Steptoe

Retail Data Privacy: Emerging Issues for a Shifting Marketplace

NRF Retail Law Summit 2021

Steptoe

Retail Data Privacy: Emerging Issues for a Shifting Marketplace

Supplemental Privacy-Related Alerts and Publications

California Consumer Privacy Act

Other State Privacy Laws

Computer Fraud and Abuse Act

Telephone Consumer Protection Act

Speaker Bios

Steptoe

California Voters Approve Expansive New Data Privacy Law, Shaking Up the CCPA

By: Michael Vatis and Daniel W. Podair

Client Alert – November 12, 2020

For over two years businesses have spent considerable energy preparing for and complying with the California Consumer Privacy Act (CCPA). Businesses now have more work to do after California voters overwhelmingly approved Proposition 24, the California Privacy Rights Act (CPRA), which completely reshapes and overhauls the CCPA. Fortunately, most of the CPRA's changes, including those that expand the rights of consumers and require affirmative action from businesses, do not become effective until January 1, 2023 and apply only to personal information collected on or after January 1, 2022. Nonetheless, given the scope of the changes effected by the CPRA, businesses should begin familiarizing themselves with the CPRA so they can sensibly plan to effectuate changes in their policies and procedures over the next year. Unfortunately, one of the most significant changes worked by the CPRA is the elimination of the 30-day "cure period" businesses have under the CCPA to fix any violations identified by the California Attorney General. This means a failure to comply with California's complicated and often ambiguous requirements will likely become much more costly.

The CPRA's most significant changes are summarized below.

Rights Related to "Sensitive Personal Information"

- The CPRA creates a new category of data called "sensitive personal information" defined as:
    - "Personal information that reveals":
        - "A consumer's social security, driver's license, state identification card, or passport number."
        - "A consumer's account log-in, financial account, debit card, or credit card number in combination with any required security or access code, password, or credentials allowing access to an account."
        - "A consumer's precise geolocation."
        - "A consumer's racial or ethnic origin, religious or philosophical beliefs, or union membership."
        - "The contents of a consumer's mail, email, and text messages unless the business is the intended recipient of the communication."
        - "A consumer's genetic data."
    - "The processing of biometric information for the purpose of uniquely identifying a consumer."
    - "Personal information collected and analyzed concerning a consumer's health."
    - "Personal information collected and analyzed concerning a consumer's sex life or sexual orientation."

    - "Publicly available" information is excluded from the definition of "sensitive personal information."

- Notwithstanding this comprehensive definition, "sensitive personal information that is collected or processed without the purpose of inferring characteristics about a consumer" is not subject to the special rights and restrictions associated with sensitive personal information under the CPRA and is to be treated only as personal information thereunder.

- A consumer is able to limit the use of her or his sensitive personal information to purposes that are "necessary to perform the services or provide the goods reasonably expected by an average consumer who requests those goods or services" and other purposes authorized by the CPRA and regulations promulgated thereunder.

- A consumer is also able to limit the disclosure of her or his sensitive personal information beyond certain purposes authorized by the CPRA and regulations promulgated thereunder.

- A business that uses or discloses sensitive personal information beyond certain purposes authorized by the CPRA and regulations promulgated thereunder must provide notice to consumers that their sensitive personal information will be used or disclosed for additional purposes and that the consumer has the right to limit the use or disclosure of her or his sensitive personal information.

Point of Collection Notices and Retention of Personal Information

- The CPRA expands the existing point-of-collection notice requirement of the CCPA by requiring that a business disclose information about (1) the sale or sharing of personal information and (2) the retention of personal information. The CPRA also applies this expansive point-of-collection notice requirement to the collection of sensitive personal information.

- Additionally, "[a] business' collection, use, retention, and sharing of a consumer's personal information [must] be reasonably necessary and proportionate to achieve the purposes for which the personal information was collected or processed, or for another disclosed purpose that is compatible with the context in which the personal information was collected, and not further processed in a manner that is incompatible with those purposes."

Agreement Related to the Sale or Disclosure of Personal Information

- When a business sells or discloses personal information to a third party, service provider, or contractor, it must enter into an agreement specifying that (1) the personal information is sold or disclosed "only for limited and specified purposes," (2) the third party, service provider, or contactor must comply with the CPRA, (3) the business is able to ensure that the third party, service provider, or contractor uses and transfers the personal information "in a manner consistent with the business' obligations under" the CPRA (4) the third party, service provider, or contractor must notify the business if they cannot meet their obligations under the CPRA, and (5) the business has "the right, upon notice…to take reasonable and appropriate steps to stop and remediate unauthorized use of personal information."

New Consumer Rights

- A consumer is provided with the right to correct inaccurate personal information pursuant to a verifiable consumer request.

- A consumer is provided with the right to opt-out of the sharing of their personal information with third parties (as opposed to the present CCPA right to opt out of only the "sale" of personal information). Notably, the definition of "sharing" includes the disclosure of personal information for "cross-context behavioral advertising, whether or not for monetary or other valuable consideration…" The CPRA defines "cross-context behavior advertising" as "the targeting of advertising to a consumer based on the consumer's personal information obtained from the consumer's activity across businesses, distinctly-branded websites, applications, or services, other than the business, distinctly-branded website, application, or service with which the consumer intentionally interacts."

- A consumer is able request that a business provide information in response to a request to know from beyond the 12 months preceding the request (which is the current period covered by such a request under the CCPA) "unless doing so proves impossible or would involve a disproportionate effort." The CPRA does not specify how far back the consumer's request may go, so it is possible a business will have to search as far back as it possibly can in response to such requests. However, this provision applies only to personal information collected on or after January 1, 2022 and does not "require a business to keep personal information for any length of time."

- A business must update their existing privacy policy disclosures to refer to these new rights afforded by the CPRA in addition to the right to receive a more expansive point of collection notice and the right to limit the use and disclosure of certain sensitive personal information.

Loyalty and Rewards Programs

- The CPRA explicitly states that it "does not prohibit a business from offering loyalty, rewards, premium features, discounts, or club card programs consistent with" the CPRA.

Sale of Personal Information

- Pursuant to one of the exceptions to the CCPA's definition of sale of personal information, when "a consumer uses or directs a business to" either "disclose personal information" or "interact with" third parties, a business no longer has to ensure that the third parties do not "also sell the personal information."

- The use or sharing of personal information with a service provider for a business purpose is no longer exempted from the definition of sale of personal information.

Security Breaches Involving Personal Information

- The CPRA expands the types of information covered under the private right of action for security breaches to include "email address[es] in combination with a password or security question and answer that would permit access to the account." Presently, CCPA only includes "nonencrypted and nonredacted personal information, as defined in" Cal. Civ. Code 1798.81.5(d)(1)(A).[1]

[1] Under Cal. Civ. Code 1798.81.5(d)(1)(A) "'Personal information' means

30-Day Cure Period and Penalties

- Critically, the CPRA removes the existing 30-day period businesses have to cure most alleged violations of the statute. Presently, businesses have 30 days to cure violations of the CCPA and escape potentially hefty fines of $2,500 for each violation and $7,500 for each intentional violation. Additionally, under the CPRA, violations involving the personal information of consumers under the age of 16 will also result in a $7,500 penalty. There must be "actual knowledge" that the consumer is under the age of 16 for the $7,500 penalty to apply.
- Businesses will still have the opportunity to cure violations of Section 1798.150 (regarding Personal Information Security Breaches) within 30 days, to the extent violations are curable. Section 1798.150 permits private plaintiffs "[t]o recover damages in an amount not less than one hundred dollars ($100) and not greater than seven hundred and fifty ($750) per consumer per incident or actual damages, whichever is greater."
- However, in investigating a potential violation, the newly created California Privacy Protection Board (which will be entrusted with enforcing the CPRA) may take into account "voluntary efforts undertaken by the business, service provider, contractor, or person to cure the alleged violation prior to being notified by the agency of [a] complaint" made by any person.
- Additionally, at least 30 days prior to the California Privacy Protection Board's consideration of an alleged violation of the CPRA and before determining whether there is probable cause to believe the CPRA has been violated, a business must be provided with “a summary of the evidence, and informed of their right to be

(A) An individual's first name or first initial and the individual's last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted or redacted:

(i) Social security number.

(ii) Driver's license number, California identification card number, tax identification number, passport number, military identification number, or other unique identification number issued on a government document commonly used to verify the identity of a specific individual.

(iii) Account number or credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account.

(iv) Medical information.

(v) Health insurance information."

(vi) Unique biometric data generated from measurements or technical analysis of human body characteristics, such as a fingerprint, retina, or iris image, used to authenticate a specific individual. Unique biometric data does not include a physical or digital photograph, unless used or stored for facial recognition purposes.”

present in person and represented by counsel at any proceeding of the agency held for the purpose of considering whether probable cause exists for believing" a CPRA violation occurred.

- "When the agency determines there is probable cause for believing [the CPRA] has been violated, it [must] hold a hearing to determine if a violation has or violations have occurred."

The CPRA makes additional changes to the CCPA, which will come into effect five days after the California Secretary of State certifies the referendum result, including the establishment of a new California Privacy Protection Board, which will implement and enforce the CCPA (and, eventually, the CPRA) and provide the Attorney General with expansive power to issue further regulations under the CCPA. The initial appointments to the California Privacy Protection Board are to be made within 90 days of its creation. "On and after the earlier of July 1, 2021, or within six months of the agency providing the Attorney General with notice that it is prepared to assume rulemaking responsibilities," the California Privacy Protection Board will assume responsibility for issuing regulations.

CPRA also extends, until January 1, 2023, exemptions from most of the CCPA's requirements for personal information collected as part of a B2B transaction or collected from employees and job applicants. Under existing law, the exemptions would have expired on January 1, 2022.

As businesses continue to refine their CCPA compliance strategies, they should do so with the CPRA in mind. Although its effective date is more than two years away, businesses would be well served by familiarizing themselves and starting to address the CPRA sooner rather than later.

Steptoe

California Attorney General Proposes More Modifications to CCPA Regulations

By: Michael Vatis and Daniel W. Podair

Client Alert – October 13, 2020

Just when you thought you finally had a handle on CCPA compliance, the California Attorney General has proposed additional modifications to the regulations that recently became final on August 14. Fortunately, the changes are minor. More significant changes to the CCPA may be just around the corner, though, if California voters approve the California Privacy Rights Act Initiative on November 3.

On October 12, 2020, California Attorney General Xavier Becerra released a new set of proposed modifications to regulations implementing the California Consumer Privacy Act (CCPA). Specifically, the modifications would:

- Require that "[a] business that collects personal information in the course of interacting with consumers offline… provide notice by an offline method that facilitates consumers' awareness of their right to opt-out" of the sale of their information. Pursuant to this requirement, "a brick-and-mortar store [could] provide notice by printing the notice on the paper forms that collect the personal information or by posting signage in the area where the personal information is collected directing consumers to where the notice can be found online." In addition, "[a] business that collects personal information over the phone [could] provide the notice orally during the call where the information is collected."

- Mandate that "[a] business's methods for submitting requests to opt-out…be easy for consumers to execute and…require minimal steps to allow the consumer to opt-out" and prohibit a business from "us[ing] a method that is designed with the purpose or has the substantial effect of subverting or impairing a consumer's choice to opt-out." In particular, a business would be prohibited from "requir[ing] more steps [in the process to opt out] than that business's process for a consumer to opt-in to the sale of personal information after having previously opted out," "us[ing] confusing language, such as double-negatives (e.g., 'Don't Not Sell My Personal Information'), when providing consumers the choice to opt-out," "requir[ing] consumers to click through or listen to reasons why they should not submit a request to opt-out before confirming their request," "requir[ing] the consumer to provide personal information that is not necessary to implement the request," or "[u]pon clicking the 'Do Not Sell My Personal Information' link…requir[ing] the consumer to search or scroll through the text of a privacy policy or similar document or webpage to locate the mechanism for submitting a request to opt-out."

- Allow a business to "require [an] authorized agent to provide proof that the consumer gave the agent signed permission to submit [a] request" to know or a request to delete. The existing language permits the business to require the consumer to "provide the authorized agent signed permission to" submit a request to know or a request to delete.

- Clarify that businesses subject to either § 999.330 (regarding processes for the opt-in to the sale of personal information by the parent or guardian of consumers under 13 years of age) or § 999.331 (regarding processes for the opt-in to the sale of personal information by consumers between 13 and 15 years of age) must "include a description of the processes set forth in those sections in its privacy policy." The existing language of the regulations only requires businesses subject to both § 999.330 and § 999.331 to take this step.

The proposed modifications will be subject to a round of notice and comment. The deadline to submit written comments is October 28, 2020 at 5:00 p.m. PDT.

Steptoe

California Extends Exemptions from CCPA for B2B and Employee Information

By: Michael Vatis and Daniel W. Podair

Client Alert – October 2, 2020

On September 30, California Gov. Gavin Newsom signed into law AB-1281, which extends until January 1, 2022 the exemptions from the California Consumer Privacy Act (CCPA) for personal information collected as part of a B2B transaction or collected from employees and job applicants. The exemptions apply to most, but not all, of the CCPA requirements. Without AB-1281, the exemptions would have expired on January 1, 2021.

The B2B exemption applies to personal information "reflecting a written or verbal communication or a transaction between the business and the consumer, where the consumer is a natural person who is acting as an employee, owner, director, officer, or contractor of a company, partnership, sole proprietorship, nonprofit, or government agency and whose communications or transaction with the business occur solely within the context of the business conducting due diligence regarding, or providing or receiving a product or service to or from such company, partnership, sole proprietorship, nonprofit, or government agency." Notably, however, the B2B exemption does not apply to the requirements to allow a person to opt out of the "sale" of her information or the prohibition on discrimination against a person who exercises her CCPA rights.

The "employee" exemption applies to personal information collected from employees, job applicants, owners, directors, officers, medical staff members, and contractors. This exemption does not apply to the requirement that a person receive a notice at or before the point of collection of personal information.

Neither exemption applies to the CCPA's private right of action for data breaches.

CCPA Regulations Take Effect, Six Weeks After CCPA Enforcement Begins

By: Michael Vatis and Daniel W. Podair

Client Alert – August 17, 2020

On Friday, August 14, 2020, California Attorney General Xavier Becerra announced that the regulations implementing the California Consumer Privacy Act (CCPA) have been approved by the California Office of Administrative Law (OAL) and are effective immediately. The attorney general had already begun enforcing the CCPA itself on July 1. But now that the regulations have taken effect, the attorney general can begin enforcing their requirements, too, which in some cases go beyond what the statute expressly requires. And the attorney general has signaled that non-compliance can lead to heavy penalties.

The attorney general first released draft regulations in October 2019 and made subsequent modifications in February and March 2020 before submitting the draft "final" regulations to OAL for its review and approval in June 2020. The final regulations that took effect on August 14 are largely the same as the June draft, with mostly technical and grammatical edits having been made. But there are a few material changes in the final version:

- The final regulations no longer require businesses that substantially interact with consumers offline to provide an offline notice of the right to opt-out of the sale of their personal information. The earlier draft regulations had suggested that businesses with brick-and-mortar stores would have to provide some form of offline notice such as prominent in-store signage, or printed versions of the notice. Now, the regulations require only that a business post the notice on its website or, if it doesn't have a website, that it use "another method," chosen by the business, to inform consumers of their opt-out right. Note, however, that the CCPA and the regulations still require businesses to notify consumers "at or before the point of collection" of the "categories of personal information to be collected and the purposes" for which the information will be used. So even if an opt-out notice does not need to be provided offline, a "notice-at-collection" does, if personal information is collected offline.

- The final regulations removed a prohibition against using "a consumer's personal information for a purpose materially different than those disclosed in the notice at collection." The regulations also no longer require a business seeking "to use a consumer's previously collected personal information for a purpose materially different than what was previously disclosed to the consumer in a notice at collection…to directly notify the consumer of this new use and obtain explicit consent from the consumer to use it for this new purpose." Despite these changes, companies that use a consumer's personal information for a purpose different from what was disclosed at the time of collection, without obtaining the consumer's consent to the new use, run the risk of running afoul of California consumer protection laws (as well as the Federal Trade Commission Act's ban on "deceptive acts or practices"). In addition, the CCPA itself still expressly states "[a] business shall not collect additional categories of personal information or use personal information collected for additional purposes without providing the consumer with notice consistent with this section."

- The final regulations remove references to the short version of the opt-out link language, suggesting that businesses must use the full "Do Not Sell My Personal Information" language in the links (on their home pages and in their privacy policies) to the online form for requesting to opt out of the sale of personal information.
- The revised regulations make it clear that a business may deny requests to know, requests to delete, and requests to opt out that are received from agents that fail to provide a signed, written permission from the consumer authorizing the agent to act on the consumer's behalf. Language suggesting that it might be sufficient for an agent to provide some other form of proof of its authority has been deleted.

Notably, the final regulations retain requirements that have confounded businesses that offer loyalty programs, sweepstakes, discount offers, and other services or programs that might constitute "financial incentives" that are offered to induce consumers to provide their personal information (or allow their information to be sold). Specifically, the final regulations still require that businesses include in their "notice of financial incentive," "[a]n explanation of how the financial incentive or price or service difference is reasonably related to the value of the consumer's data," "[a] good faith estimate of the value of the consumer's data that forms the basis for offering the financial incentive or price or service difference," and "[a] description of the method the business used to calculate the value of the consumer's data." Many businesses have waited to address these requirements, unsure of exactly how to achieve compliance and hoping that the requirements would disappear from the final regulations. Businesses that have waited therefore must scramble quickly to address these requirements, as the regulations are now already in effect.

The attorney general began enforcing the CCPA itself on July 1, 2020, sending "Notices of Violation" to businesses that were deemed not to be in compliance with the statute. The CCPA prescribes penalties of between $2,500 and $7,500 "for each violation." While this may seem like a small amount, the attorney general has signaled in the Notices of Violation that he takes a broad view of what constitutes "each violation," quoting case law stating that "what qualifies as a single violation depends on the type of violation involved, the number of victims and the repetition of the conduct constituting the violation—in brief, the circumstances of the case." It is likely, then, that the attorney general would seek to multiply the statutory penalty by, for example, the number of California residents whose personal information was collected during the period in which a business was not in compliance (such as by having an incomplete privacy policy), and by the number of technical violations. The potential costs of non-compliance are therefore more significant than they might appear at first glance.

More information about the CCPA regulations can be found in our client alerts discussing the initial draft of the attorney general’s regulations in October 2019 and the subsequent modifications in February and March 2020.

CCPA Is One Of Many Retailer Data Privacy Class Action Worries

By: Stephanie A. Sheridan and Meegan Brooks

First Published in *Law360* – May 26, 2020

The privacy landscape has drastically evolved over the last few years. On March 17, 2018, The New York Times and The Guardian simultaneously broke the story that Cambridge Analytica Ltd. had harvested the personal data of 87 million people to be used for predominantly political advertising. On May 25, the EU General Data Protection Regulation went into effect. Barely a month later, on June 28, the California Consumer Privacy Act was enacted.

The CCPA was born out of rising concerns in the wake of serious data breaches, which revealed that consumers did not understand how their personal information is collected, much less how it may be shared or sold. Once the CCPA was passed, other states considered, passed or began enforcement of their own data privacy laws.

Congress also considered federal privacy bills, several of which are still pending. And if the explosion of privacy legislation in 2018 following the Cambridge Analytica scandal was not enough to bring data privacy concerns into the public eye, there were more data breaches in 2019 than any prior year to date.

The CCPA has not been in effect for even five months, and despite proclamations that it would not provide a private right of action outside of the data breach context, several significant class actions have already been filed, attempting to bootstrap alleged CCPA violations to the unlawful prong of California's Unfair Competition Law.

The California attorney general can begin enforcing the CCPA on July 1, 2020, with civil penalties ranging from $2,500 for a nonintentional violation, to $7,500 for an intentional violation. And retailers should not expect a reprieve in enforcement in light of the COVID-19 crisis as the attorney general has stated that, if anything, he plans to step up enforcement as a result of the pandemic.

And the CCPA is not be the only new privacy law businesses will likely need to confront. On the November ballot, Californians will vote on the California Privacy Rights Act, which would not only provide additional, stricter privacy rights and obligations, it would also create the California Privacy Protection Agency, which would be responsible for enforcing and implementing consumer privacy laws and imposing administrative fines.

Aside from all of the legislative activity around privacy, the plaintiffs bar has been busy testing novel theories in consumer class actions filed against retailers for allegedly selling consumer data. A slew of new cases — brought across the country under a variety of state privacy statutes, consumer protection laws and common law — go to the same issues that spurred the enactment of the CCPA in the first place: addressing the collection, sale and use of consumers' personal data, often without their knowledge.

Prior Waves of Privacy Litigation Against Retailers Paved the Way Here

Violations of privacy laws are expensive; indeed, many include steep statutory penalties for every noncompliant transaction, which can rack up enormous damages quickly. This is why retailers have historically been the easiest, and therefore most attractive, target for privacy-related litigation. There have been two significant waves of privacy litigation against retailers, under the federal Fair and Accurate Credit Transactions Act, or FACTA, and California's Song-Beverly Credit Card Act and similar laws in other states.

FACTA prohibits retailers from printing more than the last five digits of a consumer's credit card number on a receipt. The underlying reasoning makes sense: If a consumer lost her receipt that had all of her credit card numbers and it fell into nefarious hands, the consumer's personal data could be compromised, and even sold on the lucrative black market.

However, when FACTA was amended in 2006 to also prohibit printing expiration dates on receipts, more than 500 class actions were quickly filed across the country, seeking staggering statutory penalties of up to $1,000 per violation — even though a receipt with an expiration date, but without the full card numbers, has never been shown to increase the risk of identity theft.

Retailers got another crash course in privacy litigation in 2011, when hundreds of lawsuits targeted the industry under California's Song-Beverly Act, a well-intentioned statute enacted in 1971 that restricts retailers' collection and sale of customer information. The litigation floodgates broke open following the California Supreme Court's seminal decision in *Pineda v. Williams-Sonoma Stores Inc.*,[1] which held that Song-Beverly prohibits retailers' collection of ZIP codes during credit card transactions.

The Pineda court's reasoning was based in part on retailers' technological ability to use customers' ZIP codes with their names to access their full address, which the retailer could then sell to other businesses. A subsequent slew of ZIP code cases was filed against retailers in other jurisdictions, mostly under Massachusetts' General Law Chapter 93, Section 105(a).

Suits Spurred From Violations of State Laws Prohibiting the Sale of Data

A handful of states have statutes that specifically prohibit businesses from selling consumer information to third parties in specific contexts. For example, up until July 2016, Michigan's Preservation of Personal Privacy Act, or PPPA, prohibited sellers of written materials from disclosing to third parties "a record or information concerning the purchase ... of those materials by a customer that indicates the identity of the customer," and provided penalties of $5,000 per violation.

As early as 2012, plaintiffs have used the PPPA to extract millions of dollars from publishing companies that allegedly sold customer information. In 2019 alone, settlements included matters against Conde Nast Publications Inc. ($13.75 million), Time Inc. ($7 million), Hearst Corp. ($50 million), TV Guide ($1.7 million) and Consumers Union, which publishes Consumer Reports ($16.375 million).

[1] *Pineda v. Williams-Sonoma Stores, Inc.* , 51 Cal. 4th 524, 532 (2011).

In response to these hefty settlements, the PPPA was revised in 2016 to, among other things, limit the private cause of action to consumers who suffered actual damage as a result of the alleged disclosure, and to limit their potential recovery to actual damages. Even years after the amendment, however, Playboy Enterprises Inc. just settled a PPPA case for $3.85 million; the court granted preliminary approval of the settlement on Feb. 7.

Litigation over sale of customer information has now pivoted to the retail industry, targeting retailers like The Yankee Candle Co. Inc., Apple Inc. and adult film distributor TLA Entertainment Group for allegedly selling customer information on data aggregation websites.[2] In *Bone v. Yankee Candle*, for example, the plaintiff alleged that Yankee Candle sold her personal information to data brokers, which in turn sold her information to telemarketers and other aggressive advertisers, resulting in her being "inundated with a barrage of unwanted junk mail and telephone solicitations."

The complaint included purported screenshots from data aggregation website NextMark Inc., which allegedly sells Yankee Candle's mailing list for 10 cents or more per customer. Yankee Candle filed a motion to dismiss arguing that the plaintiff lacked Article III standing, but the parties filed a stipulation of dismissal on Jan. 23 before it was decided.

Screenshots from data aggregation websites may not be as persuasive as plaintiffs in these cases hope. In *Wheaton v. Apple*, the complaint included similar screenshots, which the plaintiffs claimed supported their claim that Apple sold customers' information and musical preferences, collected from their use of the Apple store.

Apple filed a motion to dismiss arguing that the screenshots did not actually support the plaintiffs' claims, because one of the purported screenshots did not include Apple's name, and the other did not include any customers' personal information, begging the question why no facts were pled showing that the information was actually being sold. The court granted Apple's motion to dismiss on Oct. 25, 2019.

New Suits Brought Under General Consumer Protection Statutes

Aside from the compromise of personal information in data breaches, or violation of privacy statutes, consumer class actions have also targeted businesses under states' general consumer protection statutes, based on the theory that they acted unfairly or deceptively by sharing or selling customers' information. While these suits have not specifically targeted retailers, it is easy to imagine similar claims being made against retailers for allegedly selling customer information. For example:

Medical Information

In June 2019, a former patient of the University of Chicago Medical Center filed a putative nationwide class action against the university and Google Inc. for allegedly sharing patients' personal information, as part of a partnership intended to develop machine-learning techniques that could improve the quality of health

[2] *Bone v. The Yankee Candle Co. Inc.*, 19-CV-30074 (D. Mass); *Wheaton v. Apple Inc.*, 19-cv-02883 (N.D. Cal.); *Chiamulera v. TLA Entertainment Group Inc.*, 19-cv-9512 (S.D.N.Y.).

services.[3] The plaintiff alleged that by telling patients that it would protect their medical records and sharing information allegedly protected by the Health Insurance Portability and Accountability Act, the university breached contracts with its patients and also engaged in deceptive practices.

Google and the university filed separate motions to dismiss on Nov. 7, 2019, emphasizing that the shared data was deidentified and that the plaintiffs had failed to allege an actual injury and thus lacked Article III standing. The motions are currently pending.

Cell Phone Location Data

On July 16, 2019, the Electronic Frontier Foundation brought a class action and sought an injunction against AT&T Inc. and two data brokers alleging the service provider disclosed customers' geolocation information without their consent.[4] In addition to claims under the Communications Act related to cell phone geolocation data, the Electronic Frontier Foundation also asserted invasion of privacy and violation of California's consumer protection statutes.

AT&T filed a motion to dismiss, arguing that it had mooted plaintiffs' claims by ceasing the conduct at issue before the suit was filed. Each of the data aggregators also filed motions to dismiss, arguing that the Electronic Frontier Foundation had not alleged any injury and thus lacked Article III standing and failed to state a claim. These motions are currently pending.

Student Demographics

On Dec. 10, 2019, a parent filed a putative nationwide class action against The College Board alleging that it sells student data collected through its Student Search Service.[5] The plaintiff alleges that The College Board tricks students into sharing their information by misrepresenting that they do not sell students' information, instead leading students to believe that providing the information would assist their chances of receiving admission and financial aid to college.

The College Board filed a motion to compel arbitration on March 4, 2020, the briefing for which has been delayed in light of COVID-19. On May 10, the court rejected the plaintiff's request for a temporary restraining order that would have prevented The College Board from disseminating information collected during the upcoming Advanced Placement tests, in light of The College Board's representations that it would not allow test-takers to opt into Student Search during the exams.

Data Sales Actions Face Several Hurdles

In some instances, prior government investigations did the preliminary legwork for plaintiffs — including in the AT&T and College Board cases above, as well as the recent high-profile litigation against Zoom

[3] *Dinerstein v. Google, LLC*, No. 19-cv-04311 (N.D. Ill.).

[4] *Scott v. AT&T Inc.*, No. 19-cv-04063 (N.D. Cal.).

[5] *S. v. College Board*, No. 19-cv-08068 (N.D. Ill).

Technologies Inc. Other cases — including several consumer class actions arising out of the Cambridge Analytica scandal — followed on the heels of exposés in prominent newspapers.

As consumers become savvier and insist on protection of their valuable personal information, litigation over sales of consumer data will no doubt become an increasing focus of the plaintiffs' bar. Despite how attractive cases over sales of consumer data may appear, such actions will have to overcome several hurdles to proceed before they can succeed.

First, as the Supreme Court in *Spokeo Inc. v. Robins* reconfirmed, Article III standing requires that a plaintiff's injury must be particularized and concrete. Courts have rejected plaintiffs' attempts to establish standing based on arguments that the sale of their information merely increased their risk of identity theft, or deprived consumers of the economic value of their information. However, at least some courts have held that the disclosure of sensitive private information, even without further consequence, gives rise to Article III standing.[6]

Plaintiffs who overcome the standing hurdle must then state a claim, which usually requires alleging that the defendant's actions injured the plaintiff. While states' consumer protection and fraud laws vary, it is typically much easier to state a claim on an affirmative representation theory than an omission theory.

To succeed on an omission claim, plaintiffs must generally allege a duty to disclose, and that the allegedly omitted information would be material — the fact that consumers might just want to know the information is insufficient.[7]

As applied in the privacy context, plaintiffs may struggle to state a claim for deceptive conduct based on a pure omission theory — that is, that the defendant failed to notify the plaintiff that it would sell his or her information. In response, we have seen plaintiffs instead rely on defendants' affirmative statements concerning their efforts to protect customer data.

Even where a defendant does allege an affirmative misrepresentation, however, many states require plaintiffs to have actually relied on that statement to state a claim.[8]

Protective Measures

Retailers will always be interested in obtaining personal data to learn more about their customers and to attract new customers. Given that nearly every state's consumer protection laws provide a private right of action, to protect against fraud claims based on the collection or sale of consumer data, retailers should review their public disclosures, including their privacy policies, to ensure they are not vulnerable to deception claims.

[6] See, e.g., *Eichenberger v. ESPN, Inc.*, 876 F.3d 979, 984 (9th Cir. 2017).

[7] *Hodsdon v. Mars, Inc* , 891 F.3d 857, 860 (9th Cir. 2018). (no duty to disclose alleged use of slave labor in supply chain); *Hall v. SeaWorld Ent., Inc.*, 747 Fed. Appx. 449, 450 (9th Cir. 2018). (no duty to disclose alleged mistreatment of orca whales).

[8] *Sud v. Costco Wholesale Corp.*, 731 Fed. Appx. 719, 721 (9th Cir. 2018).

A best practice, which is required under the CCPA, is for retailers' privacy policies to fully disclose what data is collected, and with whom it is shared; a failure to disclose specifics could also strengthen a plaintiff's omission claim by constituting a partial disclosure. At the same time, robust privacy policies can protect retailers.

For example, notifying a consumer in advance that she consents to the company's privacy policy by doing some act — such as completing a purchase, downloading an app or enrolling in a loyalty program — can be powerful evidence of consent to the policy because it would be difficult for a plaintiff to claim she was injured where she affirmatively consented to the conduct.

Arbitration clauses and class action waivers can be valuable shields to consumer class actions, including unfair competition suits in the privacy context. While the CCPA contains a provision that on its face appears to prohibit the use of arbitration clauses with class action waivers as a means to limit class action claims, this restriction may be preempted by the Federal Arbitration Act.

Conclusion

While the CCPA has been lauded as the first comprehensive privacy statute in the country, it is far from the only threat retailers can face from the collection, use and sale of consumer data. In addition to ensuring compliance with specific statutory requirements, retailers should also more broadly assess their vulnerability to potential claims of deceptive conduct.

Retailers would also be wise to consider an overall audit of their practices to identify risk areas that may expose them to the myriad privacy-related traps for the unwary. Preventing exposure to liability in the privacy context is an area where "better safe than sorry" is a best practice most certainly worth the investment.

Steptoe

Virginia Poised to Become Second State with Comprehensive Privacy Law

By: Michael Vatis and Christopher Suarez

Client Alert – February 10, 2021

On January 29, 2021 and February 3, 2021, respectively, the Virginia House of Delegates and Virginia Senate passed the Virginia Consumer Data Protection Act (VCDPA). The legislation, if signed into law by the governor, would be the first comprehensive privacy law enacted by a state since California enacted the California Consumer Privacy Act (CCPA) and, more recently, the California Privacy Rights Act (CPRA). Though the VCDPA is not slated to take effect until January 1, 2023, it will be important for companies to understand the complicated provisions of the VCDPA much earlier, so they can begin instituting any necessary changes in their internal and public-facing policies and their information practices. The VCDPA's passage may also spur other states to enact their own privacy laws, which until now have been mired in legislative purgatory.

Some of the more significant aspects of the VCDPA are summarized below:

Scope and Exemptions

The VCDPA applies to anyone conducting business in Virginia who controls or processes personal data of at least 100,000 Virginia consumers, or who controls or processes personal data of at least 25,000 Virginia consumers and derives more than half of their revenue from the sale of personal data. The VCDPA does not apply to the following entities:

- Virginia state agencies, boards, commissions, or political subdivisions
- Financial institutions subject to the Gramm-Leach-Bliley Act (GLBA)
- Covered entities or business associates covered by HIPAA regulations
- Nonprofit organizations
- Institutions of higher education

Other provisions exempt particular types of *data*, including data covered by the GLBA, HIPAA, Fair Credit Reporting Act (FCRA), Driver Privacy Protection Act (DPPA), the Federal Educational Rights and Privacy Act (FERPA), the Farm Credit Act, and the Children's Online Privacy Protection Act (COPPA).

Despite the exemptions, the Virginia law will apply to numerous entities that control and/or process large amounts of data, including most social media platforms, large internet companies that do business in the state, and numerous other entities that engage with Virginia consumers.

Personal Data Rights

The VCDPA allows Virginia residents to invoke personal data rights and to submit requests that (1) seek confirmation that a data controller is processing the consumer's data, (2) ask to correct inaccuracies of data, (3) delete personal data provided by or obtained about the consumer, (4) obtain a copy of the personal data previously provided by the consumer, or (5) opt out of the processing of personal data for purposes of *targeted advertising, the sale of personal data, or profiling in furtherance of decisions that have legal or other significant impacts on the consumer.* Consumers can make such requests twice annually, and the data controller must respond pursuant to a timeline, provide an appeal right, and provide consumers a mechanism to submit complaints to Virginia's Attorney General.

Data Controller Responsibilities

Under the VCDPA, data controllers must limit the collection of personal data to what is adequate, relevant, and reasonably necessary for the purposes for which such data is processed. They must also implement administrative, technical, and physical data practices to protect the confidentiality of personal data. Additionally, data controllers cannot process certain *sensitive data* (including data that contains racial, genetic, or geolocation data, for example) without obtaining the consumer's consent. Controllers also must provide meaningful privacy notices, provide notice and an opt-out right with regard to any efforts to sell data or use it for targeted advertising, and provide a secure mechanism to allow consumers to exercise their consumer rights under the VCDPA. Significantly, consumers must be allowed to exercise their rights without needing to create an account with the data controller. Data controllers must also contractually protect the confidentiality and privacy of data shared with data processors, whose role must be limited and circumscribed by such contracts. They should also take reasonable efforts to ensure that any de-identified data cannot be re-identified or associated with a natural person, and are not generally compelled to provide consumers with de-identified data.

Data Protection Assessments

Data controllers are required to conduct data protection assessments of their processing of personal data for targeted advertising, the sale of personal data, the processing of personal data for purposes of profiling (where discrimination or injury may result), the processing of sensitive data, and other data processing activities that present a heightened risk of harm to consumers. Such assessments should weigh the public benefits and risks of any data processing against the risks to the rights of the consumer that may result. The Attorney General of Virginia can request and review these data protection assessments for investigative purposes.

Safe Harbors

The VCDPA states that nothing in the statute shall be construed to limit data controllers' and processors' ability to comply with federal, state, or local laws; cooperate with law enforcement; defend legal claims; perform obligations requested by consumers; take steps essential to promote life and safety; prevent and detect security breaches and harassment; engage in scientific research; or assist third parties with such activities. In addition, data controllers or processors are not restricted from collecting, using, or retaining data to conduct internal research to develop, improve, or repair products or technology; effectuate a product recall; identify and repair technical errors that impair existing or intended functionality; or perform internal operations that are reasonably aligned with the expectations of the consumers or reasonably anticipated based on the consumer's existing relationship with the data controller. Finally, data controllers are not liable for the actions of third-party controllers or processors to whom they disclose data if those third parties commit violations and the controller or processor lacked actual knowledge that the recipient of the data intended to commit a violation of the Act. However, data controllers and processors do have the burden to show that they meet any safe harbor or exemption.

Enforcement and Penalties

Virginia's Attorney General has the exclusive authority to enforce violations of the VCDPA. There is no private right of action. Before initiating any action, the Attorney General must provide 30 days written notice to a controller or processor alleging the specific provisions violated, along with an opportunity to cure the violation(s) and cease all violating activity. If the violations are not cured, the Attorney General may initiate an action that may result in statutory damages of $7,500 per violation and an injunction. The Attorney General may also recover attorneys' fees.

Steptoe

Data Security Components of New York's SHIELD Act Take Effect

By: Michael Vatis and Daniel W. Podair

Client Alert – May 5, 2020

While most businesses have been preoccupied with navigating the effects of the COVID-19 pandemic, a significant change to businesses' data security obligations has taken effect in New York. On March 21, 2020, the second part of the Stop Hacks and Improve Electronic Data Security Act (the SHIELD Act) went into effect in New York State. The SHIELD Act was signed into law in July 2019 and part of the legislation, amending New York's data breach notification law, went into effect last October. The new data security requirements are not limited to a specific industry, but apply to any person or business that owns or licenses computerized data that includes the private information of New York residents.[1]

The SHIELD Act mandates a covered business "develop, implement and maintain reasonable safeguards to protect the security, confidentiality and integrity of the private information, including but not limited to, disposal of data." To comply with the SHIELD Act, a business' data security program must include the following:

- "Reasonable administrative safeguards," such as:
    - Designating "one or more employees to coordinate the security program";
    - Identifying "reasonably foreseeable internal and external risks";
    - Assessing "the sufficiency of safeguards in place to control the identified risks";
    - Training and managing "employees in the security program practices and procedures";

[1] "Private information" is defined in N.Y. Gen. Bus. § 899-aa and includes "any information concerning a natural person which, because of name, number, personal mark, or other identifier, can be used to identify such natural person" in combination with "(1) social security number; (2) driver's license number or non-driver identification card number; (3) account number, credit or debit card number, in combination with any required security code, access code, password or other information that would permit access to an individual's financial account; (4) account number, credit or debit card number, if circumstances exist wherein such number could be used to access an individual's financial account without additional identifying information, security code, access code, or password; or (5) biometric information[.]" "Private information" also includes "a user name or e-mail address in combination with a password or security question and answer that would permit access to an online account."

    - Selecting "service providers capable of maintaining appropriate safe-guards" and requiring "those safeguards by contract"; and
    - Adjusting "the security program in light of business changes or new circumstances."
- "Reasonable technical safeguards," such as:
    - Assessing "risks in network and software design";
    - Assessing "risks in information processing, transmission and storage";
    - Detecting, preventing and responding "to attacks or system failures"; and
    - Regularly testing and monitoring "the effectiveness of key controls, systems and procedures."
- "Reasonable physical safeguards," such as:
    - Assessing "risks of information storage and disposal";
    - Detecting, preventing, and responding “to intrusions";
    - Protecting "against unauthorized access to or use of private information during or after the collection, transportation, and destruction or disposal of the information"; and
    - Disposing "of private information within a reasonable amount of time after it is no longer needed for business purposes by erasing electronic media so that the information cannot be read or reconstructed."

A small business[2] complies with the SHIELD Act's data security program requirements where its "security program contains reasonable administrative, technical and physical safeguards that are appropriate for the size and complexity of the small business, the nature and scope of the small business's activities, and the sensitivity of the personal information the small business collects from or about consumers."

In addition, any entity that is subject to and in compliance with (i) regulations promulgated pursuant to Title V of the federal Gramm-Leach-Bliley Act, (ii) regulations implementing the federal Health Insurance Portability and Accountability Act (HIPAA) and the federal Health Information Technology for Economic and Clinical Health Act (HITECH Act), (iii) the New York State Department of Financial Services Cybersecurity Regulation, or (iv) any other federal or New York State data security rule, regulation, or statute, is deemed compliant with the SHIELD Act's data security mandate. The New York State Attorney General is empowered to enforce the SHIELD Act's data security requirements and may seek injunctive relief and damages of up to $5,000 per violation. The Act, however, explicitly excludes a private right of action under the data security requirements section.

[2] A "small business" is defined as "any person or business with (i) fewer than fifty employees; (ii) less than three million dollars in gross annual revenue in each of the last three fiscal years; or (iii) less than five million dollars in year-end total assets, calculated in accordance with generally accepted accounting principles."

Steptoe

To Understand the CFAA, It Depends on What the Meaning of the Word ‘So’ Is

By: Michael Vatis

Client Alert – June 7, 2021

President Bill Clinton earned lasting notoriety for his explanation of why his statement denying a relationship with Monica Lewinsky was truthful (“it depends on what the meaning of the word ‘is’ is”). It is doubtful Justice Amy Coney Barrett’s majority opinion for the Supreme Court last week in *Van Buren v. U.S.* will earn as much ridicule from late-night comedians, despite putting so much questionable weight on a two-letter word (in this case, the word “so”). But the opinion does finally resolve an issue that has split lower courts and vexed employers, website operators, security researchers, and others for many years: whether the Computer Fraud and Abuse Act (CFAA) can be used to prosecute, or sue civilly, someone who accesses a computer with authorization, but uses that access for an improper purpose. The Court answered that question with a resounding, “No.” But the Court left unresolved a number of other questions, including what sorts of limits on access have to be transgressed in order to give rise to a CFAA violation.

The CFAA prohibits, among other things, intentionally accessing a computer “without authorization” or “exceed[ing] authorized access” and obtaining information. In *Van Buren*, a police officer had used his patrol car computer to access a law enforcement database to look up a license plate number in exchange for money from a private person who wanted information about a woman he had met at a strip club. The arrangement turned out to be an FBI sting, and after the officer used his valid credentials to look up the license plate number in the database, he was arrested and charged with violating the CFAA. The government alleged that the officer had exceeded his authorized access to the database by accessing it for an improper purpose—i.e., for personal use, in violation of police department policy. The officer was convicted and sentenced to 18 months in prison.

On appeal to the Eleventh Circuit, the officer argued that “exceeds authorized access” in the CFAA reaches only people who are authorized to access a computer, but then access information to which their authorized access does not extend. Several circuits have interpreted this clause in just this way. However, the Eleventh Circuit, like some others, adopted a broader view, holding that the clause also applies to someone who has authorization to access a computer but then uses that access for an inappropriate reason.

This broad interpretation has drawn a great deal of criticism, including by those who argue that it results in the criminalization of a great deal of everyday behavior. Anyone who violates a website’s terms of use (such as by using a pseudonym, or supplying a fake date of birth), or violates her company’s computer use policy by sending personal emails or composing personal documents on a workplace computer, would be violating the CFAA.

The Supreme Court cited such arguments as one reason the broad interpretation of “exceeds authorized access” is “implausib[le].” But the Court’s principal reason for adopting a narrow reading of the phrase turned on the word “so.” The CFAA defines “exceeds authorized access” as “access[ing] a computer with authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter." The Court devoted several pages of linguistic analysis to explaining why the word "so" must be read as restricting the entire definition to persons who are authorized to access a computer, but are not entitled to use that access to obtain or alter certain information, and why the clause cannot be read as applying to people who are authorized to obtain or alter that information but then do so for a prohibited purpose. One might charitably say that this is all a very lawyerly reading of the phrase (as was said about Mr. Clinton's exegesis of the meaning of "is"). But whatever the case, it is now the law.

Fortunately, the Court ended its opinion with a clearer enunciation of its interpretation of "exceeds authorized access": "In sum, an individual 'exceeds authorized access' when he accesses a computer with authorization but then obtains information located in particular areas of the computer—such as files, folders, or databases—that are off limits to him." This makes clear that one cannot violate the CFAA—and therefore be subjected to criminal prosecution or a civil suit—merely by using his authorized access to obtain information for an improper purpose. This may make it more difficult for employers to use the CFAA to go after rogue employees who steal company information for a competing firm, or for website operators to sue competitors who abuse their authorized access to a site's content by scraping it or otherwise mining it for commercial advantage.

Nevertheless, the Court's opinion leaves some significant questions unresolved, and therefore still leaves room for effectively using the CFAA in such situations. Notably, the Court explicitly leaves open the question of how a computer owner may limit access to particular information in order to be able to sue for violations of those limits. Some will likely misread the opinion as requiring technological barriers to access. But it may be enough to impose carefully worded limits via contractual or policy terms, as long as they are focused on prohibiting access to the information, not on prohibiting certain uses. It may also be enough to impose limits on access by certain means, while allowing access by other means. Thus, for example, a competitor might have authorization to access a website's content as a regular user, but if the website's terms prohibit scraping the same content via automated bots, then such scraping may still give rise to a CFAA violation.

So—while *Van Buren* will be widely read as limiting the ability of computer owners to use the CFAA as a legal weapon, the reality—for now, at least—is that companies can still use that statute to protect their information, as long as they give careful thought to the ways they limit access to it.

Steptoe

US Supreme Court Narrows TCPA's Autodialer Ban

By: Anthony J. Anscombe, Ashwin J. Ram, and Daniel W. Podair

Client Alert – April 2, 2021

On April 1, 2021, the US Supreme Court substantially limited the scope of the Telephone Consumer Protection Act's (TCPA) ban on automated calls and text messages by endorsing a narrow reading of the type of equipment covered under the statute.

In *Facebook, Inc. v. Duguid*, the Supreme Court held in an opinion authored by Justice Sotomayor (and joined by all other justices except for Justice Alito who concurred in the judgment but wrote separately) that to constitute an "automatic telephone dialing system" (ATDS) under the TCPA, equipment must "have the capacity either to store a telephone number using a random sequential generator or to produce a telephone number using a random or sequential number generator." No. 19-511 at 1. In doing so, the Supreme Court resolved a Circuit split as to whether the random or sequential number generator requirement applies *only* to equipment with the capacity to *produce* telephone numbers, as argued by Duguid, or whether it *also* applies to equipment with the capacity to *store* telephone numbers, as argued by Facebook. By endorsing the latter approach, the Supreme Court's ruling removes the threat of crushing statutory penalties for businesses making calls and sending text messages using technology with the capacity to store phone numbers, but not through the use of a random or sequential number generator.

Case Background

The TCPA, enacted by Congress in 1991, prohibits "using any [ATDS]" to make non-emergency calls or calls without the prior express consent of the called party to "emergency telephone line[s]," "guest room[s] or patient room[s] of a hospital," or "telephone number[s] assigned to a paging service [or] cellular telephone service." 47 U.S.C. § 227(b)(1)(A)(i)-(iii). ATDS is defined as "equipment which has the capacity—(A) to store or produce telephone numbers to be called, using a random or sequential number generator; and (B) to dial such numbers." 47 U.S.C. § 227(a)(1). The TCPA contains a private right of action and allows claimants to recover actual damages or $500 per violation, which can be tripled, at a court's discretion, for willful and knowing violations. 47 U.S.C. § 227(b)(3).

The dispute before the Supreme Court concerned a Facebook security feature that alerts users via text message of attempts to access their account from unknown devices. Despite having never signed up to receive text messages, or even a Facebook account, Duguid allegedly received numerous text message alerts from Facebook for an account associated with his phone number. In response, Duguid filed a putative class action against Facebook alleging that it violated the TCPA by sending automated text messages to phone numbers stored by Facebook each time an unknown device attempted to access an associated account. In response, Facebook argued that Duguid failed to state a claim under the TCPA because he did not allege the text messages at issue were sent using a technology with the capacity to randomly or sequentially store phone numbers per 47 U.S.C. § 227(a)(1)(A). *See generally Duguid* at 3-4.

The US District Court for the Northern District of California agreed with Facebook and dismissed Duguid's amended complaint. *Duguid v. Facebook, Inc.*, No. 15-cv-00985, 2017 WL 635117, at *3-4 (N.D. Cal. Feb. 16, 2017). However, the Ninth Circuit reversed, holding "an ATDS need not be able to use a random or sequential generator to store numbers automatically —it suffices to merely have the capacity to 'store numbers to be called' and 'to dial such numbers automatically.'" *Dugiud v. Facebook, Inc.*, 926 F.3d 1146, 1151 (9th Cir. 2019) (*quoting Marks v. Crunch San Diego, LLC*, 904 F.3d 1041, 1053 (9th Cir. 2018)).

The Supreme Court's Decision and Its Implications

In July 2020, the Supreme Court granted certiorari in *Duguid* to resolve a Circuit split with respect to their conflicting readings of an ATDS. *Compare Duran v. La Boom Disco, Inc.*, 955 F.3d 279, 283-84, 290 (2d Cir. 2020) (agreeing with the Ninth Circuit's interpretation); *Allan v. Penn. Higher Educ. Assistance Agency*, 968 F.3d 567, 579-80 (6th Cir. 2020) (agreeing with the Ninth Circuit's interpretation) with *Gadelhak v. AT&T Services, Inc.*, 950 F.3d 458, 468-69 (7th Cir. 2020) (Barrett, J.) (disagreeing with the Ninth Circuit's interpretation) and *Glasser v. Hilton Grand Vacations Co., LLC*, 948 F.3d 1301, 1306-1307 (11th Cir. 2020) (disagreeing with the Ninth Circuit's interpretation).

On April 1, 2021, the Court reversed the Ninth Circuit's decision in *Duguid* and concluded that "random or sequential number generator" modifies *both* "store" *and* "produce," as opposed to just the latter term.

First, the Court determined that reading "random or sequential number generator" to apply to *both* the terms "store" *and* "produce" adheres to the "conventional rules of grammar." Such rules, the Court argued, mandate that "'[w]hen there is a straightforward, parallel construction that involves all nouns or verbs in a series,' a modifier at the end of the list 'normally applies to the entire series.'" *Duguid* at 5 (internal citation omitted). Therefore, the Court concluded that "[i]t would be odd to apply the modifier ("using a random or sequential number generator") to only a portion of this cohesive preceding clause." *Id.* at 6. In addition, the Supreme Court focused on the presence of the comma preceding "using a random or sequential number generator," which it stated "further suggests that Congress intended the phrase 'using a random or sequential number generator' to apply equally to both preceding elements." *Id.* And finally, the Court declined to apply a number of interpretive methods advocated by Duguid, including the "rule of the last antecedent," which would be of no help to Duguid since "[t]he last antecedent before 'using a random or sequential number generator' is not 'produce'...but rather 'telephone numbers to be called.'" *Id.* at 7, 9-11.

Second, the Court concluded that "the statutory context" of the TCPA's autodialer ban mandates a narrow reading of ATDS. *Id.* at 8. The Court asserted that the TCPA's autodialer "prohibitions target a unique type of telemarketing equipment that risks dialing emergency lines randomly or tying up all the sequentially numbered lines at a single entity." *Id.* Specifically, the Court pointed to the fact that the TCPA's autodialer ban covers "'emergency telephone line[s]' and lines 'for which the called party is charged for the call'" in addition to "us[ing] an autodialer 'in such a way that two or more telephone lines of a multiline business are engaged simultaneously.'" *Id.* The Court expressed concern that a broader reading of ATDS "would take a chainsaw to these nuanced problems when Congress meant to use a scalpel" and "capture virtually all modern cell phones, which have the capacity to 'store...telephone numbers to be called' and 'dial such numbers.'" *Id.*

The Supreme Court's decision in *Duguid* will likely have significant ramifications for both TCPA litigation and compliance. The Court's narrow interpretation of "ATDS" will likely exclude many technologies used by businesses to call and send text messages to consumers. The TCPA fight may move to Congress, as the Court stated that any public desire to curb the use of telephone dialing technology that merely stores telephone numbers must be established through legislation.

For now, it is sobering to think how many companies have had to pay extortionate settlements over the last three decades, in scores of TCPA class actions, despite the presence of clear language which limited the statute's reach. The old saw that a statute should be broadly construed because it has a "remedial purpose" provides no basis to ignore the plain language of the statute. Meanwhile, the TCPA elegantly displays how the threat of crushing statutory penalties can stifle the willingness of companies to seek appellate review. It took 30 years, and a protagonist named Facebook, to obtain this decision from the Supreme Court that ultimately turned on the plain language of the statute.

Stephanie A. Sheridan

Partner

San Francisco +1 415 365 6715

ssheridan@steptoe.com

Overview

Stephanie Sheridan, who was named a *Law360* MVP in Retail & E-Commerce for the fourth consecutive year, represents retailers across the country in all aspects of litigation, as well as counseling regarding state and local laws, regulations, and agency mandates.

Stephanie's broad practice, beyond representing retailers, focuses on defending her clients in consumer class actions, website access claims, product liability, and matters involving California Business & Professions Code Section 17200 and the Consumer Legal Remedies Act. She also counsels clients on California's Proposition 65 and compliance with the mandates of the Consumer Product Safety Commission.

With her in-depth business acumen and extensive first-chair trial experience, Stephanie is known for her ability to identify prompt and creative resolutions that protect her clients' financial interests, business objectives, and customer relationships.

Her track record of defeating class certification includes the defense of a Fortune 10 company in national class actions involving allegations of consumer fraud, deceptive trade practices, warranty, and statutory claims. She has obtained dismissals of class actions against a medical device company on initial motion to dismiss; secured multiple dismissals of deceptive pricing class actions against retailers across the country, and defeated a class action on behalf of universities in consumer class actions alleging deceptive representations.

Stephanie has tried many civil jury actions to verdict, which have all resulted in defense verdicts or, in one case, a verdict that required no monetary payout from her client. Her successful defense in an alleged brain injury case was chosen by the *California Daily Journal* as one of the "Top 10 Defense Verdicts" of the year.

Stephanie also has been at the forefront of litigation related to privacy statutes and is recognized for her successful defense against FACTA (Fair and Accurate Credit Transactions Act) claims and California's Song Beverly Credit Card Act class actions.

Stephanie serves as the chair of Steptoe's Retail & E-Commerce Group and as managing partner of the firm's San Francisco office.

Bar & Court Admissions

- California
- US District Court, Central District of California
- US District Court, Eastern District of California
- US District Court, Northern District of California
- US District Court, Southern District of California
- US Court of Appeals, Fourth Circuit
- US Court of Appeals, Ninth Circuit

Education

- J.D., University of San Francisco School of Law
- B.A., San Diego State University, *magna cum laude*

Representative Matters

- Secured dismissals of multiple class actions in several states on behalf of retailers alleged to have engaged in deceptive pricing practices.
- Acted as lead national counsel for retailers and manufacturers in “no injury” consumer class actions.
- Successfully resolved and negotiated dismissals of dozens of FACTA and Song-Beverly Credit Card Act (ZIP code collection) class actions in California, as well as in other jurisdictions with similar consumer protection and privacy laws.
- Served as class action counsel for Fortune 10 company in consumer class actions in multistate matters.
- Led the defense of retailers in multi-state class action matters alleging data security and privacy violations.
- Advised clients and defended cases based on state and federal laws governing automatic-renewal and continuous service programs.
- Successfully defended several universities in consumer class actions alleging fraudulent representations about post-graduation employment opportunities, by defeating class certification.
- Active Proposition 65 practice defending retailers, fashion industry interests, and the food and nutritional supplement industry.
- Acted as national counsel for the largest domestic manufacturer of airbags for over a decade.

Noteworthy

- *Daily Journal*, Top Women Lawyers (2020)
- *Law360*, Retail & E-Commerce "MVP" (2016-2019)
- *The Recorder*, California Trailblazer (2019)
- *Super Lawyers*, Northern California, Civil Litigation: Defense (2019-2020)

- *Legal 500 US*, Dispute Resolution: Product Liability, Mass Tort and Class Actions: Toxic Tort - Defense (2019)
- *Legal 500 US*, Dispute Resolution: General Commercial Disputes (2018)
- *San Francisco Business Times*, "Most Influential Women in Bay Area Business" (2017)
- *Los Angeles Business Journal Southern California*, Apparel Awards—Law Firm Nominee (2016-2017)
- *San Francisco and Los Angeles Daily Journals*, "Top 100 Lawyers" list (2016)
- *California Daily Journal*, Top 10 Defense Verdicts of the Year

Speaking Engagements

- "Right-to-Know in the Digital Age," Retail Industry Leaders Association Retail Law Conference, October 22, 2020
- "Retail Law Transformed: New Class Action Risks in an Omnichannel Marketplace," Retail Industry Leaders Association Retail Law Conference, October 2019
- "The Future of Retail and E-Commerce – Are You Ready?," Retail Industry Leaders Association Retail Law Conference, October 2018
- "Deceptive Pricing Litigation," Retail Industry Leaders Association Retail Law Conference, October 2017
- "Shop Around: Pricing Class Action Trends," Retail Industry Leaders Association Retail Law Conference, October 2016

Professional Affiliations

- Board of Directors, Legal Momentum — the Women's Legal Defense and Fund, an organization focused on ensuring economic and personal security for all women and girls by advancing equity in education, the workplace and the courtroom
- Board of Governors, University of San Francisco School of Law

Michael Vatis

Partner

New York +1 212 506 3927

mvatis@steptoe.com

Overview

Michael Vatis is the chair of Steptoe's Privacy & Cybersecurity practice and a senior member of the appellate litigation group. Michael advises clients on compliance with US and international privacy and data security laws and regulations, data breach prevention and response, and compliance with government demands for information. He has been repeatedly cited by *Chambers* and *Legal500* as a leading practitioner in the field, and has been praised by clients as "a deep thinker [who] thoroughly analyzes issues, identifies solutions and is able to apply his analysis to business reality," and as “a great counselor” who “is realistic in his advice, takes into account business demands and has a deep knowledge of privacy regulations and enforcement.”

Michael also represents clients in appeals and in dispositive trial court motions, including in constitutional challenges to government actions, commercial disputes, and insurance coverage litigation.

Before Steptoe, Michael served eight years in the government with leading operational and policy roles in the areas of cybercrime, cybersecurity, counterterrorism, counterintelligence, and critical infrastructure protection. He was the founding head of the FBI's computer crime and infrastructure protection program; Associate Deputy Attorney General for national security matters in the Department of Justice; and Special Counsel in the Office of General Counsel at the Department of Defense, where he received the Secretary of Defense Award for Excellence.

Michael also served as the first Director of the Institute for Security Technology Studies at Dartmouth; the founding Chairman of the Institute for Information Infrastructure Protection (I3P); and Executive Director of the Markle Task Force on National Security in the Information Age.

While at Steptoe, Michael has also been involved in numerous cybersecurity and national security advisory groups. He has been a Senior Fellow at New York University Law School's Center on Law and Security; a member of the National Academy of Science/National Research Council Committee on the Policy Consequences and Legal/Ethical Implications of Offensive Information Warfare; and a member of the Commission on Cybersecurity for the 44th Presidency.

Bar & Court Admissions

- New York
- District of Columbia
- Supreme Court of the United States
- US Court of Appeals, District of Columbia
- US Court of Appeals, First Circuit
- US Court of Appeals, Second Circuit
- US Court of Appeals, Fourth Circuit
- US Court of Appeals, Fifth Circuit
- US Court of Appeals, Sixth Circuit
- US Court of Appeals, Seventh Circuit
- US Court of Appeals, Ninth Circuit
- US Court of Appeals, Tenth Circuit
- US District Court, District of Columbia
- US District Court, Southern District of New York

Clerkship

- Hon. Justice Thurgood Marshall, Supreme Court of the United States
- Hon. Ruth Bader Ginsburg, US Court of Appeals, District of Columbia

Education

- J.D., Harvard Law School, *magna cum laude;* Sears Prize Winner
- A.B., Princeton University, *magna cum laude;* Phi Beta Kappa

Representative Matters

- Regularly advise companies and non-profit organizations on privacy and cybersecurity issues, including response to data breaches and ransomware attacks and compliance with US and international laws and regulations.
- Represented producer of children's electronic learning products in class action lawsuits and FTC enforcement action arising out of data breach. Won dismissal of class action complaints and obtained favorable settlement of FTC action, and helped law enforcement apprehend hacker behind breach and secured copies of breached data. *S. v. VTech Electronics Limited* and *In Re VTech Data Breach Litigation*.
- Represent insurer in suit over damage arising from NotPetya virus, which US and other governments have attributed to Russian military intelligence. *Merck & Co., Inc., et al. v. ACE Am. Ins. Co.*
- Successfully represented child of African-American man who died after being tasered multiple times by white police officer in rural Louisiana despite not posing any safety or flight risk. Persuaded US Supreme

Court to vacate and remand Fifth Circuit decision granting officer qualified immunity from suit. *Thomas v. Nugent*.

- Successfully represented City of Durham, North Carolina in suits raising multiple constitutional and tort claims against city and its police officers arising from investigation of Duke lacrosse players for alleged rape and assault of exotic dancer. Obtained dismissal of nearly all claims in federal district court and Fourth Circuit. *Evans v. Chalmers*.
- Won unanimous decision by US Supreme Court reversing decision of Federal Circuit and holding that contracts with French companies for enriched uranium constituted the sale of goods, not of services, and were therefore covered by U.S. anti-dumping laws. This was the Supreme Court's first anti-dumping case. *S. v. Eurodif S.A.*
- Represent health care facilities, LGBTQ-services organizations, national associations of health professionals, and individual health professionals in constitutional and administrative law challenge to federal regulations repealing or limiting protections against discrimination on the basis of gender identity or sex stereotyping. *Whitman-Walker Clinic, Inc. v. U.S. Dep't of Health and Human Servs.*
- Obtained asylum for young immigrant from Democratic Republic of Congo who was the victim of severe abuse and persecution in DRC as a result of her family's political activities.
- Persuaded Sixth Circuit to interpret insurance policy as excluding all damage and loss resulting from flood in high hazard zone, unanimously reversing district court. *Federal-Mogul LLC v. Insurance Co. of Pennsylvania.*
- Wrote influential *amicus* briefs in Southern District of New York, Second Circuit, and Supreme Court concerning government's ability to use search warrant to obtain communications content stored abroad. *S. v. Microsoft Corp.*
- Represent Kohl's, Inc. in appeal to Second Circuit concerning whether the Americans with Disabilities Act requires retailers to issue Braille gift cards for visually impaired customers. *Calcano v. Swarovski N. Am. Ltd.*
- Represent United Mine Workers of America pension and benefit plans in appeals arising from bankruptcy of one of nation's largest coal mining operations. *In Re: Murray Metallurgical Coal Holdings, LLC* and *In Re: Murray Energy Holdings Co*.

Noteworthy

- *Legal 500 US*, Leading Lawyer, Media, Technology & Telecoms: Cyber Law, Including Data Protection and Privacy (2018-2020)
- *Legal 500 US*, Media, Technology & Telecoms: Cyber Law, Including Data Protection and Privacy (2017, 2019-2020)
- *Legal 500 US*, Telecoms & Broadcast: Regulatory; and Telecoms & Broadcast: Transactional (2017)
- *Cybersecurity Docket*, Named to "Incident Response 30" (2016)
- *National Law Journal*, "Trailblazers in Cybersecurity" (2015)
- *Chambers Global*, Privacy & Data Security, US (2010-2014, 2019-2021)
- *Chambers USA,* Privacy & Data Security, Nationwide (2008-2013, 2018-2020)

Speaking Engagements

- "Right-to-Know in the Digital Age," Retail Industry Leaders Association Retail Law Conference, October 22, 2020

Prior Experience

- Executive Director, Markle Task Force on National Security in the Information Age (2003-2004)
- Founding Chairman, Institute for Information Infrastructure Protection (I3P) (2001-2003)
- Director, Institute for Security Technology Studies, Dartmouth University (2001-2003)
- Founding Director, National Infrastructure Protection Center, FBI (1998-2001)
- Associate Deputy Attorney General and Deputy Director, Executive Office for National Security, US Department of Justice (1994-1998)
- Special Counsel, US Department of Defense (1993-1994)

Professional Affiliations

- Member, American Law Institute