WINSTON & STRAWN LLP

YEAR IN REVIEW

Top 10 Privacy Impacts of 2021

FEBRUARY 2022

IN THIS ISSUE

Top 10 Privacy Impacts of 2021

In this "Year in Review," Winston's Global Privacy Team highlights 10 significant privacy developments in 2021, followed by privacy developments to watch in 2022.

1
CALIFORNIA PRIVACY LAW UPDATES – CPRA AND CCPA

California The California Privacy Rights Act ("CPRA"), which amends and expands the California Consumer Privacy Act ("CCPA"), goes into effect on January 1, 2023. But importantly, once the CPRA goes into effect, consumers will have the right to access the information a business has collected about them dating back to January 1, 2022. This has companies working to come into compliance now to meet the retroactive look back.

On March 15, 2021, further revisions to the California Attorney General's CCPA regulations were approved by the California Office of Administrative Law, which, among other things, approved the use of an opt-out icon in addition to, but not in lieu of, a "Do Not Sell My Personal Information" link and prohibit businesses from using "dark patterns" to prevent consumers from exercising their rights under the law. A dark pattern is a tactic used in user interfaces to subtly trick users into taking a certain action or that prevents consumers from executing a desired action.

CCPA case law continues to develop. Over the past year the courts decided that the scope of discovery in litigation is not limited by the CCPA and that failing to plead that a breach of personal information occurred after January 1, 2020 was fatal to a CCPA complaint because the CCPA is not retroactive.

"… once the CPRA goes into effect, consumers will have the right to access the information a business has collected about them dating back to January 1, 2022."

The newly-created California Privacy Protection Agency ("CPPA") became active by the end of 2021, soliciting preliminary comments from the public on new or ambiguous issues under the CCPA regulations, including issues related to: (i) what constitutes a "significant risk" to consumers' privacy or security; (ii) opt out rights with respect to businesses' use of automated decision-making technology; (iii) the CPPA's audit authority; (iv) opt-out preference signals; (v) consumers' right to limit the use and disclosure of sensitive personal information; (vi) information to be provided in response to a consumer's request to know; and (vii) the definitions of various terms under the CPRA.

2
VIRGINIA AND COLORADO NEW PRIVACY LAWS

In 2021, Virginia and Colorado enacted new comprehensive state privacy laws. This illustrates

© 2022 Winston & Strawn LLP

the continued appetite for consumer privacy protections in the United States. These laws are significant developments for both Virginia and Colorado consumers, as well as companies conducting business in each state.

The Virginia Consumer Data Protection Act ("CDPA") becomes effective on January 1, 2023, and provides similar rights to those the CCPA affords to California residents. Notably, the CDPA also gives Virginia consumers the right to opt out of the processing of their personal data for targeted advertising, sales, or profiling in furtherance of decisions with legally significant effects concerning the consumer. However, unlike the CCPA, a "sale" under the CDPA is limited to exchanges of personal data for *monetary* consideration, and the CDPA does not contain a set revenue threshold. The CDPA also imposes several new obligations on data controllers including limiting the collection of personal data to only what is adequate, relevant, and reasonably necessary for the purpose of the processing. Data controllers are prohibited from processing "sensitive data" without consent from the consumer, and data controllers must implement "reasonable administrative, technical, and physical data security practices to protect the confidentiality, integrity, and accessibility of personal data." Data processors must conduct and document a data protection assessment for certain processing activities, including personal data for targeted advertising, the sale of personal data, and the processing of sensitive data. The Virginia CDPA does not contain a private right of action.

The Colorado Privacy Act ("CPA"), goes into effect on July 1, 2023. It is like the Virginia CDPA and the CCPA in that it affords many new privacy rights to Colorado residents. Like the CCPA, the CPA includes certain thresholds that businesses must meet for the law to apply. A business will be subject to the CPA if it produces products or services targeted to Colorado residents and (i) controls or processes personal data of more than 100,000 consumers per year, or (ii) sells personal data of at least 25,000 consumers. Notably, the CPA does not create a private right of action for Colorado residents.

3
TELEPHONE CONSUMER PROTECTION ACT DEVELOPMENTS

The Telephone Consumer Protection Act ("TCPA") remained a popular statute for the plaintiffs' bar in 2021, with nearly 2,000 lawsuits filed across the country. Filings briefly declined after the Supreme Court's keystone decision in *Facebook v. Duguid,* which adopted a narrow, defense-friendly interpretation of the statutory term "automatic telephone dialing system." But the plaintiffs' bar quickly rebounded, asking lower courts to carve out exceptions to *Facebook* to keep the statute viable. Plaintiffs also began suing under "mini-TCPA" statutes in states like Florida and Virginia, which were unaffected by *Facebook*.

Meanwhile, in November 2021, the Federal Communications Commission launched a significant new tool for TCPA compliance: the Reassigned Numbers Database. Companies can use the database to check whether a phone number has been reassigned to a new subscriber, which may help prevent "wrong number" calls or text messages—a frequent cause of TCPA class action lawsuits.

> "Plaintiffs also began suing under "mini-TCPA" statutes in states like Florida and Virginia."

4

ILLINOIS BIOMETRIC INFORMATION PRIVACY ACT DEVELOPMENTS

The litigation landscape for defendants accused of violating the Illinois Biometric Information Privacy Act ("BIPA") became even more grim over the course of 2021 because of several plaintiff-friendly decisions.

The Seventh Circuit continued a trend of making it difficult for defendants to remove BIPA cases to federal court. In *Thornley v. Clearview AI, Inc.,* the court sanctioned the plaintiff's class definition expressly limited to class members who "suffered no injury" because of the defendant's violation of section 15(c) of BIPA, finding that the suit could not proceed in federal court because of a lack of Article III standing. Because BIPA authorizes awards of statutory damages for technical violations of the statute irrespective of whether the violation caused any actual injury, *Thornley* gives plaintiffs set on remaining in state court a roadmap on how to do so.

Courts also issued plaintiff-friendly rulings on the issue of when a claim under BIPA's Sections 15(b) and 15(d) accrues. In *Watson v. Legacy Healthcare Financial Services, LLC,* the Illinois Appellate Court, First District, held that a Section 15(b) accrues, for statute of limitations purposes, with every collection of the plaintiff's information. In other words, in a case based on defendant's use of a biometric time clock to track employees' hours, each scan violates the statute. That holding extends a plaintiff's time to file suit, as the statute of limitations begins to run anew with each collection of the biometric information. Additionally, if *Watson*'s holding that each collection constitutes a violation is extended to damages, liability for BIPA violations could result in significant damages with even small classes.

"The Seventh Circuit continued a trend of making it difficult for defendants to remove BIPA cases to federal court."

The Seventh Circuit, in *Cothron v. White Castle Systems, Inc.,* considered the same issue but opted to certify the question to the Illinois Supreme Court instead of deciding the issue. Both courts distinguished the accrual issue from whether defendants owe damages for each violation, but the Seventh Circuit's opinion hinted that deciding the accrual issue may well determine how damages are calculated since both are based on the same statutory provision, 740 ILCS 14/20. Defendants will need to await a decision by the Illinois Supreme Court in 2022 to see if it either rejects *Watson* or articulates a basis to distinguish between accrual for statute of limitations purposes and damages.

5

COMPUTER FRAUD AND ABUSE ACT NARROWED

The Supreme Court's recent decision in *Van Buren v. United States* significantly narrowed the scope of liability under the Computer Fraud and Abuse Act ("CFAA"). The CFAA subjects anyone who "intentionally accesses a computer without authorization or exceeds authorized access" to criminal and civil liability. Until recently, courts have been divided as to whether the phrase "exceeds authorized access" includes the misuse of information that one otherwise has authority to access.

© 2022 Winston & Strawn LLP

In *Van Buren*, for example, a police officer accessed a police database he had authority to access for the illegitimate purpose of unmasking an undercover officer in exchange for a five-thousand-dollar payment. The officer, appealing his conviction under the CFAA, argued that the CFAA did not extend to those who misused information that they had authority to access. The Supreme Court agreed, holding that the term "exceeds authorized access" only "covers those who obtain information from particular areas in the computer—such as files, folders, or databases—to which their computer access does not extend. It does not cover those who, like Van Buren, have improper motives for obtaining information that is otherwise available."

By narrowing the CFAA's reach in the criminal context, *Van Buren* likely also limits the ability of employers to rely on CFAA's civil enforcement provisions to protect against the misuse of company information. While employers may still bring civil CFAA claims against employees who access parts of a computer without authorization, *Van Buren* likely severely limits the ability of employers to seek damages under the CFAA for the misuse of company information within the scope of the employee's authority to access.

6
NIST AND INTERNET OF THINGS REGULATION

In December 2021, the National Institute of Standards and Technology ("NIST") issued guidelines under the Internet of Things ("IoT") Cybersecurity Improvement Act of 2020 that outlined cybersecurity requirements for federally owned or operated IoT devices. The guidelines provide a framework to assist federal organizations in identifying (i) the specific use case for a potential IoT device; (ii) how the device will interact with an organization's information system; (iii) whether the practices and ongoing support of the device manufacturer or the device itself will create cybersecurity vulnerabilities; and (iv) how the introduction of a new IoT device may impact an organization's risk assessment of its information systems.

Once federal organizations have identified any potential cybersecurity risks associated with the introduction of an IoT device, the guidelines provide steps organizations can take to identify the cybersecurity requirements for the device. While the NIST acknowledges that identifying such requirements "may be challenging for some use cases," it has published a supplemental catalogue of device requirements to assist organizations in this process. The guidelines also offer steps organizations can take when an IoT device does not support all the cybersecurity requirements necessary for its incorporation into the organization's information system.

Although these guidelines only apply to federally owned or operated devices, they could influence the evolution of "appropriate" cybersecurity requirements for IoT devices in states that have enacted similar legislation.*

7
CYBERSECURITY AND LOG4J APACHE VULNERABILITY

In 2021, there continued to be a rise in ransomware attacks with far-reaching effects across multiple industries. As evidenced by Colonial Pipeline and SolarWinds, ransomware continues to disrupt industries and cripple critical infrastructure.

---

* The NIST guidelines and supplemental catalogue are available here: https://www.nist.gov/itl/applied-cybersecurity/nist-cybersecurity-iot-program/timeline.

© 2022 Winston & Strawn LLP

> “The Log4j Apache vulnerability has highlighted the potential security threats posed by the use of open-source software within businesses.”

Notably, the end of 2021 also saw the discovery of the Log4j Apache vulnerability. The Log4j Apache vulnerability, which was identified in an open-source logging utility tool commonly used in many consumer- and enterprise-facing products and services, is being actively and widely exploited by cyber threat actors. The Log4j Apache vulnerability has highlighted the potential security threats posed by the use of open-source software within businesses. The Federal Trade Commission (“FTC”) has issued a response to the Log4j vulnerability that makes clear that companies have an obligation to take reasonable steps to remediate known security vulnerabilities within their businesses, including the use of the Log4j utility.

The FTC specifically warned that failure to take reasonable steps to mitigate a known software vulnerability implicates laws including the Federal Trade Commission Act. The FTC warned that “it intends to use its full legal authority to pursue companies that fail to take reasonable steps to protect consumer data from exposure as a result of Log4j, or similar known vulnerabilities in the future.” Companies should ensure that they are protecting any personal information by implementing appropriate physical, technical, and administrative safeguards, and by also identifying and promptly remediating known vulnerabilities that could affect their business.

8

U.S. TREASURY GUIDANCE ON RANSOMWARE

After a flurry of ransomware activity in 2021, the U.S. Treasury Department’s Office of Foreign Assets Control (“OFAC”) warned of its intent to ramp up civil enforcement of laws prohibiting ransomware payments made to entities on the U.S. Sanctions List. Companies may make ransomware payments through anonymized payments systems like bitcoin without any knowledge of the recipient’s identity. While OFAC has traditionally refrained from enforcement in such circumstances, the new guidance suggests that OFAC may impose strict liability for these transactions, even where the target of the attack does not know the recipient’s identity. To determine the severity of any enforcement action, OFAC will consider the following factors:

- The extent to which a target of a ransomware attack took “meaningful” cybersecurity steps to reduce the risk of extortion by a sanctioned actor;
- The extent of the target’s cooperation with law enforcement; and
- The adequacy of a target’s Sanctions Compliance Program (“SCP”).

Because OFAC guidelines have explicitly identified the lack of an SCP as an “aggravating factor” when determining its response to a prohibited transaction, companies should promptly review their existing SCPs and consult with counsel to ensure adherence to OFAC recommendations. Those at risk of a ransomware attack should (i) ensure senior management make a commitment to OFAC compliance; (ii) conduct regular risk assessments; (iii) establish policies and procedures to identify, interdict, escalate, report, and record potentially prohibited activities; and (iv) train all appropriate personnel in OFAC compliance protocols.

© 2022 Winston & Strawn LLP

9

CROSS-BORDER DATA TRANSFERS AND STANDARD CONTRACTUAL CLAUSES

On June 7, 2021, the European Commission adopted updated standard contractual clauses ("SCCS") for the transfer of personal data from the European Economic Area ("EEA") to "third countries." The updated SCCs are designed to comply with the GDPR's restrictions related to cross-border data transfers while considering how those requirements have been interpreted by the EU Court of Justice, most notably in the 2020 *Schrems II* decision.

Among the changes contained in the new SCCs are the incorporation of Article 28 processing clauses. From a practical perspective, by tying the SCCs to Article 28, the new SCC modules that relate to controller-to-processor and processor-to-processor transfers can serve as a data processing agreement as well without the need for a separate agreement.

While *Schrems II* called the sufficiency of SCCs into question, the decision stopped short of invalidating the use of SCCs to legitimize the transfer of data out of the EEA. The Commission significantly updated and strengthened the old SCCs to address these concerns. The Commission's decision confirmed that companies may continue to rely on SCCs that were already in place prior to September 27, 2021, until December 27, 2022. At that time, all contracts must be upgraded to the new SCCs. In addition, any agreements entered after September 27, 2021 are not subject to the grandfathering period and must use the new SCCs.

10

CHINA'S NEW PERSONAL INFORMATION PROTECTION LAW

On August 20, 2021, the National People's Congress Standing Committee passed the Personal Information Protection Law ("PIPL"), to establish a personal information protection system with Chinese features that is in line with international standards. The law went into effect on November 1, 2021.

> "The PIPL retains unique Chinese features, reflecting the government's regulatory approach toward personal information."

The PIPL is similar to the GDPR. Both laws enjoy extraterritorial reach, provide various rights for personal information subjects, impose high administrative fines for infringements, and set joint liability upon the entities that jointly conduct data processing activities. However, the PIPL retains unique Chinese features, reflecting the government's regulatory approach toward personal information, including protecting the rights and interests of personal information subjects, as well as safeguarding national security and public interests.

© 2022 Winston & Strawn LLP

The PIPL contains provisions relating to national security, including PIPL Article 41, which prohibits personal information handlers from providing any personal information stored within the PRC to any foreign judicial or law enforcement agencies without approval of the authorities. PIPL Articles 42-43 further provide regulations for extraterritorial and reciprocal protection systems, specifying that the government may put the foreign entities on a list limiting or prohibiting personal information provision if they engage in any personal information handling activity harming the national security or public interests of the PRC, and adopt retaliatory measures against any country or region adopting discriminatory prohibitions, limitations, or other similar measures against the PRC in the area of personal information protection.

The PIPL enforcement provisions include business fines up to RMB 50 million or 5% of a company's turnover in the previous year. The authorities may also order the suspension of related business activities. Notably, the directly responsible person in charge and other directly responsible personnel are fined up to RMB 1 million and may also be prohibited from holding the positions of director, supervisor, high-level manager, or personal information protection officer for a certain period. In addition to the administrative liabilities mentioned above, the PIPL provides civil and potential criminal liabilities. Civil liabilities include penalties for damages and losses to the individual.

WHAT TO WATCH IN 2022:

The Winston Global Privacy Team is monitoring privacy developments on the horizon in 2022, including:

- Increased enforcement of privacy by the FTC and other Federal agencies.
- Regulatory guidance on existing state privacy laws, including the CPRA, CDPA, and CPA.
- New state privacy statutes, including, most notably, in New York and Washington.
- The transition away from the use of third-party cookies in online advertising.
- The expanded use, and subsequently increased regulation, of artificial intelligence.
- Movement on SCCs by the UK.

The privacy landscape continues to shift quickly at state, federal, and international levels. Winston's Privacy Team is monitoring these developments to provide practical guidance to mitigate risk.

© 2022 Winston & Strawn LLP

WINSTON GLOBAL PRIVACY TEAM AUTHORS

SHERYL FALK
PARTNER
Houston
+1 (713) 651-2615
sfalk@winston.com

ERIC SHINABARGER
ASSOCIATE
Chicago
+1 (312) 558-8823
eshinabarger@winston.com

KEVIN SIMPSON
ASSOCIATE
Los Angeles
+1 (213) 615-1778
kpsimpson@winston.com

PAT O'MEARA
ASSOCIATE
Chicago
+1 (312) 558-7063
pomeara@winston.com

CHRISTIAN GRAY
ASSOCIATE
Chicago
+1 (312) 558-7876
cgray@winston.com

About Winston & Strawn

Winston & Strawn LLP is an international law firm with 900+ attorneys across 15 offices in Brussels, Charlotte, Chicago, Dallas, Hong Kong, Houston, London, Los Angeles, Moscow, New York, Paris, San Francisco, Shanghai, Silicon Valley, and Washington, D.C. Additionally, the firm has significant resources devoted to clients and matters in Africa, the Middle East, and Latin America. The exceptional depth and geographic reach of our resources enable Winston & Strawn to manage virtually every type of business-related legal issue. We serve the needs of enterprises of all types and sizes, in both the private and the public sector. We understand that clients are looking for value beyond just legal talent. With this in mind, we work hard to understand the level of involvement our clients want from us. We take time to learn about our clients' organizations and their business objectives. And, we place significant emphasis on technology and teamwork in an effort to respond quickly and effectively to our clients' needs.

Visit **winston.com** if you would like more information about our legal services, our experience, or the industries we serve.

Attorney advertising materials. Winston & Strawn is a global law firm operating through various separate and distinct legal entities.