Steptoe

February 10, 2022

Privacy in the Age of Big Data: Key Developments in Retail and E-Commerce

By Stephanie Sheridan, Meegan Brooks, and Surya Kundu

www.steptoe.com

As technological innovations in e-commerce continue to explode, retailers are increasingly utilizing customer data to personalize customer experiences, prevent fraud, improve their services, and make money through third-party sales. New data analytics tools allow retailers to study a vast array of information—ranging from users' order history to their exact mouse movements—to better understand their customer base.

With any new business strategy comes risk, and plaintiffs' attorneys are seeking huge damages by using a number of novel theories to attack companies' data practices. On top of that, legislators are (at times, very slowly) responding to concerns about how businesses use personal information by proposing new consumer privacy laws that limit the collection and sale of personal information. Below, we outline the most prominent trends in privacy litigation, highlighting the considerations companies should consider to avoid finding themselves embroiled in similar cases.

Plaintiffs Turn to Right of Publicity Laws in Suits Attacking the Sale of Customer Data

While retailers have long had to face privacy lawsuits under a variety of different laws, a deluge of new cases—nearly 40 filed since October 2021—is taking a brand-new approach, claiming the sale of customer information violates right of publicity laws.

Right of publicity laws, which exist in similar forms in many states (both in statutory and common law form), prohibit the unauthorized use of a person's identifying information for commercial gain. These statutes have traditionally been invoked by celebrities and other public figures whose names have been appropriated to falsely suggest that they endorse a product or brand. In these recent lawsuits, however, plaintiffs are alleging that retailers, publishers, and credit card companies violate their "right of publicity" merely by including their names or other identifying information on mailing lists that were privately sold or rented to third parties.

Nearly all of these recent lawsuits have been filed under the publicity laws of Illinois, California, Ohio, and South Dakota, and a look at the statutes' damages provisions may help explain why: each provides for significant statutory penalties, regardless of the damage suffered by plaintiffs. Under Puerto Rico's law, for example, the penalties are up to $20,000 per violation, and up to $100,000 where violations were deliberate or due to gross negligence. Most of the suits have been filed in the state where the defendant is based, and in many cases, plaintiffs' firms have filed several suits at once in the same court, each on behalf of a different plaintiff from a different state.

Nine of these suits have been filed against retailers, and more could be on the way. The new publicity cases are still in the earliest stages, and forthcoming developments will have massive implications for retailers' customer list sharing practices. A pivotal question is whether the right to publicity even applies when the information at issue is privately sold (i.e. without any *publicity*), and is not being used to advertise a separate product (rather, the customer information is the product being sold). Case law involving similar claims indicates that judges may be skeptical of attempts like these to stretch the scope of the right to publicity. However, if some of these cases can survive motions to dismiss, retailers who use third-party data services will be at constant risk of expensive litigation.

Retail Equation Litigation Continues

A separate series of suits has targeted well over a dozen retailers for using software produced by The Retail Equation (TRE), which, according to its website, "uses statistical modeling and analytics to detect fraudulent and abusive behavior when returns are processed at retailers' return counters." Plaintiffs in these suits generally allege that the retailers invaded their privacy and violated the federal Fair Credit Reporting Act (FCRA) and state privacy and/or consumer protection laws by sharing their information with TRE, as well as by blocking them from returning items based on erroneous results from TRE's software. The plaintiffs in these suits seek to represent broad nationwide classes of anyone whose information was transmitted by a retailer defendant to TRE.

The first of these suits, *Hayden v. Retail Equation, Inc.*, was filed in July 2020 against TRE and retailer Sephora, alleging that by sharing customer information with TRE, Sephora violated right to privacy laws, California's Unfair Competition Law, unconscionability, the Fair Credit Reporting Act, and also committed defamation. In August 2020, the First Amended Complaint added claims against TRE's parent company Appriss and 13 additional retailers.

TRE filed a motion to dismiss, which the Court granted on July 6, 2020, finding, *inter alia*, that the plaintiffs had not alleged any invasion of privacy. The Court explained:

> Although personal identification information collected by retailers at the point of sale may be subject to consumers' privacy interests, Plaintiffs fail to state a claim for violation of privacy. The Amended Complaint is simply too vague. Plaintiffs allege that the Retailer Defendants collect large amounts of data about their consumers and share the collected data with TRE without the consumers' consent, but the Amended Complaint does not specify what kind of data is collected.

The Court also dismissed the plaintiffs' FCRA claim based on its finding that TRE is not a consumer reporting agency.

On July 27, 2021, the plaintiffs in *Hayden* filed a Second Amended Complaint (SAC), but this time only against TRE, Appriss, and the eight retailers for whom there were California plaintiffs.[1] The SAC includes claims for invasion of privacy and unjust enrichment, and violations of California's Unfair Competition Law, the federal Fair Credit Reporting Act, and the California Consumer Privacy Act. In August, the claims against several of the retailer defendants were voluntarily dismissed. On September 20, 2021 and October 4, 2021, many of the *Hayden* defendants filed motions to dismiss and/or motions to compel arbitration. Those motions were set for hearing on December 10, 2021, but have been continued due to a judicial reassignment.

California Consumer Privacy Act

It has now been two years since the California Consumer Privacy Act ("CCPA") took effect on January 1, 2020, and a year and a half since state enforcement began on July 1, 2020. While more than 170 CCPA claims have been filed to date, only a handful have targeted retailers, and we are only aware of one decision in any cases involving retailers. In *Gardiner v. Walmart, Inc.*, the court held twice, on March 5, 2021, and again on July 28, 2021, that the CCPA is not retroactive, and that a plaintiff cannot state a claim based on alleged violations that took place before January 1, 2020—regardless of whether the plaintiff allegedly suffered harm from the violation after the statute took effect.[2]

Courts are continuing to determine what conduct falls within the CCPA's narrow private right of action, which applies only when a statutorily-defined subset of a California resident's "nonencrypted and nonredacted" personal information "is subject to an unauthorized access and exfiltration, theft, or disclosure as a result of the business's violation of the duty to implement and maintain reasonable and appropriate security procedures and practices." § 1798.150(a)(1). In the retail context, *Hayden v. The Retail Equation*, discussed above, could shed light on this issue. There, the plaintiffs allege that the retailer defendants' practice of sharing customer return information with The Retail Equation violated the CCPA because it constituted "unauthorized access" and disclosure of personal information. The retailer defendants moved to dismiss the CCPA claim, arguing that the CCPA does not apply when retailers authorize the disclosure of information, because that precludes it from being a data breach. The plaintiffs in Hayden withdrew their CCPA claims before the retailers' first motion to dismiss was decided,[3] but later included the identical CCPA argument in their amended complaint. The retail defendants moved to dismiss again on September 20, 2021; briefing completed on November 24, 2021.

Although the CCPA's private right of action is limited, the Attorney General's (AG) office has the ability to sue for any violation of the statute, but only after providing the company with 30 days to cure the alleged noncompliance. The AG's office has released a list of "illustrative examples of situations in which it sent a notice of alleged noncompliance," many of which involve retailers. For example:

Grocery Chain: Required consumers to provide personal information in exchange for participation in its company loyalty programs, without providing the required Notice of Financial Incentive.

Consumer Electronics Manufacturer and Retailer: Used third-party online trackers on its retail website, which shared data with advertisers about consumers' online shopping, without imposing the requisite service provider contractual relationship on these third parties.

Online Clothing Retailer: Failed to provide notice of the

[1] On July 27, 2021, the other plaintiffs from the First Amended Complaint in *Hayden* filed a new suit in the Western District of Pennsylvania, named *Hannum v. The Retail Equation*, 221CV00997CB, (W.D. Pennsylvania July 27, 2021). On September 16, 2021, the same lawyers to bring the Hayden case filed a new suit against TRE, Appriss, and two retailers.
[2] *Gardiner v. Walmart Inc.*, No. 4:20-CV-04618-JSW, 2021 WL 2520103 (N.D. Cal. Mar. 5, 2021), and 2021 WL 4992539 (N.D. Cal. July 28, 2021).
[3] *Hayden v. Retail Equation, Inc.*, No. 8:20-cv-01203-DOC-DFM, 2021 WL 5024502, at *6 (C.D. Cal. July 6, 2021).

required CCPA consumer rights, including the right to know, delete, and to not be discriminated against; did not inform consumers of how to submit requests to know and delete; and did not explicitly state whether or not it had sold personal information or transferred personal information for a business purpose in the past 12 months. **Car Dealership:** Collected information from consumers who test drove vehicles at the business, without providing a notice at collection. Its privacy policy was also deficient in a number of respects.

All of the above businesses reportedly took steps to achieve CCPA compliance within the 30-day statutory cure period, and the attorney general has not announced any fines to date.

A new, more aggressive iteration of CCPA, the California Privacy Rights Act (CPRA), will take effect in 2023, and could usher in a new wave of private and public enforcement suits. For more information about the CPRA, see our alert here.

Other Comprehensive Privacy Legislation

While the CCPA remains the most prominent comprehensive privacy law in the country, it's no longer the only one. Virginia will become the second state with comprehensive data privacy regulations when its Consumer Data Protection Act (VCDPA) takes effect January 1, 2023. The VCDPA was modeled after the CCPA and the European Union's General Data Protection Regulation (GDPR) laws, but has several notable differences from both. For example, although it adopts broad definitions of personal data (similar to CCPA and GDPR), Virginia's law would not hold data controllers or processors liable for third-party violations, unless they knew about the third party's intent to violate. Colorado became the third US state with comprehensive data privacy laws in July, when it passed the Colorado Privacy Act set to take effect on July 1, 2023. Neither Virginia nor Colorado include a private right of action in their privacy statutes.

Many other proposed state privacy laws have failed to pass, in large part due to disputes over whether or not to include a private right of action, including Connecticut and Oklahoma. But some of these states' legislatures are reviving their previous attempts. On January 11, 2022, newly revived comprehensive data privacy laws containing at least some private right of action were introduced in the Washington State Senate and in the Florida House. (though a competing proposal omitting any private rights of action was also introduced in the Florida Senate.) Similar proposals are also pending in Massachusetts, New York, and Mississippi.

Still, the majority of pending privacy laws do not include a private cause of action, including measures pending in Pennsylvania, Maryland, and Indiana. In Indiana, Senate Bill 358 was unanimously passed by the Senate on February 1, 2022; if enacted, the law would take effect on January 1, 2025.

Session Replay Litigation Is Out

One hot litigation trend from last year—concerning "session replay" technology—has practically come to a halt. Although several dozen of these cases were filed in spring and summer 2021, none have been filed in recent months. This is likely due to the fact that one of these cases, *Johnson v. Blue Nile, Inc.*,[4] is currently pending in front of the Ninth Circuit, and will resolve the question of whether the state wiretapping statutes at issue in these suits even apply to session replay technology.

Session replay technology allows a company to play back any visitor's online session—including their clicks, typing, and scrolling—often in order to make sure that websites operate properly (such as after an update, or in response to a glitch), or to make the websites easier to navigate. These cases are normally filed under California, Pennsylvania, or Florida wiretapping

statutes, based on the theory that when a consumer navigates a website, he or she is communicating with the online retailer, and that the vendors who offer session replay technology engage in "wiretapping" by intercepting those alleged communications without the customer's consent.

[4] *Johnson v. Blue Nile, Inc.*, No. 20-cv-08183-LB, 2021 WL 1312771, *1 (N.D. Cal. Apr. 08, 2021). (pending review by the 9th Cir.).
[5] *Johnson v. Blue Nile, Inc.*, No. 20-cv-08183-LB, 2021 WL 1312771, *1 (N.D. Cal. Apr. 08, 2021). (pending review by the 9th Cir.).
[6] See also *Graham v. Noom, Inc.*, No. 20-cv-06903-LB, 2021 WL 1312765, *1 (N.D. Cal. Apr. 08, 2021).

Courts thus far have generally granted defendant's motions to dismiss on the basis that using session replay technology is not wiretapping. Specifically, they have ruled that (1) online shopping is not a "communication" that can be wiretapped; (2) session replay technology vendors are not "intercepting" anything because they are directly involved in the consumer's use of the website; and (3) there is no reasonable expectation of privacy for consumers in the context of online shopping.

The court in *Johnson v. Blue Nile, Inc.*[5] held that collecting customer data through session replay technology is not an unlawful "interception" of information because Blue Nile and its software vendor were parties to separate communications with the plaintiff. That is, there were direct communications between the vendor and the plaintiff, and separate direct communications between Blue Nile and the plaintiff, rather than a single communication between Blue Nile and the plaintiff that the vendor intercepted.[6]

The *Blue Nile* case has been on appeal since August 13, 2021. The opening brief was filed on December 1, 2021, and the answering brief is not due until February 25, 2022. If the Court reverses the district court, then the wave of session replay cases is almost certain to return.

Biometric Privacy Suits Are Growing

More and more retailers have introduced virtual try-on tools that use biometric technology to recreate the fitting room experience for their online consumers. Many others use fingerprinting to track when employees clock in and out. But as the popularity of these tools grow, so does the legal risk from the growing number of biometric data privacy lawsuits. The majority of these lawsuits have been filed under Illinois's Biometric Information Privacy Act (BIPA), which is the only state biometric privacy law to provide a private right of action. Passed in 2008, BIPA prohibits a business from "collect[ing], captur[ing], purchas[ing], receiv[ing] through trade, or otherwise obtain[ing]" a person's biometric data—which plaintiffs have claimed include fingerprints, face and body scans, voice, typing style, and data regarding any other physiological or behavioral characteristics—without first providing written notice of the company's biometric data collection, retention, and storage practices and obtaining written consent. In 2019, the Illinois Supreme Court held that individuals can bring claims under BIPA even if they have not been injured by the defendant's failure to satisfy these notice and consent requirements.[7]

BIPA also requires business to "store, transmit and protect" biometric data "in a manner that is the same as or more protective than" its treatment of other confidential or sensitive information, and imposes a blanket prohibition on "sell[ing], leas[ing], trad[ing] or otherwise profit[ing] from" a person's biometric information, though other disclosures are permitted after obtaining informed consent.

Under BIPA, consumers can sue for statutory damages up to $1,000 for each negligent violation and up to $5,000 for intentional or reckless violations, making it particularly attractive to plaintiffs' firms. Likely for that reason, over 750 BIPA suits have been filed since its passage. These lawsuits typically allege that a business collected the plaintiff's data without first obtaining adequate informed consent, even if in connection with a legitimate employment function, marketing purpose, or product feature. Many of these suits have targeted retailers that offer virtual try-on features (for example, Zenni Optical and Mary Kay), makers of "smart" products (Proctor & Gamble was sued over Oral-B smart toothbrush and Subaru was sued over its DriverFocus system), and employers who use fingerprinting technology for timekeeping and security purposes. Given the steep penalties, BIPA cases often settle for millions of dollars—last year, social media giant TikTok settled a BIPA case for a whopping $92 million.

The Seventh Circuit and the Illinois Supreme Court are currently considering the appeal of *Cothron v. White Castle*,[8] and the important questions of what constitutes a "violation" for the purpose of calculating statutory damages. There, the plaintiff claimed her employer, defendant White Castle, repeatedly violated BIPA each week for nearly ten years when it collected and stored her fingerprint, which she scanned each week in order to access her weekly paystubs and sign various documents. The plaintiff argued that while she *had* initially consented to the practice in 2007, that consent was invalidated upon BIPA's 2008 passage and the new

[7] *See Rosenbach v. Six Flags Ent. Corp.*, 2019 IL 123186, 129 N.E.3d 1197 (January 25, 2019).
[8] *Cothron v. White Castle System, Inc.*, No. 20-3202 (7th Cir. 2021)

requirements therein, and sought enormous penalties based on each distinct weekly violation—even though the circumstances of each scan (and, of course, the fingerprint) were largely identical.

White Castle filed for judgment on the pleadings and, among other things, argued that defining "violation" in this manner would lead to absurd results that the legislature could not have intended. White Castle appealed the trial court's rejection denial of its motion and the Seventh Circuit held oral arguments on September 14, 2021. On December 20, 2021, the Seventh Circuit asked the Illinois Supreme Court to weigh in on the issue. The Illinois Supreme Court's forthcoming decision will have an enormous impact on the scope of defendants' liability in BIPA cases, as well as the statute's attractiveness to plaintiffs.

Other Legislation Governing Biometric Data

While BIPA remains the most frequently litigated biometric privacy statute, it's certainly not the only one. Texas (in 2009) and Washington state (in 2017) passed biometric privacy laws placing similar disclosure and protection obligations upon businesses, but permit certain limited commercial uses of biometric data after obtaining consent. Neither includes a private cause of action.

But BIPA may not hold this unique position for long. On January 4, 2022, Kentucky legislators introduced HB 32, a BIPA copycat biometric privacy law with identical provisions, including its consent requirements, prohibitions on profits, private right of action, and damages amounts. While this measure has yet to clear the initial committee stages, if passed, it could usher a second wave of cases as numerous and burdensome as the BIPA litigation. Additionally, several other states including Maryland and New York are also considering biometric laws with private rights of action, but these measures are more permissive than BIPA and may be amended as they move past the early stages of consideration.

At least two cities have jumped into the biometric fray, and passed narrower measures authorizing private causes of action. New York City's biometric privacy rule will take effect in July, and will require all food and drink establishments and places of entertainment in New York City that collect, retain, convert, store, or share "biometric identifier information" from customers to post clear, conspicuous notices near all customer entrances to their facilities. The NYC law provides a private right of action (but only after giving businesses notice and 30 days to cure) with damages ranging from $500 to $5,000 per violation, plus attorneys' fees. Portland, Oregon's ban on private businesses using facial recognition technology is already in effect and authorizes individuals to sue for $1,000 per day for each day of violation plus attorney's fees.

CONCLUSION

In this ever-digitizing world, where concepts like "the metaverse" have become household conversation topics, it's widely understood that information from nearly every transaction or piece of communication is stored by someone, somewhere. On the one hand, this offers omnilateral benefits—companies are able to receive comprehensive insights for maximizing business, and consumers receive products that are tailored to their interests. On the other hand, this proliferation of data collection has induced significant pushback.

Recently-enacted legislation aims to draw a line between acceptable uses of personal information and violations of privacy, and plaintiffs are using those laws to target companies in hopes of securing a nice payday. Understanding the facts and outcomes of recent lawsuits against companies that use technology like session replay, and biometrics, and the Retail Equation; and being familiar with the statutes at play in those cases, will go a long way toward helping executives and in-house counsel craft sensible data privacy practices