LAW360

Portfolio Media. Inc. | 111 West 19th Street, 5th floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

Privacy Litigation To Watch In 2023

By **Allison Grande**

Law360 (January 2, 2023, 12:02 PM EST) -- The recent explosion of litigation accusing a wide range of companies of violating wiretap and video privacy laws through the technology they deploy on their websites will continue to proliferate in 2023, joining robocall and biometric privacy disputes that have long plagued businesses and also show no signs of abating.

"2023 is going to be the biggest year yet in terms of privacy litigation, and there's going to be more of these cases ... than ever before," said Eric Troutman, the founder of the Troutman Firm, which specializes in Telephone Consumer Protection Act litigation and compliance work.

Here, Law360 looks at the privacy litigation and trends that bear watching this year.

Website Tracking Claims on the Rise

Class action litigation accusing major brands across an array of industries of surreptitiously eavesdropping on users through "session replay" software and chat bots deployed on their websites has taken off in recent months, fueled by rulings out of the Ninth and Third circuits that boosted statutes in California and Pennsylvania prohibiting the unauthorized interception of electronic communications.

"2022 saw an explosion of class actions claiming that session-replay technology on websites violates state wiretap laws," Michael Daly, a partner at Faegre Drinker Biddle & Reath LLP, said. "Businesses should review their practices and disclosures now if they haven't already, as this trend will continue into 2023 and perhaps beyond."

The web tracking lawsuits began flooding in after the Ninth Circuit held in its May decision in Javier v. Assurance IQ LLC that businesses must obtain prior express consent from all parties to a communication before recording under the California Invasion of Privacy Act and can't wait until after the recording has begun to obtain this permission.

The Third Circuit handed further ammunition to the plaintiffs bar in its **August decision** in Popa v. Harriet Carter Gifts Inc., which revived claims that session replay software that allows websites to track and record visitors violates Pennsylvania's anti-wiretapping law. The appellate panel concluded that there's no exemption to liability under the state law for companies that are direct parties to electronic communications and that websites can't track users' scrolling, typing and other interactions with the site without first obtaining their explicit approval.

In pushing for rehearing, defendants Harriet Carter Gifts and NaviStone Inc. **alerted the Third Circuit** in September that the panel ruling had prompted the filing of at least 10 similar lawsuits against major out-of-state companies such as Meta Inc., GameStop Inc., Expedia Group Inc. and Zillow. The argument wasn't enough to sway the Third Circuit, which **denied the rehearing bid** in October.

John A. Yanchunis, who leads the class action department at plaintiffs firm Morgan & Morgan, said much of this conduct has only been recently brought to light by privacy advocates, researchers and even former employees who have been swept up by mass layoffs at major tech companies.

"The discovery that this conduct has been occurring" has been driving these suits, Yanchunis said.

He added that plaintiffs would have found a way to go after companies for their alleged tracking

practices even without a hook like the California Invasion of Privacy Act, which allows consumers to recover damages of up to $5,000 per violation. But having that law and other state and federal wiretap statutes at their disposal provides "a greater level of certainty and solid foundation for the adequacy of these claims," according to Yanchunis.

Attorneys on both sides of the bar said that, since this strand of wiretap litigation is still in its infancy, they'll be watching closely in 2023 to see how courts receive these claims and how they come down on unresolved issues around whether these statutes are meant to cover the alleged web tracking conduct.

"These cases are going to develop the law," Yanchunis said.

The recent appellate court cases are Popa v. Harriet Carter Gifts Inc. et al., case number 21-2203, in the U.S. Court of Appeals for the Third Circuit, and Javier v. Assurance IQ LLC, case number 21-16351, in the U.S. Court of Appeals for the Ninth Circuit.

Meta Pixel Takes Center Stage

Meta Pixel, a code snippet and user tracking tool embedded in many websites, has also prompted a wave of litigation against both the companies that use the code and Meta Platforms Inc. itself.

The Atlantic, ESPN Inc., CNN parent Warner Bros. Discovery Inc., the National Basketball Association and Paramount Global are among some of the website operators across a variety of industries who **have been hit** with putative class actions in recent months for allegedly violating the Video Privacy Protection Act by disclosing private information related to users' video-viewing habits to Meta through the Pixel tool.

These lawsuits are largely being propelled by "a confluence of factors, including the plaintiffs bar's continued search for a federal privacy statute or common law vehicle to attack the ubiquitous use of cookies and other website tracking technologies that provide consumers with all of the hallmark features of the modern website," said Marshall Baker, counsel in the class actions group at Akin Gump Strauss Hauer & Feld LLP.

The plaintiffs bar appears to have found that hook in the VPPA, a statute that was enacted in 1988 in response to the disclosure of then-U.S. Supreme Court nominee Robert Bork's video rental history and prohibits the knowing disclosure of personal information that identifies an individual as having requested or obtained specific video materials. The law also allows for the recovery of $2,500 per violation.

David A. Straite, a partner at plaintiffs firm DiCello Levitt Gutzler LLC, noted that these cases are picking up steam not because the disclosure of video viewing habits is "any more egregious" than the unlawful sharing of other information but because there "happens to be a statute that requires standalone consent for the disclosure of that data."

Following a few court decisions that have refused to ax these claims, "a noticeable portion of the plaintiffs bar has gone all-in on these cases and, although it is still early, we see no slowdown on the horizon," Baker said.

As these cases move forward, attorneys will be watching to see how courts deal with the many unresolved issues raised by the plaintiffs pressing their claims under the VPPA.

These questions include "which entities can properly be said to fall within the VPPA's ambit; what, exactly, constitutes 'personally identifiable information' under the statute; and how will courts construe the VPPA's requirement that disclosures of that information be 'knowingly' made," Baker said.

Seamus Duffy, co-chair of the class action practice group at Akin Gump, added that these disputes "may not fare well, or age well, at the summary judgment or class certification stages because we think, in many cases, the actual facts adduced in the discovery process will show either that the website owner isn't engaged in the kind of business activity the statute was meant to regulate or that the underlying activity doesn't actually involve the disclosure of users' video content selections in the

way the VPPA was intended to prohibit."

"From an industry perspective, it is important because these cases challenge so much of what it means to offer a modern, aesthetically pleasing and functional website that interacts with consumers and across the web in all of the appropriate ways we are all accustomed to and expect," Duffy added.

The Meta Pixel is also at the heart of separate litigation that the social media giant is currently embroiled in over its alleged collection of confidential patient information and tax filing data.

An anonymous Maryland hospital patient launched a putative class action **in June** accusing Meta of violating the medical privacy of millions of Americans through the Pixel tool. The lawsuit claimed that the company knows — or should have known — that the web tracker is being improperly used on hospital websites, resulting in Facebook receiving such data as when a person registers as a patient, signs in to a patient portal or sets an appointment, among other information.

Meta has countered that while its Pixel tool is offered as a code that allows website developers to gather analytics information about people who visit their websites, it tells health care providers not to send Meta sensitive data.

More recently, two anonymous Facebook users hit Meta with another suit **in December** accusing the company of breaking privacy and taxpayer protection laws by collecting sensitive information from popular tax filing websites H&R Block, TaxAct and TaxSlayer through its Pixel tool.

These disputes, particularly the one related to the transfer of health care information, have "opened up a Pandora's box of data privacy issues," according to Aloke Chakravarty, a partner at Snell & Wilmer LLP.

"They've added scrutiny as to what data is made available to web beacons, how they are configured and who configures them, and the specter that more data than expected may have been incidentally captured from health care providers and more than consumers and clients may have expected," Chakravarty said.

A bulletin about online tracking technologies released by the U.S. Department of Health and Human Services' Office for Civil Rights on Dec. 1 is also poised to fan the flames of this fight, according to attorneys.

The guidance lays out the obligations of entities covered by the Health Insurance Portability and Accountability Act when using online tracking technologies like Meta Pixel or Google Analytics that collect and analyze information about how internet users interact with a regulated health provider's website or mobile app.

According to HHS, "regulated entities are not permitted to use tracking technologies in a manner that would result in impermissible disclosures of [electronic protected health information] to tracking technology vendors," an assertion that plaintiffs are likely to seize on in litigation challenging technology like the Meta Pixel on hospital websites, attorneys say.

"Plaintiffs in hospital privacy cases I imagine will cite to the HHS alert one way or another," Straite, the plaintiffs'attorney, said. "The bulletin is huge and something that privacy advocates would say is a matter of common sense, since if someone is going to a hospital website, they don't expect that their communications are getting sent to Google or Facebook."

"Someone can put a tracker on their website, but where it crosses the line is when visitors' information is then being reported to Google or Facebook without consent," Straite added. "These examples of what's happening with health and other extremely sensitive data is a way to bring public awareness to these practices."

The cases are In Re Meta Pixel Healthcare Litigation, case number 3:22-cv-03580, and Doe et al. v. Meta Platforms Inc., case number 3:22-cv-07557, both in the U.S. District Court for the Northern District of California.

States Take Lead On Robocalls, Big Paydays In Spotlight

Litigation under the Telephone Consumer Protection Act continues to proliferate after the U.S. Supreme Court in its **April 2021 ruling** in Facebook v. Duguid narrowed the types of dialing equipment covered by the federal statute. While there was an initial dip in what had been a crush of disputes, the plaintiffs bar has now shifted to claims alleging violations of the law's do-not-call list provisions and prerecorded calls, which weren't covered by the high court's ruling.

"This TCPA is still alive and well and making money for the plaintiffs bar," Troutman said.

Another shift since the Facebook decision has been an increased focus on state "mini-TCPA" laws, particularly the one in Florida that was amended in July 2021 to broaden the definition of what qualifies as an autodialer, set specific requirements for obtaining prior express written consent for automated telemarketing and texts, establish tighter new limits on the timing and quantity of call attempts, and allow for statutory damages of between $500 and $1,500 in addition to attorney fees, among other things.

"Though colloquially called 'mini' TCPAs, the laws in some states are actually broader in scope — so much broader, in fact, that their constitutionality is questionable at best," said Daly, the Faegre Drinker partner. "In the absence of a Congressional response to the Supreme Court's Facebook decision — which held that the TCPA's autodialer restrictions only apply to equipment that generates telephone numbers randomly or sequentially — this shift toward state-law claims will undoubtedly continue in 2023."

During 2023, attorneys will be watching not only the dozens of cases that have popped up under the Florida law but also whether more states move to amend or establish their telemarketing statutes.

"We're usually talking about waiting for this Supreme Court or that federal court TCPA decision," Mark Eisen, partner and co-chair of the class action practice at Benesch Friedlander Coplan & Aronoff, said. "But as each year goes on, we're looking more at what states might do and where they're trying to fill in the blanks."

As focus shifts to the states, there will still be some TPCA issues to watch in federal court, including the longstanding fight over the legality of the massive statutory damages awards that are possible under the statute, which includes minimum penalties but no cap.

"How aggressively will appellate courts reduce aggregate statutory damages awards, either on standing or excessiveness grounds, and will the Ninth Circuit's recent decision in Wakefield v. ViSalus , rejecting a $925 million verdict, gain traction in other jurisdictions?" Stroock & Stroock & Lavan LLP partner Stephen J. Newman said in reflecting on major issues to monitor.

The Ninth Circuit **in October** sent a jury's $925 million robocall award against health supplement maker ViSalus back to the lower court for reconsideration, finding that an Oregon federal judge failed to apply a test for determining if the damages are unconstitutionally excessive. Practitioners on both sides of the TCPA bar will be closely tracking what happens on remand, Daly said.

"[The TCPA's] legislative history — which shows that Congress expected claims to be pursued individually in small claims court, not collectively in class actions — makes it a perfect vehicle for challenging damages on due process grounds and challenging certification on superiority grounds," Daly added.

The TCPA damages case is Wakefield v. ViSalus Inc., case number 3:15-cv-01857, in the U.S. District Court for the District of Oregon.

Biometric Privacy Law's Parameters To Be Further Defined

Last year brought several notable developments in the growing universe of claims under Illinois' unique Biometric Information Privacy Act, including a Chicago federal jury **in October** awarding a class of BNSF Railway employees $248 million in statutory damages for collecting and using their fingerprints for identity verification at job sites without providing required notices.

Notably, the dispute hinged on the allegation that BNSF "hadn't checked all the statutory boxes under BIPA" by providing proper notice rather than on the assertion that their data had been breached or disclosed to unauthorized sources, noted Jane Metcalf, a partner in the litigation department at Patterson Belknap Webb & Tyler LLP.

"That's a result that should give everyone pause," Metcalf said. "It defies logic to make a company pay $248 million for a harmless, technical mistake."

BNSF **has urged** the court to revisit the "unprecedented" damages award, arguing that the sum is unconstitutional and clearly unreasonable given the lack of harm suffered by the class members.

Besides watching how the challenge to the massive damages award unfolds, attorneys say 2023 is poised to bring other major rulings that promise to shed light on the current plethora of unresolved issues over the scope and applicability of the statute, which has been on the books since 2008 but took nearly a decade to become a prominent fixture in the courtroom.

"At this point, we're still seeing heavy litigation on threshold issues that really scratch the surface of fundamental issues such as what's covered by the statute," Eisen said. "Unlike a statute like the TCPA, which has been pretty aggressively litigated for the past 20 years, in the BIPA context, we're still trying to find out what definitions will carry the day."

The Illinois Supreme Court is expected to rule soon on two significant disputes that have already been fully briefed and argued before the court, noted Jason Rosenthal, principal and chair of the commercial litigation group at Much Shelist PC.

In Cothron v. White Castle Systems, the high court **will decide** when a claim accrues under BIPA, while the justices in Tims v. Black Horse Carriers **have been tasked** with tackling the issue of the applicable statute of limitations for the various types of BIPA violations.

"These decisions will directly affect the scope of liability and the damages exposure for BIPA defendants," Rosenthal said. "In fact, many BIPA lawsuits have been stayed pending these two decisions."

Other issues set to be notable in the BIPA world in 2023 include the rise in BIPA claims against websites that offer virtual try-on features, the ability to obtain insurance coverage for litigation brought under the statute and whether other states will follow the example set by the Illinois law, which to date is one of three state biometric privacy statutes but the only one to contain a private right of action.

"Companies that are collecting or otherwise involved with biometric information need to review their policies to make sure they are compliant," Rosenthal said. "Additionally, other states are considering enacting legislation similar to BIPA, so it's not enough to simply monitor the Illinois law, particularly for those doing business in other jurisdictions."

The cases are Rogers v. BNSF Railway Co., case number 1:19-cv-03083, in the U.S. District Court for the Northern District of Illinois, as well as Latrina Cothron v. White Castle System Inc., case number 128004, and Tims et al. v. Black Horse Carriers Inc., case number 127801, both before the Illinois Supreme Court.

--Editing by Emily Kokoll.