BRANN & ISAACSON
ATTORNEYS AND COUNSELORS AT LAW

NAVISTONE®

AN ADVERTISER'S GUIDE TO DATA PRIVACY IN 2023

Written by Brann & Isaacson and sponsored by NaviStone, Inc.

TABLE OF CONTENTS

I. EXECUTIVE SUMMARY

Online sellers face an increasing risk of class action lawsuits, private attorney general actions, mass arbitrations, and federal and state enforcement actions alleging violations of privacy laws. These risks arise not only out of the ever-expanding number of new state laws targeting website privacy and regulating online practices and disclosure requirements, but out of the application of federal and state wiretapping and video confidentiality statutes, common law doctrines (including invasion of privacy), and general consumer protection laws relating to false or misleading business practices. Collectively, these laws, and the court decisions applying them, establish an expansive and growing understanding of "privacy," and, not surprisingly, the odds of businesses being caught by surprise are increasing at a dizzying pace. To date, much of the focus has been on the rapidly growing number of class actions seeking per violation penalties (principally claims under federal and state wiretapping and similar statutes) for ordinary "under the hood" website communications, but that risk is expanding to the prosecution of lawsuits seeking nationwide injunctions or the filing of numerous, simultaneous arbitration proceedings, all of which have the potential to result in extreme costs to online sellers even in the absence of any harm to consumers.

The trend towards new and expansive consumer privacy statutes adopted by states has been triggered by the activities of the major online search and social media companies such as Google and Meta/Facebook, as well as the historical inability of plaintiffs' lawyers to convince courts that consumers suffer any harm from ordinary online information collection and marketing practices. Privacy statutes allow for state enforcement actions and can open the courthouse doors because

many do not require any showing that the complained of practices have injured website visitors in any way.[1]

While the task of compliance may seem both daunting and a moving target, by understanding the multifaceted nature of their privacy obligations and risks, online sellers can implement protective measures not only to maximize compliance, but also to provide meaningful defenses to class action lawsuits and mass arbitrations as well as to demonstrate corporate good faith and due diligence in the face of government investigations. At the very least, these steps can make a company that operates a website a less appealing target in a target-rich environment. Please note, however, that this white paper is not intended to constitute legal advice and should not be relied upon as such. Because the specific facts and circumstances confronting every company are different, you should work closely with privacy counsel of your choosing in navigating these issues.

II. BACKGROUND

A. A Brief History of Online Privacy Regulation

In the United States, privacy related legal obligations have existed for over one hundred years. As early as 1890, scholars took note of the growing legal recognition of an individual right to privacy.[2] Until quite recently, the focus was on protection from the prying eyes of government

[1]For example, virtually all websites – governmental, educational, and commercial – rely on communications made by a visitor's web browser directly to third parties for purposes ranging from supporting ordinary (and expected) website functionality to participating in online and offline marketing efforts. In attacking these practices via class action lawsuits, plaintiffs' lawyers have dug up age-old anti-wiretapping laws, which provide for steep "per violation" penalties which could obviate the need to prove that any actual injury has occurred. The current targets of choice are websites that use "session replay" services, mainly because those services create what appears to be – but isn't – a "camera in the room" recording of individual visitor interactions with the site.

[2]Warren, Samuel D. and Brandeis, Louis D., "The Right to Privacy," *Harvard Law Review*, Vol. 4, No. 5 (December 15, 1890) (https://www.jstor.org/stable/1321160) (the "[i]nstaneous

and criminals, not the collection and use of information by law-abiding private businesses. That original focus led to the enactment of a series of laws, including the federal Wiretap Act of 1968, which established rules for the execution of wiretaps by law enforcement on telephonic (voice) communications and the Federal Privacy Act of 1974, which placed strict controls on the federal government's collection, use, and disclosure of personal information.

In the 1980s, the focus of privacy legislation began to tilt away from concerns about the government towards protection of personal information more generally. The Wiretap Act was amended by Congress in 1986 with the Electronic Communications Privacy Act ("ECPA") which, among other things, changed the law in four critical respects. *First*, it extended the reach of wiretapping restrictions from voice to electronic communications, *i.e.*, "signs, signals, writings, images, sound, data, or intelligence of any nature transmitted in whole or in part by wire, radio, electromagnetic, photoelectric or photo-optical systems." *Second*, it included prohibitions on access to stored communications, not just those "in transit" which were covered by wiretapping prohibitions. *Third*, it extended the statute's reach to conduct by private individuals and businesses. *Fourth*, it included a private right of action to permit individuals to sue private parties for violations of the law with significant penalties for each violation. Thirty years later, these changes became the basis of class action lawsuits against companies both offering and receiving behavioral analytic services on the World Wide Web, as discussed in greater detail below.[3]

---

photographs and newspaper enterprise have invaded the sacred precincts of private and domestic life; and numerous mechanical devices threaten to make good the prediction that 'what is whispered in the closet shall be proclaimed from the housetops.'" *Id.* at 195 (citation omitted).

[3] 1986 also brought the Telephone Consumer Protection Act which established a nationwide "do not call" registry and imposed a variety of rules and practices on companies promoting sales by phone. Among the new rules was a consumer right to "opt out" of receiving promotional telephone calls, a novel concept at the time, but one that reverberated for decades to come. It is noteworthy that, despite calls for them to do so, neither the federal government nor the states chose

What followed the 1986 amendment of the ECPA were a series of highly targeted federal privacy laws impacting commercial business practices, but no general federal privacy laws, regulations, or standards applicable to all companies. For example, 1996 brought the Health Insurance Portability and Accountability Act ("HIPAA") which, among other things, imposed on the health care industry strict rules protecting the confidentiality of patient information. HIPAA required "covered entities," including health plans and most health care providers, to provide a Notice of Privacy Practices to consumers. Two years later, Congress enacted the Children's Online Privacy Protection Act ("COPPA"), which not only imposed restrictions on the collection through *websites only* of personal information of children under the age of 13 but required the publication of COPPA-compliant privacy policies for those sites falling within the reach of the law. That same year, 1998, brought the Video Privacy Protection Act ("VPPA"), which created a civil action for the non-consensual disclosure of "personally identifiable information," which is defined to include "information which identifies a person as having requested and obtained specific video materials or services from a video tape service provider."[4] In 1999, the Gramm Leach Bliley Act ("GLBA")

---

to adopt a comparable "do not mail" registry for postal promotions, satisfied, presumably, with the industry's voluntary approach embodied in the do not mail registry established and run by the Data Marketing Association (then known as the Direct Marketing Association). https://www.dmachoice.org/register.php

[4]The VPPA was enacted in response to the disclosure of the video rental history of Judge Robert Bork, a nominee to the United States Supreme Court. See Note, "The Video Privacy Protection Act as a Model Intellectual Privacy Statute," 131 Harv. L. Rev. 1766 (2018) (available online at https://harvardlawreview.org/2018/04/the-video-privacy-protection-act-as-a-model-intellectual-privacy-statute/). If you are curious about the films rented by Judge Bork, none of which are salacious and many of which are considered among the best movies ever made, you can find it here: https://letterboxd.com/adamwaldowski/list/robert-borks-video-rental-history/ More importantly for advertisers, the VPPA has recently become the basis for class action lawsuits against online retailers and publishers, mainly because it includes a $2,500 penalty per violation and the possibility of both punitive damages and the recovery of attorneys' fees. See Germain, Thomas, "Is Every Website That Plays Videos Breaking An '80s Privacy Law?", October 15, 2022 (https://gizmodo.com/video-privacy-protection-act-class-action-lawsuits-1849660417). Websites

imposed information privacy requirements, including disclosure obligations, on financial institutions. Finally, in 2003, Congress passed the CAN-SPAM Act regulating the use of promotional emails, a statute triggered by and written to preempt a far more onerous commercial email law enacted by the State of California.

Beginning in 2018, however, the adoption of new *state* privacy statutes began in earnest and targeted the internet, seeking to fill the vacuum created by an increasingly divided and inert Congress. As explained below, these new efforts to restrict and regulate online business practices, with California leading the charge, took a page from what many perceived as an intense and overreaching European project to impose a wide range of costly and difficult privacy obligations on private business.[5] The results have been predictable: a growing welter of complex laws in different states with inconsistent definitions and obligations, some at cross-purposes with others, and each speaking its own local legislative dialect. Not only was this patchwork of locally imposed requirements on an inherently interstate commercial network exactly what the Founders hoped to avoid by granting the U.S. Congress the ultimate power to regulate trade between the states, it clashed with the core principle of the GDPR project—to create *uniform* EU privacy rules and

---

that offer video content should familiarize themselves with the VPPA and its requirements. Several states, including California, Delaware, Iowa, Louisiana, New York, and Rhode Island enacted versions of the VPPA that ban the sale of video rental records, and Michigan has extended the law to the rental, borrowing, and purchasing of books. *See* CT Gen. St. § 53-450; MD Code Art. 27 § 583; Mich. Law § 1712. Under all of these laws, a violation occurs upon the disclosure of someone's identity – a more complex concept than one might think – coupled with the titles of what they've viewed or read.

[5]As explained below, Europe's General Data Protection Regulation (or "GDPR"), which became effective in 2018, codified wide-ranging obligations on companies that collected, processed, or disclosed private information concerning citizens of the European Union. The GDPR, grounded in Europe's generally more paternalistic view of the role of government, helped to trigger the new era in statutory privacy laws in the United States and, later, across the globe.

prevent different rules from one European country to another. Even if Congress acted, however, it is unclear whether a uniform federal internet privacy law could fully displace the power of each state to protect the privacy rights of its own citizens through onerous, additive requirements. For now, the latter issue is purely academic. Comprehensive internet privacy bills have foundered in Congress almost every year for the past two decades. Just like the Beckett character facing an endless wait for the mysterious Godot, online merchants have no choice but to move forward through the ever-growing thicket of state online privacy laws while waiting for Congress to show up.[6]

B. Website Privacy

For decades, commercial websites in the United States faced targeted and limited privacy obligations, including in terms of publishing privacy policies. Both the federal government and the states took a cautious approach to regulation for a variety of reasons, including a desire not to interfere with the growth of internet commerce; a lack of technological expertise; and a consensus that voluntary practices, promoted by trade associations and industry leaders, could best address public concerns about private, commercial activity. In 2000, this began to change as California took limited steps towards a general regulation of website privacy practices, but other states did not immediately follow suit.[7] The federal government, despite dozens of attempts, failed to coalesce around federal internet privacy requirements of general applicability.

---

[6]Beckett, Samuel. 2006. Waiting for Godot. London, England: Faber & Faber ("Where I am, I don't know, I'll never know, in the silence you don't know, you must go on, I can't go on, I'll go on.").

[7]In fact, it was not until 2004 and 2005 that California took the lead in formally establishing privacy-related obligations for all websites, first under the California Online Privacy Protection Act ("CalOPPA"), Cal. Bus. & Prof. Code §§ 22575 *et seq*., which in 2004 imposed rudimentary privacy policy disclosures for all companies transacting business with California consumers and, a year later, with its "Shine the Light" law, Cal. Civ. Code 1798.83, which imposed additional

Class action lawsuits over privacy issues, now a major and growing threat facing internet sellers, began to fill the regulatory gap, commencing with groundbreaking lawsuits against DoubleClick, Inc. ("DoubleClick") over its online advertising network, as discussed below.[8] These early lawsuits, though ultimately unsuccessful, represented a shot across the bow of nascent online commerce, and their aggressive approach – using privacy claims as the engine of potentially ruinous class action lawsuits – would surface again a decade later. Understanding the *DoubleClick* lawsuit and the parallel investigation of DoubleClick by the Federal Trade Commission ("FTC") is essential to an understanding of the core principles of World Wide Web privacy, which principles have informed laws passed both by Congress and, more recently, a significant and growing number of states.

The *DoubleClick* Decision. On March 28, 2001, Judge Naomi Buchwald of the U.S. District Court in Manhattan issued her landmark and encyclopedic 71-page decision dismissing

---

disclosure obligations on companies that shared personal information. Among other things, CalOPPA required companies to disclose by category any personally identifiable information they collected, the categories of third parties with which such information was shared, an explanation of the means (if any) by which a consumer could review/change such information, and an explanation of how the website operator would notify consumers of material changes to its privacy policy. *See* https://consumercal.org/about-cfc/cfc-education-foundation/california-online-privacy-protection-act-caloppa-3/.

[8]DoubleClick was sued in a raft of simultaneous lawsuits in federal courts across the United States. *Steinbeck v. DoubleClick,* 00 Civ. 5705, C.A, N.O. 8N.O. 8:00–98 (C.D. Cal) on July 31, 2000 and *Freedman v. DoubleClick,* 00 Civ. 7194, 2:00–1559 (E.D. La) on September 22, 2000; *Healy v. DoubleClick,* 00 Civ. 0641(NRB); *Donaldson v. DoubleClick,* 00 Civ. 0696(RMB); *Wong v. DoubleClick,* 00 Civ. 1253(NRB); *Mandel v. DoubleClick,* 00 Civ. 1290(RMB); *Cohen v. DoubleClick,* 00 Civ. 1349(JSM); *Katz v. DoubleClick,* 00 Civ. 1552 (UN–RMB); *Bruce v. DoubleClick,* 00 Civ. 1572(JGK); *Gibson v. DoubleClick,* 00 Civ. v1596 (U–RMB); *Lehner v. DoubleClick,* 00 Civ. 1813 (U–NRB); *Gassman v. DoubleClick,* 00 Civ. 1897 (U–NRB); *Rand v. Doubleclick* 00 Civ. 6398(NRB). These cases were consolidated for pre-trial proceedings, and were dismissed, together, by a single federal court decision. *In re DoubleClick Inc. Priv. Litig.*, 154 F. Supp. 2d 497 (S.D.N.Y. 2001).

claims against internet marketing pioneer DoubleClick. It was a decision so granular, authoritative, and well-reasoned, that no appeal was taken despite its impact on dozens of pending cases and an army of plaintiffs' attorneys across the United States, and it would be many years before those plaintiffs' lawyers again summoned the nerve to assert privacy claims through class action lawsuits.[9] It is important to note that the *DoubleClick* lawsuit was filed on the heels of DoubleClick's acquisition in 1999 of Abacus Direct, a direct marketing service provider with a database containing the names and addresses of American consumers with associated demographic information and data about household purchasing patterns. Concerns were raised immediately by privacy groups about the possibility of DoubleClick combining anonymous "clickstream" data with names and addresses obtained via the acquisition of Abacus.[10]

---

[9]As explained below, class action lawyers started applying older laws, many written long before the modern internet, to retail websites, including laws governing wiretapping, and asserting common law claims for invasion of privacy. Many were dismissed. *See, e.g., Allen v. Quicken Loans Inc.*, No. CV1712352ESMAH, 2018 WL 5874088, at *1 (D.N.J. Nov. 9, 2018); *Cohen v. Casper Sleep Inc.*, No. 17CV9325, 2018 WL 3392877, at *1 (S.D.N.Y. July 12, 2018). Others, however, survived dismissal, and ended up settling, some for hundreds of millions of dollars, after years of costly litigation. *In re Facebook, Inc. Internet Tracking Litig.*, 956 F.3d 589 (9th Cir. 2020*), cert. denied sub nom. Facebook, Inc. v. Davis*, 141 S. Ct. 1684, 209 L. Ed. 2d 464 (2021). At the heart of many of these cases was the question of what constituted private "personal information" or the "content of communications" that was protected by law. *See, e.g., In re Zynga Priv. Litig.*, 750 F.3d 1098 (9th Cir. 2014) (finding that referrer header information, which included a social network user's unique ID, and the visited website address did not constitute protected "content" under federal wiretapping laws). A similar trend has been observed in connection with the VPPA. While class actions had previously been filed under the law against retail stores that sold or rented video products, including against Redbox, Best Buy, and Netflix (which originally rented DVDs), lawsuits have now been filed against companies that offer video content online.

[10]The FTC's resolution of the DoubleClick investigation established a bedrock principle of consumer privacy protection: the separation of "clickstream" data on the one hand from names, addresses, and other personally identifiable information ("PII") on the other. State data breach laws, enacted in the in the wake of the *DoubleClick* investigation, relied on this principle in establishing the categories of data the disclosure of which triggered a variety of compliance obligations. Although the definitions varied, they effectively enshrined the importance of segregating PII from clickstream data. Thus, as a general matter, only data breaches involving PII

At the time it was sued, DoubleClick was the largest Internet advertising service. It acted as an intermediary between websites looking to place or host online banner advertisements. It offered advertisers the ability not only to place their advertisements on select websites, but to have those advertisements presented to visitors considered most likely to be interested in their products. To provide this service, DoubleClick compiled user profiles "utilizing its proprietary technologies and analyses in cooperation with its affiliated Web sites," the court explained.[11] What was novel at the time, but became commonplace in relatively short order, was DoubleClick's use of cookies to identify website visitors as they navigated the websites of its clients and JavaScript to send information to DoubleClick about the activities of those visitors on client websites. To deliver its services, DoubleClick built profiles of these visitors (or, more accurately, profiles of the computers visiting those websites using web browsing software, including inferences regarding the users of those computers). By the time DoubleClick attracted the attention of class action lawyers and regulators, it had compiled more than 100 million individual user profiles.

The public knew little about DoubleClick and its advertising business until June 1999, when the company announced its purchase of Abacus Direct Corp. ("Abacus"). Over the years, Abacus had created profiles for roughly ninety percent of Americans including their "names, addresses, telephone numbers, retail purchasing habits, and other personal information . . . ."[12] In the wake of that acquisition, the public interest groups, the FTC, and class action lawyers took notice, and reacted with alarm that "DoubleClick planned to combine its database of online profiles

---

would trigger action under state data breach laws and a later-enacted plethora of state data breach laws. Not surprisingly, definitions of PII ended up differing from state to state.

[11] *In re DoubleClick Privacy Litigation*, 154 F.Supp.2d 497, 502 (S.D.N.Y. 2001).

[12] *In re DoubleClick Privacy Litigation*, 154 F.Supp.2d at 505.

with Abacus' database of offline customer profiles in order to create a super-database capable of matching users' online activities with their names and addresses."[13] Not long after the FTC launched an investigation, DoubleClick's CEO announced publicly that "he had made a 'mistake' by planning to merge DoubleClick's and Abacus' databases . . . ."[14] The FTC closed the investigation after finding that the information used by DoubleClick for its online advertising network "contains only no PII [personally identifiable information]" and that DoubleClick required its clients to disclose in their privacy policies their use of DoubleClick's services to target advertising to consumers.[15]

If nothing else, the *DoubleClick* lawsuits were creative. For example, they asserted claims under Title II of the federal Electronic Communications Privacy Act ("ECPA")[16], which prohibits unlawful access to certain stored electronic communications, arguing, among other things, that the placement of cookies on a consumer's hard drive constituted "hacking."[17] They also contended that, in causing communications to be sent directly from visitor's web browsers to DoubleClick, unlawful wiretapping had occurred in violation of the Federal Wiretap Act, and that DoubleClick had violated the Computer Fraud and Abuse Act ("CFAA") in what they described as gaining allegedly unlawful access to visitors' computers.[18] The CFAA claim foundered, however, because

---

[13]*Id.* (citing 18 U.S.C. § 2510, *et seq*.).

[14]*Id.*

[15]Letter from Joel Winston, Acting Associate Director, Division of Financial Practices, FTC, to Christine Varney, Esq., Hogan & Hartson, Outside Counsel for DoubleClick, January 22, 2001.

[16]18 U.S.C. § 2701 *et seq*.

[17]*In re DoubleClick Privacy Litigation*, 154 F.Supp.2d at 507.

[18]*Id.* at 514-15 (citing 18 U.S.C. § 1030, *et seq*.).

the plaintiffs could not establish that any of DoubleClick's activities had caused them to suffer any injury.

In dismissing the cases against DoubleClick, Judge Buchwald expressed skepticism about applying laws enacted *prior to the internet* to regulate the operation of the websites, particularly in the face of Congressional awareness of DoubleClick's practices and continuing debate over if and how to regulate those practices. "Indeed," Judge Buchwald wrote, "Congress is currently considering legislation that specifically recognizes and regulates the online harvesting of user information," including laws that impose "substantial notice and opt-out requirements on Web site operators *who, unlike DoubleClick, compile personally identifiable information from users*."[19] After her decision, the case promptly settled.[20] It should be noted that the recent trend in lawsuits under the VPPA might likewise be subject to Judge Buchwald's admonition, but, for now, federal courts appear unfazed in applying a law that was written to control the activities of video rental stores to websites that deliver videos online, albeit with some limits.[21]

---

[19] *Id.* at 526 (emphasis added).

[20] A copy of the settlement agreement is available online at https://epic.org/wp-content/uploads/privacy/internet/cookies/dblclkproposedsettlement.pdf. In the settlement, DoubleClick paid no money to consumers. It did, however, agree to post for a period of two years an easy-to-understand privacy policy explaining its online ad serving activities, including its use of cookies and pixel tags and offering "[r]epresentative examples of interest categories" the company uses for its Intelligent Targeting service. It also agreed to limit company access to collected data on what amounted to a "need to know basis," and to purge its log files on a weekly basis and purge all backup tapes on a quarterly basis for data that was more than three years old. More importantly, DoubleClick promised not to merge PII with non-PII "clickstream" data collected across websites until there was an agreement between government and industry on privacy standards permitting it. The plaintiffs' lawyers split a fee of $1,800,000.

[21] The VPPA also includes, among other things, the obligation to destroy personally identifiable information as soon as practicable, requiring companies who are subject to its requirements to undertake an audit and analysis of the information they collect and retain about

For its part, as discussed in greater detail below, the Federal Trade Commission ("FTC"), in addition to enforcing highly specific federal laws,[22] began examining website privacy policies and taking the first steps toward holding online retailers accountable for being truthful in any privacy-related statements they chose to make.[23] Awakened by highly publicized data breaches, dozens of states began adopting data breach notification laws, imposing numerous, often inconsistent obligations not only on internet retailers, but on every company that maintains personal information about consumers.[24]

---

those who rent, buy, or license video content from them to establish defensible rules governing the storage and retention of such information.

[22]*See, e.g., United States v. Tinyco, Inc.*, 14-cv-04165 (2014), https://www.ftc.gov/system/files/documents/cases/140916tinycocmpt.pdf.

[23]The FTC brought cases against numerous companies for failing to live up to privacy policy representations about their collection and use of visitor information, even though the posting of those policies was strictly voluntary in most instances. https://www.ftc.gov/sites/default/files/documents/cases/2012/08/120809googlecmptexhibits.pdf.

[24]By 2012, 46 states, the District of Columbia, Puerto Rico, and the U.S. Virgin Islands had enacted laws imposing reporting and disclosure requirements in the event of a data breach and requiring companies to comply with laws in effect in the states where each affected consumer lived. https://www.brannlaw.com/eyes-on-ecom-law/data-breaches-some-lessons/ Now every state has such a law.

III. THE MODERN WEBSITE PRIVACY MINEFIELD

Seizing on rising concern over and regulation of data breaches and taking a cue from Europe's enactment of the GDPR,[25] privacy rights groups used the referendum process to present to California voters radical new privacy rules far beyond what any legislature – even the California Assembly – had ever attempted. Until that time, California had taken a more hands off approach, focusing almost exclusively on disclosure, and without the punitive measures presented in the referendum, including radical new class action rights. The California Assembly took notice and shut down the referendum with a somewhat toned down, but heavily rushed alternative statute (which evolved over time into the California Consumer Privacy Act ("CCPA") that sought to balance individual privacy rights with at least a passing desire not to crush the online commerce eco-system that was a large and growing part of California's economy. These events in California set the table for today's complex privacy landscape.

A. U.S. Privacy Laws in Context: The GDPR

Back to the Future. To understand the modern U.S. privacy laws, it is important to understand its roots, including the pioneering privacy project undertaken by the European Union ("EU") and its member states. Specifically, Europe's General Data Privacy Regulation ("GDPR") led the world in a reimagining of internet privacy regulation, and one that began taking root in radically expanded state privacy laws years later in the United States. The GDPR included obligations unheard of under U.S. law, including consumer access to private data as well as a so-

[25]Indeed, as discussed below, an understanding of the GDPR is essential to understanding compliance obligations of comparable privacy laws in the United States, that sought to import its highly restrictive approach to data collection, data usage, and the handling of PII. *See* https://gdpr-info.eu.

called "right to be forgotten." An understanding of the GDPR is in many ways the best starting point for understanding the new and expanding privacy law landscape in the United States.

The EU's GDPR, enacted in 2016, and effective since May 25, 2018, was the most stringent privacy law in the world at the time of its enactment, and in many ways, retains that title to this day. As the first significant, comprehensive data privacy law, the GDPR enshrined in law core privacy principles that can be found in many subsequent privacy laws in other jurisdictions. While there are important differences between the privacy regime created by the GDPR and those that have been created in the United States, there are also broad thematic overlaps, which enable companies subject to regulation under more than one set of privacy laws the potential to leverage their GDPR compliance efforts in service of their efforts to comply with U.S. privacy laws.

GDPR Scope v. U.S. Laws. The GDPR regulates the processing of personal data that takes place within the EU, and the processing of personal data of data subjects, *i.e.*, EU consumers, regardless of where the processing takes place. "Personal data" is defined broadly as any information relating to an identified or identifiable natural person, and, like the definition of "personal information" contained in California law, for example, encompasses both directly identifying information, such as name and address, and information such as IDs or other online identifiers to the extent that identifier can be tied to an identifiable person. The GDPR imposes obligations on both data "controllers," who determine the purposes and means of processing personal data, and to data "processors," who process personal data on behalf of a controller.

As is the case with the U.S. state laws, discussed in greater detail below, the EU asserts the authority to regulate the personal data of its citizens and residents, so U.S. companies are required to analyze their business footprint to determine the extent of their exposure to EU regulatory

authority, including whether they have a substantial customer base in Europe, or substantial web traffic from Europe.

The GDPR Concept of Notice. A fundamental principle underlying the GDPR is that individuals ("natural persons," in the GDPR's parlance) have a fundamental right to the protection of their personal data. Accordingly, data should only be processed when the controller has a lawful basis for the processing. For operators of commercial websites, the most common lawful basis for processing under the GDPR is *consent* – that is, the data subject has been provided with notice of the processing and has consented to the processing. The GDPR requires that data subjects be provided with information describing data collection and processing, including the purpose for which the data is collected, the recipients of the collected data, and the basis of the collection. Importantly, the GDPR prohibits a data controller or processor from processing personal data for purposes other than the purposes for which it was originally collected (under U.S. law, it may be possible to expand such purposes by later obtaining the consent of the persons to whom the data pertains). The GDPR also imposes a duty of data minimization and purpose minimization: controllers should collect and process only the data needed for specified, lawful purposes, and maintain it for no longer than necessary or required for such purposes.

GDPR: Rights of Individual Data Subjects. The GDPR was the first privacy law to provide robust rights to individual data subjects. Several of the key data subject rights enshrined in the GDPR have echoes in the more recent U.S. privacy laws, in particular the right of access, the right of data portability, and the right to deletion (also known as the "right to be forgotten"):

Right of Access: The GDPR provides data subjects with a right to access personal data about the data subject that a data controller has collected and maintains. A data subject also has the right to request and be provided with a copy of the personal data a controller

maintains about the data subject. This right is like the rights of access provided under U.S. state law.

Right to Rectification: The GDPR provides data subjects with the right to request that personal data a controller has collected about the data subject be corrected.

Right to Erasure ('Right to be Forgotten'): The GDPR provides data subjects with the right to have their personal data deleted by a data controller, subject to certain exceptions, including where the data controller's continued preservation and processing of the personal data is necessary for the exercise of freedom of expression, or is required by law.

Right to Restrict Processing: The GDPR provides data subjects with the right to demand that the controller restrict the processing of data subject's personal information where the data subject contests the accuracy of the data or challenges the basis of the processing as unlawful.

Right to Data Portability: Under the GDPR, data subjects have the right to obtain their personal data in a portable, machine-readable format, and have the right to transmit the data to another controller.

Right to Object to Processing: The GDPR provides data subjects with the right to object to the processing of his or her personal data, including for direct marketing purposes.

Prohibition on Automated Individual decision-making, including profiling: Under the GDPR, data subjects have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning the data subject, or significantly affects the data subject.

As explained below, several of the individual data subject rights established by the GDPR can now be found in U.S. privacy laws. The rights of a data subject to request access to personal

information that a data controller has collected about the data subject, to obtain a copy of that data in a usable form, and to request that data be deleted (unless an exception applies) are core features of most recent privacy legislation in the United States. Several of the GDPR's data subject rights, including the right to restrict processing, the right to object to processing, and the prohibition on automated decision-making, do not have direct analogues in U.S. privacy law, although the right to opt-out of certain types of data sharing (*e.g.*, for targeted advertising and direct marketing) can address the same set of concerns. More substantively, some states (such as Virginia) frame the right to opt-out of targeted advertising as a right to opt-out of the processing (not sharing) of data for targeted advertising purposes. In that light, it could be deemed a "right to restrict processing for certain purposes."

Data Security Under the GDPR. The GDPR requires that data controllers and processors "implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk," to prevent unauthorized access to personal data. The greater the sensitivity of the personal data, and the greater the potential harm from unauthorized access, the more robust the required security measures will be. In the event of a data breach, the GDPR also requires notification to the relevant supervisory authority within 72 hours, and notification to the data subject without undue delay. Similar obligations apply under U.S. law, with every state having enacted some type of data breach notification law. Any company that maintains personal data must have in place a written information security program, and a data breach response plan, that will enable the organization to respond quickly to any security incident, involving legal counsel and insurance, as appropriate, and to make required notifications within the timelines established by law.

GDPR Penalties. The GDPR provides data subjects with the right to lodge a complaint against a data controller with a relevant supervisory authority and provides data subjects with the right to an "effective judicial remedy" against a controller itself. A data subject who has suffered material or non-material damage because of an infringement of the GDPR has the right to receive compensation from the controller or processor for the damage.

Although the GDPR does provide a private right of action to data subjects, private enforcement of rights through class action litigation is not a feature of EU law in the way that it is in the United States. Rather, controllers and processors subject to the GDPR can expect robust enforcement by governmental regulators, which are empowered by the GDPR to impose truly significant fines for infringements of the GDPR. The maximum administrative fines that can be imposed under the GDPR are 20,000,000 Euros, or 4 percent of global annual revenue, whichever is higher. New U.S. privacy laws feature greater regulatory enforcement power, and California, for now, limits class action lawsuits to instances involving data breaches.

GDPR: Lessons for U.S.-based Companies. U.S.-based companies, of course, should consider their own exposure to the European market, and to European regulation, to determine whether they have obligations under the GDPR. There is significant overlap between the core principles of the GDPR, including about notice, data minimization, and the implementation of systems to enable the exercise of individual data subject rights, and it is possible to build systems for compliance that address obligations under both the GDPR and U.S. privacy laws. Even companies that do not do business in Europe would do well to pay attention to privacy developments on the European continent, given the role the EU has played in setting the agenda for privacy regulation worldwide.

B. The New Wave of U.S. Privacy Laws

Against the backcloth of the GDPR, California has led the way with new and highly complex privacy laws applicable to all retail websites. In the absence of a universal, nationwide privacy law—whether in the form of a uniform code adopted by each state or a federal act passed by Congress to pre-empt competing state requirements—there exists a vacuum in the protection of consumer information that the states have begun to fill, starting with California, and spreading, in 2023, to other jurisdictions.

When coupled with other existing, albeit more narrowly-tailored privacy laws, such as Nevada's online privacy law [NRS 603A.300 *et seq.*]—not to mention data security laws cropping up from coast to coast—the trend is clear: without a uniform national law to govern consumer privacy matters, state laws will continue to pop up to fill the void—leaving companies scrambling to comply with a patchwork of varying, and perhaps competing, obligations.

i. California

California continues to be in the forefront of consumer privacy regulation in the United States. The California Consumer Privacy Act ("CCPA") [Cal. Civ. 1798.100 *et seq.*] first took effect in 2020, and California's Attorney General has been authorized to enforce the CCPA only since July 1, 2020. Despite the relative newness of the CCPA, however, California voters wasted little time adopting *another* consumer privacy law, the California Privacy Rights Act ("CPRA"). Sellers now must continue their efforts to comply with the CCPA, while preparing for the CPRA, which took effect on January 1, 2023, with an enforcement date of July 1, 2023, overseen by a new state agency, the California Privacy Protection Agency.[26]

[26]For more on the agency, *see* its website at https://cppa.ca.gov/.

The CPRA is designed to bolster the provisions of the CCPA, "further protect[ing] consumers' rights" and potentially clarifying some of the muddier compliance questions. This "CCPA 2.0" will apply to a business that collects or shares personal information about 100,000 or more households annually—double the threshold under the CCPA—or that generates more than 50% of their annual revenue from *sharing* personal information (the CCPA was previously limited to companies that *sell* personal information).

The CCPA already provides California consumers with a right to access personal information that a covered business has collected about them, a right to request that personal information be deleted, and a right to opt out of the "sale" of their personal information. The CPRA adds a consumer right to correct inaccurate personal information held by a business, and, for information collected on or after January 1, 2022, expands consumers' right-to-know beyond the current twelve-month lookback period. The CPRA also introduces the concept of "sensitive personal information" as a separate category subject to heightened protections, including usage limitations and transparency requirements. "Sensitive personal information" includes social security numbers, drivers' licenses, passport numbers and financial information, as well as precise location, racial and ethnic origin, information pertaining to religious beliefs, genetic or health information, and sex life or sexual orientation information.

Finally, the CCPA requires companies to honor consumer opt-outs of the "sale" of their personal information. Since the statute's adoption, however, there has been some debate about whether the common practice of using cookies, scripts, and other technology from third party advertising networks to serve personalized advertising across the internet constituted a "sale" of personal information subject to this opt out right. The CPRA seeks to resolve that debate, making a distinction between "cross-context behavioral advertising" (targeting advertising to a consumer

based on consumer's personal information obtained from the consumer's activity with respect to other activities or businesses) and "non-personalized advertising" (targeting advertising based solely on information obtained during a customer's current interaction with a business). Under the CPRA, California consumers are entitled to opt out of the sharing of their personal information for cross-context behavioral advertising, and businesses covered by the statute must provide consumers the option to opt in or out of marketing cookies.

ii. Virginia

Like the CPRA, Virginia's new Consumer Data Protection Act ("CDPA") [SB 1392] had a delayed start of January 1, 2023. *Unlike* the CPRA, the path to enforcement action is through the attorney general's office—only California has permitted individual consumers a limited right to police these protections.

The CDPA applies to all persons that conduct business in the Commonwealth and either (i) control or process personal data of at least 100,000 consumers or (ii) derive over 50 percent of gross revenue from the sale of personal data and control or process personal data of at least 25,000 consumers. Once triggered, the CDPA outlines specific responsibilities and privacy protection standards for data controllers and processors. Controllers are required to enter into contracts with processors to govern the processing of personal data by a processor on behalf of the controller, setting out the rights and obligations of both parties.

Virginia consumers have the right to the following, under the CDPA:

- Confirm whether the controller is processing the consumer's personal data, and, if so, can access such personal data;
- Correct inaccuracies in the personal data;
- Delete personal data;

- Request that the controller port the consumer's personal data in a readily usable format;
- Opt-out of the processing of personal data for purposes of targeted advertising;
- Opt-out of the sale of personal data; and
- Opt-out of profiling that results in legal or significant effects concerning the consumer (*such as* decisions that result in the denial of financial or lending services, housing, insurance, education enrollment, criminal justice, employment opportunities, healthcare services or access to necessities).

Consent is required to process "sensitive data" which includes racial or ethnic origin, religious beliefs, mental or physical health diagnosis, sexual orientation, citizenship or immigration status, genetic or biometric data, personal data collected from a known child, and precise geolocation data.

iii. Colorado

The Colorado Privacy Act [C.R.S. 6-1-1301] is also slated to take effect in 2023—although in July, not January. It safeguards a similar set of consumer rights, including the right to opt out of targeted advertising, the sale of personal data, and profiling (the automated processing of personal data to analyze or predict certain characteristics about an individual), as well as the right to access, correct, delete, or obtain a portable copy of one's data. The law specifically envisions the availability of a user-selected universal opt out mechanism to allow exercise of these rights but delays the effective date of this requirement until 2024 and promises technical specifications to come.

One thing that is new about the law is that it requires a company to set up an internal appeal process for denials of a consumer request. Colorado also has a few other novel aspects. For example, companies are obligated to create loyalty program disclosures, to the extent they

have a loyalty program (and many companies do) that collects information that may be subject to any of the statutory provisions. Colorado also includes the concept of a "data protection assessment," which must identify and weigh the benefits that flow from a given data processing activity to the controller, the consumer, and other stakeholders and the public, against the potential risks to the rights of the consumer associated with the processing, as mitigated by safeguards the controller can employ to reduce the risks.

It is worth noting that DPAs must be made available upon request to the Colorado Attorney General, who may evaluate them for compliance with Colorado law. As such, these assessments are effectively subject to audit. A similar risk of audit exists in Virginia, as well. Both Virginia and Colorado establish an affirmative duty of data minimization – the concept that a data controller should collect only so much data as is necessary to accomplish a specific disclosed purpose and should maintain that data only so long as necessary to accomplish the purpose.

Like Virginia, Colorado also distinguishes between the categories of data "controllers" and data "processors." Colorado carries a privacy notice requirement, mandating that a controller specify what types of personal data are collected or processed, and why; as well as how a consumer may exercise their rights.

Controllers are required to take reasonable measures to secure personal data from unauthorized acquisition. (The Colorado Attorney General's Office has recently published guidance as to data security best practices.) Indeed, a controller must conduct a data protection assessment (weighing the benefits and risks and considering mitigation measures) for all processing activities that present a heightened risk of harm to consumers, such as for purposes of targeted advertising, selling data, or processing sensitive data. As with its counterparts in Virginia

and California, sensitive data (data revealing racial or ethnic origin, health condition, sexual orientation, genetic information, or citizenship status) is subject to heightened requirements under the Colorado law. Colorado spells out an "opt in" consent condition for processing sensitive data or data concerning minors.

Paralleling Virginia, there is no private right of action, but Colorado gives local district attorneys as well as the state attorney general the ability to enforce the law—potentially expanding the number of enforcement actions by expanding the number of enforcers. For the first 18 months of the statute's effect, an enforcer must send a notice of violation and allow for a sixty-day cure period, prior to filing a lawsuit.

iv. Utah

Utah's Consumer Privacy Act (S.B. 227) applies to businesses that (i) have $25 million in annual gross revenue and (ii) process the data of at least 100,000 consumers, or businesses that process the data of at least 25,000 consumers and derive at least 50 percent of gross revenues from selling personal data. This Act is also slated to take effect in 2023—but not until December 31, 2023. Similar to the Virginia and Colorado statutes discussed above, there is no private right of action created by Utah's Consumer Privacy Act. However, the state attorney general can impose a fine of up to $7,500 per violation, so the enforcement power lies with the state.

Under Utah's statute, consumers have the following rights:

- The right to access personal data that is being processed;
- The right to delete personal data;
- The right to request that the controller port the consumer's personal data in a readily usable format;
- The right to opt out of the sale of their personal data;

- The right to opt out of processing used for targeted advertisements; and
- The right to nondiscrimination.

Utah businesses must present notice and an opportunity to opt out before collecting sensitive personal data. Sensitive personal data is defined to include racial or ethnic origin, religious beliefs, mental or physical health diagnosis, sexual orientation, citizenship or immigration status, genetic or biometric data, and precise geolocation data—identical to Virginia's definition, save for the exclusion of personal data collected from a known child.

Similar to Colorado, there is a privacy notice requirement: privacy notices provided by the business must detail the categories of personal data processed and the purposes for processing each category, how consumers can exercise their rights, the categories of data shared with third parties and the categories of third parties with whom data is shared, and information about any sale of data or targeted advertising with instructions on how to opt out. Lastly, there is also a cure period in the Utah statute, just like Colorado. The difference, however, is that Utah provides for a thirty-day cure period, and it is not limited to the first eighteen months—it extends indefinitely, unless the statute is changed.

It should be noted that Utah's consumer privacy act is considerably more relaxed and business-friendly than the others. As one example, while enforcement is vested in the attorney general, it requires a referral from the Division of Consumer Protection. As another, the right to delete extends only to data provided by the consumer to the business.

v. Connecticut

Similar to the Colorado statute, the Connecticut Data Privacy Act (Public Act No. 22-15) becomes effective on July 1, 2023. Connecticut's statute applies to any business that processes the data of at least 100,000 consumers, excluding purely payment transactions, or any business that

processes the data of at least 25,000 consumers and derives at least 50 percent of gross revenues from selling personal data. There is no private right of action created by the Connecticut Data Privacy Act, the same as every other state except for California. The enforcement power in Connecticut rests with the state attorney general, who can impose a fine of up to $5,000 for each *willful* violation under the Connecticut Unfair Trade Practices Act. It is important to note that, while other states can levy fines for any violation, Connecticut focuses on *willful* violations.

Connecticut provides consumers with the following rights:

- The right to access personal data that is being processed;
- The right to correct inaccuracies in the personal data that is processed;
- The right to delete personal data;
- The right to request that the controller port the consumer's personal data in a readily usable format;
- The right to opt out of the sale of their personal data; and
- The right to opt out of processing used for profiling and targeted advertisements.

Further, like Virginia, Connecticut business must obtain consent before processing sensitive personal data. Connecticut defines sensitive personal data identical to Virginia: racial or ethnic origin, religious beliefs, mental or physical health diagnosis, sexual orientation, citizenship or immigration status, genetic or biometric data, personal data collected from a known child, and precise geolocation data.

The Connecticut statute requires privacy notices to detail the categories of personal data and the purposes for processing, how consumers can exercise their rights and appeal, the categories of data shared with third parties and the categories of third parties with whom data is shared, information about any sale of data or targeted advertising, a clear and conspicuous link to a

webpage for opting out of processing for sales or targeted advertising, and an active email address for how to contact the business. Lastly, Connecticut has a cure period identical to Colorado: a sixty-day cure period for the first eighteen months (until January 1, 2025).

C. Enforcement of U.S. Privacy Laws

Because of the diffuse nature of U.S. privacy laws, businesses face enforcement efforts from three different directions: the FTC, state attorneys general and local district attorneys, and plaintiffs' lawyers (through a variety of channels—generally, class actions, private attorney general actions (also known as "PAGA" lawsuits), and arbitrations (including mass arbitrations, which is a growing threat).

The FTC enforcement has been targeted and relatively limited. While there are some high-profile FTC cases, most are settled quietly, and the areas of enforcement reflect shifting agency priorities over the years. In many instances, the FTC has focused its attention on holding companies to the promises they make in online privacy policies, which underscores the need for companies to audit their compliance with their published privacy policies and to modify them as needed to address evolving online information collection and marketing practices. The FTC's focus underscores one of the most important tasks facing online sellers: to clearly and accurately disclose the kinds of information it collects through its website, how it collects such information, what is done with such information, and how it is used and disclosed.

As discussed below, it is also critical that companies work with their online service providers collaboratively to ensure that these obligations are met. In many instances, service providers—and their contracts—are vague concerning important matters including how they collect and use information, and they often leave it to their clients not only to discover the answers to such questions, but how to describe those answers in their consumer-facing privacy

policies. State enforcement actions in the privacy arena are a relatively new phenomenon outside of the area of data breaches, but they are certain to increase given the wave of new legislation being enacted.

The greatest enforcement risk for online sellers arises from private enforcement through litigation and arbitration. Unlike enforcement by governmental agencies, prosecutors, and state and local government attorneys, the attorneys who pursue private enforcement are generally not moved by evidence of good corporate citizenship or even a demonstration that consumers—their clients—were not harmed in any way by a company's practices. Private actions can result in a combination of "damages" or penalties (often in extraordinary amounts irrespective of consumer harm), injunctive relief (imposing costly compliance obligations under the scrutiny of the courts, and often more onerous than those imposed in the absence of a court order), and, in the case of mass arbitrations, draconian dispute resolution fees including arbitrator compensation. These legal actions generally share a common theme: identifying and exploiting "violations" to secure large settlements from which plaintiffs' lawyers can receive a 25 percent (or greater) cut. Because of the high stakes, the private actions are generally resolved by high dollar settlements before the courts are able to address the merits of the dispute. Thus, the considerable uncertainty surrounding privacy laws and their reach is rarely clarified, which sets the backdrop for the next round of litigation or arbitration.

The bad news is that, for private plaintiffs' attorneys, there is seemingly no end to the kinds of claims they are willing to bring, using a variety of theories—and statutes—that are rife with uncertainty in terms of their application to online commerce. Their theories can include not only invasion of property, but conversion, negligence, misrepresentation, fraud, trespass, and breach of contract, some of which turn on nuances of individual state laws. They can also

seek declaratory judgments and injunctions (as reflected in the *DoubleClick* settlement discussed earlier). They often invoke laws which predate the internet—including state wiretapping laws—with novel arguments, focusing on statutes which impose flat penalties for every violation. If these cases—almost inevitably brought as class actions—survive motions to dismiss, they are propelled into costly and one-sided discovery against the defendant businesses, including depositions of employees (including high-ranking company officials) and burdensome requests for "all" electronically and physically maintained documents relating to the subject matter of the litigation. The cost of compiling, reviewing, and producing such materials—including intra-corporate communications as well as emails with vendors and service providers—can be staggering.[27]

There is some good news in that, thus far, only one state has explicitly included a private right of action in the new state wave of state privacy laws. The Virginia, Utah, and Connecticut statutes will be enforced by the state attorney general. The Colorado statute will be enforced by the state attorney general and local district attorneys. The bad news is that the one state to provide for a private right of action is California, one of the biggest markets in the country with one of the most active class action bars. And the mere fact that a federal or state law does not explicitly provide for a private right of action does not mean that clever plaintiffs' lawyers

[27]Many companies responded to the class action threat by including arbitration agreements in their online terms. Unfortunately, to be effective, such clauses must be agreed to as part of a contract with an online visitor, and consumers in privacy class actions are often mere visitors to a website who have not registered with the website or made an online purchase that could result in a binding obligation to arbitrate. Moreover, a handful of law firms representing consumers have responded to arbitration requirements by threatening to file, or filing, thousands of individual arbitrations, each of which can subject a company to thousands of dollars in arbitration fees (usually immediately due and payable). The pressure to settle in those instances is immense. Uber was recently hit with arbitration fees of $91 million when its arbitration agreement was upheld. https://www.bloomberg.com/news/articles/2022-04-19/trump-lawyer-sticks-uber-with-astronomical-arbitration-bill

cannot find a way to litigate or arbitrate privacy claims under other state laws, from wiretapping prohibitions to generic consumer protection statutes.

i. California's Private Right of Action

Under section 1798.150 of the CCPA, any consumer whose nonencrypted and nonredacted personal information is subject to an unauthorized access and exfiltration, theft, or disclosure because of a business's failure to implement and maintain reasonable security procedures and practices may file a civil lawsuit and obtain the following relief:

- The greater of actual damages or statutory damages between $100 and $750 per violation;
- Injunctive or declaratory relief; and
- Any other relief the court deems proper.

This section specifically provides for private enforcement via a class action lawsuit—although a 30-day cure provision technically permits businesses to avoid liability, and, therefore, a private lawsuit.

This provision is targeted and narrowed, limited to the amount of data breach violations based on unreasonable conduct by a business in handling personal consumer information. (Note that the CPRA will expand the private right of action somewhat, but still limit it to the data breach context.) It has nonetheless spawned a significant amount of litigation.

Two years into the CCPA experience, we now have a body of court decisions that suggest what the future may hold. The results are mixed.

On the positive side of the ledger, a federal court in northern California affirmed the core principle that the statute means what it says: CCPA class actions may only be pursued for data breach violations. *See McCoy v. Alphabet, Inc.*, Case No. 5:20-cv-05427 (N.D. Cal.). On

the negative side, data breach cases with per-violation damages, raise the specter of massive potential liability. In *Atkinson v. Minted Inc.*, No. 3:20-cv-3869 (N.D. Cal.), the plaintiff alleges the exfiltration of *73.2 million* consumer records. *See also Flores-Mendez v. Zoosk, Inc.*, No. 3:20-cv-4929 (N.D. Cal.) (30 million user records); *Rahman v. Marriott International*, No. 20-cv-654 (N.D. Cal.) (5.2 million consumers). Even "small" cases may have several hundred thousand consumer records at issue. *See Alma Fidela Cercas v. Ambry Genetics Corp.*, No. 8:20-cv-792 (C.D. Cal.)

Class action plaintiffs' counsel take an expansive view of what constitutes an unauthorized "breach," extending it to the sharing of usernames and passwords. *In re Zoom Video Communications Inc. Privacy Litig.*, No. 5:20-cv-2155 (N.D. Cal.). They will also include it in a laundry-list complaint alleging other privacy violations, such as the ones we discuss elsewhere in this paper. *See In re Ring Litig.*, No. 2:19-cv-10899 (C.D. Cal.) (one of eight causes of action). Moreover, CCPA claims may be brought in courts throughout the country, not just in California. These courts are (understandably) less familiar with California law and may issue idiosyncratic rulings as a result. A South Carolina federal court recently permitted a potential class action to go forward under the CCPA under the theory that a third-party SaaS provider developed software solutions to process the personal information of consumers shared with the service provider's customers. *See In re Blackbaud Inc., Customer Data Breach Litig.*, No. 3:20-MN-02972-JMC (D.S.C.). Given the availability of per-violation statutory penalties, we would anticipate more of these lawsuits in the future, particularly under the more expansive CPRA provisions coming into effect in 2023.

IV. CONCLUSION

Despite the complexity of today's regulatory environment, courts are starting to provide guidance that can help companies reduce their risks. For example, recent federal court decisions underscore the importance of providing notice to consumers of your information practices. These decisions evidence the fact that now, more than ever, companies should redouble their efforts to publish privacy policies in wording that is both more informative and easier for the lay person to understand. They should also give careful thought to creative ways to presenting privacy-related information and providing customers with options in terms of how they wish their information to be used. For example, companies are turning increasingly to the use of so-called "pop-ups" to provide notice to consumers about their use of cookies, the information they collect, and how that information may be used or disclosed.[28] For example, a pop-up could provide as follows, with appropriate intra-site hyperlinks (but we caution that any pop-up will need to be carefully crafted to address your specific circumstances and practices):

> If you choose to browse our website, we and selected third parties may be sent information about you and your browsing activity for purposes of advertising, marketing, and website analysis, including through cookies. To learn more about this, please read our **Privacy Policy**. By clicking **ACCEPT**, you agree to our use of cookies for these purposes. Click **DECLINE** if you wish to opt out of cookies other than those strictly necessary for the use of our website. By clicking either button below, you agree to our website **Terms and Conditions**.
>
> **ACCEPT** **DECLINE**

Companies should also take care to select and work with vendors who are committed to

[28]The use of pop-ups to address privacy issues is a recent development among websites in the United States, not taking hold in any meaningful sense until well after January 1, 2020, when California's CCPA when into effect. https://www.latimes.com/business/technology/story/2021-09-01/what-are-website-cookies-how-do-they-impact-internet-data These pop-ups are in addition to the long-established practice of including privacy policy links at the bottom of a website's home page as required by California's statutory predecessor to the CCPA, CalOPPA. CalOPPA set the standard for privacy policy disclosures from 2004 through 2019. Cal. Bus. Prof. Code § 22577.

protecting consumer privacy, and to seek out knowledgeable legal counsel both to help them navigate existing minefields and to provide notice of new obligations that are appearing on the horizon. You should carefully review with them (1) the kinds of information they obtain or collect in connection with visits to your website, *e.g.*, does it include personal information, information typed into form fields, or keystroke logging?; (2) the uses to which such information may be put, including whether it will be shared with other companies or used for purposes other than your own; (3) whether it will be shared, directly or indirectly, with other companies; and (4) the steps they have taken to keep such information secure and to comply with applicable privacy laws.

Finally, you should work closely with your own legal counsel in connection with privacy compliance. While we have provided an overview of governing laws and their developmental backdrop, this is not legal advice and should not be relied upon as such. Your privacy attorneys can work with you to address your specific business practices and assist you in developing a company-specific privacy compliance program in this rapidly changing environment.

BRANN & ISAACSON
ATTORNEYS AND COUNSELORS AT LAW

NAVISTONE®