WINSTON & STRAWN LLP

YEAR IN REVIEW

Top 10 Privacy Impacts of 2020

FEBRUARY 2021

IN THIS ISSUE

Top 10 Privacy Impacts of 2020

Amid the global pandemic, 2020 witnessed the debut of new privacy laws and an explosion of privacy and data security issues arising from the switch to remote work and use of communications technologies to support that work. On January 28, 2021, Winston's Global Privacy Practice hosted a webinar to discuss ten significant privacy developments in 2020, which are highlighted below.

1. CALIFORNIA PRIVACY RIGHTS ACT (CPRA)

California continues to lead the way on privacy regulation. On November 3, 2020, California voters approved Proposition 24, creating the California Privacy Rights Act ("CPRA"). The CPRA, which builds on the state's existing California Consumer Privacy Act ("CCPA"), will go into effect on January 1, 2023.

The CPRA builds on the CCPA by introducing new consumer privacy rights and expanding existing rights. Notably, the CPRA created the new category of "sensitive personal information," which includes 20 new data elements, including government identifiers, geolocation, race, genetic data, biometric or health information, and sex life or sexual orientation. The CPRA provides consumers new rights, including disclosure obligations when data is collected, limitations on data use to purposes that "are necessary to perform the services or provide the goods reasonably expected," and a limit on the time that companies can retain the data. The CPRA includes a new consumer right to opt-out of the "sharing" of personal information for cross-context behavioral advertising, and the right for minors to opt-in to the sharing of their personal information for behavioral advertising purposes. The CPRA includes a new right to correct inaccurate information held about a consumer by businesses and the right to opt-5out of automated decision making. In addition to these newly created rights, the CPRA expands several existing CCPA rights, including the right to know and the right to data portability. The CPRA also imposes several affirmative data security requirements on businesses, including mandating the implementation of "reasonable security procedures and practices" for applicable personal information.

> "The CPRA created the California Privacy Protection Agency ("CalPPA"), which is responsible for implementing and enforcing privacy protections."

The new law expands enforcement and liability for failure to comply. The CPRA created the California Privacy Protection Agency ("CalPPA"), which is responsible for implementing and enforcing

privacy protections. The CPRA final regulations are required to be adopted by July 1, 2022. In addition to heightened regulatory activity, the CPRA increases the risk of litigation. The CPRA expands the private right of action by including consumer login credentials to the list of data types that may be actionable if breached and impacts the previous ability to cure data breaches.

Compliance with the EU's General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA) are not sufficient to meet the new CPRA requirements. Moving forward, covered businesses should carefully review their existing California privacy compliance programs and incorporate new practices and processes to address the new and expanded obligations under the CPRA. In addition, companies should closely monitor any subsequent changes to the CPRA, which permits the Attorney General, and subsequently the newly created CalPPA, to issue additional regulations that may materially affect businesses' compliance obligations.

> "...the California legislature continues to make changes to the CCPA."

2. CALIFORNIA CONSUMER PRIVACY ACT– "FINALIZATION" AND ENFORCEMENT

After much fanfare, the CCPA went into effect on January 1, 2020. However, the law was not officially enforced by Office of the Attorney General ("OAG") until July 1, 2020, and the OAG was further delayed in finalizing the CCPA's implementing regulations until August 2020. The OAG released a fourth set of proposed regulations on December 10, 2020, but even with the "final" regulations in place, CCPA compliance continues to be a moving target. These draft revisions to the regulations would, if they are approved as written, clarify that businesses selling personal information must provide consumers with a notice of the right of the sale of personal information even where the business is interacting with the consumer offline. In addition, the fourth set of regulations brings back the requirement that businesses place a "button" on their website that links to a mechanism allowing individuals to submit opt-out requests.

In addition, the California legislature continues to tinker with the CCPA. In September 2020, the governor signed two amendments to the CCPA that, respectively, adjusts the law's exemption of certain types of medical and health information, and extends the CCPA's exemption regarding employment and business-to-business information until January 1, 2022. Regarding the medical information exemption, the amendment is intended to align with Health Information Portability and Accountability Act (HIPAA)'s treatment of de-identified protected health information and to avoid a gap in requirements between the two laws. With the amendment, the CCPA no longer applies to information that is 1) derived from protected health information and 2) is de-identified according to HIPAA's standards for de-identified information.

While the CCPA has been in effect for over a year, and enforced for over six months, the OAG has not publicly disclosed any enforcement actions. Given the notice-and-cure provisions in the CCPA's enforcement provisions, it is likely that the OAG will work with companies to identify and remediate non-compliance before issuing any major penalties. However, the OAG is expected to begin issuing public enforcement actions, which may be useful both in showing the OAG's enforcement priorities and helping provide guidance on the law, such as whether the OAG views the use of online behavioral advertising trackers as a "sale" of personal information under the law.

3. CCPA CLASS ACTION LITIGATION

It did not take long for the plaintiff's bar to take advantage of the CCPA's much-publicized private right of action after the law took effect in January 2020. Within weeks, several class actions were filed against companies that allegedly suffered a breach of personal information. This resulted in several relatively quick individual settlements; however, a rather high-profile class-wide settlement with children's clothing retailer Hannah Andersson would follow. The Hannah Andersson breach was typical of early breach litigation under the CCPA, with the plaintiff attempting to retroactively apply the CCPA to a breach that occurred before the CCPA's effective date. Before the Northern District of California, the parties reached a settlement of $400,000, as well as mandatory remedial privacy and security improvements. There is reason to suspect that the settlement (which equated to approximately $2 per class member) may have come at a discount, given the retroactive issue.

In a another closely watched suit relating to a March 2020 data breach allegedly affecting several million Marriott guests, a California District Court dismissed the suit for lack of standing. The underlying breach affected individuals' names, contact information, genders, birth dates, and loyalty account numbers. However, the breach did not affect any of the categories of personal information requiring data-breach notification under California law. The court cited Ninth Circuit precedent for data-breach litigation wherein plaintiffs are required to demonstrate that a breach involved data of a certain level of sensitivity to assert a cognizable injury. Numerous CCPA data-breach class actions remain pending, and additional settlements and decisions are expected in the near-term.

In addition, several early CCPA class action disputes highlight the plaintiff's bar probing the contours of the law's private right of action. Plaintiffs are seeking to apply the CCPA to non-California residents, even though the CCPA's private right of action limits itself to "consumers" whose data was breached and defines "consumer" to mean a California resident. In addition, plaintiffs are attempting to broaden the private right of action by arguing that a failure to comply with the CCPA's technical disclosure and consumer rights requirements constitutes a failure of state unfair-competition and/or consumer-protection laws. Several complaints have been consolidated into large multidistrict litigation matters, such as a class action currently being defended by TikTok. With the CPRA further expanding private right of action, we expect this litigation to continue to expand.

> "In addition, several early CCPA class action disputes highlight the plaintiff's bar probing the contours of the law's private right of action."

4. GDPR DEVELOPMENTS AND SCHREMS II

The second full year of the GDPR saw increases in the overall number of fines issued, a renewed focus on protecting consumers and consumer data, a much-anticipated decision from the European Court of Justice invalidating the Privacy Shield, and the publishing of updated draft Standard Contractual clauses ("SCCs") by the European Commission.

EU countries imposed over 220 fines in 2020, led by Spain (128 fines), Italy (34 fines), Romania (26), Sweden (15), Belgium (13), and Norway (11). Notably, these fines related to collecting and maintaining personal data—including medical diagnoses and records of time off—of employees in violation of the GDPR, making promotional calls without consent even after the data subject had registered

with the public "Do Not Call" registry, and excessive data retention and inappropriate handling of data breaches.

In the latest chapter of Austrian privacy activist Max Schrems' challenge to data transfers to the United States, on July 16, 2020, the European Court of Justice issued a decision finding that the U.S.-EU Privacy Shield did not offer adequate protection against intrusions by the U.S. government under its surveillance powers. The court invalidated the entire regime, which required companies to find alternative means of transferring data to the U.S. In the Schrems II decision, the European Court of Justice reaffirmed the validity of the existing SCCs as a means of transferring data outside the EU, but noted that data controllers may need to review such transfers while considering all the circumstances to see whether any supplemental measures are required to provide the appropriate level of protection.

On November 12, 2020, the European Commission issued a draft set of revised and updated SCCs while seeking to address deficiencies in the SCCs that were last updated in 2010. The draft SCCs include a requirement that the data importer must state that it has no reason to believe that the laws of the transferee country (including those concerning government access to personal data) prevent the data importer from fulfilling its obligation to protect personal data. Data importers will be expected to conduct Transfer Impact Assessments and to keep adequate records of those assessments. The draft SCCs include many of the same terms that data controllers and data importers now include in separate Article 28 agreements.

5. BIOMETRIC INFORMATION PRIVACY ACT CASE LAW DEVELOPMENTS

The Seventh Circuit issued two major decisions in 2020 that analyzed what kinds of Biometric Information Privacy Act Case Law (BIPA) claims belong in federal court. The first was *Bryant v. Compass Group USA, Inc.,* which held that violation of an individual's right to informed consent under Section 15(b) of BIPA creates injury-in-fact and thus federal jurisdiction over the claim. Bryant held that the lack of a publicly available retention policy required by Section 15(a) of BIPA does not harm the plaintiff as an individual—it only violates a right owed to the public in general—so a plaintiff suffers no injury-in-fact from its mere violation, and federal jurisdiction is lacking over such claims.

> "The year also brought about the demise of a frequently made but never-accepted defense to BIPA claims."

This holding from Bryant led numerous federal courts to sever plaintiffs' Section 15(a) claims and remand them to state courts while retaining the rest of the suit in federal court. This claim-splitting created a headache for defendants, who in these cases are typically the proponents of federal jurisdiction. Months later, *Fox v. Dakkota Integrated Systems* corrected that over-reading of Bryant by holding that there was jurisdiction over other Section 15(a) claims, *e.g.*, where a defendant is alleged to have violated its retention guidelines with respect to plaintiff's information. After Dakkota, litigants and courts now have a clearer picture of the boundaries of federal jurisdiction over Section 15(a) claims.

The year also brought about the demise of a frequently made but never-accepted defense to BIPA claims. The First District Appellate Court held in *McDonald v. Symphony Bronzeville Park LLC* that claims for statutory damages under BIPA are not preempted by the Illinois Workers' Compensation

Act. The court's opinion reserved the question of whether the Workers' Compensation Act would bar a claim for actual damages. But, for BIPA purposes, the answer to that lingering question should have minimal impact, as the ability to recover high statutory damages on a classwide basis has been the catalyst for the explosion of BIPA class action litigation that has been seen.

With few merits decisions in BIPA cases on the books, most defenses remain untested. Two defenses, however, have proved viable at the pleading stage—labor-law preemption and mandatory arbitration—and in 2020, BIPA plaintiffs continued to struggle to plead around them.

> "There also continues to be movement on facial-recognition regulation at the municipal and state level."

6. FACIAL RECOGNITION REGULATION

While BIPA remains the highest-profile law regulating the use of facial recognition technology, several other jurisdictions proposed or enacted similar regulations in 2020. Several states considered biometric legislation in 2020, including Louisiana, Idaho, Maryland, New York, and South Carolina. While these bills vary in scope and impact, most closely follow the BIPA model, while some also include consumer-rights requirements like those contained in the CCPA. At the federal level, Senators Merkley and Sanders introduced the National Biometric Information Privacy Act of 2020 in August 2020. While the bill did not gain traction, the introduction of the bill demonstrates the trend towards greater biometric enforcement as well as the legislative appetite to continue pushing for increased regulation of biometric technology.

There also continues to be movement on facial-recognition regulation at the municipal level. Notably, the city of Portland issued a general ban on the use of facial-recognition technology in places of public accommodation, effective January 1, 2021. Unlike other municipalities, which have issued bans on the use of facial recognition by police and other public entities, Portland's ban applies to any "private entity" and prohibits the use of the technology "any place or service offering to the public accommodations, advantages, facilities, or privileges whether in goods, services, lodgings, amusements, transportation or otherwise." Importantly, like BIPA, Portland's ban comes with a private right of action and statutory damages of up to $1,000 per day, which goes even beyond BIPA's per-violation damage calculation.

In addition, already in 2021, the New York legislature has introduced its newest effort at regulating biometric information with Assembly Bill 27, the New York Biometric Privacy Act. This bill closely mirrors the technical notice and consent requirements in BIPA. In addition, the bill contains a private right of action with statutory damages of up to $1,000 for each negligent violation and $5,000 for each intentional or reckless violation. While New York has previously tried, and failed, to pass biometric regulation several times in the past, AB 27 has bipartisan support and appears to have a greater chance of enactment than previous attempts.

7. IOT REGULATION

On December 4, 2020, the President signed the Internet of Things Cybersecurity Improvement Act of 2020, a new federal law aimed at establishing minimum security requirements for Internet of Things (IoT) devices that are used or controlled by the federal government.

> “The passing of the federal IoT security law represents an important step forward in the regulation of the security of IoT devices...”

The law directs the National Institute of Standards and Technology (“NIST”) to develop standards and guidelines for the appropriate use of federally owned or operated IoT devices. These guidelines will be focused on the secure development, identity management, patching, and configuration management of IoT devices. The NIST standards are to be based on existing guidelines, standards, and best practices that have been developed by governmental agencies and the private sector to date. Under the law, NIST is also directed to work with the Department of Homeland Security, industry experts, and cybersecurity researchers to publish guidelines on reporting, coordinating, publishing, and receiving of information about security vulnerabilities that threaten governmental agency information systems, including any resolutions to such vulnerabilities.

The passing of state and federal IoT security laws represents an important step forward in the regulation of the security of IoT devices, which have become increasingly well-known for their easily exploitable security vulnerabilities. As the federal IoT security law does not apply to the private sale of IoT devices, IoT device manufacturers should keep an eye on the developing IoT security regulatory landscape and evolution of “reasonable security” standards.

8. TCPA CASE LAW DEVELOPMENTS

In 2020, the Telephone Consumer Protection Act (“TCPA”) continued to dominate the consumer class-action space: nearly 2,000 TCPA cases were filed in federal court alone; hundreds of millions of dollars in damages were awarded or upheld on appeal; and countless cases were settled for untold sums. Meanwhile, companies struggled to comply with the TCPA, as new and pending rulings by the Federal Communications Commission and the U.S. Supreme Court scrambled the already complex statute.

In May 2020, the Supreme Court decided *Barr v. American Association* of Political Consultants, which presented a First Amendment challenge that threatened to strike down the TCPA in full. At issue was the statute’s so-called government debt exemption. The TCPA generally forbids auto-dialed calls to cell phones without proper consent, but the statute contains an exemption for calls to collect government-backed debt. The Supreme Court ruled that this exemption impermissibly favored government speech—but instead of striking down the entire TCPA, the Court severed the exemption, and the statute lives on. However, the members of the Court could not agree on the retroactive effect of the severance, leaving open the possibility that TCPA claims from 2015 through May 2020 are not actionable. A lower-court split has developed on this issue, and the Court will likely need to weigh in again.

> “... FCC issued a long-awaited declaratory ruling that significantly narrowed some of the TCPA’s key exemptions.”

Next, in December 2020, the FCC issued a long-awaited declaratory ruling that significantly narrowed some of the TCPA’s key exemptions. The TCPA regulates pre-recorded calls to cell

phones and residential landlines. The FCC's recent ruling imposed a three-call limit on the number of pre-recorded calls to residential landlines for a wide number of call categories, including informational calls for non-telemarketing purposes, debt-collection calls, health care calls, and more. Companies that make pre-recorded calls should carefully review the FCC's detailed ruling and consider retaining TCPA counsel to ensure ongoing compliance.

9. BREXIT

When the United Kingdom voted to withdraw from the European Union in 2016, it would have been impossible to predict that the U.K. would not officially withdraw from the European Union until January 31, 2020. In the interim, the GDPR took effect on May 25, 2018. As part of the transition period, the U.K. and the EU agreed that the GDPR would continue to apply in the U.K. through December 31, 2020. After such time, the U.K. would be a third country to whom EU personal data could not be transferred without an adequacy determination or the use of the other measures set forth in Articles 46-49 of the GDPR. The U.K. passed its own version of the GDPR, the U.K. GDPR, which took effect on January 1, 2020, and which works in concert with the Data Protection Act of 2018.

One notable provision that to date has flown under the radar for most companies, is the requirement under Article 27 of the GDPR that requires companies processing personal data of individuals within the EU to appoint an EU representative if they are not already established within the EU. The U.K. GDPR contains an analogous provision that requires companies to appoint a UK-based representative if they are not already established in the U.K. For U.K.-based companies and EU-based companies, this may require that they appoint a representative in the other's territory. For companies based in other countries who are processing personal data relating to EU and U.K. individuals, they will need to appoint representatives in both the EU and the U.K.

Notably, in January 2021 the U.K. and the EU agreed to a continued extension of the GDPR transition period, which gives both sides up to an additional six months to enable the EU to promulgate and adopt an adequacy determination. Should that process fail, companies in the U.K. will need to use the SCCs, Binding Corporate Rules, or other means of transferring personal data from the EU to the U.K.

10. CYBERSECURITY AND THE GROWTH IN RANSOMWARE

In the wake of the COVID-19 pandemic, we have seen a rise in cyberattacks, including ransomware and extortion. Given the increased use of remote work, these attackers focused their attack vectors on social engineering (*e.g.*, phishing attacks) as well as exploiting insecure remote desktop protocol, VPN connections, and file-sharing connections or sites.

Attackers are increasingly using a ransomware model designed to both lock down the victim's information systems and exfiltrate sensitive data from the victim. This hybrid approach allows the attacker to gain extortion leverage by threatening to post sensitive information on the dark web if ransom demands are not met. Unfortunately for the victim, the exfiltration of data also increases the likelihood that the security incident may constitute

> "As a result of the increased sophistication of these attacks and the twist of extortion, average ransomware payments are rising."

a reportable data breach under applicable data-breach-notification laws. As a result of the increased sophistication of these attacks and the twist of extortion, average ransomware payments are rising. While the bad actors may tailor a ransom demand to the perceived size and value of the victim, observers are seeing an exponential increase in the initial ransom demands, with some initial demands reaching over $40 million.

The end of 2020 also saw the discovery of the sophisticated Solar Winds attack, the scope of which is still under investigation. This highly complex attack involved malicious code embedded in software and distributed through the supply chain reaching thousands of companies. It will have far-reaching implications as to how companies vet their vendors and work to improve detection of threats to quickly respond to stabilize systems.

As these cyber tactics have proven highly profitable for attackers, and international crackdowns on attacker groups have been ineffective, this trend will likely continue in 2021, even as workers (may) begin to start returning to the office.

The Winston Global Privacy Team is monitoring privacy developments on the horizon in 2021, including state and federal legislation, data security standards and best practices, data privacy litigation, and international data privacy developments.

WINSTON GLOBAL PRIVACY TEAM AUTHORS

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

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

ALESSANDRA SWANSON
PARTNER
Chicago
+1 (312) 558-7435
aswanson@winston.com

SAMANTHA PHILLIPS
ASSOCIATE
San Francisco
+1 (415) 591-1432
saphillips@winston.com

SEAN WIEBER
PARTNER
Chicago
+1 (312) 558-5769
swieber@winston.com

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

CHRIS COSTELLO
SENIOR E-DISCOVERY ATTORNEY
Los Angeles
+1 (213) 615-1742
cccostello@winston.com

KEVIN SIMPSON
ASSOCIATE
Chicago
+1 (312) 558-9378
kpsimpson@winston.com

WINSTON GLOBAL PRIVACY TEAM

PETER CROWTHER
PARTNER
London
+44 20 7011 8750
pcrowther@winston.com

SARAH SUSNJAR
PARTNER OF W&S SELARL
Paris
+33 1 53 64 81 33
ssusnjar@winston.com

STEVE GRIMES
PARTNER
Hong Kong
+852 2292 2138
sgrimes@winston.com

About Winston & Strawn

Winston & Strawn LLP is an international law firm with 950+ 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.