WILMERHALE

Year in Review: 2023 Data Protection Litigation Trends

March 20, 2024

2023 was an active year for data protection-related litigation. Plaintiffs continued to advance creative theories of liability against businesses, using both older and more established privacy laws (such as the Telephone Consumer Protection Act and the Biometric Information Privacy Act) and newer laws (such as the California Consumer Privacy Act). Plaintiffs also continued to bring lawsuits against companies after data breaches, while also looking to explore causes of action related to companies' use of web trackers.

This client alert summarizes notable data protection-related litigation trends from 2023 in all of these categories. Businesses should continue to pay attention to these topics in 2024 (and beyond), as plaintiffs are likely to become more active in this space, especially given the imminent effective date of Washington's My Health My Data Act (which creates a private right of action for privacy violations related to consumer health data).

To stay up to date on these developments and others, please subscribe to the WilmerHale Privacy and Cybersecurity Blog.

Table of Contents

WILMERHALE

Year In Review: 2023 BIPA Litigation Takeaways

JANUARY 31, 2024

This post is part of a series of articles we are doing on 2023 data protection litigation trends. To stay up to date with our writings, please subscribe to the WilmerHale Privacy and Cybersecurity Blog.

Since its enactment in 2008, Illinois's Biometric Information Privacy Act (BIPA) has produced a wave of privacy-related litigation across the United States, and 2023 was no exception. Last year featured hundreds of new BIPA cases in both federal and state court. There were also four notable BIPA decisions by the Illinois Supreme Court, all of which will impact how the law will be interpreted in future cases.

As we explain below, many 2023 BIPA cases expand the scope of liability for entities that process biometric data pursuant to the law. These cases also continue to leave important questions unanswered, such as how the law applies to certain healthcare entities and third-party claims. It is likely that many of these issues, as well as a host of new ones, will come up in 2024 cases.

For companies that process biometric information, compliance obligations continue to grow with the introduction of new state privacy laws. For example, new state comprehensive privacy laws often regulate biometric data as "sensitive" data, and many require companies to obtain consent before processing biometric data (similar to BIPA). Additionally, Washington's My Health My Data Act (MHMDA) regulates biometric data and—like BIPA—also includes a private right of action. These new compliance obligations are, of course, on top of companies' obligations to process biometric information in Illinois in accordance with BIPA.

In this blog post, we highlight some of the key BIPA rulings and trends from 2023. We identify notable trends that companies should focus on from last year's cases and provide an analysis of some cases that showcase these trends.

BIPA Background

BIPA is a privacy law that regulates the use of biometric information like fingerprints, eye scans, voiceprints, and facial geometry scans. Section 15 of BIPA imposes various obligations on entities that interact with or process biometric data. For example, the law requires that entities obtain an individual's consent before collecting, obtaining, or disclosing that individual's biometric information. It also requires entities to develop, publicly disclose, and comply with a written data retention and deletion policy.

BIPA includes a private right of action for parties that have been aggrieved by a BIPA violation. It also includes a statutory-damages provision which states that a prevailing party may recover $1,000 or for each negligent BIPA violation and $5,000 for each intentional or reckless BIPA violation (or actual damages if they exceed these amounts). The combination of a private right of action with a statutory-damages provision has led to widespread class action litigation under the law.

A BIPA violation accrues with each unauthorized collection or disclosure of biometric information.

In arguably the most consequential BIPA decision of 2023, *Cothron v. White Castle System, Inc.*, the Illinois Supreme Court held that a BIPA violation accrues each and every time an entity collects or discloses biometric information without consent, not just the first time it does so.

In Cothron, a class of employees sued their employer—White Castle—alleging violations of BIPA. The suit focused on White Castle's fingerprint-based system that employees used to access their pay stubs and computers: The complaint alleged that White Castle collected and disclosed the employees' fingerprints without consent each time they accessed the fingerprint-based system, a practice that continued over many years.

In a 4-3 decision, the Illinois Supreme Court held that "[a] party violates … [BIPA] when it collects, captures, or otherwise obtains a person's biometric information without prior informed consent. This is true the first time an entity scans a fingerprint or otherwise collects biometric information, but it is no less true with each subsequent scan or collection." The court applied the same logic to disclosure, concluding that each unauthorized disclosure of biometric information is a distinct BIPA violation.

The majority's reasoning in Cothron suggests that an entity processing an individual's biometric information repeatedly or on a regular basis could be liable for hundreds or thousands of discrete BIPA violations. This dramatically expands the scope of liability for companies that interact with biometric data. In Cothron itself, for example, White Castle estimated that the majority's interpretation of the statute could subject it to devastating and astronomical damages awards exceeding $17 billion (the majority opinion drew a stinging dissent, joined by three justices of the court). This might explain why lawsuits asserting BIPA claims jumped by 65% in Illinois state courts following the Cothron decision. But as explained below, the decision's brief discussion of damages under BIPA may provide a small silver lining for entities that process biometric information.

For more information about the Cothron decision, see our prior blog post.

BIPA's statutory-damages provision may be discretionary, not mandatory.

Until this year, courts and commentators often assumed that BIPA's statutory-damages provision functions like a liquidated-damages clause in a contract, automatically granting plaintiffs $1,000 per negligent violation of BIPA and $5,000 per intentional or reckless violation. But several 2023 cases cast serious doubt on that assumption.

At the end of its decision in *Cothron*, the Illinois Supreme Court said that it "appears that the General Assembly chose to make damages discretionary rather than mandatory under the Act." The Court provided very little additional explanation for this conclusion and its comment was certainly dicta. But it could nevertheless profoundly change damages in BIPA cases. Lower courts have already begun to seize on this language. For example, a court recently vacated a $228 million jury award that was calculated by multiplying the number of violations by the per-violation figure provided in the statutory-damages

provision.[1] The court concluded that this calculation method was not appropriate because damages under BIPA are discretionary. So the court ordered a new trial on damages to allow a jury to determine the appropriate damages amount.

If damages under BIPA are discretionary, not mandatory, it remains unclear how a court or jury is expected to determine the proper damages award[2]. This area of BIPA case law is likely to develop quickly and could look radically different in the coming months and years.

A five-year statute of limitations applies to BIPA claims.

In February 2023, the Illinois Supreme Court clarified that individuals have five years after an alleged BIPA violation to bring their claims. In *Tims v. Black Horse Carriers, Inc.,* the Illinois Supreme Court was asked to decide which of two statutes of limitations applies to BIPA claims: (1) Illinois' one-year statute of limitations for privacy and defamation claims, or (2) Illinois's "catchall" five-year statute of limitations. The Court unanimously agreed that the general five-year statute of limitations applies. This gives plaintiffs more time to bring claims, and—particularly when considered alongside the Illinois Supreme Court's decision in Cothron—represents another case expanding the scope of liability for entities that handle biometric data.

For more information on the Tims decision, see our prior blog post.

Healthcare entities received a BIPA win in 2023.

While many of the year's BIPA decisions ruled in favor of plaintiffs and against entities that handle biometric information, healthcare entities received a favorable ruling from the Illinois Supreme Court regarding the scope of BIPA's "healthcare exemption."

Mosby v. Ingalls Memorial Hospital arose from two class-action suits brought on behalf of registered nurses against the hospitals for which they worked. In both cases, the nurses alleged that the hospitals collected their fingerprints to verify their identities before they could access a medication-dispensing system, and that the hospitals did so without first obtaining consent.

The nurses argued that BIPA's healthcare exemption excludes only patient biometric data. The court rejected that interpretation of the healthcare exemption. It unanimously concluded that the healthcare exemption excludes from BIPA's reach any information "used for a particular purpose—health care treatment, payment, or operations—regardless of the information's source." Because the nurses' biometric data was collected and used in the course of providing healthcare treatment, BIPA did not cover the hospitals' collections of biometric data.

Continuing uncertainty about third-party liability in BIPA cases.

A recurring issue in BIPA cases concerns which entity or entities may be subject to BIPA liability. Often, more than one entity touches an individual's biometric data: For example, an employer could request the biometric data of an employee but rely on a third-party vendor to collect and process biometric data. Questions then arise as to which entity or entities are properly subject to suit.

In several 2023 cases, courts held that third-party processors and vendors can be liable under BIPA, even when those entities do not directly interface with the individual who provided biometric data. For example, one court held that a third-party provider of biometric systems could be held liable, observing that "BIPA's text does not suggest a carveout for third-party vendors," and that an individual can suffer

"many individual injuries at the hands of many individual defendants who violated BIPA."[3] In another case, the court held that Amazon could be held liable even though it was a back-end service provider. Because Amazon stored face images on its cloud-based storage and used algorithms to extract and analyze the facial geometry of the images, the Court concluded that Amazon collected and possessed biometric information as defined by BIPA.[4]

But other cases in 2023 suggest a limit to the scope of third-party liability. In one case, for example, the court granted Microsoft's motion to dismiss because the company was merely "a vendor to the third-party that provided the biometric timekeeping technology and services to [the plaintiff's] employer." The court stressed that while "several courts have extended BIPA to apply to third-party providers that supply biometric collection technology and services, no case has extended BIPA to vendors for such third-party providers."[5] And in another case, the court dismissed a BIPA claim because the complaint failed to allege that Microsoft "actively obtained" the plaintiff's biometric data when Microsoft merely provided back-end cloud services for the entity that collected the plaintiff's biometric information.[6]

The extent to which different entities can be held liable often turns on fine-grained factual distinctions in the complaint. Courts carefully analyze the actions of defendants to assess whether a given entity collects, possesses, or disseminates data within the meaning of BIPA.

Courts continue to carefully parse the factual allegations made in a complaint.

In case after case in 2023, courts drew very fine distinctions between cases based on the allegations in the complaint. For standing purposes, for example, one court drew a distinction between a complaint that alleges only that the defendant profited from the use of the plaintiff's biometric data (insufficient to confer standing) and a complaint that alleges that the defendant profited and deprived the plaintiff of the opportunity to profit from their biometric data (sufficient to confer standing).[7] And in other cases, courts carefully scrutinized the allegations concerning a defendant entity's actions to determine whether the entity "collect[ed]" data within the meaning of BIPA, drawing on small differences between the complaint and existing case law to determine whether a given defendant could be held liable.[8]

Parties in BIPA litigation should recognize that even small differences in phrasing and factual allegations within a complaint can affect whether a case survives a motion to dismiss.

---

[1] *Rogers v. BNSF Ry. Co.*, No. 19 C 3083, 2023 WL 4297654 (N.D. Ill. June 30, 2023).

[2] *See, e.g., Tapia-Rendon v. United Tape & Finishing Co.*, No. 21 C 3400, 2023 WL 5228178 (N.D. Ill. Aug. 15, 2023) (recognizing that damages may be below the statutory amount of $1,000 per violation but offering no explanation of how to calculate per-violation damages).

[3] *Johnson v. NCR Corp.*, 2023 WL 1779774 (N.D. Ill. Feb. 6, 2023).

[4] *Rivera v. Amazon Web Servs., Inc.*, No. 2:22-CV-00269, 2023 WL 4761481 (W.D. Wash. July 26, 2023); *see also Kyles v. Hoosier Papa LLC*, No. 1:20-CV-07146, 2023 WL 2711608 (N.D. Ill. Mar. 30, 2023) (holding that a franchisor could be held liable even though the franchisee was principally responsible for the collection and processing of biometric data).

[5] *Jones v. Microsoft Corp.*, 649 F. Supp. 3d 679 (N.D. Ill. 2023).

[6] *Clark v. Microsoft Corp.*, No. 23 C 695, 2023 WL 5348760 (N.D. Ill. Aug. 21, 2023).

[7] *Gorgas v. Amazon.com, Inc., No. 22 CV 5159, 2023 WL 4173051 (N.D. Ill. June 23, 2023).*

[8] *See, e.g., Clark v. Microsoft Corp., No. 23 C 695, 2023 WL 5348760 (N.D. Ill. Aug. 21, 2023); Rivera v. Amazon Web Services, No. 2:22-cv-00269, 2023 WL 4761481 (W.D. Wash. July 26, 2023).*

Authors

Kirk J. Nahra

PARTNER

Co-Chair, Artificial Intelligence Practice and Co-Chair, Cybersecurity and Privacy Practice

kirk.nahra@wilmerhale.com

+1 202 663 6128

Ali A. Jessani

SENIOR ASSOCIATE

ali.jessani@wilmerhale.com

+1 202 663 6105

WILMERHALE

Year in Review: 2023 Web Tracking Litigation and Enforcement

FEBRUARY 2, 2024

This post is part of a series of articles we are doing on 2023 data protection litigation trends. To stay up to date with our writings, please subscribe to the WilmerHale Privacy and Cybersecurity Blog.

2023 saw a rise in class action litigation related to internet tracking technology employed by companies to enhance user experience. Web tools like pixel systems, chatbots, and session replay software are used by company websites to collect and analyze user activity. Plaintiffs allege in these cases, for example, that personal data was collected, shared with third parties, and monetized for targeted advertising, allegedly all without user consent. Most of these class action lawsuits were brought in California, taking advantage of various wiretapping and anti-hacking statutes in the state. Although some of these claims have made it past the motion to dismiss phase of litigation, whether these cases will ultimately be successful remains to be seen; there are substantial hurdles that will need to be met before these cases proceed (along with substantial defenses under all the relevant legal claims).

Companies use various web tracking systems to collect consumer data and optimize user experience on their websites. Pixel systems and session replay software are common web tracking devices at issue in these lawsuits. A pixel is an invisible snippet of code embedded in a website that tracks user activity. Session replay software records user interaction with a website and creates a reproduction of the user experience for the website host. These tracking systems can record data such as clicks, pages visited, keystrokes, scrolls, and information entered into forms. Also, trackers may collect user-specific data, such as IP address, location, operating system, or browser type, typically used for targeted advertising. These tracking systems are often developed by third-party vendors and sold or provided to companies for installation on their websites. In addition to these web tracking tools, companies are also increasingly offering chatbots to users to help personalize their experiences. A chatbot is a computer program installed on websites that simulates human conversation with users, often for customer service purposes. These technologies have been used routinely by companies in virtually all industries to improve how the websites function and assist users in utilizing the sites.

The class action cases implicating these web tools raise a variety of legal theories and claims. Common law claims recurring in most web tracking lawsuits include breach of contract, invasion of privacy, and larceny. Alleged violations of various California statutes are also common in these lawsuits, including the

California Invasion of Privacy Act (CIPA), Unfair Competition Law (UCL), Confidentiality of Medical Information Act (CMIA), and Comprehensive Computer Data Access and Fraud Act (CDAFA).

Courts have discussed that each lawsuit is fact-specific, and whether claims get past the motion to dismiss phase depends on allegations made by the plaintiff and factual support for the same. Courts have been grappling with similar questions, like whether data collected by tracking systems is the type of personal information these statutes are intended to protect. Courts are also split on whether vendors of tracking technology should be exempted from liability as merely an extension of website host companies. This is particularly discussed when the vendor provided the product but did not use any data for its own purposes.

On top of litigation risk, companies should also be aware that the use of web trackers is top of mind for regulators, including the Federal Trade Commission and the Department of Health and Human Services (as evidenced in this joint letter the agencies sent out last year). It is likely to continue to be an enforcement priority in 2024.

In the rest of this post, we provide an overview of the specific California laws that plaintiffs use to bring lawsuits against companies that utilize these types of web tools as well as a sampling of these cases. We are happy to answer any questions you may have about this trend.

I. California Statutes Involved in Web Tracking Class Action Litigation

a. California Invasion of Privacy Act

Most class action plaintiffs have included claims under Sections 631 and 632.7 of the California Invasion of Privacy Act. In order to receive damages under CIPA, a plaintiff must show that there was a violation of the privacy rights provided under the statute. No other separate showing of injury is required, and CIPA provides $5,000 of statutory damages for each violation of the statute.

> Liability under Section 631 of CIPA can be broken into four clauses:
>
> 1. where a person intentionally taps, or makes any unauthorized connection with, any telegraph or telephone wire, line, cable, or instrument;
>
> 2. where a person willfully, and without consent of all parties to the communication, reads, or attempts to read or to learn the contents of, a communication while it is in transit;
>
> 3. where a person uses, or attempts to use or communicate, any information obtained through clauses (1) and (2); and
>
> 4. where a person aids or conspires with any person or persons to do any of the acts or things mentioned above.

Courts have been clear that the first clause applies only to communications through telegraph or telephone wire and not to internet communications. It also does not apply to plaintiffs who accessed websites through a smartphone, which has been characterized by courts as using a phone as a computer, not as a telephone. For this reason, complaints that involve this type of website activity, rather than communicating via telephone, have been dismissed.

CIPA was designed to prevent unlawful eavesdropping. Therefore, the second clause of Section 631 contains a party exception. This exempts from liability a person who is a party to the communication at

issue because a party cannot eavesdrop on its own conversation. Some courts have granted defendants' 12(b)(6) motions to dismiss, determining the party exception applies to the third-party company providing the web tracking software. In these cases, courts characterize the third-party vendor as merely an extension of the website host's company. Additionally, some courts have applied the party exception because the third party does not access or use the data for their own purposes. Courts are split on whether use or nonuse of the data is decisive on the party exception issue.

Because of the barriers associated with the first and second clauses, litigants have sued companies under the fourth clause, alleging that the website hosts are assisting third-party technology companies in unlawful wiretapping. To succeed under the fourth clause against a website host company, a plaintiff must also adequately allege a violation of one of the first three clauses against the third-party company. Some plaintiffs have struggled to do so because of the same issues discussed above.

Litigants have also brought claims under Section 632.7, which prohibits a person from intercepting and recording a communication between two telephones. Again, this section requires that the communication be over the telephone. Therefore, in cases where individuals used smartphones to access websites, they were deemed to be using their phone as a computer rather than as a telephone. These types of claims have generally been dismissed.

b. Computer Data Access and Fraud Act

The Computer Data Access and Fraud Act is also known as California's Anti-Hacking Law. Under this statute, a person can be liable if they knowingly access a computer system or data without permission. Liability can also occur if the person uses the data to wrongfully control or obtain money, property, or data, or takes or copies that data without permission.

Courts disagree on how to define "without permission." In some cases, the fact that a plaintiff merely did not consent to access of their data does not rise to the level of liability under the CDAFA. These courts interpreted the term "without permission" to mean the defendant overcame technical or code barriers to accessing the information. In these cases, plaintiffs were unable to overcome a 12(b)(6) motion for this claim. Other times, courts took up a broader definition of "without permission" using a plain meaning approach, which allowed the claim to survive.

c. Unfair Competition Law

Litigants suing under California's Unfair Competition Law may run into issues with standing. The UCL grants standing when a person suffers an injury in fact and has lost money or property because of the defendant's unfair competition. Therefore, there must be a showing of economic injury caused by the unfair business practice. It is helpful to plaintiffs that the Ninth Circuit previously held that users' browsing history had a specific financial value. However, to survive a 12(b)(6) motion to dismiss, plaintiffs must allege specific factual allegations of the economic value of their data. In general, UCL claims do not appear to be successfully moving past the motion to dismiss phase in web tracking class action lawsuits

d. Confidentiality of Medical Information Act

The California Confidentiality of Medical Information Act prohibits the unauthorized disclosure and negligent preservation of medical information. Plaintiffs must claim their medical information was disclosed without consent and that it was improperly viewed or accessed. Some CMIA claims may survive the motion to dismiss phase if the pleading contains factual support for the plaintiff's belief that their data

was improperly viewed, like in *Doe v. Regents*, discussed below. Otherwise, assumptions that data was improperly accessed will likely cause a CMIA claim to be dismissed.

II. Example Cases

a. Healthcare Entities

Many cases involving healthcare entities concern pixel systems installed on these entities' websites and patient portals. Plaintiffs complain that these pixels collect sensitive patient information and then transmit that personal health information to the third-party vendor that provides the pixel technology, without patient consent.

In *Cousin v. Sharp Healthcare*, plaintiffs alleged that Sharp Healthcare disclosed patient health information through a pixel tracking tool on its website. The plaintiffs' complaint included five causes of action: (1) breach of fiduciary duty; (2) violation of common law privacy intrusion against seclusion; (3) invasion of privacy under the California Constitution; (4) violation of CMIA; and (5) violation of CIPA.

In this case, the court discussed some of the issues with the plaintiffs' complaint, including that the complaint was missing factual support for plaintiffs' contention that their personal information was disclosed. In addition, the court questioned whether data about researching doctors, looking for providers, and searching for medical specialists is considered protected health information. Because of these pleading defects, the court dismissed all claims. In this case, the court also addressed damages in regard to the plaintiffs' invasion of privacy claim and stated that California's constitutional provision protecting the right of privacy supports a cause of action for an injunction, but not a private right of damages.

In *Doe v. Regents of University of California*, the plaintiff made similar claims regarding use of pixel tracking. The plaintiff asserted that she entered data into her patient portal related to heart issues and high blood pressure and later received targeted advertisements related to her conditions on her social media, including one for high blood pressure medication. The plaintiff's CIPA claim was dismissed because the defendant is a public entity and therefore had immunity. However, the plaintiff's CMIA, common law intrusion against seclusion, and breach of implied contract claims all made it past the defendant's motion to dismiss. The court remarked that the plaintiff's allegation regarding the targeted advertising she saw provided plausible factual support for a CMIA claim. Additionally, when discussing the plaintiff's intrusion against seclusion claim, the court observed that personal medical information is some of the most sensitive information about an individual, suggesting that this data is the type that should be protected. In regard to damages, the court in Regents also determined that the plaintiff could only seek an injunction, not monetary damages, for claims falling under Article 1, Section 1, of the California Constitution.

b. Retail Companies

Chatbots are often used on retail company websites to allow customers to ask customer service questions. In *Swarts v. Home Depot*, a plaintiff alleged that Home Depot recorded his conversation with a chatbot without his consent, in violation of wiretap laws. Here, the plaintiff's claims included violations of CIPA, UCL, and the Wiretap Act. Because of the barriers discussed above with CIPA, the CIPA claims were dismissed with leave to amend. The plaintiff's UCL claim was dismissed with no ability to amend, because the court determined that the plaintiff could not meet the threshold requirements for UCL, including an economic injury.

Session replay software reproduces, for the website host, users' interactions on the website, including movements, clicks, page visits, scrolling, and keystrokes. Several class action lawsuits against retail companies involve the use of session replay. For example, in *Love v. Ladder Financial, Inc.*, plaintiffs sued both Ladder Financial (Ladder) and FullStory (the vendor of the session replay software), alleging that Ladder used FullStory's session replay tool to collect data in a way that constituted wiretapping. The plaintiffs alleged violations of CIPA and UCL, and invasion of privacy under the California Constitution. Both Ladder and FullStory filed motions to dismiss, which were both granted on January 11, 2024. The plaintiff has since filed an amended complaint against Ladder.

Authors

Kirk J. Nahra

PARTNER

Co-Chair, Artificial Intelligence Practice and Co-Chair, Cybersecurity and Privacy Practice

kirk.nahra@wilmerhale.com

+1 202 663 6128

Samantha J. Kanekuni

ASSOCIATE

samantha.kanekuni@wilmerhale.com

+1 202 663 6135

Ali A. Jessani

SENIOR ASSOCIATE

ali.jessani@wilmerhale.com

+1 202 663 6105

WILMERHALE

Year in Review: 2023 TCPA Litigation

FEBRUARY 15, 2024

This post is part of a series of articles we are doing on 2023 data protection litigation trends. To stay up to date with our writings, please subscribe to the WilmerHale Privacy and Cybersecurity Blog.

The Telephone Communications Privacy Act (TCPA) has always been a hotbed for privacy litigation, especially given the prevalence of companies' use of marketing communications and the law's private right of action for certain violations. 2023 saw an increase in TCPA-related litigation compared to the previous year. This potentially indicates that plaintiffs are looking to test new theories of liability against companies despite the Supreme Court's 2021 decision in *Facebook v. Duguid*.

The TCPA makes it unlawful for a person to place calls to cellular and certain specialized telephone lines using an automated telephone dialing system ("ATDS") without prior consent (and the consent standard is heightened for marketing or promotional calls).[1] The Supreme Court's decision in *Duguid* severely limited claims under the TCPA by narrowing the definition of what constituted an ATDS.[2] In that case, the Court considered whether the TCPA encompasses any device that can "store" and "automatically dial" telephone numbers, even if the device "does not use a random or sequential number generator.[3] The Supreme Court agreed with Facebook (now Meta), confirming that an ATDS refers to equipment that either stores telephone numbers randomly or sequentially, or produces telephone numbers randomly or sequentially.

In the years since, plaintiffs have been searching for other paths to establish liability for TCPA violations with varying levels of success. 2023 featured the Ninth Circuit as a leading voice in shaping the post-*Duguid* landscape, while some disagreements at the district court level teed up interesting questions on how far reaching the Supreme Court's definition of an ATDS is. There was particular focus on footnote 7 of *Duguid*, which plaintiffs hoped would reopen the pathways to liability. That footnote potentially expands the definition of an ATDS to include many predictive dialers, but plaintiffs have had mixed success thus far with these claims.

This blog post summarizes a few of the most notable TCPA cases from 2023. We will continue to keep you posted on notable TCPA developments through the WilmerHale Privacy and Cybersecurity Blog.

***Trim v. Reward Zone USA, LLC*, 76 F.4th 1157 (9th Cir. 2023)**

The Ninth Circuit upheld the dismissal of a putative class action suit against Reward Zone USA, LLC. The lawsuit alleged that the company sent several unsolicited text messages, which the plaintiffs claimed was a "prerecorded voice message" as prohibited by the TCPA. The plaintiffs argued that the use of "voice" in the statute should be read broadly to mean "an instrument or medium of expression," because the statute is remedial and had been significantly compacted by *Duguid*.[4] Plaintiffs had amended their complaint to include this new theory after the Supreme Court handed down Duguid. Plaintiffs also argued that their position was supported by the FCC. Defendants filed and were granted a 12(b)(6) Motion to Dismiss for failure to state a claim.[5]

The court affirmed the motion to dismiss in a unanimous opinion, holding that the statutory text is unambiguous and the statutory scheme clear. The court's opinion was based in "the ordinary meaning of voice" and "the statutory context of the TCPA."[6] Text messages do not count as "artificial or prerecorded voices" because they are not audible sounds.[7] Further, reading "voice" to include text messages would make other statutory provisions duplicative or nonsensical.[8] The panel held that since Congressional intent was clear, it did not need to consider the other interpretative tools offered by the plaintiffs in support of their position.[9]

***Pascal v. Concentra*, 2023 WL 2929685, (9th. Cir. 2023) (cert. denied).**

Reward Zone was not the only Ninth Circuit decision to narrow the potential reach of the TCPA. The Ninth Circuit issued a brief affirmance in *Pascal v. Concentra* dismissing the plaintiffs' claims that Concentra violated the TCPA when it sent out job recruitment text messages to people on a pre-produced list. The lawsuit was another putative class action filed before Facebook shifted the TCPA landscape, forcing plaintiffs to find new theories of liability.

Defendant Concentra used the online texting service Textedly to send text messages specifically targeted to physical therapists in California. Defendant uploaded a list of phone numbers, which were then assigned a sequential ID number in Textedly's database. Concentra used Textedly to simultaneously send marketing text messages to an entire class of ID numbers which included Pascal. Plaintiff argued that Concentra used an ATDS to send its marketing text messages because Textedly stored sequentially generated ID numbers, as prohibited by the TCPA.[10]

The court disagreed; a device that uses a "sequential number generator" to store numbers only qualifies as an ATDS if it sequentially generates telephone numbers. The court came to a similar conclusion in *Borden v. eFinancial*, LLC in 2022, holding that a device that generates sequential identifying numbers while dialing was not an ATDS.[11] Pascal fully forecloses any possibility that the TCPA outlaws sequentially or randomly generating anything other than a telephone number.

***Perrong v. Bradford*, 2023 WL 6119281 (E.D. Penn. 2023)**

Some plaintiffs have tried to take advantage of an ambiguous footnote in Facebook. Footnote 7 of the opinion leaves open the possibility that an ATDS could "use a random number generator to determine the order in which to pick phone numbers from a preproduced list."[12]

The plaintiff in *Perrong v. Bradford* alleged that Bradford, a state legislator, used an ATDS and a prerecorded voice to place five phone calls to his phone number. Bradford provided a preproduced list to a third-party, Cleo, LLC, who placed the calls. Plaintiff alleged that this violated the TCPA because Cleo called the numbers sequentially. Defendants filled a 12(b)(6) Motion to Dismiss for failure to state a claim.

The court granted the motion to dismiss the claims based on the use of an ATDS. A system must generate the numbers dialed; it cannot simply pull the numbers from an imported list. The court did not cite to Footnote 7 in its memorandum. The court's opinion also noted that Bradford was not engaged in telemarketing for purposes of the FCPA.

***Scherrer v. FPT Operating Company*, 2023 WL 4660089 (D. Colo. 2023)**

Federal courts were not unanimous in adopting the strict view of Footnote 7. The U.S. Federal Court for the District of Colorado did not agree with the Eastern District of Pennsylvania and broadly construed the Act. Appellants and Amici Curiae in *Reward Zone and Pascal* used this opinion to support their arguments.[13]

Class action plaintiffs in *Scherrer v. FPT Operating Company* survived a motion to dismiss after alleging a device that selected numbers from at imported list at random was an ATDS. The complaint alleged that FPT used an "automatic dialing system to automatically call lists of leads." According to plaintiffs, the system can generate and store random or sequential telephone numbers, then call in the stored order.[14]

The court found these allegations sufficient to "state a claim of relief that is plausible on its face."[15] The order denying the motion to dismiss made extensive reference to Footnote 7.[16] Despite admitting that the footnote was dicta, the court relied on the Supreme Court's reasoning "based on its recency and due to the dearth of controlling precedent on point."[17]

---

[1] 47 U.S.C. § 227(b)(1)(A).

[2] 592 U.S. 395 (2021).

[3] *Id*. at 398 (internal alterations omitted).

[4] *Trim*, 76 F.4th at 1163.

[5] *Id*. at 1160.

[6] *Id*. at 1161.

[7] *Id*.

[8] *Id*. at 1162.

[9] *Id*. at 1163.

[10] *Pascal v. Concentra, Inc.*, 2021 WL 5906055 at 1-3 (N.D. Cal. 2021).

[11] *Borden v. eFinancial, LLC*, 53 F.4th 1230 (9th Cir. 2022).

[12] *Facebook*, 592 U.S. at 407, n. 7

[13] *See Trim v. Reward Zone*, 2023 WL 8601417 (U.S.) (brief in support of petitioner); *Pascal v. Concentra, Inc.*, 2023 WL 5606641 (U.S.) (supplemental brief of petitioner).

[14] *Scherrer*, 2023 WL 4660089 at 5.

[15] *Id*. at 2 (internal quotations omitted).

[16] *Id*. at 2-4.

[17] *Id*. at 3.

Authors

Kirk J. Nahra

PARTNER

Co-Chair, Artificial Intelligence Practice and Co-Chair, Cybersecurity and Privacy Practice

kirk.nahra@wilmerhale.com

+1 202 663 6128

Aaron W. Cheese

ASSOCIATE

aaron.cheese@wilmerhale.com

+1 202 663 6027

Ali A. Jessani

SENIOR ASSOCIATE

ali.jessani@wilmerhale.com

+1 202 663 6105

WILMERHALE

Year in Review: CCPA Litigation Trends from 2023

MARCH 1, 2024

This post is part of a series of articles we are doing on 2023 data protection litigation trends. To stay up to date with our writings, please subscribe to the WilmerHale Privacy and Cybersecurity Blog.

While the California Consumer Privacy Act (CCPA) is most known for its onerous privacy compliance obligations, the law also provides for a limited private right of action for certain data breaches. Section 1798.150(a)(1) of the CCPA allows consumers to sue a business if consumers' "nonencrypted and nonredacted personal information" is subject to unauthorized access and exfiltration, theft, or disclosure caused by a business's failure to "implement and maintain security procedures and practices." Cal. Civ. Code. § 1798.150(a)(1). Damages available to consumers under this private right of action provision can be as high as $750 per violation. Courts can also provide consumers injunctive or declaratory relief and "any other relief the court deems proper." Cal. Civ. Code. § 1798.150(a)(1)(B) and (C).

Plaintiffs have been testing this provision since the law went into effect in 2020, and 2023 was no different. In this article, we look at some notable litigation trends in cases brought under the California Consumer Privacy Act (CCPA) last year. Our key takeaways from the cases we reviewed involve the following include the following:

1. Courts analyzed companies' specific privacy practices to determine if the data breach alleged in the lawsuit was a result of the company's "failure to implement and maintain reasonable security procedures and practices," as required by the CCPA.
2. Courts looked for substantial compliance with the CCPA's right to cure provision, which provides companies with the opportunity to "cure" alleged violations before an affected consumer can bring a lawsuit against the company for violation of the CCPA.
3. While most cases where the CCPA's private right of action is implicated involve a true data breach, consumers do not necessarily need to prove that a data breach occurred in order to move forward with a claim.

We have provided additional details on each of these takeaways below.

In addition to the law's private right of action, companies should also be aware of CCPA enforcement by the California Attorney General ("California AG") (and eventually by the California Privacy Protection Agency (CPPA)). The California AG's office recently brought its second announced enforcement action

under the law. It is likely that both the California AG and CPPA will significantly expand their enforcement actions under the law in the coming months.

To stay up to date on any of these developments, please subscribe to the WilmerHale Privacy and Cybersecurity Blog.

2023 CCPA Litigation Trends

1. Cases discussing a business's "failure to implement and maintain reasonable security procedures and practices"

Throughout the year, courts pointed to a wide array of different actions (or lack thereof) that demonstrated businesses' "failure to implement and maintain reasonable security procedures and practices." See Cal. Civ. Code. § 1798.150(a)(1).

For example, in *Durgan v. U-Haul Int'l Inc.*, No. CV-22-01565-PHX-MTL, 2023 WL 7114622 (D. Ariz. Oct. 27, 2023), the Court ruled that the Plaintiffs, who are customers of U-Haul, has sufficiently pleaded a violation of § 1798.150(a) by alleging that U-Haul International should have "destroyed the data it no longer had a reasonable need to maintain or only stored data in an Internet-accessible environment when there was a reasonable need ... to do so and with proper safeguards." Plaintiffs also identify fourteen cybersecurity best-practices that Defendant should have followed but allegedly did not. The court also found that plaintiffs have sufficiently shown a causal connection between Defendant's purported failure to implement reasonable security procedures and the hackers' ability to infiltrate plaintiffs' personal information. For example, if U-Haul had utilized an adequate filtering software, the phishing emails that caused the data breach would never have reached the employees' inboxes.

2. Cases implicating the CCPA's right to cure

Courts also addressed the CCPA's right to cure provision. §1798.150 of the CCPA requires an affected consumer to give a business thirty days' notice of a CCPA violation before initiating any lawsuit for individual or class-wide statutory damages. See Cal. Civ. Code. § 1798.150(b). If the business actually cures the noticed violation and informs the consumer in a written statement that the violations have been cured and no further violations will occur, the CCPA bars an individual or class-wide statutory damages action against the business.

It is important for businesses to *actually* cure the violations. In *Florence v. Ord. Express, Inc.*, No. 22 C 7210, 2023 WL 3602248 (N.D. Ill. May 23, 2023), the Court found that, instead of curing the alleged violation in response to consumer's notice, Defendant Order Express enhanced its security measures which amounted to the "implementation and maintenance of reasonable security procedures and practices"—rather than a cure—under § 1798.150(b). The Court also found that Order Express' response to consumer's notice did not explain how its enhanced security measures actually cured the alleged CCPA violation. For example, Order Express did not encrypt consumer's personal identifying information or delete the information it no longer needed to maintain on its internet-accessible network.

Simply stating that the violation has been cured is not enough to prevent consumers from raising a CCPA claim in court. In *Prutsman v. Nonstop Admin. & Ins. Servs.*, Inc., No. 23-CV-01131-VC, 2023 WL 5257696 (N.D. Cal. Aug. 16, 2023), the Court denies Defendant Nonstop Administration & Insurance Service's argument that plaintiffs have failed to state a claim because Nonstop has already cured the

alleged violations. Stating that the violations have been cured, however, “does not render implausible the plaintiffs’ allegations to the contrary.”

Another court made a distinction between circumstances where a notice is required and where it is not. In *Guy v. Convergent Outsourcing, Inc.*, No. C22-1558 MJP, 2023 WL 4637318 (W.D. Wash. July 20, 2023), the Court clarifies that a pre-suit notice is not required where a consumer is seeking non-statutory damages. However, a pre-suit notice is required if a consumer is seeking statutory damages.

If a consumer sends a CCPA violation notice, companies should provide the complaining consumer with a written statement stating that the violations have been cured, explaining the steps taken to cure the violations, and assuring that no further violations will occur.

3. Cases that do not explicitly allege a data breach

A pair of cases against Wells Fargo in the Southern District of California indicate that the unauthorized access of a consumer’s personal information, even when not subject to true “data breach”, is sufficient to bring a claim under the CCPA’s private right of action.

In *Alexander v. Wells Fargo Bank, N.A.*, No. 23-CV-617-DMS-BLM, 2023 WL 8358550 (S.D. Cal. Dec. 1, 2023) and *Ramos v. Wells Fargo Bank, N.A.*, No. 23-CV-0757-L-BGS, 2023 WL 5310540 (S.D. Cal. Aug. 17, 2023), the Court disagreed with Wells Fargo that Plaintiffs failed to bring a claim under the CCPA because they did not allege that their information was disclosed as the result of a data breach. The Court held in *Ramos* that "[Wells Fargo] does not point to any authority that would require Plaintiff to plead that there was a data breach,” and found that Plaintiff sufficiently pled a claim under CCPA. Ramos, No. 23-CV-0757-L-BGS at 2. In both cases, Plaintiffs sufficiently pleaded a CCPA violation by alleging that, because of Wells Fargo’s failure to properly maintain Plaintiffs’ nonredacted and nonencrypted information, unknown individuals accessed and withdraw funds from their Wells Fargo bank accounts without Plaintiffs’ knowledge, permission, or authorization. *Ramos*, No. 23-CV-0757-L-BGS at 2; *Alexander*, No. 23-CV-617-DMS-BLM.

Associate Arabi Hassan co-authored this blog post.

Authors

Kirk J. Nahra

PARTNER

Co-Chair, Artificial Intelligence Practice and Co-Chair, Cybersecurity and Privacy Practice

kirk.nahra@wilmerhale.com

+1 202 663 6128

Ali A. Jessani

SENIOR ASSOCIATE

ali.jessani@wilmerhale.com

+1 202 663 6105

Year in Review: Top 2023 Data Breach Litigation Trends

MARCH 15, 2024

This post is part of a series of articles we are doing on 2023 data protection litigation trends. To stay up to date with our writings, please subscribe to the WilmerHale Privacy and Cybersecurity Blog.

One of the main risks that a company faces after a data breach is a potential lawsuit. Plaintiffs often will allege creative statutory and common law theories of harm after they learn that their personal information has been subject to a breach. However, one of the initial hurdles that plaintiffs face is meeting the standing requirement under Article III for federal court actions. This is particularly challenging for plaintiffs that have not experienced any actual misuse of their data at the time of filing their lawsuit. They rely instead on the argument that they face a substantial risk of *future harm*, which is sufficient for standing. This argument has faced challenges in federal courts, especially after the Supreme Court's 2021 decision in *TransUnion v. Ramirez*, which ruled that a risk of future harm alone is not enough to establish standing to sue for damages. The Court left open the possibility, however, that a risk of future harm could confer standing if it also caused some other concrete harm to the plaintiffs, such as emotional distress, financial losses, or mitigation costs.

Since then, some federal circuit courts have adopted this reasoning and allowed data breach plaintiffs to proceed with their claims for damages, while others have dismissed them for lack of standing. This post examines data breach litigation cases in 2023, with a specific focus on how courts have evaluated standing claims that have implicated the *TransUnion* decision.

In light of the increasing number of data breaches, companies should pay close attention to data breach litigation trends. While the Supreme Court's *TransUnion* decision made it harder for plaintiffs to establish standing based on a mere risk of future harm, some lower courts have found ways to allow such claims to proceed if the risk has caused some other concrete injury. Companies should be aware of these developments and take proactive steps to prevent data breaches, mitigate their impact, and prepare to defend against potential lawsuits.

To stay up to date on these developments, please subscribe to the WilmerHale Privacy and Cybersecurity Blog.

Background

Plaintiffs in data-breach cases often sue before their breached data is misused. To establish standing in federal court, they often do not claim an actual injury, but a risk of future identity theft or fraud. The Supreme Court's 2021 decision in *TransUnion v. Ramirez* appeared to deal a blow to such plaintiffs; it held that the risk of future harm alone cannot support standing to sue for damages.[1] But three federal circuit court decisions—one in 2022[2] and two in 2023[3] —have revived the hopes of plaintiffs who claim a risk of future harm. These decisions have held that data-breach plaintiffs have standing to seek damages based on an imminent risk of future identity theft or fraud, if that imminent risk has already caused them some separate, concrete harm.[4]

To establish standing to sue in federal court, plaintiffs need to show that they have suffered an injury in fact, traceable to the defendant, and redressable by *the relief sought*. An injury in fact, in turn, must be concrete and either actual or imminent. In 2023, data-breach decisions focused on this injury in fact requirement, as plaintiffs continued to sue before actually suffering an injury, claiming instead a substantial risk of future harm. While such a risk can confer standing to sue *for injunctive relief*, the Supreme Court made clear in *TransUnion v. Ramirez* that mere risk alone cannot support standing to seek *retrospective damages*.[5] The Court suggested, however, that the "risk of future harm" could give rise to standing in an action for damages where the risk "itself causes a *separate* concrete harm."[6]

Overview of Notable 2023 Data Breach Litigation Decisions

In 2023, the First and Second Circuits seized on this suggestion from *TransUnion*, holding that a plaintiff who has established an imminent risk of future identity theft or fraud can sue for damages where they separately establish a present, concrete harm arising from the risk of future injury.[7] Among other theories discussed below, the First and Second Circuits concluded that plaintiffs already suffered concrete harms because they spent time and money mitigating the risks that their breached data will be misused. These decisions bring the First and Second Circuits into alignment with the Third Circuit's 2022 decision in *Clemens v. ExecuPharm Inc.*[8]

A 2023 decision by the Seventh Circuit, by contrast, indicated that, after TransUnion, the risk of future data misuse can only support standing to seek injunctive relief, and never a suit for damages.[9]

The Eleventh Circuit also weighed in. While the Eleventh Circuit reasoned that after TransUnion, "a mere risk of future harm, without more, does not give rise to Article III standing for recovery of damages," the panel held that the publication of plaintiffs' data on the dark web constituted a present, concrete injury.[10]

The rest of this article provides additional details on these cases, focusing on the "concreteness" and "imminence" prongs of the standing test that these decisions focused on.

1. Concreteness

The First and Second Circuits—as well as district courts across the country—advanced several different theories for how plaintiffs can demonstrate a present, concrete harm based on a future risk of identity theft or fraud.

- **Mitigation Costs.** The most widely accepted theory—embraced by both the First and Second Circuits—is that plaintiffs suffer a concrete harm when they spend time and money mitigating the risk of identity theft and fraud.[11] Notably, one district judge used a defendant's offer to pay for

credit monitoring services as evidence that a plaintiff's decision to take additional mitigation actions was reasonable.

- **Emotional Distress.** Courts disagreed on whether emotional distress caused by the risk of identity theft can constitute a concrete harm. In *Whitfield v. ATC Healthcare Services, LLC*, a district court in Brooklyn held that the plaintiff established standing based on the anxiety, sleep disruption, and fear she experienced because of her "financial security concerns."[13] But in *Florence v. Order Express, Inc.*, a district court in Chicago—which otherwise held that the plaintiffs had standing—concluded that emotional distress based on fear of future harm is too abstract to confer standing.[14]
- **Public Disclosure of Private Facts.** In *TransUnion*, the Supreme Court analyzed whether plaintiffs alleged a concrete injury by considering whether their harms bore a "'close relationship' to a harm 'traditionally' recognized as providing a basis for a lawsuit in American courts."[15] The *TransUnion* Court specifically found that plaintiffs whose inaccurate credit reports were shared with third parties had established a concrete injury, because those plaintiffs "suffered a harm with a 'close relationship' to the harm associated with the tort of defamation."[16] Pointing to *TransUnion*, some courts, including the Second Circuit, reasoned that the "exposure" of personal information "to unauthorized third parties" constitutes a present, concrete harm because it bears a relationship to the common-law tort of public disclosure of private facts.[17]

2. Imminence

Before plaintiffs can establish a separate, concrete harm based on the imminent risk of identity theft or fraud, they must show that the risk is in fact imminent. In evaluating imminence in the data-breach context in 2023, federal courts have continued to apply the three factors first summarized by the Second Circuit in *McMorris v. Carlos Lopez & Associates*: (1) whether the data was intentionally hacked, (2) whether the data is especially sensitive, and (3) whether some portion of the dataset has already been misused.[18]

- **Whether the data was intentionally hacked.** Where hackers target a database to steal personal information, courts are "more willing to find a likelihood of future identity theft or fraud."[19] Where, by contrast, a thief steals a laptop, its not as obvious that the thief's purpose is to misuse personal data stored on the computer—the thief may simply want the laptop.[20]
- **Whether the data is especially sensitive.** Courts have reasoned that when breached data is highly sensitive and difficult to change (e.g., a Social Security number), plaintiffs are more vulnerable to identity theft, and therefore the risk is more imminent.[21] The lack of sensitive data can defeat standing, as one 2023 district court decision shows. In *Perkins v. CommonSpirit Health*, a district court in Chicago dismissed a putative class action in part because the breached data "consisted only of non-sensitive demographic information," and not the kind of "sensitive information, such as social security numbers and credit card information that would make future losses not only possible but imminent."[22]
- **Whether some portion of the dataset has already been misused.** Courts have differed significantly in the weight they assign this factor. In *Bohnak v. Marsh*, the Second Circuit found an imminent risk even where plaintiffs failed to show that any breached data had actually been misused or even published on the Dark Web.[23] A district court in Kansas, by contrast, treated the lack of any misuse as dispositive, holding that "[w]ithout any misuse to date, … the risk of future injury [is] too attenuated to establish standing."[24] And one district court decision in Puerto

Rico suggested a middle ground: while actual misuse of some of the dataset is not required, the court held, the plaintiff had still failed to show imminence because "she does not allege that the information has actually been put for sale or otherwise published."[25]

---

[1] 594 U.S. 413, 436 (2021).

[2] Clemens v. ExecuPharm Inc., 48 F.4th 146 (3d Cir. 2022).

[3] Webb v. Injured Workers Pharmacy, LLC, 72 F.4th 365 (1st Cir. 2023); Bohnak v. Marsh & McLennan Cos., 79 F.4th 276 (2d Cir. 2023).

[4] *Webb*, 72 F.4th at 376; Bohnak, 79 F.4th at 286; Clemens, 48 F.4th at 155-56.

[5] *TransUnion*, 594 U.S. at 435-36.

[6] *Id.* at 436.

[7] *Webb*, 72 F.4th at 376; Bohnak, 79 F.4th at 286.

[8] *See Clemens*, 48 F.4th at 155-56.

[9] Dinerstein v. Google, 73 F.4th 502, 515 (7th Cir. 2023).

[10] Green-Cooper v. Brinker International, Inc. (11th Cir. 2023).

[11] *Webb*, 72 F.4th at 376; *Bohnak*, 79 F.4th at 286; *see also* Whitfield v. ATC Healthcare Services, LLC, 2023 WL 5417330 *4 (E.D.N.Y. Aug. 22, 2023); Florence v. Order Express, Inc., 2023 WL 3602248 *6 (N.D. Ill. May 23, 2023).

[12] *Florence*, 2023 WL 3602248 at *6.

[13] *Whitfield*, 2023 WL 5417330 at *4.

[14] *Florence*, 2023 WL 3602248 at *6.

[15] *TransUnion*, 594 U.S. at 424.

[16] *Id.* at 432.

[17] *Bohnak*, 79 F.4th at 285-86; *Florence*, 2023 WL 3602248 at *5 ("Since disclosure of private information is a sufficiently close common-law analogue for Plaintiff's alleged harm, the injury is concrete."); Miller v. Syracuse University, 2023 WL 2572937 *8-9 (N.D.N.Y. Mar. 20, 2023).

[18] 995 F.3d 295, 301-03 (2d Cir. 2021).

[19] *Bohnak*, 79 F.4th at 288.

[20] Farley v. Eye Care Leaders Holdings, LLC, 2023 WL 1353558 *3 (M.D.N.C. Jan. 31, 2023).

[21] Webb, 72 F.4th at 376.

[22] 2023 WL 6520264 *2 (N.D. Ill. Oct. 5, 2023).

[23] *Bohnak*, 79 F.4th at 289 ("We recognize that Bohnak … has not alleged any known misuse of information in the dataset accessed in the hack. But … such an allegation is not necessary to establish

that an injury is sufficiently imminent to constitute an injury in fact."); *see also Clemens*, 48 F.4th at 154 ("[M]iuse is not necessarily required.").

[24] Masterson v. Ima Financial Group, Inc., 2023 WL 8647157 *8 (D. Kan. Dec. 14, 2023); *see also* McCombs v. Delta Group Electronics, Inc., 2023 WL 3934666 *5 (D.N.M. June 9, 2023) (dismissing for lack of standing where "over a year has passed since the data breach and McCombs fails to allege that any of the compromised PII—whether hers or that of the proposed class—has been misused")

[25] Rivera-Marrero v. Banco Popular de Puerto Rico, 2023 WL 2744683 * 12 (D.P.R. Mar. 31, 2023).

Authors

Kirk J. Nahra

PARTNER

Co-Chair, Artificial Intelligence Practice and Co-Chair, Cybersecurity and Privacy Practice

kirk.nahra@wilmerhale.com

+1 202 663 6128

John Barna

ASSOCIATE

john.barna@wilmerhale.com

+1 202 663 6004

Ali A. Jessani

SENIOR ASSOCIATE

ali.jessani@wilmerhale.com

+1 202 663 6105