continued reliance on SCCs will impose significant burdens on companies with respect to both analysis and documentation.

CYBERSECURITY — MORE THAN AN I.T. PROBLEM

2021 was an eventful year across the board, and the cybersecurity world was no exception (and indeed contributed to some of the chaos). Here are some of the highlights from this year and what it means for the year ahead:

- **Log4J and Other Supply Chain Attacks.** The vulnerability in Apache's Log4J software, discovered in early December, capped off a tumultuous year of large-scale supply-chain attacks. We can expect the effects of the Log4J vulnerability will be felt well into 2022 as more exploits of this widespread vulnerability come to light. If businesses were not already taking steps to shore up security in their supply chain, they should be now.
- **Cybersecurity Mandates Presage More Industry-Specific Rules.** The Department of Homeland Security ("DHS"), in particular the Transportation Security Administration, has issued several directives mandating that businesses related to certain critical infrastructure, such as surface transport and pipelines, adopt particular cybersecurity practices. Further, the FTC has published its first draft of updates to the Gramm-Leach-Bliley Act's ("GLBA's") Safeguards Rule, which could bring more prescriptive cybersecurity requirements to the financial services industry. In the absence of legislation, we may expect more regulation to come on an industry-by-industry basis as regulatory agencies step into the gap.
- **Increased Government Outreach and Collaboration.** Government actions in the cyber world are not limited to rules and enforcement actions; 2021 also saw increased outreach and collaboration between the federal government, industry, and the public at large. The Cybersecurity and Infrastructure Security Agency ("CISA"), the National Security Alliance and the National Institute of Standards and Technology ("NIST") have all published numerous resources on their websites to assist organizations. At the state level, the Information Technology Industry Council provided state officials with an action plan to assist in prioritizing cybersecurity investment and modernization. Further, CISA and DHS have reached out to foster partnerships with private-sector companies to share threat knowledge and risk mitigation strategies by forming advisory and leadership councils. Looking ahead to next year, it is likely that cross-collaboration between sectors is a trend that will continue to increase in response to an ever-changing threat landscape.
- **NYDFS Steps Up Enforcement.** The New York Department of Financial Services ("NYDFS") was one of the first authorities to issue comprehensive cybersecurity regulations, and in 2021 NYDFS began to flex its enforcement muscles. Several multimillion dollar fines should put financial services firms on notice that NYDFS is more than prepared to hold companies accountable, and that non-compliance could end up being very expensive.

All signs point to cybersecurity staying on the front pages and at the top of policymakers' and regulators' priority lists in 2022.

The FTC Adopts New Cybersecurity Benchmarks

In October 2021, the FTC updated the Safeguards Rule by creating new enforceable requirements concerning how financial institutions must implement and maintain their information security programs. While the Safeguards Rule only applies directly to those entities over which the FTC has jurisdiction under the GLBA, the FTC seems likely to incorporate these new data security benchmarks into other data protection enforcement and rule-making activities, which may influence judicial interpretations of consumer protection and similar statutes, as well as other regulators who will likely look to the FTC for guidance in their own enforcement efforts. More generally, the amendments reflect a broader trend under the Biden Administration to push companies to improve their cyber hygiene.

The Amended Safeguards Rule

At the time the Safeguards Rule was originally promulgated in 2002, the FTC did not provide comprehensive guidance about what security measures or elements financial entities should implement, leaving each institution free to define the specifics of its own security programs based on the size and complexity of the financial institution, the sensitivity of the personal data under its control, and foreseeable internal and external risks to customer information. With these latest amendments, however, the FTC clearly identifies specific tools, tactics, and measures that it expects as a baseline of reasonable security.

Covered Financial Institutions

The Safeguards Rule governs the cybersecurity practices of certain financial institutions. The FTC amended the scope of the Safeguards Rule by substantively expanding the definition of "financial institution" to include "any institution the business of which is engaging in an activity that is financial in nature or incidental to such financial activities as described in section 4(k) of the Bank Holding Act of 1956, 12 U.S.C. 1843(k)," which now includes the act of "finding." The act of "finding" includes "bringing together one or more buyers and sellers of any product or service for transactions that the parties themselves negotiate and consummate." Under the new definition of "financial institution," mortgage brokers and payday lenders are now subject to the Safeguards Rule.

Although the amended Safeguards Rule expands the scope of the FTC's enforcement jurisdiction to cover additional entities, it also creates a new and important exception for smaller financial institutions that maintain customer information for fewer than 5,000 customers. The FTC recognized that smaller financial institutions may not have the resources to design and implement an extensive data security program. Therefore, smaller financial institutions are not required to comply with every component of the Safeguards Rule, but the FTC did encourage these entities to implement an information security program suited to their size and complexity.

Required Aspects of an Information Security Program

In addition to expanding the scope of covered institutions, the amended Safeguards Rule adds several new elements that covered financial institutions must include in their information security programs. Among other things, covered financial institutions must:

- Base their information security program on a risk assessment that identifies reasonably foreseeable internal and external risks to the security of customer information that could result in unauthorized use or disclosure of the information and assess the sufficiency of any existing safeguards in place to mitigate those risks;
- Implement additional safeguards to mitigate the risks identified through risk assessments, such as multifactor authentication ("MFA"), procedures that monitor and log activity of authorized users, and encryption at rest and in transit;
- Implement policies and procedures to ensure that personnel adequately enact and comply with the information security program;

- Oversee service providers;
- Establish a written incident response plan that is designed to respond promptly to, and recover from, any material security event; and
- Require regular written reports to the board of directors, equivalent governing body, or senior official responsible for the information security program about the overall status of the information security program and material matters related to the information security program.

The FTC acknowledged that financial entities may incur significant costs in implementing additional data security measures to comply with the Safeguards Rule. However, the FTC noted that there are cost-effective options for many of the requirements, and the Safeguards Rule provides flexibility for each financial institution to determine what security measures are appropriate for itself as long as the measures are compliant with the Safeguards Rule.

Key Takeaways

Financial services companies must assess whether they are now subject to the Safeguards Rule via the expanded scope of the amended "financial institutions" definition. Additionally, those financial institutions within the scope of the Safeguards Rule should evaluate whether their existing security controls and practices comply with the amended Safeguards Rule and if not, implement new information security measures as needed. Finally, the increased focus on regulating cybersecurity and privacy appears consistent across various federal agencies under the Biden Administration, so even financial institutions subject to other regulators (such as the SEC) would be well advised to model their programs on the FTC's updated Safeguards Rule.

The SEC Prioritizes Cybersecurity and Data Privacy Enforcement

In recent years, the Securities and Exchange Commission (the "SEC") has increasingly prioritized the implementation of appropriate measures to protect consumer and non-public information. The SEC issued guidance in 2018 regarding public companies' public disclosures related to cybersecurity; last year, the Commission's focus on cybersecurity and privacy crystalized into several enforcement actions. In 2021, the SEC announced three settlements stemming from companies' failures to implement appropriate data security policies and procedures or to adequately disclose the known effects of a data security breach involving personal information. Moving forward, public companies and other companies that fall within the SEC's ambit should carefully analyze both their data security practices and their disclosures about such practices to comply with evolving requirements related to data security and cybersecurity.

Cybersecurity and Data Security Requirements under SEC Regulations

In its 2021 Examination Priorities, the SEC identified a primary focus for registered investment advisers and broker dealers on measures to "safeguard customer accounts and prevent account intrusions, including verifying an investor's identity to prevent unauthorized account access."[1] Additionally, the SEC has emphasized the need to limit

[1] SEC Office of Compliance Inspections and Examination, 2021 Examination Priorities, at p. 24, available at https://www.sec.gov/files/2021-exam-priorities.pdf.

user access to data systems and to utilize procedures that leverage security features like MFA.[2]

The SEC has two primary tools to regulate the cybersecurity and privacy practices of companies. First, Regulation S-P requires every broker-dealer, investment company, and investment advisor registered with the SEC to adopt written policies and procedures "that address administrative, technical and physical safeguards for the protection of customer records and information."[3] These policies must be reasonably designed to (1) insure the security and confidentiality of customer records and information; (2) protect against any anticipated threats or hazards to the security or integrity of customer records and information; and (3) protect against unauthorized access to or use of such records that could result in substantial harm or inconvenience to customers.

Second, the SEC may require public issuers to make certain disclosures under the Securities Act of 1933 and the Exchange Act of 1934, and regulations promulgated thereunder. In 2018 guidance, the SEC said, "Given the frequency, magnitude and cost of cybersecurity incidents, the Commission believes that it is critical that public companies take all required actions to inform investors about material cybersecurity risks and incidents in a timely fashion, including those companies that are subject to material cybersecurity risks but may not yet have been the target of a cyber-attack."[4]

Enforcement for Failure to Implement Proper Security Measures

In August 2021, the SEC announced three enforcement actions — against the Cetera Entities, Cambridge Investment, and KMS Financial Services. Each of these companies had experienced a data security breach involving unauthorized third parties taking over cloud-based email accounts. The SEC determined that the companies had failed to implement MFA and other data security measures that would have detected the unauthorized access and promptly alerted the companies to the intrusion.

As part of the settlements, the SEC censured each company and imposed penalties ranging from $200,000 to $300,000. These enforcement actions show that the SEC expects regulated entities to implement appropriate data security measures to mitigate the risk of data security incidents, and in the event that those incidents occur, promptly remediate the data security breach.

Public Disclosures About Cybersecurity

The SEC released guidance in 2018 regarding cybersecurity issues that "would be helpful for companies to consider" in making public disclosures.[5] Among other things, the SEC recommended that companies disclose: (i) prior cybersecurity incidents, including severity and frequency; (ii) the adequacy of preventative actions taken to reduce cybersecurity incidents; (iii) aspects of the company's business or operations that give rise to material cybersecurity risks, including industry-specific or third-party supplier and service provider risks; (iv) costs associated with maintaining cybersecurity protections, including insurance or payments to service providers; (v) the potential for reputational harm stemming from a cybersecurity incident; (vi) existing or pending laws and regulations that may affect cybersecurity requirements to which the company is subject; and (vii) litigation, regulatory investigation, and remediation costs associated with cybersecurity incidents.

Despite the SEC's guidance, many public companies only superficially reference, or do not include at all, such information in their Form 10-K and Form 10-Q documents or other public disclosures. Until 2021, however, the SEC had not brought enforcement actions related to a public company's failure to disclose this information. Specifically, the SEC brought an enforcement action against Pearson, a publicly traded, London-based multinational educational publishing and services company, after Pearson omitted material facts in its 2019 Form 6-K disclosure about a data

[2] SEC Office of Compliance Inspections and Examinations, Cybersecurity and Resiliency Observation, at p. 3, available at https://www.sec.gov/files/OCIE%20Cybersecurity%20and%20Resiliency%20Observations.pdf.

[3] 17 CFR § 248.30(a).

[4] Securities and Exchange Commission, *Commission Statement and Guidance on Public Company Cybersecurity Disclosures*, 17 C.F.R. Parts 229 and 249 (2018) at 4, available at https://www.sec.gov/rules/interp/2018/33-10459.pdf.

[5] Securities and Exchange Commission, *Commission Statement and Guidance on Public Company Cybersecurity Disclosures*, 17 C.F.R. Parts 229 and 249 (2018) at 13–14, available at https://www.sec.gov/rules/interp/2018/33-10459.pdf.

security breach that occurred in 2018.[6] In its Form 6-K disclosure, Pearson had noted that data security incidents were a hypothetical risk to its business, but failed to disclose that it, in fact, had experienced a breach. For failing to make adequate disclosures in violation of Section 13(a) of the Exchange Act, the SEC imposed a civil penalty of $1,000,000 on Pearson.

[6] *See* Securities and Exchange Commission, *In the Matter of Pearson plc*, Order Instituting Cease-and-Desist Proceedings, Aug. 16, 2021, https://www.sec.gov/litigation/admin/2021/33-10963.pdf.

Key Takeaways

The SEC's focus on cybersecurity practices should give regulated companies reason to assess their data security practices, implement and maintain appropriate data security and cybersecurity measures, and make adequate public disclosures about their cybersecurity practices and risks, including whether they have experienced data security incidents impacting personal data. This is likely to remain an enforcement priority of the agency throughout 2022 and in the coming years.

Financial Services Beware — NYDFS Ramps Up Enforcement of the Cybersecurity Regulation

In 2017, NYDFS promulgated a Cybersecurity Regulation (the "Cybersecurity Regulation") that set forth requirements concerning data security for institutions licensed by the NYDFS, including financial services companies and insurance producers. The Regulation includes many specific substantive and documentary obligations — e.g., covered entities must implement detailed data security measures, such as written policies and procedures that cover 14 areas of cybersecurity and technology, including MFA, data encryption, a written incident response plan, third party service provider requirements, appointment of a Chief Information Security Officer ("CISO") and regular penetration testing and vulnerability assessments. Most importantly, the cybersecurity program and the written policies and procedures must be based on a formal risk assessment, which has been conducted in accordance with written risk assessment policies and procedures, and covered entities must certify compliance with the Cybersecurity Regulation on an annual basis. Even as many companies adopt a number of the required technical cybersecurity practices, many covered entities unknowingly fail to meet the documentary and process requirements and leave themselves open to an enforcement action.

Recent Enforcement Activity

Over the past year, the NYDFS has brought several enforcement actions for non-compliance with the Cybersecurity Regulation. In 2020 and 2021, NYDFS assessed fines in the range of $1,500,000 - $3,000,000 to covered entities for violations of the Cybersecurity Regulation. The impacted companies were cited for, among other things, filing a false certification of compliance to NYDFS, failure to implement MFA (or a reasonable equivalent), and failure to perform a cybersecurity risk assessment. NYDFS enforcement has been made on a per-violation basis, which means that if a violation is found,

then a false certification is considered to be an additional violation on top of that. The calculation of potential fines appears to be made on a per-day basis, so the potential fines may rise very quickly.

In addition to undertaking enforcement actions, the NYDFS has provided FAQs on its website that offer guidance on various requirements under the Cybersecurity Regulation,[1] including recently posted FAQs focused on risk assessments. These FAQs note that "a cyber assessment framework is a useful component of a comprehensive risk assessment,"[2] and recommend that entities use a framework that "best suits their risk and operations." The Department's guidance offers the FFIEC Cyber Assessment Tool, the CRI Profile, and the NIST Cybersecurity Framework as examples.

Additionally, the NYDFS recently emphasized in the FAQs that covered entities must utilize MFA for accessing internal networks — such as email, document hosting, and other cloud-based services — from external networks, unless a covered entity's CISO has approved in writing reasonably equivalent or more secure access controls. NYDFS also clarified that MFA must be used on third-party service provider networks that hold non-public information (as defined under the Cybersecurity Regulation). NYDFS took the step of emphasizing this particular technical control because lack of MFA is a weakness that threat actors typically exploit to gain access to networks.

The Cybersecurity Regulation's limited exemptions are harder to meet and exempt covered entities from fewer of its portions than may be expected. The FAQs explain how the operations, revenues and assets of affiliates must be included in exemption calculations.

Next Steps

It is expected that NYDFS will continue to rigorously enforce the Cybersecurity Regulation in 2022. In light of the aggressive actions of NYDFS, it is recommended that all covered entities, especially those with insurance or insurance producer licenses, carefully review their current compliance policies and procedures, with an eye to closing any gaps.

[1] FAQs: 23 NYCRR Part 500 — Cybersecurity, New York Department of Financial Services, available at https://www.dfs.ny.gov/industry_guidance/cyber_faqs (last visited Jan. 24, 2022).

[2] *Id.*

Biden Administration Cyber Executive Order — Ambitious Goals, Significant Work Remains

On May 12, 2021, President Biden signed a long-awaited Executive Order on Improving the Nation's Cybersecurity (the "Executive Order" or the "Order"). The Order is intended to address the threat to U.S. public- and private-sector entities presented by "persistent and increasingly sophisticated malicious cyber campaigns." Rather than directing federal government agencies to impose any regulatory solutions or proposing any legislative fixes, however, the Executive Order seeks to leverage alternative sources of authority—including the government's purchasing power and its convening power— to incentivize improved cybersecurity hygiene and practices.

While the impact is likely to be felt most directly by companies that do business with the federal government, the Order has potentially broader implications. For example, the Order directs the creation of guidance on software supply-chain security and the creation of a consumer-labeling pilot program regarding the security of Internet of Things ("IoT") devices and consumer software. These efforts could lead to standards that become industry norms or baseline expectations for information and communications technology ("ICT") companies regardless of whether they contract with government entities, or could even be adopted and integrated into the cybersecurity policymaking and enforcement efforts of agencies like the SEC and the FTC.

Leveraging the Government's Purchasing Power

In light of the fact that many significant recent cyber attacks have targeted government systems by infiltrating private-sector software and services, the Executive Order is focused primarily on the government's use of ICT products and services, particularly cloud services, produced by the private sector. In particular, the Order directs:

- Relevant government agencies to establish a number of contractual obligations and requirements in the Federal Acquisition Regulation ("FAR") regarding record keeping, reporting, transparency, and supply-chain security. For example, the Order directs the agencies to recommend changes to ensure that private-sector service providers share data, information, and reporting related to cyber incidents or potential incidents relevant to any agency with which they have contracted, and that the service providers collaborate with federal cybersecurity or investigative agencies in their investigation of and response to incidents or potential incidents involving federal systems.
- Federal agencies to amend their cybersecurity strategies to adopt certain practices, including: accelerating movement to secure cloud services; centralizing and streamlining access to cybersecurity data; and investing in both technology and personnel to match these modernization goals.
- That "the migration to cloud technology shall adopt Zero Trust Architecture, as practicable," and that relevant agencies must work with the Federal Risk and Authorization Management Program to develop security principles governing cloud providers for incorporation into agency modernization efforts.
- That agencies must adopt MFA and encryption for data at rest and in transit, to the maximum extent consistent with federal records laws and other applicable laws.

What's Next?

One of the major challenges presented by these directives is timing. For example, while changes to the FAR can sometimes take years, the Order directs many of these changes to be proposed or released within 60, 90, or 180 days. Further, the agencies tasked with leading these efforts — such as CISA — are already busy with numerous other priorities and may need additional resources to get these directives over the finish line. The Order's directives hinge on a number of key concepts, such as "cyber incident," that need to be defined because of potentially broader implications for policymaking, but it is unclear how the various agencies involved can create such definitions in a cohesive way. Finally, the Order has no clear jurisdictional hook to compel or incentivize participation in efforts beyond changes to the FAR — like the creation of the Cyber Safety Review Board — regardless of what companies may think of the merits of these ideas.

We know that the Administration has been hard at work on implementing the EO. For example, NIST has issued requests for comment on the consumer labeling program it is supposed to have completed with the FTC by February 2022. Likewise, OMB issued a memo in August 2021 on logging practices for federal government agencies, and followed that up with a memo in January 2022 on implementing zero-trust approaches. The clearest takeaway, however, is that a significant amount of work remains to be done in 2022.

Leveraging the Government's Convening Power

The Executive Order also seeks to encourage improved cyber hygiene and posture by leveraging the government's convening power. The Order directs the NIST, CISA and other agencies to establish guidance and standards, and in so doing, seeks to bring interested stakeholders together to ensure that the standards account for their interests. Among other things:

- **Software Supply Chain Security.** The Order directs NIST to adopt guidelines for "enhancing software supply chain security." The guidance should address secure software development environments and mechanisms for demonstrating the security of such environments, including by employing automated tools to perform functions like maintaining trusted source code supply chains and checking for known or potential vulnerabilities (and remediating, as appropriate), and providing a purchaser a "Software Bill of Materials" for each product directly or by publishing it on a public website.
- **Consumer Labeling Pilot Program.** NIST is directed to coordinate with the FTC and other agencies to develop consumer-labeling pilot programs for IoT devices and consumer software. Per the Order, the criteria for the labeling program should "reflect increasingly comprehensive levels of testing and assessment that a product may have undergone." Notably, the Order seems to recognize that industry participation may be an issue: "This review shall focus on ease of use for consumers and a determination of what measures can be taken to maximize manufacturer participation."
- **Cyber Review Board.** Finally, the Order creates a new Cyber Safety Review Board (the "Board") charged with reviewing and assessing significant cyber incidents. The Board would be comprised of both federal government and private-sector representatives. Reports indicate that the Biden Administration views the creation of the Board as an effort to replicate in the cyber world the success that the National Transportation Safety Board has had in investigating major incidents involving automobiles, airplanes, and other forms of transportation.

DESCRIPTION OF OUR PRACTICE

In the 21st century, information — whether it is data about your customers, your business, or your people — is an indispensable asset, and the ability to use and protect that information is mission-critical. Navigating an increasingly complex web of state, federal and international laws — whether responding to a security incident, building a privacy or security program, or integrating privacy by design into innovative new products and services — is an essential component of that effort. For over 20 years, Willkie attorneys have counseled a wide range of U.S. and multinational clients on privacy and cybersecurity issues and leveraged their broad base of knowledge and experience, including as regulators and senior in-house attorneys, to help clients minimize their legal risks and achieve their business goals.

Our multidisciplinary practice includes attorneys with in-depth experience in all aspects of cybersecurity and privacy law and in complementary practices, such as Internet, technology and communications, securities regulation and enforcement, intellectual property, mergers and acquisitions, complex litigation, antitrust and competition, insurance, and consumer protection. Our close collaboration across offices and legal disciplines enables us to provide clients with comprehensive, practical advice for their data-related issues and opportunities.

We provide practical guidance to companies, and counsel clients on all aspects of privacy and cybersecurity risk, including:

- Designing and implementing global compliance programs
- Global incident response, planning, reporting, and remediation
- Regulatory proceedings (including before the FTC, SEC, FCC, and DOJ, as well as non-U.S. regulators)
- Litigation related to privacy and security practices and data security incidents
- Legislative and Regulatory Policy Advice and Advocacy
- Privacy and security risk and impact assessments
- Product development, digital innovation and transformation
- Crisis management
- Transaction diligence and analysis
- Drafting privacy and security policies
- Drafting and negotiating vendor contracts
- Corporate governance and SEC issues

Our attorneys have substantive experience advising clients on numerous privacy and cybersecurity laws and regulations in the U.S. and around the world, including:

- EU/UK Privacy (GDPR, ePrivacy Directive, Data Protection Act 2018)
- U.S. State Privacy and Cybersecurity (e.g., CCPA and CPRA, BIPA, Virginia, Colorado, NY SHIELD Act)
- U.S. Federal and State Financial Privacy and Cybersecurity (e.g., GLBA, Reg SCI, NY DFS Cybersecurity Regulation, Safeguards Rule, FCRA/FACTA)
- U.S. Federal and State Marketing (e.g., CAN-SPAM, TCPA)
- U.S. Federal and State Healthcare Privacy and Cybersecurity (e.g., HIPAA/HI-TECH, CURE Act)
- U.S. Children's Privacy (e.g., COPPA, FERPA)
- U.S. Communications and Media Privacy (e.g., Cable Act, VPPA, Communications Act)
- U.S. Government Access to Information (e.g., ECPA, SCA, CLOUD Act, FISA)
- U.S. General consumer protection (e.g., FTC Act)

SELECTED EXPERIENCE FROM 2021

Some examples of the matters in which Willkie's Cybersecurity and Privacy attorneys have represented and advised clients include:

- We advised Kaseya on its response — including briefings with senior law enforcement and national security stakeholders and coordinating appropriate notifications to customers and regulators around the world — in the wake of one of the largest and most highly publicized ransomware attacks in history.
- We advised a client in negotiating a Consent Order with the New York Department of Financial Services (NY DFS) arising from an investigation into alleged violations of the NY DFS Cybersecurity Regulation.
- We have represented numerous clients before the FTC and SEC including in rulemakings, enforcement proceedings, and other investigations.
- We have advised major tech, media, social media, and financial service companies on critical compliance issues arising from statutory and regulatory obligations, particularly those arising from new legal regimes such as GDPR and CCPA, as well as compliance issues arising from enforcement activities and consent decrees.
- We regularly advise clients on efforts by Congress and state legislatures to enact privacy and cybersecurity legislation, including by analyzing legislation under consideration and developing advocacy strategies.
- We have advised multiple clients in the context of enforcement proceedings before EU data protection regulators – including in Germany, Austria, and Italy – related to compliance with GDPR and member state privacy laws.
- We have represented major technology companies and others in litigation arising from alleged non-compliance with state and federal laws, including CCPA, BIPA, and TCPA.
- We have advised and represented clients on numerous M&A matters and other transactions, including major investments in companies leading innovation in big data, artificial intelligence (AI), automated vehicles, healthtech, insuretech, and fintech.
- We have advised major publicly traded companies and financial institutions on SEC policy-making, rulemakings, investigations, and enforcement activities, related to cybersecurity and privacy activities.
- We advised a major international energy conglomerate on compliance with the Transportation Security Agency Pipeline Cybersecurity Directive.
- We advised a major financial services client on the development of a multinational HR performance program and the appropriate use of data collected as part of the program.
- We have advised major consumer electronics companies, media companies, and financial companies on cybersecurity and privacy training for their employees.

WHO WE ARE

Daniel K. Alvarez
Partner
Co-Chair, Cybersecurity and Privacy Practice Group
+1 202 303 1125
dalvarez@willkie.com

Laura E. Jehl
Partner
Co-Chair, Cybersecurity and Privacy Practice Group
+1 202 303 1056
ljehl@willkie.com

Elizabeth Bower
Partner
Litigation
+1 202 303 1252
ebower@willkie.com

Justin L. Browder
Partner
Asset Management
+1 202 303 1264
jbrowder@willkie.com

James R. Burns
Partner
Asset Management
+1 202 303 1241
jburns@willkie.com

Michael J. Gottlieb
Partner
Litigation
+1 202 303 1442
mgottlieb@willkie.com

Elizabeth P. Gray
Partner
Litigation
+1 202 303 1207
egray@willkie.com

Sameer Advani
Partner
Litigation
+1 212 728 8587
sadvani@willkie.com

Eugene L. Chang
Partner
Intellectual Property
+1 212 728 8988
echang@willkie.com

Jeffrey B. Clancy
Partner
Corporate & Financial Services
+1 212 728 8603
jclancy@willkie.com

Amelia A. Cottrell
Partner
Litigation
+1 212 728 8281
acottrell@willkie.com

Matthew S. Makover
Partner
Intellectual Property
+1 212 728 8739
mmakover@willkie.com

Wesley R. Powell
Partner
Litigation
+1 212 728 8264
wpowell@willkie.com

Heather M. Schneider
Partner
Intellectual Property
+1 212 728 8685
hschneider@willkie.com

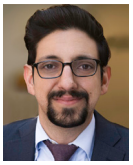
Spencer F. Simon
Partner
Intellectual Property
+1 212 728 8525
ssimon@willkie.com

Simona Agnolucci
Partner
Litigation
+1 415 858 7447
sagnolucci@willkie.com

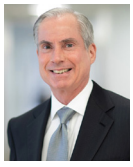
Alexander L. Cheney
Partner
Litigation
+1 415 858 7418
acheney@willkie.com

Benedict Y. Hur
Partner
Litigation
+1 415 858 7401
bhur@willkie.com

Jonathan A. Patchen
Partner
Litigation
+1 415 858 7594
jpatchen@willkie.com



Eduardo Santacana
Partner
Litigation
+1 415 858 7421
esantacana@willkie.com



Matthew D. Berger
Partner
Corporate & Financial Services
+1 650 887 9388
mberger@willkie.com

Tiffany Lee
Partner
Corporate & Financial Services
+1 650 887 9398
tlee@willkie.com

Amanda S. Amert
Partner
Litigation
+1 312 728 9010
aamert@willkie.com

Michael G. Babbitt
Partner
Intellectual Property
+1 312 728 9070
mbabbitt@willkie.com

Craig C. Martin
Partner
Litigation
+1 312 728 9050
cmartin@willkie.com

Michelle Clark
Partner
Antitrust & Competition
+44 203 580 4737
mcclark@willkie.com

Henrietta de Salis
Partner
Asset Management
+44 20 3580 4710
hdesalis@willkie.com

Simon Osborn-King
Partner
Litigation and Compliance
+44 20 3580 4712
sosborn-king@willkie.com

Dominique Mondoloni
Partner
Litigation
+33 1 53 43 45 68
dmondoloni@willkie.com

Richard M. Borden
Counsel
Corporate & Financial Services
+1 212 728 3872
rborden@willkie.com

Stefan Ducich
Associate
Cybersecurity and Privacy
+1 202 303 1168
sducich@willkie.com

Marilena Hyeraci
Associate
Cybersecurity and Privacy
+39 02 76363 1
mhyeraci@delfinowillkie.com

Nicholas Chanin
Associate
Cybersecurity and Privacy
+1 202 303 1164
nchanin@willkie.com

Michelle Bae
Associate
Cybersecurity and Privacy
+1 202 303 1166
ebae@willkie.com

Kari Prochaska
Associate
Cybersecurity and Privacy
+1 312 728 9080
kprochaska@willkie.com

Amelia Putnam
Associate
Cybersecurity and Privacy
+1 202 303 1089
aputnam@willkie.com

Amal Ibraymi
Associate
Cybersecurity and Privacy
+1 212 728 3524
aibraymi@willkie.com