

iapp



US Data Privacy Litigation Report 2026

Table of contents

Introduction.....	ii	Part 4: The Video Privacy Protection Act.....	30	Part 7: Daniel's Law and public officials' privacy....	50
Overview.....	v	Consent to disclosure under the VPPA.....	31	New Jersey's Daniel's Law	50
Part 1: Breach of contract and warranties.....	1	When is a defendant a video tape service provider?.....	31	How can entities comply with Daniel's Law?	51
Breach of express contract.....	2	Which consumers have a cause of action under the VPPA?.....	32	Part 8: Shareholder actions.....	52
Breach of implied contract.....	2	When does a VTSP knowingly disclose PII?	35	What is a shareholder derivative action?	52
Breach of express warranty.....	2	What qualifies as PII under the VPPA?	35	Derivative actions based on privacy incidents	53
Breach of implied warranty.....	2	Putting VPPA compliance into practice	36	A growing role	53
Courts see an implied contract to protect personal information collected as a condition of employment.....	3	Part 5: The California Consumer Privacy Act private right of action.....	38	Contacts.....	54
Plaintiffs less successful in the absence of consideration.....	3	What claims can plaintiffs allege under the private right of action?.....	39		
Third party terms: Device-level permission and non-signatory enforcement of contracts.....	4	What does it mean to be a consumer?.....	39		
The wording of policies and terms can limit or defeat claims.....	5	What qualifies as personal information?	39		
Warranty claims fail when nonexistent or expired.....	6	What is a business?.....	39		
Courts may find enforceable contracts but no breach of privacy	6	What is a security breach?.....	40		
Courts at the pleading stage hesitate to determine contract validity.....	7	Reasonable security procedures and practices ..	41		
The consent defense	7	Exceptions and exemptions	42		
How do businesses avoid breach of contract and warranty claims?	9	Damages	42		
Part 2: The California Invasion of Privacy Act.....	11	Notice and cure	42		
Section 631(a): The eavesdropping provision.....	12	Private right of action settlements.....	43		
Section 632: The recording device provision.....	18	Conclusions and takeaways.....	43		
Section 632.7: The telephone provision.....	20	Part 6: Biometrics and consumer health data.....	45		
Section 638.51: The pen register provision.....	21	BIPA requirements	46		
Part 3: The Federal Wiretap Act	24	BIPA definitions and exclusions	46		
When is prior consent obtained?.....	25	BIPA exemptions	46		
A party to a communication is safe from direct liability.....	26	Scope of BIPA's private right of action.....	47		
An exception to an exemption: The crime-tort exception	27	Notable BIPA settlements.....	47		
How businesses can mitigate Wiretap Act liability.....	28	Washington state's My Health My Data Act	48		
		New York's Biometric Privacy Act.....	49		
		Conclusion.....	49		

Introduction

Understanding how plaintiffs assert their privacy rights, how defendants contest liability, and how the courts interpret and apply privacy laws to new and emerging uses of data and technology is essential for organizations of every shape and size. Increasingly, individuals and certified classes of ordinary citizens are asserting their privacy rights around an assortment of issues at the frontiers of digital governance, from web tracking to data breaches to biometric privacy.

It is critical for organizations to understand recent trends in privacy litigation to better position themselves and adjust compliance practices to reduce enterprise risks stemming from data collection, processing and use. Litigants alleging privacy violations are not only grounding their claims in newer state privacy laws, such as the California Consumer Privacy Act, Washington state's My Health My Data Act and New Jersey's Daniel's Law, but they are also marshalling long-standing privacy statutes like the California Invasion of Privacy Act against modern-day data uses. In sum, this report acknowledges the significance of private litigation and class-action lawsuits in contesting privacy violations in the U.S., tracking the trends and distilling compliance insights.

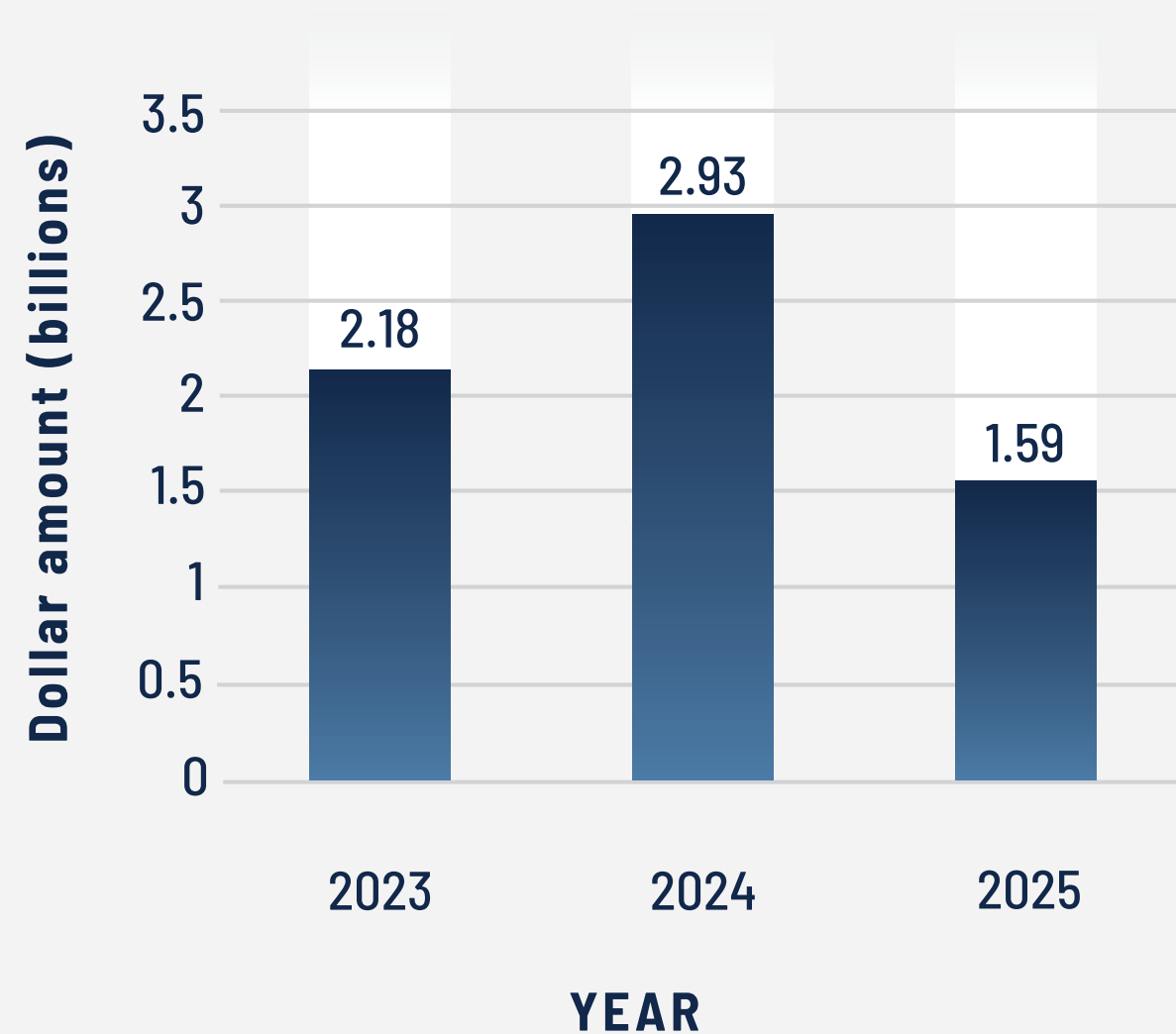
U.S. courts continue to set new, albeit fragmented, precedents with respect to privacy, which are continuing to cascade throughout the judicial system. As the court explained in [Lopez v. Apple](#), "data privacy law is [a] developing area of law posing inherent risks [meaning] that a new decision could shift the legal landscape as to the certifiability of a class, liability, and damages."

Data privacy litigation by the numbers

Research indicates that private settlements in the data privacy domain have ballooned to a total figure exceeding USD2.5 billion over the past three years. However, that number may be much larger.

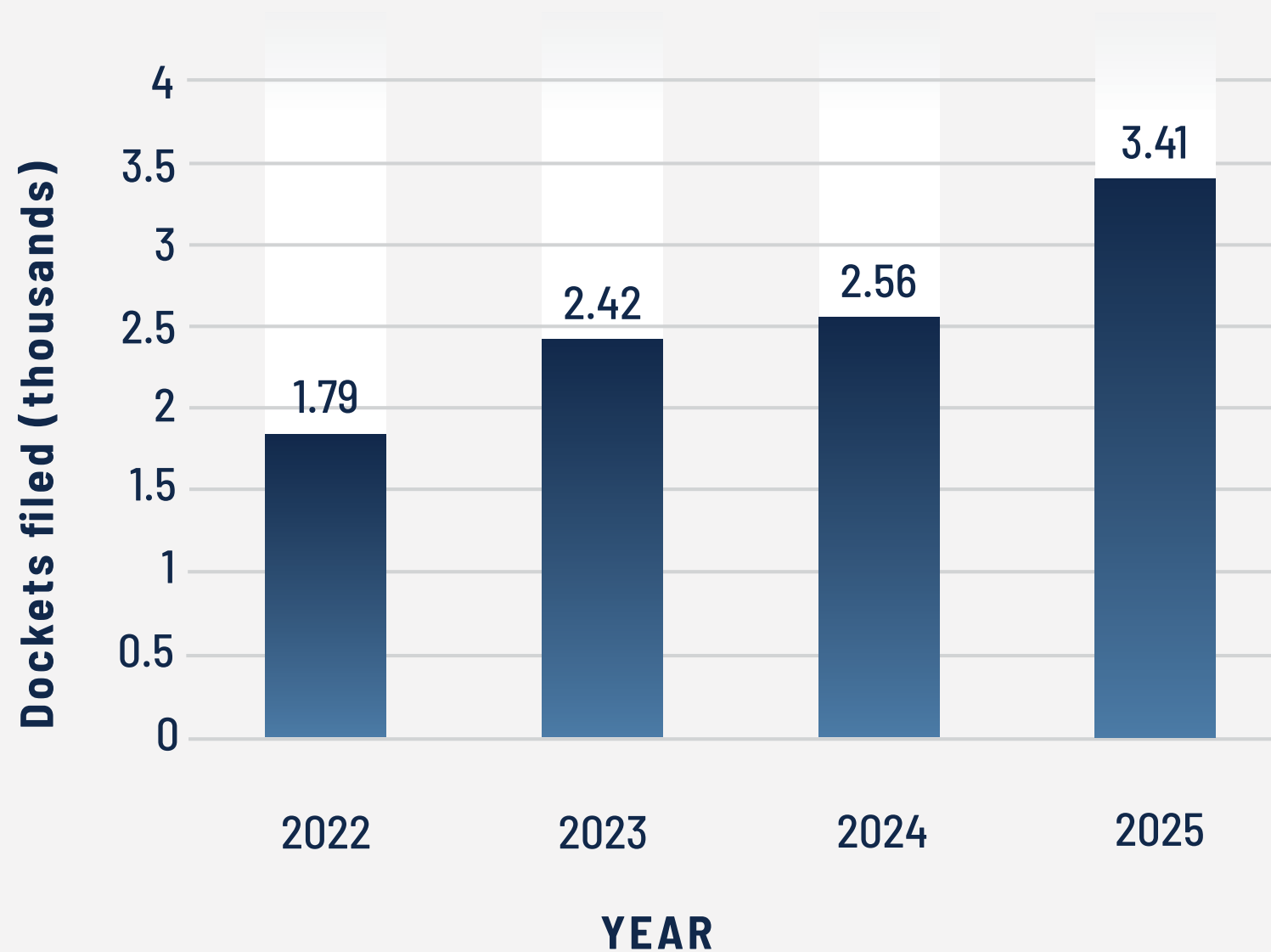
To illustrate, the [2026 Duane Morris Class Action Review](#) found the top 10 largest privacy class-action settlements in 2025 totaled USD801.8 million, with a further USD515.8 million stemming from the top 10 largest data breach settlements. This does not include actions under long-established statutes such as the Biometric Information Privacy Act (USD136.6 million), Telephone Consumer Protection Act (USD69.1 million) and Fair Credit Reporting Act (USD74.7 million).

Total dollar amounts from the largest settlements across five areas of data privacy litigation



Added together, the top 10 largest class-action settlements across five different privacy and security-related areas — a total of 50 settlements — amounted to USD1.59 billion in 2025. These top 50 relevant settlements were even higher in 2024, totaling USD2.93 billion; that number was USD2.187 billion in 2023.

Number of data privacy dockets filed in state and federal courts



While annual settlement totals may be moderating, the growing number of cases filed appears to cancel that out to a certain degree. In fact, data privacy litigation in the U.S. is at an all-time high. WestLaw Edge Litigation Analytics estimates the number of data privacy cases filed from 2022 to 2025 reached over 10,000, including 1,799 in 2022; 2,420 in 2023; 2,565 in 2024; and 3,414 in 2025. That upward trajectory is projected to continue through 2026.

Overview

As the analyses in this report demonstrate, the case law emerging from private litigation around data privacy violations adds a new dimension to the enforcement of privacy rights and the demands of compliance. Read comprehensively, the judgments espoused in the cases herein generate legal obligations for businesses that collect, store and share personal information. With each new settlement, dismissal and decision, data privacy continues to be a source of living law, constantly reshaping our understanding of the impact that digital governance has on individual lives and business practices.

This report is divided into eight parts.

Breach of contract and warranties

This part examines breach of contract and warranty claims in the context of data privacy. It explains when courts have allowed complaints to proceed and when they have granted defendants' motions to dismiss. This first section also shows where and how individuals have leveraged a company's privacy notice, terms of service or other contractual arrangement to assert privacy violations.

The California Invasion of Privacy Act

This part analyzes litigation under the long-standing California privacy law originally passed to protect citizens against unauthorized wiretapping. The decades-old statute is now being repurposed by individuals to claim that website tracking by third parties amounts to a form of unlawful digital eavesdropping.

The Federal Wiretap Act

This part explores Title I of the Electronic Communications Privacy Act, a statute that prohibits unauthorized wiretapping and continues to be applied to modern technology. Notably, the crime-tort exception continues to divide courts.

The Video Privacy Protection Act

This part discusses a federal law that was originally drafted in the heydays of brick-and-mortar video rental stores but now has been broadly applied to online video services. Several provisions of the law are up for debate.

The California Consumer Privacy Act's private right of action

This part analyzes the private right of action under the CCPA, which can be brought for unauthorized data disclosures that remain uncured, carrying statutory damages between USD100 and USD750 per consumer.

Biometrics and consumer health data

This part examines litigation under the Illinois Biometric Information Privacy Act as well as the private right of action in recently enacted and proposed consumer health data privacy laws like Washington state's My Health My Data Act.

Daniel's Law and public officials' privacy

This part focuses on lawsuits filed under a New Jersey privacy statute that protects the personal information of judges and other public officials, as well as the First Amendment arguments that challengers have raised against it.

Shareholder actions

This part examines how shareholders have sought to hold organizations accountable through private litigation for alleged misconduct or inaction around data privacy issues.

A note on jurisdiction and civil procedure

The following report is based on cases filed in both U.S. federal and state courts, which are not equally weighted from a precedential standpoint. For example, decisions by federal courts do not bind state courts and vice versa. Furthermore, a decision by a lower court, such as a trial court, does not bind a higher court, such as an appellate court. Interested parties should pay careful attention to which authority is binding and which is merely persuasive in the jurisdiction in which they sit.

In addition, few of these cases have resulted in final judgment. Instead, the vast majority have been settled, dismissed or granted summary judgment during the early stages of litigation. As such, the ensuing analysis of case law provides substantial insight into what allegations constitute a valid claim under various causes of action, but less so into the import that juries give evidence in these cases. The takeaways from settlements, dismissals and summary judgments are nonetheless valuable in better understanding how to increase compliance and mitigate digital risk.



Part 1: Breach of contract and warranties

Private plaintiffs are increasingly bringing data privacy claims under theories of breach of contract and breach of warranty. These legal claims are often the result of privacy incidents or violations and seek to leverage a company's own privacy notice, terms of service, advertisements, cookie banners or other public statements as contractual commitments or assurances.

Breach of contract is a common law claim that traditionally requires the existence of an enforceable contract, nonperformance amounting to a breach of the contract, and damages caused by the breach. A breach of warranty is similar to a breach of contract, though it typically involves the misrepresentation of a fact or condition warranted to be true that affects the quality or performance of a good.

Breach of contract and breach of warranty claims have a long-standing history as causes of action and have generated an enormous amount of relevant case law before plaintiffs began raising arguments in the context of privacy incidents.

Breach of express contract

An express contract forms when competent parties reach a meeting of minds and explicitly state their terms either orally or in writing, and said terms create mutual obligations upon the parties. The concept of an express contract dates back centuries, and courts typically find them enforceable based on clear, agreed-upon promises. Today, express contracts can include service agreements, employment contracts and commercial transactions. These contracts require clear duties such as access, payment terms and timelines.

Breach of implied contract

A contract does not always need to be written or spoken out loud to be enforceable. Courts have long recognized that contractual obligations can arise from behavior or circumstances signaling a mutual intention between parties to form a contract, even if no written or spoken terms are agreed upon.

Depending on the circumstances, implied contracts can be invoked in service transactions where the nature of the parties' interactions and conduct implies an agreement. For example, some patients have argued that an implied contract arose from a healthcare provider's advertisement that committed to keeping all patient data secure through industry-leading practices. They then claimed that inadequate security measures, which exposed patient data, breached that implicit promise.

Breach of express warranty

Express warranties arise when a seller makes a specific claim or assurance about a product or service that becomes part of the basis of the bargain, sale or exchange. Express warranties are often seen in the context of product sales as they cover promises regarding performance standards, quality or compliance with specifications.

Breach of implied warranty

Similar to express warranties, implied warranties have deep roots in U.S. sales law, particularly the Uniform Commercial Code, which codifies different implied warranties. Most relevant to data privacy litigation are the implied warranty of merchantability, which assures goods are fit for ordinary use, and the implied warranty of fitness for a particular purpose, which assures goods fit a buyer's specific needs. In a consumer product context, these implied warranties protect buyers against defects or misrepresentations in goods or services, even if not expressly mentioned.

Summary of breach types in the context of data breaches

Type of breach	Definition	Privacy incident example
Breach of express contract	Explicitly stated terms are violated by one party	A company explicitly promises not to share user data but does so
Breach of implied contract	Contract based on conduct or circumstances is violated	A company collects sensitive information, implying a duty to protect it but fails to do so due to lax security
Breach of express warranty	Specific promises or assurances about a product/ service are not met	A company advertises zero data logging, but logs user activities, which are exposed in a data breach
Breach of implied warranty	Obligations based on the nature of the product/service are violated	A cloud service implicitly promises secure storage, but data is leaked due to poor or outdated security practices

Courts see an implied contract to protect personal information collected as a condition of employment

Some courts have allowed breach of contract claims regarding privacy incidents to proceed past the motion to dismiss stage on the theory that employers who collect personally identifiable information as a condition of employment enter an implied contract to protect the personal information they now possess.

The plaintiffs in [McFarlane v. Altice USA](#) comprised employees whose information was accessed after a phishing attack. The plaintiffs alleged they entered an implied contract with the company to protect this data through the use of reasonable industry standards when Altice required them to disclose their personal information as a condition of employment.

Likewise, in [Haney v. Charter Foods North](#), the U.S. District Court for the Eastern District of Tennessee denied an employer's motion to dismiss their employees' breach of implied contract claim where the employer experienced a data breach that accessed the employees' private information. The employees alleged they were required to provide their employer with personal information as a condition of employment, and therefore the parties entered implied contracts where the employer agreed to safeguard such information and promptly detect any breaches. The court agreed that an implied contract arose due to this conditional exchange and that the employer was required to take reasonable steps to protect employee information.

Similarly, in the case of [Sequoia Benefits and Insurance Data Breach Litigation](#), the defendant provided employee management software to the plaintiffs' employer. The U.S. District Court for the Northern District of California denied the defendant's motion to dismiss a breach of contract claim. After the defendant experienced a data

breach, the plaintiffs alleged that the defendant had entered into contracts with their client — i.e., the plaintiffs' employer — to perform services, contracts which were made in part for the benefit of the plaintiffs and with the intent and expectation that the plaintiffs' PII would remain private and be adequately protected from unauthorized disclosure. Ultimately, the plaintiffs argued that the defendant breached the contracts by permitting unauthorized third parties to access and exfiltrate the plaintiffs' PII.

Finding for the plaintiffs, the court pointed to case law where employees alleged they were intended third-party beneficiaries of contracts between a defendant and its customers that required the defendant to take appropriate steps to safeguard employees' information.

These cases follow the judicial trend that emphasizes the reasonable expectations of privacy created by a company's own statements while simultaneously considering whether a reasonable consumer would interpret those statements as binding promises.

This thinking was followed in [In re BetterHelp Data Disclosure Cases](#) where BetterHelp allegedly disclosed customer information to various third parties for advertising purposes and the third parties' own purposes, revealing that customers were seeking and/or receiving mental health treatment. This disclosure occurred despite BetterHelp's privacy assurances throughout their website and interactive forms.

The court held that the plaintiffs sufficiently identified the particular promises that BetterHelp made, including assurances to keep customer information confidential and disclosures that would constitute a breach of those promises. As such, the plaintiffs' breach of implied contract claim was allowed to proceed.

Plaintiffs less successful in the absence of consideration

Where consideration — a mutual exchange of promises necessary to establish a valid contract — is lacking, plaintiffs are less successful.

In [Nienaber v. Overlake Hospital Medical Center](#), the defendant's website implemented browser plugins, which enabled the unauthorized disclosure of patient information to third parties. Nevertheless, the U.S. District Court for the Western District of Washington dismissed the plaintiff's breach of implied contract claim. Notably, the plaintiff demonstrated that the defendant's privacy policies did not cover disclosure to third parties for marketing purposes and that the disclosed information was protected under the Health Insurance Portability and Accountability Act.

Yet, the court reasoned that the plaintiff neither alleged she paid the defendant for medical services nor that the defendant received consideration for its promises to safeguard the plaintiff's information. Although the plaintiff alleged the provision of her data alone in exchange for services established an implied contract, the court found she failed to allege any invitation by the defendant showing that it assented to secure personal information in exchange for such remuneration.

Furthermore, even the defendant's privacy notice was insufficient to form a contract. Rather, these documents served to inform patients of their rights and the duties imposed on healthcare providers by statutory provisions. As such, they were not contractual in nature.

In [Rodriguez v. Google](#), the plaintiffs argued Google created a unilateral contract by providing a button to adjust a user's privacy settings. They asserted that toggling the button to turn off web and app activity created a unilateral contract with Google and, accordingly, Google would not collect their data.

The district court determined that providing a button for consumers to choose whether data related to their activities was saved to their accounts was insufficient to give rise to an enforceable contract. The court held that, although the button might create an expectation among users that data will not be collected, such action was not negotiated or bargained for terms in the manner contracts require, and Google did not offer or receive anything in exchange for a user turning off the button.

Third party terms: Device-level permission and non-signatory enforcement of contracts

Users of third-party apps may expect their communications with those apps to be confidential. However, an underlying device-level agreement may permit a hardware provider to intercept those interactions.

For instance, in [Hammerling v. Google](#), the U.S. Court of Appeals for the Ninth Circuit affirmed the district court's dismissal of the plaintiffs' breach of contract claim, where the plaintiffs alleged Google violated its privacy policy by collecting data from Android users pertaining to their activity on third-party apps. Indeed, Google's policy explained it collects data about users' activity on third-party sites and apps that use Google's services. Among those enumerated services was the Android operating system itself, meaning that Google was authorized to intercept any data from an app running on its hardware. While the court distinguished third-party apps operating on non-Android devices, the policy nevertheless expressly contemplated the collection that the plaintiffs alleged, resulting in no breach of contract.





Relatedly, even if a third party has not signed a contract, they may still be able to enforce its terms. In [Perry-Hudson v. Twilio](#), the Northern District of California granted the defendant's motion to compel individual arbitration. In this case, the plaintiff interfaced with Keeps, a hair loss treatment company, but sued Twilio, the company whose software was used to collect his information and send him targeted ads. Twilio was a nonsignatory to Keeps' terms and conditions, which contained an arbitration clause that Twilio moved to enforce.

Holding for Twilio, the court first found that the link to the terms and conditions was reasonably conspicuous because it was displayed directly beneath a "Continue" button, the sign-in screen lacked clutter, and, although the link was the same color as the rest of the text, the black font contrasted with the white background.

Furthermore, the court decided that Twilio could enforce the arbitration agreement. It came to this decision because the plaintiff's claims were rooted in whether Twilio's use of his personal information was unlawful, which turned on the disclosure of personal information to third-party vendors discussed in Keeps' privacy policy and incorporated into its terms and conditions. Additionally, the plaintiff alleged interdependent and concerted misconduct by Keeps and Twilio, i.e., Keeps disclosed personal information to Twilio, which Twilio illegally intercepted; these allegations were intimately connected with the obligations of the underlying agreement. As an equitable matter, it was only fair, in the eyes of the court, that Twilio be permitted to enforce Keeps' arbitration clause.

The wording of policies and terms can limit or defeat claims

The survival of a plaintiff's breach of contract claim will typically turn on the specific language of the relevant statement as well as the circumstances in which the defendant's breach allegedly occurred. Furthermore, limitations within privacy statements can preclude claims.

In [Bass v. Facebook](#), the plaintiffs alleged breach of contract and breach of implied contract against Facebook where hackers exploited a coding vulnerability and stole the access tokens of 69,000 users, leading to the theft of the information of 29 million worldwide users.

In its order on Facebook's motion to dismiss, the lower court determined that Facebook's data use policy and terms of service were construed as contractual promises to limit data sharing, and the plaintiffs properly alleged such contractual promise was violated. However, the plaintiffs' breach of contract claims ultimately failed because Facebook's terms of service included an accessible, procedurally fair and sufficiently clear limitation-of-liability clause.

Furthermore, the retroactive nature of a contract may change from one provision to the next. In [Hartley v. University of Chicago Medical Center](#), the court dismissed the defendant's motion for summary judgment for breach of contract but granted the defendant's motion to strike the plaintiff's class-action claims, where the plaintiff initiated an Electronic Communications Privacy Act claim against the defendant in October 2022 and subsequently agreed to the defendant's terms of use, effective August 2023.

There, the terms of use agreement included a dispute resolution provision that required parties to notify one another before "commencing a formal proceeding." The court held the plaintiff commenced her formal proceeding 10 months before the effective date of the dispute resolution provision, and therefore this provision did not apply — even to the plaintiff's subsequent amended complaints since the amended complaints did not contain new claims. On the other hand, the court found the plaintiff did breach the terms' class-action waiver provision since it applied to any claims, whether pending or not, including the plaintiff's ongoing claim filed in October 2022.

Warranty claims fail when nonexistent or expired

Many warranty claims have been dismissed for either lack of specificity or because privacy notices are not typically seen as warranties. In the case of [Google Assistant Privacy Litigation](#), the court determined the plaintiffs had not identified terms of an express warranty within the provisions of the privacy notice. In the same case, which included the disclaimer, "to the extent permitted by law, we exclude all warranties" within the defendant's terms of service, the court upheld the disclaimers as a defense against the allegations of implied warranties.

Additionally, most warranties are effective from the time the customer first receives the associated goods to some future date. As the plaintiffs in [Riordan v. Western Digital Corporation](#) discovered, such is the case even when continuous maintenance is performed on a digital good or service: While an update may suggest a renewal of the product, it does not supplant the original date of delivery.

There, the Northern District of California granted the defendant's motion to dismiss the plaintiffs' claim under California's Song-Beverly Act, which provides an implied warranty of merchantability and fitness, where the plaintiffs alleged that the defendant failed to properly secure the plaintiffs' data within its data storage devices. The plaintiffs' allegations rested on the defective devices themselves, but also the defendant's maintenance of faulty web portals that provided remote access to the devices. While the Song-Beverly Act afforded an effective warranty period of one year following delivery of goods and a four-year statute of limitations, the court found the plaintiffs failed to include in their complaint the date of purchase and therefore barred their claim. Furthermore, the court rejected the plaintiffs' argument that the defendant's ongoing maintenance of the faulty web portal continuously extended the warranty period.

Courts may find enforceable contracts but no breach of privacy

A party may promise to keep personal data private. If they merely disclose information that does not amount to personal data, the party has not broken that promise.

In [Rand v. Eyemart Express](#), the court dismissed the plaintiffs' breach of contract claim, where the plaintiffs alleged the defendant, the owner of a prescription eyewear website, breached their privacy statement's promise not to disclose individually identifiable health information without consent. The court found that the plaintiffs did not sufficiently allege that they entered personal health information into the website. At most, they alleged that they visited the website to look at glasses they could order in-store and intended to search for eye doctor contact information while on the website, neither of which amount to IIHI under HIPAA.

Similarly, the court in [John Doe v. Google](#) dismissed the plaintiffs' breach of express contract claim. The plaintiffs alleged that Google unlawfully collected their private health information using source code embedded on their healthcare providers' websites.

The court found that while Google promised to only collect health information if voluntarily provided by users, the plaintiffs did not adequately allege that the data transmitted to Google contained their private health information since they failed to allege where on a web property the source code existed. Further, although the plaintiffs alleged Google broke its promise not to use health information for personalized advertising, the court found the plaintiffs failed to allege they actually received any personalized advertising based on their health information.

The court also rejected the breach of contract claim based on language in Google's Terms of Service mandating that users of Google's services respect the rights of others; unsurprisingly, the court found this language bound users, not Google. Additionally, the court found that Google promised to protect its own services against fraud and abuse, not Google users.

Finally, the court dismissed the plaintiffs' breach of implied contract claim. While the plaintiffs alleged an implied contract claim to the extent that Google's terms are not express contracts, the court found an implied contract cannot exist where an express contract covers the same subject.

Courts at the pleading stage hesitate to determine contract validity

Faced with a motion to dismiss, courts can be hesitant to decide whether a valid contract has arisen or if the plaintiff has properly alleged a breach. There is often simply not enough evidence in the record at this stage to make such a determination.

For example, in [Okash v. Essentia Health](#), the court declined to assume the defendant's privacy policy constituted a valid contract, reasoning that the policy was a browsewrap agreement, the enforceability of which depended on its adequacy of notice. The adequacy of notice, in turn, was a fact-bound question that could not be determined on a motion to dismiss.

On the other hand, in [Doe v. Genesis Health System](#), the U.S. District Court for the Central District of Illinois held that because the defendant provided no controlling authority indicating otherwise, it would decline to rule as a matter of law that a privacy policy does not constitute an express contract. It therefore denied the defendant's motion to dismiss the plaintiff's breach of express contract claim. Further, while the defendant argued that the plaintiff did not allege any completed direct financial loss, the court found that the plaintiff did allege "monetary damages," and must be given an opportunity to prove their damages before the claim is dismissed.

The consent defense

User consent is a primary legal basis for processing personal data as well as a common defense to liability under various privacy laws. While it does not take a breach of contract claim for a consent defense to arise, the issue of whether a user consented to the collection and processing of their data depends on the existence of mutual assent as to the terms of that transaction. Moreover, it often involves a contract-like agreement, e.g., a privacy policy, cookie banner or terms and conditions, to which a user must assent — impliedly or expressly — in order to engage with the associated services.

In [In re Google Gmail Litigation](#), the plaintiffs alleged Google routed all emails received by Gmail users through a device from which Google acquired message content and other information used to create metadata and annotations on users. Even so, the court held that, due to Google's disclosures about these alleged interceptions from a "panoply of sources," the plaintiffs could have learned of the alleged interceptions and therefore had implicitly consented.



Determining consent can be a fact-intensive exercise

As with the existence of a valid contract and the elements of a claim, showing that consent was given can be a fact-intensive exercise. As such, some courts may be unwilling to dismiss the issue early in litigation without the assistance of discovery and evidence.

To illustrate, the U.S. District Court for the Central District of California denied the defendant's motion to dismiss the plaintiff's CIPA claims on consent grounds in [Rodriguez v. Autotrader.com](#). Although the defendant's website had a banner that explicitly informed visitors that their information would be shared with third parties, the court held that the issue of whether the plaintiff implicitly consented to that disclosure turned on whether the banner was sufficiently conspicuous and whether it sufficiently disclosed how the defendant would use the plaintiff's data, a matter which could not be determined at the pleading stage.

The factual particularities of consent also have an impact on class certification. In [Conner v. Fox Rehabilitation Services](#), the U.S. Court of Appeals for the Third Circuit affirmed the district court's order denying class certification, where questions about individualized consent surrounding class members' Telephone Consumer Protection Act claims of unsolicited advertisements via

fax precluded predominance. Specifically, each claim would require individualized review of whether the defendant sought permission to send faxes, what the defendant informed each class member about these faxes, how each class member provided their consent, whether the fax received fit within the contours of any consent provided, and whether a class member invited the fax in some other way.

Collected consent can defeat claims at the pleading stage

On the other hand, the Northern District of California in [Lakes v. Ubisoft](#) had more facts available from the pleadings and therefore granted the defendant's motion to dismiss the plaintiffs' various claims — both common law and statutory — on consent grounds. In this case, the plaintiffs used the defendant's website, which purportedly used Meta's tracking pixel and disclosed the plaintiffs' PII to Meta without the plaintiffs' consent, to download games that contained cinematic portions while logged into their Facebook accounts.



Ruling for the defendant, the court found that consent was elicited in all cases. The plaintiffs were presented with a cookie banner when they first arrived at the website and were required to affirmatively accept Ubisoft's terms of use, terms of sale and privacy policy during account creation; every time the plaintiffs made a purchase they were again presented with the privacy policy. The court noted that a binding contract is created if a plaintiff is provided with the terms of service in the form of a hyperlink, and it is sufficient to require a user to affirmatively accept the terms even if the terms are not presented on the same page as the acceptance button.

Consent obtained by browwrap versus clickwrap agreements

A browwrap agreement, oftentimes linked in the footer of a website, assumes consent to its terms based on the user's continued use of the website. In contrast, a clickwrap agreement requires a user to affirmatively assent to its terms, typically by clicking on a checkbox, before the user can access the website or its services. While both types of agreements must be conspicuously placed to be enforceable, the browwrap needs to be more so since it does not require affirmative assent.

In [Popa v. Harriet Carter Gifts](#), the U.S. District Court for the Western District of Pennsylvania found a browwrap agreement sufficiently conspicuous to imply that the plaintiff consented. There, the court granted the defendant's motion for summary judgment of the plaintiff's Wiretapping and Electronic Surveillance Control Act claim, where the defendant's ecommerce website had a privacy policy posted in the footer presented as a white link against a blue background. The policy stated that the defendant collects certain information to process orders, enhance the shopping experience and communicate with customers; it also addressed access to customer information by third parties.

Finding for the defendant, the court reasoned that the consent provisions of WESCA establish an objective standard and that the enforceability of a browwrap agreement turns on whether the notice of the terms is reasonably conspicuous on the webpage. Notably, the hyperlink was labeled "Privacy Statement" rather than some generic term, it was displayed in white font against a blue background in the footer of every page, and a link could also be found in the drop-down menu directly below "Email Us."

In [Washington v. Flixbus](#), the U.S. District Court for the Southern District of California addressed a clickwrap agreement, granting the defendant's motion to dismiss the plaintiff's CIPA and invasion of privacy claims. There, Flixbus integrated Facebook's tracking pixel into the website that the plaintiff used to buy a bus ticket, allowing Facebook to intercept the plaintiff's communications, including personally identifiable information and a private travel itinerary.

During checkout, the plaintiff was presented with a checkbox affirming he read the privacy policy and agreed to the terms and conditions, which were appended to the checkbox notice via hyperlinks; the court likened this to a clickwrap agreement, whereby the plaintiff was required to consent before completing his purchase. Further, a 10-minute timer started when the plaintiff entered the checkout process, within which time the plaintiff was required to complete his purchase or else be directed to restart.

The court concluded that Flixbus' privacy policy and terms and conditions explicitly notified users of the use of cookies and tracking pixels to disclose certain data to the defendant's business partners. Moreover, the countdown timer put the plaintiff under no obligation to complete the checkout process, and the plaintiff could access the privacy policy and terms and conditions at any time via hyperlinks in the footer of the website.

Importantly, the court distinguished Flixbus' clickwrap agreement from a browwrap agreement, the latter of which requires more than a conspicuous hyperlink on every page. Here, the plaintiff was presented with a conspicuous hyperlink to the defendant's policies and was required to affirm that he agreed to be bound by the stated terms in order to complete his purchase.

How do businesses avoid breach of contract and warranty claims?

Breach of contract and warranty, as well as use of the consent defense, are evergreen arguments in data breach and privacy litigation. In reviewing the recent case law, a few trends emerge.

First, express contracts, such as an employment contract that requires the provision of personal information, can create an implied contract between the employee and any third-party vendors used by the employer. Likewise, a contract between a user and a service provider may extend to a third-party vendor whose conduct is deeply entwined with the service provider and which constitutes the subject of the allegations.



Furthermore, a contract may explicitly extend to third-party apps that rely on the operating system of one of the contracting parties, surprising users who expect their communications with those third parties to be private. Still, these broad interpretations have limits: Maintenance updates of digital services do not necessarily extend the effective period of an implied warranty.

Importantly, the existence of consideration, such as monetary compensation for a service provided, can be the difference between a valid contract and an unenforceable assumption that one exists. In fact, personal data may suffice as consideration where it is provided in exchange for a good or service, though a contracting party should be clear on the terms. Providing one's data may, for example, entitle one to the provision of a service, but it does not necessarily mean the service provider is contractually obligated to safeguard that data.

The retroactivity of a contract can also turn on the terms, with some provisions applying only to future events and others applying to events in general. Moreover, a promise to protect personal data only applies if personal data is actually alleged.

Furthermore, the facts available in a pleading on the issues of contract validity, a prima facie claim, and consent can make or

break a motion to dismiss or class certification. While the factual complexity of determining the conspicuousness of a privacy notice may bail out a plaintiff's claim until further discovery can take place, the very same complexity can preclude a finding of predominant issues amongst a class of plaintiffs.

Finally, the distinction between browsewrap and clickwrap agreements remains important, especially the level of conspicuousness required by the former. While some courts maintain that consent is assessed by an objective standard, "The [4Ps](#)" described by the Federal Trade Commission, i.e., prominence, presentation, placement and proximity, to determine conspicuousness may take different forms.

Whether or not conspicuousness is in the eye of the beholder, close questions concerning breach of contract, warranty and consent remain abundant. As such, privacy professionals and lawyers in this space should keep close tabs on these developments, what they mean for current risk, and how they can be leveraged in future litigation.

Part 2: The California Invasion of Privacy Act

Old state wiretapping laws have inspired vigorous data privacy class-action lawsuits, requiring consumer-facing businesses to determine whether the consumer tracking technologies used on their websites put them at risk of litigation.

Among this recent litigation trend is a decades-old wiretapping law from California that has been used to spearhead privacy class-action lawsuits against businesses using tracking tools on their websites and has motivated plaintiffs elsewhere who seek to apply their states' wiretapping laws to digital tracking and analytics.

The California Invasion of Privacy Act is an extensive wiretapping statute passed in 1967 due to rising concerns of eavesdropping amid the advancement of wiretapping technology during the Cold War era. Decades later, plaintiffs are alleging that businesses use website tracking tools to collect consumers' data in a manner that violates CIPA. Many of these cases focus on Section 631(a) of the act, although Sections 632 and 638 have also been invoked in privacy-related complaints.

Parties that violate any of these provisions can face fines of USD2,500 for each violation. Parties that previously violated CIPA can be fined up to USD10,000 for further violations.

Section 631(a): The eavesdropping provision

Section 631(a) is long and multifaced with four distinct clauses that each carry a separate cause for liability: intentional wiretapping of a telephone wire; willfully reading, or attempting to read, the contents of a communication in transit without the consent of all parties; using any information so obtained; or aiding a party in the commission of any such acts.

In the landmark case in CIPA litigation, [Javier v. Assurance IQ](#), the Ninth Circuit found the second clause of this section covered internet communications and was not limited to traditional phone conversations. There, the court found the plaintiff properly alleged the defendant's use of third-party session replay software captured his "demographic information and medical history" in real time without his prior consent and allowed the claim to survive the defendant's motion to dismiss.

Recent litigation is primarily focused on clause two, the scope of which has expanded to cover modern technology. This is because clause one does not apply to communications over the internet, as clarified by [Ramos v. Gap](#); clauses three and four require an underlying violation of either clause one or two. But just within clause two, there are multiple statutory elements that plaintiffs must plead in order to properly state a claim. In many cases, defendants file a motion to dismiss based on inadequate pleadings of each of these elements, which, in turn, prompts judicial interpretation of each decisive term.

When is consent obtained under Section 631(a)?

As with most privacy claims, a primary hurdle for plaintiffs to overcome when lodging CIPA § 631(a) complaints is the matter of consent. *Javier v. Assurance IQ* is again a defining case. The Ninth Circuit found that prior consent was required before Javier's communications with Assurance's website could be intercepted by an undisclosed third party. Following that, the Northern District of California held on remand that the plaintiff did not impliedly consent to third-party ActiveProspect's collection of his information.

There, the plaintiff visited the defendant's website to obtain a life insurance quote, entered personal information into a webform, and was required to consent to the website's privacy policy and terms of service to view the quote. The website used ActiveProspect's code to record electronic communications of visitors to the website, conduct which was disclosed in the privacy policy.

The court found the plaintiff's use of the website and completion of the webform suggested implied consent to Assurance's collection of his information. However, this consent did not transfer to ActiveProspect's collection practices after the plaintiff entered his information but before he consented to the privacy policy. The defendants also failed to show that the plaintiff continued using the website after he received constructive notice that ActiveProspect was collecting his information.

The defendant further argued that, given the ubiquity of services like ActiveProspect's across the internet, disclosing its tools is technologically impractical. The court was unpersuaded and concluded that obtaining consent remains a regular occurrence on the internet and the ubiquity of a service does not automatically confer consent to its data collection practices. Indeed, Javier pled that he did not know his information was disclosed when it was collected, and the court treated that as true on a motion to dismiss.

Nevertheless, the court granted the defendant's ensuing motion to dismiss on statute-of-limitations grounds, finding the webform's design put Javier on notice of the privacy policy and a potential CIPA claim. The page was uncluttered, Javier had full and immediate opportunity to read the privacy policy, the clickwrap agreement was clear and legible, and the privacy policy and terms of service were in blue font, that is, the universal signal of a hyperlink.

Further, the court found the privacy policy disclosed evidence sufficient to put Javier on inquiry notice of a wiretapping claim. Although written in the present tense, the policy indicated that it applied throughout use of the website and stated that Assurance might collect information, such as what Javier entered into the webform, and may use third parties to assist with its services.

Another illuminating case on the matter of consent is [Griffith v. TikTok](#), where the plaintiffs alleged that TikTok intercepted information about non-TikTok users when they visited third-party websites on which TikTok's pixel software was installed. As to express consent, the court found that while the third-party sites that employed the pixel software disclosed they would share user information with advertisers and service providers, they did not specifically disclose that TikTok was among those vendors.

Given the heightened privacy concerns specific to TikTok, the court found that reasonable users would not necessarily understand their information would be shared with the defendants based on vague disclosures. Further, the court found the plaintiffs did not impliedly consent to the interception merely because they continued using the third-party sites after filing their lawsuit. In fact, requiring the plaintiffs to do so would "unfairly undercut ... standing to seek injunctive relief."

Finally, *Rodriguez v. Autotrader.com* suggests that consent is often a question of fact that may be premature on a motion to dismiss. There, the defendant's website installed third-party tracking software on the plaintiff's browser, capturing and sending identifying information, including search queries, to third parties.

The court rejected the defendant's argument that the plaintiff had impliedly consented to sharing her information with third parties based on the existence of a banner disclosing such practices. The answer, the court held, depended on how conspicuous the banner was, which was unclear at the pleading stage. Because the plaintiff alleged that she did not consent and this detail was uncontradicted, the court accepted it as true in the absence of further discovery or judicial notice.

The party exception

A common defense to a Section 631(a) clause two claim is that the alleged eavesdropper is actually a party to the conversation. As the foundational case *Rogers v. Ulrich* held, a party to a conversation cannot eavesdrop under the law.

For example, in *Cole v. Quest Diagnostics*, the plaintiffs alleged the Facebook tracking pixel was incorporated into Quest's website and that, when they retrieved their medical test results, Quest transmitted their personal information to Facebook.

Finding for the defendant, the Third Circuit held that the tracking pixel directed the user's browser to communicate separately with Facebook — albeit concurrent with communications to Quest's website — making Facebook a party to those communications to which it was an intended recipient. Following precedent from in the case of *Google Cookie Placement Consumer Privacy Litigation*, the court found that Facebook, as a party unto itself, would have no need to acquire information from transmissions to which it was not a party. Further, that the plaintiffs were unaware of this separate communication was irrelevant.

In *Karwowski v. Gen Digital*, the plaintiffs installed the Avast Online Security & Privacy browser extension to prevent third parties from tracking and collecting their data. The plaintiffs alleged that Gen Digital, the owner of Avast, was unlawfully intercepting communications between the plaintiffs and their search engines, charging Avast was a known party to the communications and Gen Digital was not. The Ninth Circuit held for the defendant, finding that the plaintiffs referred to themselves as users of both Avast and Gen Digital and explicitly acknowledged Gen Digital was potentially a necessary party for Avast website verification.

Similarly, in *Ramos v. Gap*, the Northern District of California dismissed the plaintiff's claim, where the defendant used Bluecore software embedded in its marketing emails to monitor customer behavior when interacting with the defendant's emails and website. The court held that the plaintiff failed to allege the defendant monitored the content of any emails other than those sent by the defendant and was therefore a party to any communications in question.

Is there a third-party eavesdropper?

Related to the party exception, the existence of a third-party eavesdropper is an essential element of the second clause of Section 631(a). The foundational cases on this issue are *Rogers v. Ulrich*, where Ulrich used a tape recorder to record his conversation with Rogers and then shared it with a third party, and *Ribas v. Clark*, where Clark listened to a conversation between Ribas and his ex-wife. In *Rogers*, the court found no third-party eavesdropper; in *Ribas*, the court did. Following this precedent, modern courts venture to determine whether a party is more like the tape recorder in *Rogers* or the friend in *Ribas*.

Oftentimes, this distinction comes down to whether the third party is using the intercepted communications for its own purposes, such as to improve its services or merely recording and storing the information for the benefit of the first party.

In *Jones v. Tonal Systems*, the Southern District of California found the third party akin to a tape recorder. Specifically, the court held that allegations that third-party vendor Drift analyzed the plaintiff's conversations with the defendant and collected data about the plaintiff's activity only supported the inference that Drift received and stored communications for the defendant's benefit. This made Drift an extension of the defendant — like the tape recorder in *Rogers* — and therefore it was not a third-party eavesdropper.

The court in *Williams v. DDR Media* arrived at a similar conclusion. There, the plaintiff's interaction with the defendant's website was recorded by third-party software used to document users' consent to receive telemarketing calls. The court found the software vendor Jornaya was more akin to a tape recorder because it had merely recorded the communication for retrieval by DDR Media rather than for its own purposes.

Another relevant question is whether the required threshold is actual use for one's own purposes or merely the capability to do so. Courts differ on whether an actual use requirement swallows the third clause of Section 631(a), which explicitly prohibits the use of a communication obtained in transit, or reinforces the tape recorder-friend distinction. The logic behind this is that a tape recorder has no ability to use a recording for its own purposes, but a friend does.

To illustrate this, the court in [Graham v. Noom](#) found no third-party eavesdropper because the plaintiffs failed to allege the third party "intercepted and used the data itself." Thus, the court reasoned the software vendor's use of the data was comparable to that of a tape recorder. Since the vendor did not make further use of the visitors' data, its conduct did not give rise to liability under the statute.

On the contrary, the court in *Javier v. Assurance IQ* did find a third-party eavesdropper where Javier pled that ActiveProspect had the mere capability to use the information for any other purposes, that is, beyond the ordinary function of a tape recorder. It was irrelevant whether ActiveProspect had the intent to actually use the information for its own benefit. There should be no use requirement, the court reasoned, read into the second clause of Section 631(a), as the court in *Graham v. Noom* did. Not only would this swallow the third clause of Section 631(a), but the Ribas court did not consider Clark's use of the information she acquired.

An emphasis on mere capability to use has arisen elsewhere. For instance, in [Torres v. Prudential Financial](#), ActiveProspect software was again at issue. This time, the software made the plaintiffs' interactions with Prudential's webform accessible to certain ActiveProspect employees for troubleshooting purposes. The court found that ActiveProspect was a third-party eavesdropper because these employees were capable of accessing and viewing session replay data for its own ends.

This reasoning was also implied by *Rodriguez v. Autotrader.com*, where search queries were shared with a third-party search engine provider and third-party advertisers. While the court conceded the search engine provider was a close question, it concluded there was no showing that the advertising companies were "merely providing a tool that aids the Website," making these entities third-party eavesdroppers.

Likewise, in [Taylor v. ConverseNow Technologies](#), the court found ConverseNow Technologies to be a third-party eavesdropper because the company had the capability to use intercepted customer phone calls for its own purposes — for example, to improve its services and refine its algorithms.

In another example, the court in [Rodriguez v. Ford Motor Co.](#) found the plaintiff sufficiently alleged the defendant's software service provider had the capacity to do more than store the website's chat communications and could use it to create an extensive customer dataset to use for its own purposes.

What is considered contents of a communication?

Clause two of Section 631(a) further requires that a third-party eavesdropper intercept the "contents" of a communication, not merely its "record information." A CIPA claim follows the same analysis and definitions of the ECPA of 1986. The ECPA defines contents as "any information concerning the substance, purport, or meaning of [a] communication." However, the statute does not cover record information, such as a communication's metadata. A helpful analogy is a letter in the mail. The letter itself contains the content of the communication, whereas the envelope, with addresses and postage, contains mere record information.

Some district courts have allowed CIPA lawsuits to proceed beyond motions to dismiss where the complaints sufficiently allege the data points collected — such as the users' clicks, swiping, scrolling, mouse movements, geolocations, IP addresses and typing — were content within the meaning of the statute. For example, in [Saleh v. Nike](#), the court found the plaintiff sufficiently pleaded the defendant's vendor had collected the contents of communications. Despite information such as "names, addresses, telephone numbers, and email addresses" commonly being record data, this information could become content when entered into a form on a website.

Furthermore, in [Doe v. Eating Recovery Center](#), the court concluded the URLs reflecting the plaintiff's navigation to websites about anorexia, treatment options and a self-assessment form conveyed more substantive information than basic identification and address information, i.e., record information, and constituted content. Likewise, in [Crano v. Sojern](#), the court held that the interception of information like hotel name and location, room price, check-in and check-out dates, and reservation completions amounted to the content of communications.

However, other courts found collecting users' visit dates and time stamps, IP addresses, locations, browser types, device types and metadata are not content within the meaning of CIPA.

In [Yoon v. Lululemon](#), the court rejected the plaintiff's argument that third-party software intercepted the contents of her communications with the defendant through data about her keystrokes, IP address, location and browser type, among others, because "none of these pieces of data constitutes message content in the same way that the words of a text message or email do."

Likewise, in *Ramos v. Gap*, the court found the plaintiff's allegations that the third-party intercepted the time, date, device type, geolocation and engagement with content only amounted to record information. In *Jones v. Tonal Systems*, the court concluded that while the plaintiff alleged she engaged with the chat feature on the defendant's website, such action was not enough to demonstrate that she shared more than record information.

Furthermore, in [Ingrao v. Addshoppers](#), the court determined the plaintiffs only showed that Addshoppers tracked their webpage visits but not that they provided any personal information to the website, failing to allege the defendant intercepted the contents of their communications.

What does it mean to read or learn?

An additional element for clause two liability requires that a third-party eavesdropper read or learn the contents of a communication, not merely passively receive them without comprehending their meaning.

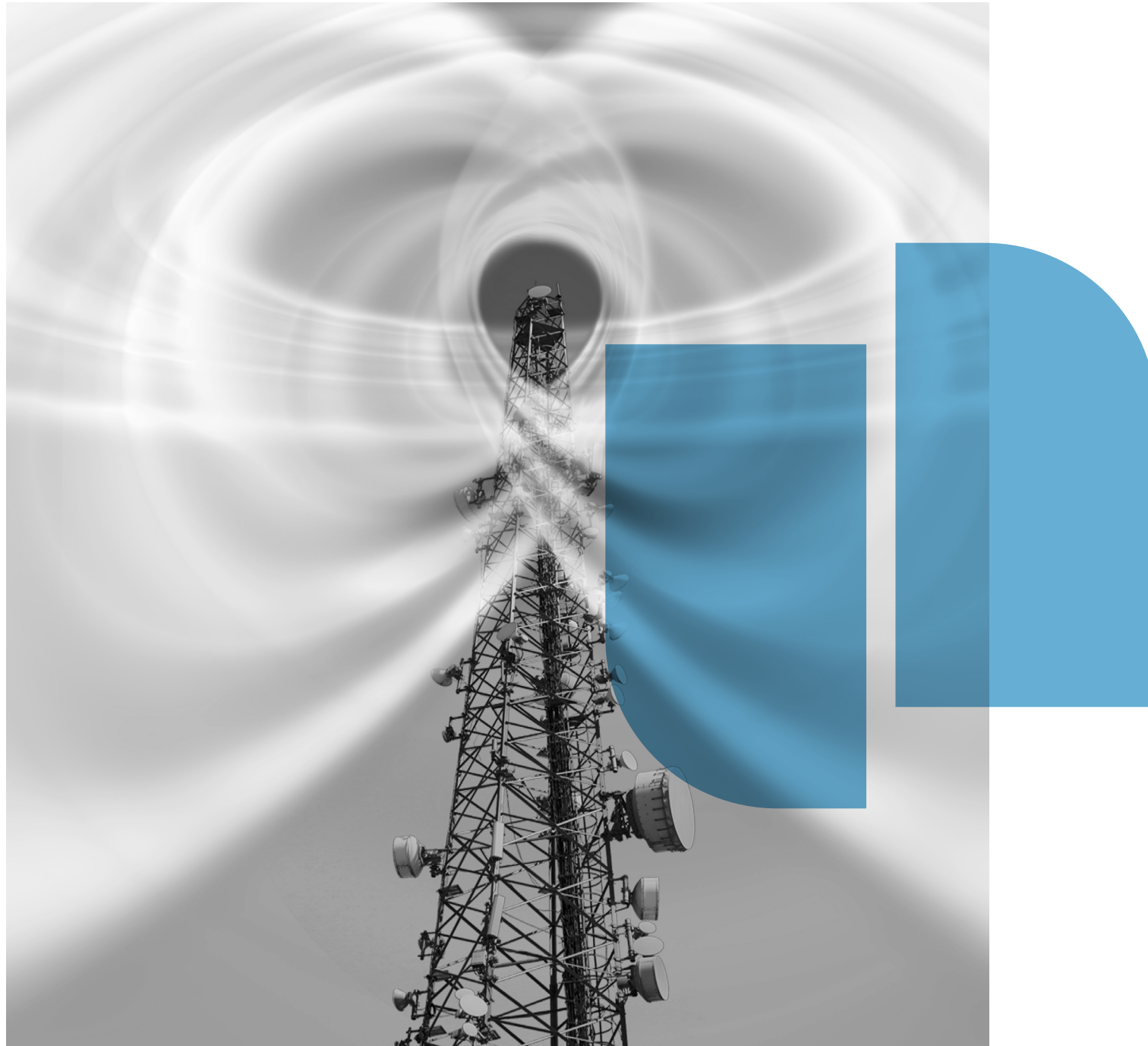
For example, the Torres court found that although ActiveProspect's session replay software functionally read certain data for the purpose of hashing sensitive data, this process operated on a predetermined and mechanical basis "with no intelligible understanding of those values required," meaning

no statutory reading took place. Similarly, in *Doe v. Eating Recovery Center*, the court held that Meta's automated filtering out of privacy protected information did not amount to reading since this process did not result in understanding the substantive meaning of the communication. While Doe argued that mere interception constitutes a step towards an "attempt to learn," the court reasoned such an interpretation would render the prohibition in CIPA § 632 meaningless.

In *Ramos v. Gap*, the complaint simply failed to allege that Bluecore, the alleged third-party eavesdropper, read the URLs that contained content information. Moreover, regarding Bluecore's reading of content entered into the defendant's website, the plaintiff did not allege that he entered any information into the website. Although the court in *Williams v. DDR Media* sympathized with the notion that reading a use requirement into the second clause of Section 631(a) threatens to swallow the third clause, it nonetheless found that Jornaya merely recorded the conversation for DDR and therefore did not read or learn the meaning of the communication.

And in *John Doe v. Google*, the plaintiffs alleged that healthcare providers placed Google pixels on their websites, enabling the company to unlawfully track, collect and monetize their private health information. The court held the plaintiffs failed to allege that Google intentionally read or learned the contents of private health communications, since they did not identify which webpages contained the problematic source code nor that the company intentionally or willfully received private health information.





When is a communication in transit?

As a final matter, the second clause of Section 631(a) requires that a third-party eavesdropper attempt to read or learn the contents of a communication while the communication is in transit. This issue comes down to the sequence of events.

In [Riganian v. LiveRamp Holdings](#), the complaint alleged that LiveRamp's event listeners intercepted user communications with various webpages after user inputs were made but before they were received by the webpage. This, the court held, set forth a theory of how LiveRamp read the intercepted content in real time and simultaneously with their transit to the webpage. Similarly, in *Rodriguez v. Autotrader.com*, the plaintiff alleged that her queries were rerouted to the third-party search engine provider and shared with advertising companies. The court concluded this created a reasonable inference that her queries were read during transit. In *Taylor v. ConverseNow*, the court found the plaintiff plausibly pled a claim of real-time interception because while she believed she was only speaking to the intended recipient, the call was actually routed through third-party AI voice assistants.

On the other hand, the Griffith court determined the plaintiffs' communications were not intercepted in transit because the pixel software only shared their information with the defendants after it was received by the third-party site. To hold otherwise, the court said, would defy the narrow definition of "interception" adopted by the Ninth Circuit in [Konop v. Hawaiian Airlines](#), which focused not only on timing but also on sequence. Similarly, in *Doe v. Eating Recovery Center*, the court found that Meta's receipt of URLs and browsing activity through the defendant's use of Meta Pixel to improve their internet advertising did not occur while the information was in transit. The court held that Meta processed the information only after it passed from the plaintiff to the defendant.

The court in *Torres v. Prudential Financial* took a similar stance, concluding that ActiveProspect reassembled the session replay data for analysis only after it was stored on their server, not while it was in transit from the plaintiffs to the defendant. And while ActiveProspect employees could ultimately learn the substantive meaning of the session replay data, that inquiry was not relevant here where the sequence of events was what mattered.

Relatedly, the court in *Crano v. Sojern* held that the defendant did not intercept the plaintiff's booking information while it was in transit. The plaintiff merely alleged Hilton and Marriott could redirect her communications to third parties like Sojern, not that Sojern intercepted them before they reached their intended recipient.

Finally, the Ninth Circuit came to a similar conclusion in [Boulton v. Community.com](#). The court held that a text message the plaintiff believed she sent to the music artist LL Cool J's personal number but was actually sent to his Community-provided number was not accessed in transit because Community could only read the text after it had reached its intended recipient. The appellate court also rejected Boulton's argument that "being received at" prohibits any nonconsensual access to communications merely received in California, whether in transit or not.

How can entities comply with Section 631(a) while using analytic tracking technologies?

While courts may refer to CIPA as a total mess, with one calling it "borderline impossible to determine whether a defendant's online conduct fits within the language of the statute," businesses can still take various steps to mitigate the risk of potential CIPA violations. Privacy notices and terms of use policies should be readily available to website visitors and should detail the types of trackers used on the business' website. The notice should also inform visitors of what data

will be collected while using the website and provide a mechanism for opting out of data collection.

Businesses should also consider configuring the settings of tracking software to limit or reduce the amount of personally identifiable information, only collecting the data needed to provide necessary analytics. Organizations should also consider discontinuing and deleting unnecessary or redundant trackers to avoid over-collecting data that could be interpreted as content under CIPA and other wiretapping laws.

Businesses can also take lessons from the case law. Implied consent is likely not transferable to an undisclosed party nor does continued use of a website imply consent to third-party interception. In fact, to say that continued use of a website implies consent to interception would undermine standing to seek injunctive relief since it would be impossible to show that the plaintiff will suffer irreparable harm if they cannot use the website. Furthermore, conspicuous banner notices may be enough to obtain the implied consent of website visitors, but that issue is likely premature for the pleading stage.

Express consent may not be retroactive to a time before it was obtained, even where a privacy policy applies during all times that a user interacts with a website. In other words, if a user hasn't explicitly agreed to interception by a third-party, even the broadest privacy policy is not guaranteed to apply.

Another critical takeaway regarding consent is that obtaining consent for third-party interceptions based on vague disclosures may turn on the privacy concerns surrounding the third party. Indeed, a party like TikTok — whose "size, foreign ownership, and perceived activities" made it less likely that a reasonable user would expect them to be lumped into vague disclosures about data collection by service providers — might require a more granular disclosure to

ensure proper consent is obtained. Regarding the party exception, the technical recipient of a user's communication is likely a party to that communication — and exempt from clause two liability — even if the user doesn't intend that party to be the recipient. For example, if software or code directs a user's browser to communicate directly with an unknown third party, the recipient is probably a party to the communication, irrespective of the user's intention. Moreover, pleadings matter. If a plaintiff refers to themselves as a user of the alleged third party, or if the third party is necessary for the functionality of one of the communicating parties, courts are likely to treat that third party as a participant in the communication.

The tape recorder-friend dichotomy is helpful in cases of possible third-party eavesdroppers, though it can be somewhat misleading. While the relevant question is whether the third party merely recorded the information for the benefit of the first party as a tape recorder would or used the communication for its own purposes like a friend would, courts have added a further distinction: Whether the friend category requires actual use for one's own purposes or merely the capability to do so.

Query whether an actual use requirement in the second clause of Section 631(a) swallows the third clause or reinforces the tape recorder-friend distinction. It's true that a tape recorder can't use a recording for its own purposes, but it's also true that a friend can use a recording and possess the mere capability to do so. Perhaps, like CIPA more generally, the tape recorder-friend distinction is outdated and only confuses modern fact patterns.

As such, businesses should closely review procurement contracts and monitor third-party vendors to ensure their conduct will not leave them at risk for litigation.

Equally important is the envelope-letter dichotomy when clarifying content versus record information. Like the words in a letter, the substance of one's web activity is usually content. But like the words on an envelope, the routing information necessary to facilitate web activity is likely only record information.

Moreover, a third-party eavesdropper must actually comprehend the contents of the communication, not merely receive it in a passive manner. Dichotomy notwithstanding, there is disagreement on what information may be "contents," so businesses must clearly inform website users what information will be collected by the tracking tool while using the site. By providing an option for users to opt out of data collection, they can consent to the use of these tracking tools and their data collection.

Lastly, the sequence of the interception in relation to the sending and receiving of the communication is key. A third-party eavesdropper must intercept the communication while it is in transit, not after it has been delivered to the recipient. And "being received at" is also an active concept; it does not include communications that were received in the past.

Following this case law comprises a significant step towards understanding the nuances of CIPA, at least those contained in the second clause of Section 631(a).

Section 632: the recording device provision

Aside from Section 631, CIPA contains other sections that carry liability risk. One such provision is Section 632, the so-called "recording device" provision. While not as dense as Section 631, it nonetheless poses interpretative hurdles for litigants to dispute and courts to clarify.

Section 632(a) punishes any person who intentionally and without consent from all parties eavesdrops on a confidential communication using an amplifying or recording device. It does not matter whether the parties are communicating in person or "by means of a telegraph, telephone, or other device, except a radio." Reviewing the relevant litigation, the term "confidential communication" likely receives the most heated debate.





When is a communication confidential?

Section 632(c) defines "confidential communication" as "any communication carried on in circumstances as may reasonably indicate that any party to the communication desires it to be confined to the parties thereto." There is a presumption that internet communications do not reasonably give rise to an expectation of confidentiality, though at least one court in [In re Meta Pixel Healthcare Litigation](#) found that presumption was overcome.

In that case, the Northern District of California found that the plaintiffs properly alleged their internet communications were confidential where the Meta Pixel transmitted their patient information to Meta when they logged into patient portals on their medical provider's website. The communications included information about doctors, medical conditions and appointments. For the purposes of a preliminary injunction, the court found the plaintiffs would likely be able to show a reasonable expectation their communications were confidential because patient-status and medical-related communications between patients and providers are protected by federal law and are uniquely personal.

Courts have also likened the confidentiality analysis to the reasonable expectation of privacy analysis. Following that logic, the court in *Griffith v. TikTok* distinguished the facts at hand from those alleged in [In re Facebook, Inc. Internet Tracking Litigation](#). In the latter, the Ninth Circuit found that the plaintiffs plausibly alleged a violation of their reasonable expectation of privacy where Facebook tracked the plaintiffs' browsing data even when they were logged out of Facebook. The appeals court supported its finding with the fact that Facebook collected a huge amount of personalized information that could be tied to the user's identity, allowing it to "gain a cradle-to-grave profile without users' consent."

The Griffith court, on the other hand, found the plaintiffs' allegations against TikTok lacked this level of egregiousness, holding that they failed to demonstrate that the defendants recorded their confidential communications. There, the plaintiffs alleged TikTok installed pixel software and an API tool on third-party websites to collect information about non-TikTok users when they visited those websites in violation of Section 632.

However, the court found the plaintiffs were not TikTok users and the defendant did not have profile information necessary to identify the data collected by the pixel software as belonging to them. Nor did they identify any especially sensitive information collected from them by the defendant. Moreover, the defendant's pixel software was installed on a relatively small percentage of websites, preventing it from capturing the plaintiffs' comprehensive browsing history.

The medium of communication may also be conclusive. In fact, the definition for confidential communication excludes "a communication made in a public gathering or ... in any other circumstance in which the parties ... may reasonably expect that the communication may be overheard or recorded." As such, in *Boulton v. Community.com*, where the plaintiff alleged her text messages to LL Cool J were intercepted, the Ninth Circuit concluded that text messages are by nature recorded and therefore cannot be understood as confidential communications under Section 632, which explicitly excludes communications that may be overheard or recorded.

However, a phone call is a different story, so long as the party alleging a violation has not consented to the call being recorded and sensitive information is shared. In *Taylor v. ConverseNow*, the plaintiff alleged the defendant's AI voice assistant answered her call to the pizza chain Domino's, during which she provided her name, address and credit card information. Finding that a confidential communication took place, the court pointed out the plaintiff alleged that she shared her personally identifiable information and personal financial information and did not consent to the call being recorded.

Takeaways from Section 632 case law

There are a couple of takeaways from the case law. Regarding confidential communications under Section 632, internet communications are likely not confidential unless they involve sensitive information that has a reputation for being kept private. Information like medical data that is protected by federal law or a relationship between parties that gives one the means to build personalized profiles on individuals might qualify as confidential.

This analysis is comparable to the reasonable expectation of privacy analysis — if there's no reasonable expectation that the communication will be kept confidential, then it's likely not confidential. Relevant questions include: Did the plaintiff behave privately and is there an objective expectation that the communication should be private? Would the plaintiff reasonably expect their communication to be disclosed as alleged? And is the intrusion highly offensive? Determining answers to these questions can be helpful.

Furthermore, confidentiality can also depend on the medium of communication: A text message, which is inherently recorded, is excluded while a phone call that includes sensitive information is likely not.

Section 632.7: The telephone provision

Section 632.7 is a less litigated provision of CIPA that turns on the medium of communication. This section prohibits the interception of a communication between two telephones — or such assistance to another party — regardless of whether one or both phones are landlines, cordless or cell phones. However, courts have interpreted this provision somewhat narrowly, especially as it pertains to 21st century technology.

For instance, in *Jones v. Tonal Systems*, the plaintiff alleged he used his smart phone to engage with the chat feature of the defendant's website, which, unbeknownst to the plaintiff, included an API run by third-party vendor Drift that created and stored transcripts of the plaintiff's communications. Dismissing the plaintiff's claim, the court cited copious precedent finding that this provision does not encompass web-based messages sent from the internet browser of a smartphone. Further, the court concluded that any application of Section 632.7 to a communication involving only one telephone, such as in *Licea v. Old Navy*, is likely misguided. Old Navy relied on dicta from a California Supreme Court [case](#) that analyzed the meaning of "confidential communication" under Section 632, which was not at issue in *Jones*.

The conclusion that Section 632.7 does not apply to communications involving only one telephone is supported by the Ninth Circuit in *Boulton v. Community.com*. The court affirmed the dismissal of the plaintiff's claim because they alleged the defendant was a social media platform and therefore their text message to the platform was not received by a telephone. This implies the plaintiff's claim would fail even if the device she texted from were deemed a telephone.

Section 638.51: The pen register provision

Another popular avenue for CIPA litigation arises in Section 638.51. This section prohibits the installation of a pen register or trap and trace device without a court order.

Section 638.50 defines a pen register as "a device or process that records or decodes dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted, but not the contents of a communication." This can generally be thought of as a device that captures the outgoing numbers dialed by a telephone.

On the other hand, a trap and trace device is defined as "a device or process that captures the incoming electronic or other impulses that identify the originating number or other dialing, routing, addressing, or signaling information reasonably likely to identify the source of a wire or electronic communication, but not the contents of a communication." This can be thought of as a device that captures the incoming numbers received by a telephone.

Importantly, Section 638.51 exempts providers of electronic or wire communication services from liability when they use either device to operate or maintain their services; protect their rights and property; protect themselves and users from fraudulent, abusive or unlawful use of the service; or obtain user consent.

The applicability of both definitions and exemptions is routinely disputed through litigation.

What constitutes consent under Section 638.51?

As with so many interception claims, consent by the impacted party is a surefire defense. That said, a website that consents to the installation of tracking software on a visitor's browser is likely not the user of the software.

In *Rodriguez v. Autotrader.com*, the plaintiff visited the defendant's website, which immediately and without consent, installed third-party tracking software on their browser in order to deliver targeted advertising. The plaintiff also made a search query on the website involving private information that was shared with third parties. Defending against a Section 638.51 claim, the defendant argued that it was the user of its website and therefore, like a telephone call recipient that installs caller ID on their telephone, consented to the installation of the tracking software. However, the court concluded that the website installs the software on a visitor's browser before they have any opportunity to consent to the defendant's privacy policy, making the visitor the user who must consent.

Furthermore, although the defendant argued that any reasonably informed visitor would understand their IP address would be collected when visiting a website and therefore implicitly consent to that collection, the court found the plaintiff alleged the software captured more than just her IP address, such as her operating system information, browser information, geolocation data and email address.

The court in [Levings v. Choice Hotels](#) explicitly concluded that a user does not automatically consent to the collection of their IP address whenever they visit a website; a holding to the contrary, the court said, would render CIPA's pen register provision meaningless.



Meanwhile, the court in [Rodriguez v. Plivo](#) held that the plaintiff implicitly consented to the collection of her IP address since the "Plaintiff's computer could not have accessed [the] Defendant's website unless it provided her IP address."

What is the meaning of a device or process?

Perhaps the most contentious point of disagreement in regard to Section 638.51 lies in the meaning of "device or process," used to define both a pen register and a trap and trace mechanism. In fact, two state court rulings out of the same county came to opposite conclusions as to how broadly the word device should be applied. One [expert](#) noted that these "results offer a cautionary tale of what can happen when trial judges, without guidance, are tasked with interpreting how laws should apply to technologies that they may not fully understand."

In the first case, [Licea v. Hickory Farms](#), the plaintiff alleged the defendant's website installed a pen register and trap and trace software on her personal device in order to collect her IP address. The Los Angeles Superior Court granted the defendant's demurrer, finding the plaintiff failed to allege what device or process operated by the defendant constituted a pen register, and that internet connected devices — and the particular tracking technology that may be installed thereon — do not fall within the statute's scope. The court distinguished the IP address contained in this complaint from precedent where a unique digital fingerprint was involved, emphasizing that public policy rejects the plaintiff's interpretation of CIPA because every entity that collects an IP address from a potential plaintiff would be in violation, "potentially disrupt[ing] a large swath of internet commerce."

In [Levings v. Choice Hotels](#), the plaintiff alleged the defendant installed a pen register on their laptop after visiting the company's website, allowing it to perform identity resolution and collect

information like the plaintiff's name, address, voter registration status, employment information and familial relations. A different judge in the Los Angeles Superior Court denied the defendant's demurrer, concluding that the plaintiff properly pled the illegal use of a pen register by stating the defendant deployed a software device and process that recorded information from the plaintiff's device and used that information to install tracking code on it. The court held that a more detailed description of the software was not required at the pleading stage.

Some [onlookers](#) find the narrow holding in Hickory Farms better supported by legislative history and case precedent. For example, relevant California Assembly and Senate committee discussions only addressed pen registers in the context of landline and mobile phones. In further support of this narrow reading, the court in [Licea v. Cinmar](#) rejected the idea that related CIPA sections, like 631(a) and 632.7, should include smartphone technology because modern amendments have not been made to specifically exclude it.

The problem is CIPA pen registers and trap and trace devices are not, by definition, limited to the context of telephones or telegraphs. This detail led the court in Riganian v. LiveRamp to hold the pen register definition is not limited to telephones because Section 638.51, unlike other related sections, does not specifically refer to telephones.

Therefore, the drafters knew how to refer to specific types of technology, but in the pen register case, intentionally decided not to. Similarly, in [Greenley v. Kochava](#), the court noted that in drafting Section 638.51, the legislature was specific as to the type of data a pen register collects, but vague as to the form of the collection tool, implying that the provision could encompass modern software on modern equipment. There, the court found the plaintiff sufficiently alleged the defendant's embedded tracking software was a "process" under CIPA's definition of a pen register.

Still, courts continue to push back on this logic. For example, in [Aviles v. LiveRamp](#), the Los Angeles Superior Court weighed in again, finding that a beacon installed on users' browsers by the defendant's website to collect IP addresses did not constitute a pen register or a trap and trace device. As to the former, the plaintiff did not allege the beacon collects all outgoing addressing information from users' browsers, and as to the latter, they merely alleged that the beacon collects the information of incoming visitors — as if the defendant had installed a trap and trace device on its own website.

In [Variety Media v. Superior Court](#), the California Second District Court of Appeal, is reviewing and may lend definitive guidance on this issue.

Which type of data does Section 638.51 regulate?

If the type of device that Section 638.51 regulates remains unclear, perhaps the type of data this ambiguous device must collect has been sorted out. While [Greenley v. Kochava](#) found that the defendant's software development kit, collected personal and geolocation data and effectively fingerprinted unique devices, did constitute a pen register, the court in [Licea v. Hickory Farms](#) held that a device that merely collects IP addresses was not equivalent.

The court in *Rodriguez v. Plivo* agreed with this distinction, finding that an IP address that reveals a device's state, city and zip code is not the type of sensitive data with which the Greenley court was concerned. In [Casillas v. Transitions Optical](#), the court put it bluntly: "obtaining IP addresses from ordinary user access does not violate the pen register statute." And in [Heeger v. Facebook](#), the court held that IP addresses are afforded a lower level of privacy protection because internet users are generally aware that they disclose this information to third parties anytime they access websites.

Likewise, the court in [Gabrielli v. Insider](#) dismissed a Section 638.51 claim after finding the plaintiff lacked standing. The plaintiff alleged the defendant's use of a third-party tracker on its website, which logged visitors' IP addresses, constituted an illegal pen register. However, the court rebuffed the plaintiff's arguments, concluding that an IP address does not reveal personal information of a visitor and its collection and disclosure does not constitute an invasion of privacy redressable by a federal court.

Courts have spoken to other types of data as well. In *Price v. Headspace*, the plaintiff alleged the defendant used a pixel to capture the numbers, emails and routing addresses of users that visited its website. Importantly, the pixel also collected images of users' interest in the defendant's services. The court held that Section 638.51 does not apply to such a pixel since images constitute the contents of a communication, which is specifically excluded from the definitions of pen register and trap and trace devices under Section 638.50.

How can entities mitigate Section 638.51 liability?

Section 638.51 has its nuances and unsettled provisions. For instance, the meaning of "device" remains contentious as well as the issue of whether "pen registers," as defined, can be installed on modern, internet connected equipment. However, as some courts have pointed out, other CIPA sections refer specifically to outdated technology, but this section does not. Does that mean a more expansive interpretation of device should prevail? Also, it matters how the device actually performs — whether it collects all outgoing routing information or just enough to communicate with a user's browser could be the difference between being within scope or out.

Questions over consent to the use of a pen register also remain. While it is not a defense for a website to consent to the installation of a pen register on a visitor's browser, the issue of whether a website visitor implicitly consents to the collection of their IP address remains in dispute. Perhaps it is best to simply get explicit consent for this type of collection.

Fortunately, the scope of data that a pen register collects is relatively settled: IP addresses and images — that is, content — are not protected by CIPA Section 638.51.

With this information, digital responsibility professionals can inch closer to a comprehensive grasp on CIPA applicability and risk. Although some questions are more certain than their answers, what can feel like an insurmountable legal task can become less so with a growing framework of case law.

As litigation under CIPA continues, businesses using tracking technologies must closely monitor court decisions and make sure their tracking tools are reasonable, proportional and well maintained to limit the collection of personal information that can lead to unnecessary and expensive litigation.



Part 3: The Federal Wiretap Act

In 1986, Congress passed the Electronic Communications Privacy Act to update the Federal Wiretap Act of 1968. Title I of the ECPA, often referred to as the Wiretap Act, punishes "any person who (a) intentionally intercepts ... any wire, oral, or electronic communication," among other related conduct.

The Ninth Circuit has held that the term intercept has a narrow definition and requires that a communication be acquired during transmission rather than while in storage. In *Boulton v. Community.com*, where the intended recipient of a text message was alleged to have intercepted the communication, the Ninth Circuit found such was not the case since the defendant only could have accessed the text after it was received, that is, while it was in electronic storage.

Furthermore, interception cannot be speculative. In [Rodriguez v. ByteDance](#), while the plaintiffs explained how CapCut could obtain communications in transit, they failed to allege that the defendants in fact intercepted their communications — that is, how it occurred, to whom and what the communications contained.

Unlike CIPA, Wiretap Act liability can be defeated with the prior consent of only one party to a communication. As such, it's helpful to understand up front what prior consent means under the Federal Wiretap Act framework.



When is prior consent obtained?

Section 2511(2)(d) of the ECPA contains the following exception: A person may intercept a communication "where such person is a party to the communication or where one of the parties to the communication has given prior consent to such interception."

In order to properly obtain consent for purposes of the Federal Wiretap Act, transparency must be specific but need not be exact. Indeed, [courts](#) have held that "Congress intended the consent requirement to be construed broadly," meaning excessively granular disclosures are not necessarily required.

For example, in *Lakes v. Ubisoft*, the plaintiffs alleged the defendant's website shared their unique Facebook ID and video request data with Meta via pixel software when they visited the site to download video games while logged into their Facebook account. That said, anytime a user visited the website, they were presented with a browserwrap agreement that conferred consent to the use of cookies by Ubisoft and its partners to offer targeted advertising. Furthermore, users were required to affirmatively accept Ubisoft's terms of use, terms of sale and privacy policy when they created an account; users were also presented with the privacy policy again when they made a purchase on the site. The privacy policy informed users that their information would be shared with third parties.

Nevertheless, the plaintiffs argued these notices were not sufficient. In their view, the disclosures did not adequately explain the defendant's practice of exposing the plaintiffs' Facebook ID combined with the titles of video games they downloaded, or that Meta itself would collect PII through the pixel. They pointed to case law where consent defenses were rejected: In [Brown v. Google](#), the court found that Google's disclosures failed to specifically disclose the alleged data collection would occur during private browsing mode. In [Calhoun v. Google](#), the court found that Google's various notices, when read in conjunction,

would not necessarily inform a reasonable user that they were consenting to the alleged data collection. And in the case of *Meta Pixel Healthcare Litigation*, the court held that a generalized notice did not adequately disclose Meta's collection of protected health information.

Case law notwithstanding, the Northern District of California accepted Ubisoft's privacy policy as sufficiently granular where it explicitly stated the defendant uses various technologies to collect data when its services are used, and it allows partners to set and access cookies on users' devices. Moreover, the court found that only the defendant's privacy policy was at issue — as opposed to additional agreements and notices — and as such, a reasonable user would understand that they are consenting to the use of cookies by third parties.

Since the Federal Wiretap Act is a one-party consent law, the service provider's consent can also defeat liability. In *John Doe v. Google*, the plaintiffs alleged their healthcare providers permitted Google to place pixels on their websites, giving it the ability to collect and monetize plaintiffs' PHI. Under these circumstances, it was clear to the Northern District of California the healthcare providers consented to installing Google source code on their websites. Even assuming the healthcare providers were misled by Google into installing the source code without fully understanding how it operated, that would require the heightened pleading standard of Federal Rule of Civil Procedure 9(b) necessary for allegations of fraud, which was not present.

A party to a communication is safe from direct liability

Intimately related to prior consent, the party exemption arises under the same language in Section 2511(2)(d). Like CIPA, a party to a communication cannot be liable under the Wiretap Act for intercepting that communication.

In *Karwowski v. Gen Digital*, the court found the party exemption applied where the owner of a browser extension intercepted communications between appellants and the internet search engines they used. While the plaintiffs alleged they shared their communications with the Avast Online Security & Privacy browser extension, they claimed they did not do so with Gen Digital. Finding for the defendants, the Ninth Circuit held that Gen Digital was a party to the communication since the plaintiffs referred to themselves as Gen Digital users and explicitly acknowledged that Gen Digital was potentially a necessary party for website verification.

Likewise, in *Doe v. Genesis Health System* where the defendant allegedly disclosed PII and PHI to third parties via tracking technology on its website, the Central District of Illinois held that Genesis was a party to the communication because the intercepted communications could not have occurred without the involvement of the intended recipient, that is, Genesis.

The same was the case in *Crano v. Sojern*. The Northern District of California granted the defendant's motion to dismiss the plaintiff's Federal Wiretap Act claim, where Sojern collected information entered by the plaintiff on a website operated by Hilton and Marriott. Because both Hilton and Marriott, parties to the communications, consented to Sojern's involvement, a necessary element to the plaintiff's claim was missing.



An exception to an exemption: The crime-tort exception

While prior consent and the party exemption are relatively straightforward, the limitation on these liability carveouts can be more nuanced. Drawing again on Section 2511(2)(d), the exemptions discussed above apply "unless [a] communication was intercepted for the purpose of committing any criminal or tortious act in violation of the Constitution or laws of the United States or of any State."

Conduct that constitutes a crime-tort is intuitive in that it either meets the definition of a statutory crime, or it follows the general formulation for an invasion of privacy. That formulation consists of an intrusion upon a reasonable expectation of privacy, which was highly offensive. For example, the Northern District of California in [Riganian v. LiveRamp](#) found the crime-tort exception applied where the plaintiffs alleged LiveRamp collected their PII, including digital identifiers from countless sources; aggregated this data into a single identity profile; and sold such profiles on its data marketplace without meaningful consent.

Likewise, in [Smith v. Rack Room Shoes](#), allegations that Rack Room, contradictory to its privacy policy, embedded third-party code in its website that shared users' information with third parties — including URLs, user browsing activity, PII and email accounts — amounted to a crime-tort and the resulting exception. And in [Hartley v. University of Chicago Medical Center](#), the court found the crime-tort exception adequately pleaded where the plaintiff alleged the defendant disclosed to a third party her access to a healthcare provider's patient portal along with identifying information, thereby revealing her status as patient in violation of HIPAA.

In contrast, the plaintiff in [B.N. v. Oregon Reproductive Medicine](#) failed to plead a crime-tort exception. The plaintiff only alleged that she visited public-facing webpages and entered queries on those

pages. The U.S. District Court for the District of Oregon found the complaint did not sufficiently allege the interception of confidential information, as the complaint failed to show that any information regarding the physician with whom the plaintiff scheduled an appointment or any treatment details had been disclosed. Nor did the plaintiff allege the defendant specifically disclosed any information to a third party. She did not claim the defendant's website was the only online source where she input information related to medical services nor that she received targeted advertising close in time to using the defendant's website.

The U.S. District Court for the District of Minnesota in [Okash v. Essentia Health](#) came to a similar conclusion, holding that the crime-tort exception did not apply because the plaintiff's data was intercepted from a public-facing portion of a website.

This distinction notwithstanding, there are further interpretative nuances to the crime-tort exception that make its applicability unsettled.

Intentional, separate and independent conduct

First, courts clarify that the alleged criminal or tortious act must be intended at the time of the interception. In [R.S. v. Prime Healthcare Services](#), the court found the temporal intent component of the crime-tort exception well pled. The plaintiff alleged that, by installing pixel software and programming its webpages to share protected communications with third parties, the defendant intended to disclose the plaintiff's private information upon interception. Similarly, the court in [Smith v. Rack Room Shoes](#) found the plaintiffs adequately alleged that Rack Room intended to disclose customers' personally identifiable information to third parties at the time of interception.

In contrast, the [John Doe v. Google](#) court declined to find the sufficient level of intent required by ECPA claims, where the plaintiff merely alleged Google may have been aware that protected information was being transmitted to third parties.

Secondly, courts hold that the crime-tort must be separate and apart from the interception itself. For example, in [Smith v. Rack Room Shoes](#), the plaintiffs alleged the defendant intended to disclose personally identifiable communications that it had promised not to collect or use, and this constituted a further tort, i.e., an invasion of privacy, beyond the initial interception. Likewise, the court in [R.S. v. Prime Healthcare Services](#) found the "separate and independent" component satisfied, where the plaintiff alleged that the defendant's disclosure, not merely its interception, violated HIPAA. There, the court also found that it was irrelevant that the disclosure simultaneously happened with the interception since the defendant's purpose to disclose private information to third parties remained the same at the time of interception.

But not all courts are so lenient. The court in [Okash v. Essentia Health](#) held that the alleged simultaneity of the defendant's interception and the disclosure of the plaintiff's personal information to third parties defeated the separate and independent component of the crime-tort exception.

Finally, the Central District of California made an important distinction in [Saedi v. Clearblue](#) regarding the separate and independent component. An interception constituting a violation of a separate anti-wiretapping statute, e.g., CIPA, does not amount to a separate crime-tort. In other words, "allowing plaintiffs to bootstrap an alleged CIPA violation to invoke the crime-tort exception in ECPA ... would allow the exception to swallow the rule."

Courts disagree on whether commercial purposes provide a liability shield

Equally important to the crime-tort analysis is the contentious issue of whether an interception carried out for commercial purposes can shield a defendant from the crime-tort exception, even where the defendant has committed a crime-tort, albeit inadvertently. A curious split exists amongst courts on this issue.

For example, many cases have followed the U.S. District Court for the Southern District of New York's line of reasoning set forth in [In re DoubleClick Privacy Litigation](#), which concluded that DoubleClick's purpose to make money by providing valuable web services shielded it from Wiretap Act liability, even "if any of its practices ultimately prove tortious." To sum up, the court stated, "a culpable mind does not accompany every tortious act."

The court in *Doe v. Genesis Health* agreed. Because the interception must be "for the purpose of committing ... any tortious act" for the exception to apply, the court concluded that the crime-tort exception "requires a specific intent that the defendant knew its acts were [unlawful]." And since Genesis used tracking technology for marketing and advertising purposes rather than with the specific intent of committing a violation of HIPAA, the crime-tort exception did not apply.

Likewise, in [Cape Cod Healthcare](#), the U.S. District Court for the District of Massachusetts found that the plaintiff failed to make factual allegations that the defendant's primary motivation for installing tracking technology and disclosing PHI was for the purpose of committing a crime or tort, as opposed to commercial gain or convenience — violations of HIPAA, invasion of privacy and breach of confidentiality notwithstanding.

But other courts have pushed back. The court in *Riganian v. LiveRamp* held that a commercial purpose does not shield a defendant from the crime-tort exception, reasoning that exploiting unlawfully obtained information is not permissible merely because it is profitable.

Likewise, the U.S. District Court for the Northern District of Illinois in [Stein v. Edward Elmhurst Health](#) quipped, "it would be odd to exclude an otherwise criminal or tortious act solely because it was motivated by financial gain. That's like saying that a bank robber's purpose was not to commit a crime — it was to make money." The Stein court also made a statutory construction argument, explaining that "criminal or tortious" modifies "act" rather than "purpose." As such, the statute requires a purpose of committing an act — one that may happen to be criminal or tortious. An interpretation to the contrary would import a mens rea element into the statute, which Congress could have included but, the court argued, did not.

Similarly, the court in *R.S. v. Prime Healthcare Services* concluded that the defendant's financial gain was contingent on disclosing HIPAA-protected information to third parties, and therefore any monetary gain did not immunize the defendant from ECPA liability. Otherwise, the court mused, the law would fail to penalize blackmail that relied on the disclosure of protected information merely because the end goal was to make money.

In [Sussman v. American Broadcasting Companies](#), the Ninth Circuit suggested alignment with this holding, stating that a "lawful purpose does not mean that the interception is not also for a tortious or unlawful purpose."

How businesses can mitigate Wiretap Act liability

Though it's been several decades since the Wiretap Act assumed its current form, disagreement over the scope of its provisions continues through the present. Still, close analysis of the settled — and unsettled — language can put businesses on a strong footing as they seek to mitigate liability.

First of all, it's worth noting that the Wiretap Act is relatively defendant friendly. Courts have narrowly construed the term intercept and denied the plaintiffs who merely allege interception of a speculative nature.

Further, consent can be properly obtained through disclosures that are specific but not necessarily exact. The consent provision of the statute is to be construed broadly, meaning disclosures and transparency obligations need not be overly granular, refer to the specific type of data collected nor the particular third parties with whom it is shared. Nonetheless, businesses should ensure that varying notices do not provide conflicting or ambiguous disclosures.

Importantly, this is a one-party consent law, meaning that the consent of a service provider alone — in most cases, the defendant — can defeat a claim. What's more, if the defendant is necessary for a web transaction or is the intended recipient to a communication, they are likely a party to the communication and safe from direct liability under the party exemption.

However, if a party commits a crime-tort in tandem with the interception, an exception to exemption may arise. Here, a crime-tort is exactly what it sounds like: Conduct that amounts to a statutory crime or tortious activity, the latter of which follows the elements of an invasion of privacy.

While courts agree the crime-tort must be intended at the time of interception but remain independent from the interception itself, they are divided over whether a commercial purpose shields a defendant from liability. The question comes down to statutory construction. Does the language of Section 2511(2) (d) say, in essence, "for the purpose of committing any crime or tort," or does it say, "for the purpose of committing any act, which also happens to be a crime or tort"? District courts disagree.

All said, there is precedent from the U.S. Court of Appeals for the Seventh Circuit in [Desnick v. American Broadcasting Companies](#) suggesting that an incidental tort does not defeat the party exemption, but that holding arose in the context of the media exercising its First Amendment rights, albeit in a potentially tortious manner. Whether First Amendment rights outweigh one's privacy interests is a complex [topic](#) worthy of separate discussion.

Indeed, the crime-tort exception remains in dispute. Even so, familiarity with the general contours of the Wiretap Act and its highly litigated provisions will give entities an upper hand in developing business strategies that ensure pragmatic compliance.



Part 4: The Video Privacy Protection Act

During the Senate confirmation hearings of Judge Robert Bork in 1987, a newspaper published his video rental history. While the 146 movie titles disclosed in the article were unremarkable, the incident prompted Congress to enact the Video Privacy Protection Act to protect the privacy of consumers who rented or purchased video cassette tapes and similar audiovisual materials.

The VPPA was amended once in 2012 to provide means of obtaining consent through the internet but has otherwise maintained its original language. As plaintiffs explore modern theories of liability, the scope of the law has been tested, creating circuit splits and sending one question to the [Supreme Court](#): What constitutes a consumer under the statute? This question is scheduled for the Court's October Term 2026.

The act provides statutory damages of no less than USD2,500 per violation, punitive damages, attorneys' fees and equitable relief. Because of these per violation damages, liability under the VPPA can be particularly costly.

Consent to disclosure under the VPPA

The VPPA sets out its own standard of informed, written consent under Section 2710(b)(2)(B), which must be distinct and separate from consent given for any other legal or financial obligations of the consumer. Consent must be given no more than two years before disclosure is sought, and the provider must give the consumer the ability to opt out from disclosures in a clear and conspicuous manner.

In *Lakes v. Ubisoft*, the Northern District of California found the defendant's privacy policy and cookie banner elicited adequate consent on all fronts. First, the consent was distinct and separate from other legal obligations. While the privacy policy and cookie banner contained other disclosures and statements, such as options to change and clarify consent preferences, the court agreed that these were not consumer obligations.

Further, consent was written and informed since the website prompted users with the option to "Set Cookie Preferences," allowing them to individually permit or decline particular cookie types; the plaintiffs were not required to sign onto any legal or financial obligations that would distract from their consent to the use of cookies and pixels on the website. Finally, the timing requirements for VPPA consent were met since consent was elicited each time a purchase was made on the website, and that consent lasted for two years, i.e., the statute of limitations for a VPPA claim.

On the other hand, in *Plotsker v. Envato*, the Central District of California declined to dismiss the plaintiff's VPPA claim on a consent basis. There, the court found the defendant's data collection disclosures were insufficiently explicit. "They merely state that Defendants collect information on user activity, that no personally identifiable information is collected by cookies, and that Defendants will use third party advertisers to serve ads."

When is a defendant a video tape service provider?

Under the VPPA, a video tape service provider is defined as "any person, engaged in the business ... of rental, sale, or delivery of prerecorded video cassette tapes or similar audio visual materials."

In *Christopherson v. Cinema Entertainment*, the plaintiff watched free movie trailers on the defendant's website and then started receiving movie advertisements on her Facebook page. The plaintiff alleged the defendant — a chain of movie theatres — tracked her online activity using the Meta Pixel and shared it with Meta in violation of the VPPA. The U.S. Court of Appeals for the Eighth Circuit held the defendant was not a VTSP under the statute because it did not provide video cassette tapes, nor does the moviegoing experience qualify as "similar audio visual materials."

The court reasoned that unlike a video cassette, which provides a viewer with some control, a movie at a theatre plays from start to finish with no opportunity to pause, rewind or fast forward. Similarly, even if the free trailers on the defendant's websites amounted to "similar audio visual materials," it was not engaged in the business of providing them. Its business was selling movie tickets and concessions, not advertisements in the form of web trailers. If the opposite were true, any company that delivered online video advertisements — McDonalds, for example — would fall within the VPPA's ambit.

Likewise, the Central District of California Court in *Walsh v. California Cinema Investments* held that cinemas were not VTSPs. They do not "deliver" videos because they "do not give their customers a possessory interest in the movies they show." And without providing a possessory interest, movie theaters do not rent videos by displaying them. Furthermore and like Christopherson, the fact that cinemas provide trailers on their websites does not amount to being in the business of delivering audiovisual materials.

The Ninth Circuit came to a similar conclusion in *Osheske v. Silver Cinemas*, where the defendant disclosed to Facebook the title and showtime of a film for which the plaintiff had bought a ticket. Not only did the defendant's ticket sales and in-theater experiences fail to amount to "similar audio visual materials," but the legislative context surrounding the VPPA was concerned with privacy and intellectual freedom in the home and living room, not a public space like a movie theatre.

However, the court did find a VTSP in *Plotsker v. Envato*. The defendant, an operator of an online library of over 100,000 pre-recorded videos, was alleged to generate revenue by offering paid subscriptions to the library. The plaintiff alleged he signed up for the defendant's services in exchange for access to the library. While Envato offered assets other than videos and therefore claimed it was not "engaged in the business" of providing videos, the court noted their inventory of stock videos amounted to 6.5 million assets, second only to their inventory of photos. Moreover, stock videos appeared first under the website's "Browse by category" header.

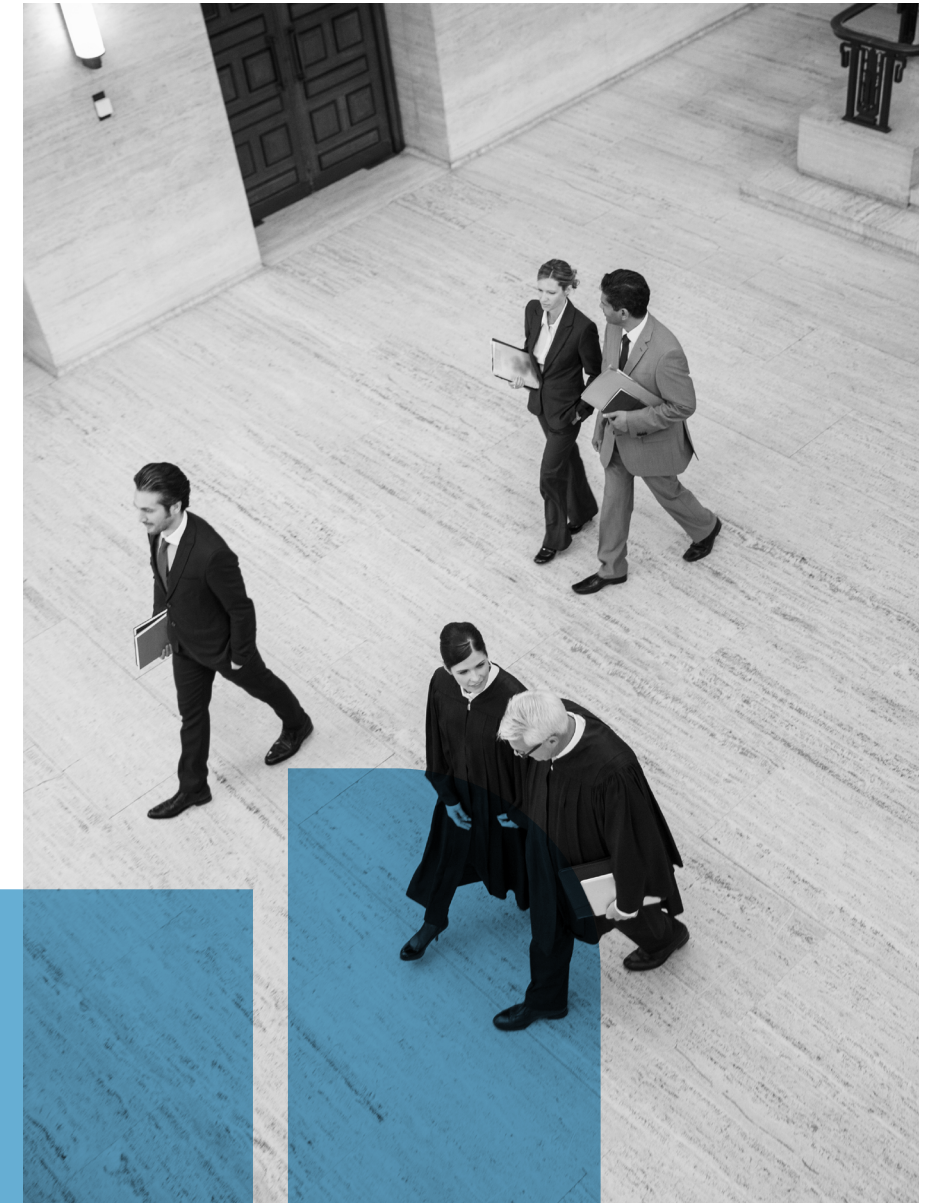
The Northern District of California Court also found a VTSP in [Cole v. LinkedIn](#), where the plaintiff alleged that she subscribed to LinkedIn Premium and watched video content on the LinkedIn Learning platform, information that was disclosed through the Facebook Tracking Pixel, now referred to as the Meta Pixel. While the defendant argued that its video content was incidental to its primary business of offering a professional networking platform, the court disagreed. Not only did the complaint exclude discussion of LinkedIn's services other than the video content on LinkedIn Learning, but in order to state a VPPA claim, "video production need not be a video tape service provider's 'overarching focus or particular field of endeavor.'"

Finally, the Court for the Western District of Michigan in [Goodman v. Hillsdale College](#) found the defendant was a VTSP, where Hillsdale hosted videos on its website and used them to prompt donations, sell materials, promote its online learning program and collect data for marketing purposes. In order to be "engaged in the business of" video delivery as required by the VTSP definition, the court held that a party need not turn a profit, produce revenue from or be primarily involved in delivering videos. Rather, a party may simply gain valuable information in exchange for providing video access, dabble in video delivery and deliver videos that are sufficiently related to the party's primary purpose — in this case, education — for the party's work to be significantly tailored to the production and delivery of videos.

Which consumers have a cause of action under the VPPA?

Only a consumer has a VPPA cause of action. Under Section 2710(a)(1), a "consumer" is "any renter, purchaser, or subscriber of goods or services from a video tape service provider." Some courts combine this definition with that of a "video tape service provider." Using this approach, a "consumer" is someone who rents, purchases or subscribes to a video tape service provider's video cassette tapes or similar audiovisual materials. However, this statutory portmanteau is hotly debated, with courts disagreeing over whether "goods or services" connotes just those products that relate to audiovisual materials or any products provided by a VTSP.

[Pileggi v. Washington Newspaper Publishing](#) expresses the narrow, defendant-friendly interpretation. The plaintiff alleged the defendant's website shared the videos she watched on the website with Facebook via the Meta Pixel. While she also subscribed to the defendant's email newsletter, which was embedded with news videos and hyperlinks, she did not allege they shared information about her viewing of newsletter videos or that she accessed the website via newsletter hyperlinks.





Holding the plaintiff was not a "consumer" under the statute, the U.S. Court of Appeals for the District of Columbia Circuit first reasoned it is a video that a consumer must subscribe to, not just any good provided by a VTSP. After all, the statute's title and liability section are centered around videos and those that market them, and the noun "video" throughout the statute refers to the relevant good to which a consumer must subscribe.

Moreover, the penalty provisions suggest that the statute's liability be construed narrowly since the stringency of liquidated damages weighs against judicial expansion and the punitive damages are meant to punish and deter wrongdoing, not make the plaintiff whole. An expansive reading of the word consumer, the court suggested, would permit someone who bought a ticket to a baseball game to sue the team owner after they watched a free video on the team's website years later, but would exclude someone who merely watched a free video on the team's website since they never purchased anything from the team.

Further, the court found that while the definition of "consumer" does not use the word "video" to describe "goods or services," the definition does require that those goods or services come from a VTSP. Since videos are the most contextually relevant good or service to come from a VTSP, those goods or services within the consumer definition must refer to videos.

Likewise, in [Salazar v. Paramount Global](#), the U.S. Court of Appeals for the Sixth Circuit held that the plaintiff was not a "consumer" where he subscribed to an online newsletter associated with 247Sports.com but did not receive additional access to video content beyond that of a normal visitor.

As such, the court found that "goods or services" within the definition of consumer must be read in the context of the statute as a whole: "the full definition of 'consumer' ... does not encompass consumers of all 'goods or services' imaginable, but only those 'from a video tape service provider.'" In other words, a person is a consumer only when they subscribe to video cassette tapes or similar audiovisual materials. The court conceded that the U.S. Courts of Appeals for the Second and Seventh Circuits held that so long as a person subscribes to a VTSP's products, they are a consumer — no matter what the product is. Moreover, the VPPA's definition of PII, which uses video to describe "materials or services," is the limiting factor in keeping VPPA claims linked to the provision of video goods or services. However, the Sixth Circuit pointed out that the PII definition uses the term "includes" and is therefore illustrative, not exhaustive. Hence, the PII definition is not limiting at all, meaning the consumer definition must do this limiting work by implying "video" to describe "goods or services."

Similarly, in [Brown v. Learfield Communications](#), the plaintiff provided his PII to subscribe to an email newsletter for the Texas Longhorns athletics website operated by the defendant. The newsletter linked subscribers to videos on the team website, which were accessible whether a visitor was a newsletter subscriber or not. Unbeknownst to the plaintiff, the defendant added the Facebook tracking Pixel to the website, which allegedly shared the plaintiff's PII with Facebook. The U.S. District Court for the Western District of Texas first found that the term "subscribes" within the definition of "consumer" does not require an exchange of money for access to goods or services since this does not account for the way society interprets "subscriber" nor would it uphold the VPPA's purpose to protect privacy.

Nevertheless, the court held for the defendants, reasoning that, as a matter of statutory construction, a VPPA "consumer" is a person who consumes audiovisual materials, not just any products or services from a VTSP nor just any products sold by a person who also happens to sell audiovisual materials, e.g., a department store. As the plaintiff failed to allege a contingent relationship between the newsletter subscription and access to the website's video content, they were not subscribers to audiovisual materials and therefore not "consumers" under the VPPA.

The Southern District of New York also declined to find a "consumer" in [Hughes v. NFL](#). While the court's reasoning was related to the fact the plaintiff failed to allege the proper goods and services, it was primarily focused on the term "prerecorded" within the VTSP definition. Although the plaintiff alleged that his NFL+ subscription provided him with access to content and features only available to subscribers, the court ultimately sided with the defendant because he failed to plead that he viewed prerecorded video content through the platform.

On the other hand, cases like [Salazar v. NBA](#) express the broader, plaintiff-friendly interpretation. There, the U.S. Court of Appeals for the Second Circuit held the plaintiff was a "consumer," where he shared personal information in exchange for access to an online newsletter. After watching videos on NBA.com while logged into his Facebook account, Salazar's personal viewing information was transmitted to Meta via the Facebook Pixel, allegedly in violation of the VPPA. First, the court held the newsletter constituted "goods or services" because the term goods and services in the definition of "consumer" is not limited to audiovisual materials, and since that definition does not include the term "audio visual material" whereas other provisions of the statute do.

Moreover, the definition of "video tape service provider," which is elemental to "consumer," encompasses "any" person engaged in the provision of audiovisual materials, meaning audiovisual content need only be part of their business. According to the Second Circuit, it is the definition of "personally identifiable information" that limits the statute's scope. While this provision may be illustrative due to the use of "includes," it also uses the term "video" to clarify that the statute's privacy protections are concerned with those transactions involving video materials or services and no other products or services.

Furthermore, the court held the plaintiff was a "subscriber" to the goods and services because someone doesn't need to spend money to be a VPPA "subscriber." Not only would an interpretation to the contrary render "subscriber" superfluous since "purchaser" and "renter" — which entail spending money — are already included, but the plaintiff's provision of personal information to the NBA created a relationship distinct from those with casual NBA.com viewers who were not signed up for the newsletter.

In [Yershov v. Gannett Satellite Information Network](#), the U.S. Court of Appeals for the First Circuit was also concerned with the meaning of "subscriber" within the definition of "consumer." There, the plaintiff alleged the defendant's USA Today mobile app, which he downloaded to his Android device, collected the titles of the videos he viewed as well as his device ID and GPS location and shared them with a third party in violation of the VPPA.

Holding that Yershov was a "subscriber" and therefore a "consumer," the court agreed that if "subscriber" required some sort of monetary payment, it would be rendered superfluous by the two preceding terms, i.e., "renter" and "purchaser." The court also distinguished the facts in Yershov from those in [Ellis v. The Cartoon Network](#), where the U.S. Court of Appeals for the Eleventh Circuit enumerated several factors that can designate a subscription such as payment, registration, commitment, delivery, expressed association or access to restricted content. While Yershov didn't pay for the app, he did provide consideration in the form of personal information and established a relationship with USA Today that was different than the one formed by someone who merely visits a website through a web browser.

In [Gardner v. MeTV](#), the Seventh Circuit concluded likewise. There, the plaintiffs alleged they signed up for MeTV through the defendant's website, providing email addresses and zip codes in exchange for a more personalized viewing experience. MeTV allegedly embedded the Meta Pixel into its website and shared the plaintiffs' information with Facebook. Finding that the plaintiffs were "consumers" under the VPPA, the court agreed the statute does not require that "goods or services" be videotapes or streams, that any purchase or subscription from a VTSP satisfies the definition of "consumer," and that furnishing valuable data in exchange for benefits can create a "subscriber."

In *Goodman v. Hillsdale College*, the U.S. District Court for the Western District of Michigan also agreed: "A free account on a website can create enough of a relationship between the user and the operator of the website to qualify as a subscription." There, most videos provided by the college could not be accessed without an account, which required entering a full name and email address. Therefore, the plaintiffs were subscribers and hence, consumers.

Comparably, in *Cole v. LinkedIn*, the court found that Cole was a "consumer" because she alleged she subscribed to LinkedIn Premium and watched video content on LinkedIn Learning through that subscription. And while some LinkedIn Learning content was available to users without a subscription, her allegations that "to use LinkedIn Learning ... users must subscribe to LinkedIn Premium for a cost of \$39.99/month" permitted the court to infer that viewing most LinkedIn Learning videos required a subscription.

When does a VTSP knowingly disclose PII?

Only a defendant who "knowingly discloses" the PII of a consumer is liable under the VPPA. While this term is relatively straightforward, that has not kept litigants from disputing its meaning.

Courts have consistently held that a "knowing" disclosure arises when it is alleged that a defendant knowingly installed tracking software with the understanding that it transmits users' PII. Moreover, the Western District of Texas held in [Cochenour v. 360Training.com](#) that purposely targeting any and all users with a Facebook ID, regardless of whether the defendant knew for certain that any particular user had an ID, nonetheless amounted to knowing disclosure.

As for disclosure itself, the court in *Goodman v. Hillsdale College* held that the defendants were responsible for the disclosure of the plaintiffs' information. This was so even though the plaintiffs' Facebook IDs were automatically sent to Meta via the Meta Pixel without being accessed by the college, despite the plaintiffs' consent to Meta's tracking of their activity on other websites when they signed up for Facebook. The court concluded that there was no statutory support for the idea that "disclose" does not include automated activities, nor did the defendant argue that the consent provided to Meta was sufficient for VPPA purposes.

Further, the *Goodman* court distinguished the instant facts from those in [Mollett v. Netflix](#), where the Ninth Circuit found a defendant did not disclose protected information. The plaintiffs in *Mollett*, unlike *Goodman*, alleged that Netflix violated the VPPA when it provided users' personal information to the users themselves, who could in turn disclose it to third parties. This, for obvious reasons, was not the same as the college's disclosure to Meta in *Goodman*.

What qualifies as PII under the VPPA?

The VPPA defines PII to "include information which identifies a person as having requested or obtained specific video materials or services from a video tape service provider."

Two lines of thought have emerged in determining whether a plaintiff has alleged disclosure of "personally identifiable information" as defined under the VPPA. The reasonable foreseeability standard asks whether it is reasonably foreseeable that the information will reveal the identity of the individual and the videos they obtained. Conversely, the ordinary person standard asks whether an average person could identify the individual and the videos they obtained using the disclosed information.

The First Circuit established the reasonable foreseeability standard in *Yershov v. Gannett*. Noting that it was Congress' aim "to establish a minimum, but not exclusive, definition of [PII]" and therefore used the term "includes" to begin the definition, the court found that the defendant's disclosure of the plaintiff's device ID and GPS location and his viewing activity was reasonably and foreseeably likely to reveal which videos Yershov obtained, and therefore the alleged information fit within the PII definition.

In *Goodman v. Hillsdale College*, the Western District of Michigan followed the Sixth Circuit's expansive understanding of PII as decreed in *Salazar v. Paramount Global* — albeit the Sixth Circuit was dealing with the term "consumer," not PII. The *Goodman* court pointed out that a defendant can have knowledge of the fact that the recipient of the disclosure can readily use the information to determine a user's identity whether the information is decipherable by an ordinary person or not. And even if the ordinary person standard were applied to the *Goodman* facts, the court held that the college's disclosure of the plaintiffs' Facebook ID and the URLs that include the title of the page visited would still constitute PII.

Alternatively, in [In re Nickelodeon Consumer Privacy Litigation](#), the Third Circuit charted the ordinary person standard, concluding that IP addresses, browser fingerprints and unique device identifiers did not constitute "personally identifiable information" for VPPA purposes. "To an average person," the court surmised, "an IP address or a digital code ... would likely be of little help in trying to identify an actual person."

In this case, the plaintiffs asserted Viacom disclosed the data of children who viewed videos on its websites to Google, permitting Google to track specific users across time. Finding that the VPPA's definition of PII was static, the court pointed to the statute's legislative history, which aimed to prevent disclosures of information that identified an actual person's video-watching habits, as well as its definitional differences, despite amendments, from statutes like the Children's Online Privacy Protection Act — which allows for regulatory expansion of the meaning of PII. Further, the court posited that a broader reading of PII could result in anomaly, outlawing the use of third-party cookies on any website that streams video content.

The Second Circuit followed the ordinary person standard in [Solomon v. Flipps Media](#), finding that the URLs of the plaintiff's video viewing activity, in tandem with her Facebook ID, did not constitute "personally identifiable information" when embedded in a long string of code known as a GET request. The court preliminarily agreed that the VPPA's PII definition covered information capable of being used to identify a consumer's viewing history. That said, it ultimately held that the ordinary person standard is more suitable in distinguishing PII because it better informs VTSPs of their obligations under the statute — that is, it entails an objective analysis as opposed to speculating what a third party might reasonably and foreseeably do with the information.

Likewise, the Ninth Circuit applied the ordinary person standard in [Eichenberger v. ESPN](#), concluding the disclosure of the plaintiff's Roku device serial number and the identity of the videos that he watched were not PII under the VPPA. The court reasoned the statute did not intend to prohibit "a resourceful private investigator who could, with great effort, figure out" who disparate information applied to, nor was it drafted to require a VTSP to discern what a third party could or would do with information that, on its face, appeared nonidentifying. Regarding the facts at hand, the court held the disclosed information

could not identify an individual unless it was combined with other data that ESPN neither disclosed nor possessed.

Applying this precedent, the Central District of California found that the plaintiffs in *Plotsker v. Envato* sufficiently alleged PII where the defendant disclosed their Facebook IDs and URLs and titles of the webpages they visited. This information, the court concluded, would readily permit an ordinary person to identify the plaintiffs. The Northern District of California came to the same conclusion on similar facts in *Cole v. LinkedIn*.

While these standards might appear at odds, the First Circuit holding in *Yershov* was rather narrow, confined to the facts as pled. In fact, the court noted that the disclosure of GPS location data "would enable most people to identify" an individual's home or work address, almost mirroring the ordinary person standard. The First Circuit also conceded that the link between identity and information can, at some point, become too attenuated.

Putting VPPA compliance into practice

The VPPA is just one more dated privacy law that plaintiffs are seeking to apply in modern circumstances. As case law tests its limits, what can businesses glean to avoid liability?

In terms of consent, recall that Congress did update the VPPA to allow for consent obtained by electronic means. Even so, the original three elements to written, informed consent remain. Ask yourself: Is consent obtained in a way that is distinct from other consumer obligations? Is it renewed at least every two years? And is the ability to opt out clear and conspicuous? Vague, generalized disclosures are insufficient, and entities should not rely on consent obtained by third parties for their own data-collection practices because such consent may not meet the VPPA bar.

As for the characteristics of a VTSP, courts agree that they must provide video cassette tapes or audiovisual materials that a user can control; that is, they provide the user with some possessory interest. Movie theatres do not qualify. Not only are they engaged in the business of selling tickets and concessions rather than providing trailers that may constitute audiovisual materials, but the VPPA is concerned with the privacy of the home and living room, not public spaces like a theatre.

However, videos need not be the only asset provided by a VTSP nor their overarching focus. Furthermore, the exchange of money is not required: A party can be implicated as a VTSP when they provide video access in exchange for personal information.

Perhaps most importantly, the meaning of "consumer" is contentious. Indeed, there is a circuit split over whether a consumer must subscribe to goods and services that relate to audiovisual materials or simply to any product provided by a VTSP. Both interpretations appear reasonable though the consumer protective spirit of the law would seem to suggest a more plaintiff-friendly reading. Furthermore, must a subscriber — in order to be a consumer — spend money, or is it enough to provide personal information in exchange for video access? Hopefully, the Supreme Court will provide clear answers to these questions when *Salazar v. Paramount Global* is decided.

In contrast, the confines of knowing disclosure possess more clarity. Merely installing tracking software with the knowledge that it discloses users' PII will suffice, regardless of a VTSP's knowledge of which users share protected information and which do not. In addition, an automatic disclosure to a third party is enough to meet the required mental state, so long as the defendant has configured the tracking software to do so.

Finally, regarding the limits of PII, courts disagree on whether to apply the reasonably foreseeable standard or the ordinary person standard. The former posits that a defendant may discern the capacity of a third party to identify an individual from information that appears to be nonidentifying. The latter removes this subjective analysis and considers what an average person could do with the information. While the ordinary person standard provides a straightforward test for defendants to apply, it does not account for the tremendous means of identification that modern data brokers and analytics firms possess.

These insights will help businesses comply with the VPPA in its modern context. Moreover, awareness of the undecided provisions will help potential defendants develop a reliable compliance strategy.



Part 5: The California Consumer Privacy Act private right of action

Section 1798.150 of the California Consumer Privacy Act, as amended by the California Privacy Rights Act, provides a [private right of action](#) that allows private plaintiffs to bring civil actions against businesses in certain circumstances.

The CCPA is the only comprehensive state privacy law passed so far to include a private right of action. Although the other comprehensive state privacy laws contain enforcement avenues for public authorities, such as attorneys general and government agencies, only the CCPA allows private plaintiffs to sue for certain violations. Washington state's My Health My Data Act and Illinois' Biometric Information Protection Act both provide for private rights of action, but they are limited to health and biometric data, respectively. Vermont's legislature passed a bill containing a private right of action, but Gov. Phil Scott, R-Vt., vetoed it partly due to the [controversial inclusion](#) of a private right of action, "which would make Vermont a national outlier, and more hostile than any other state to many businesses and non-profits." Vermont's H 212 remains the only comprehensive state privacy bill to be vetoed.

Against this backdrop, how does the CCPA's private right of action work? Which consumers can sue which businesses over what kind of data breaches and when?

What claims can plaintiffs allege under the private right of action?

To survive a motion to dismiss, a private action must comply with several requirements. First, the statute states that private plaintiffs may only file actions as defined by Section 1798.150, the private right of action section, and cannot allege violations of other sections of the CCPA or any other law. The private right of action section is generally understood to encompass security breaches of personal information. In line with this reading, the Northern District of California in [McCoy v. Google](#) dismissed the plaintiff's claim under the CCPA; the plaintiff alleged the defendant used a software program to monitor and collect personal data when users used non-Google applications on their Android devices. In dismissing the claim, the court reasoned there were no allegations of a security breach. Likewise, in [In Re TikTok Consumer Privacy Litigation](#), the Northern District of Illinois held that the CCPA "provides for [a private right of action] only in the context of a defendant's failure to prevent data breaches, not for unauthorized collection of personal information."

However, these [limits](#) to the private right of action have been recently tested. For example, in [Shah v. Capital One](#), the Northern District of California allowed a CCPA claim to proceed where the plaintiffs alleged the defendant collected, used and sold their personal information to third parties through website trackers without consent. As such, the court held that the plaintiffs need not allege a data breach to state a CCPA claim. The Shah court relied on precedent from [M.G. v. Therapymatch](#), where the same district court permitted a claim under Section 1798.150 alleging that the defendant embedded Google Analytics code on its website, allowing Google to collect website users' protected mental health information. This court, in turn, relied on a Southern District of California ruling in [Ramos v. Wells Fargo](#). There, the court concluded that the plaintiff stated a CCPA claim, notwithstanding a failure to allege a data breach. The plaintiff

alleged that unknown third parties allegedly accessed his financial information because of the defendant's failure to properly maintain the plaintiff's plain text information.

What does it mean to be a consumer?

To fall within the purview of the private right of action, each plaintiff must be a natural person who is a California resident, that is, a "consumer." Consumers cannot be business entities, as per [Kostiv and Associates v. Payink](#). There, the Los Angeles County Superior Court held that a company alleging that its clients' information was leaked could not assert a CCPA claim because it is not a natural person.

Moreover, in order to qualify as a California resident, one must be in the state for other than a temporary or transitory purpose. One may also be a resident if they are outside the state for a temporary or transitory purpose so long as they are also domiciled in the state.

What qualifies as personal information?

A claim under the private right of action must concern the plaintiff's unencrypted and unredacted personal information. For the purposes of the private right of action, personal information refers to two categories of information: the plaintiff's first name or initial and last name in conjunction with "data elements" like a social security number, financial information or medical information, at least one of which is unencrypted or unredacted. Alternatively, an email address or username in combination with the corresponding password or security question and answer that would permit access to the account constitutes personal information.

Allegations of personal information cannot be vague or ambiguous. For example, the Northern District of California in [Gardiner v. Walmart](#) dismissed the plaintiff's CCPA claim because it did "not

sufficiently allege disclosure of Plaintiff's personal information." While the plaintiff alleged that the purported breach compromised full names, financial account information, credit card information and other PII, the court concluded that he did not specifically "allege the disclosure of a credit or debit card or account number, and the required security or access code to access the account."

What is a business?

For purposes of the private right of action, a defendant must be a "business," defined as an entity that collects consumer personal information, determines how and why that information is processed and meets certain threshold requirements, such as annual gross revenues in excess of USD25 million. In [Rosado v. Zuckerberg](#), where the plaintiff alleged that he developed the Facebook website and that Mark Zuckerberg falsely claimed that he was the original developer of the social media platform, the Southern District of New York dismissed the plaintiff's CCPA claim because, for purposes of such a claim, a defendant cannot be a natural person. Moreover, in [Keown v. International Association of Sheet Metal Air Rail Transportation Workers](#), the U.S. District Court for the District of Columbia declined to find that a labor union was a business.

On the other hand, the U.S. District Court for the District of South Carolina held that the plaintiffs in the case of [Blackbaud Customer Data Breach Litigation](#) adequately alleged the defendant was a business because, among other things, it used consumers' personal data to provide and improve its services and was registered as a data broker in California — the definition of which requires that the entity be a business. Likewise, the U.S. District Court for the Northern District of Georgia in [Miller v. Nextgen Healthcare](#) held that because the plaintiffs pled that Nextgen "use[d] consumers' personal data ... to develop, improve, and test [its] services," they adequately alleged that the defendant was a business.

If, however, an entity receives information from a business and processes it according to that business's instructions, then the defendant is likely a service provider. A consumer may not bring a private right of action claim against an entity in its capacity as a service provider. In [In re Accellion Data Breach Litigation](#), the defendant was not considered a business because the plaintiffs merely alleged the company "enabled" the transmission of their PII rather than determining how and why it was transmitted. That said, and as elucidated in the case of [NCB Management Services Data Breach Litigation](#), entities can be both a service provider and a business, and the fact that they are both does not insulate them from private right of action liability.

What is a security breach?

The private right of action only applies to allegations if the plaintiff's personal information was involved in a security breach, that is, "subject to unauthorized access and exfiltration, theft, or disclosure." In [Rodriguez v. River City Bank](#), the Sacramento County Superior Court held there are at least "two prerequisites to a claim under [the PRA]: (1) 'unauthorized access' to the 'personal information' and (2) either 'exfiltration, theft, or disclosure' of that 'personal information.'" As such, the court threw out the plaintiff's claim because he alleged exfiltration, theft or disclosure — a bank employee downloaded customer data to a personal storage device and sent the information to a third party — without alleging unauthorized access — the bank employee was, in fact, authorized to access the data.

Courts generally agree that the plaintiff must allege that unauthorized access actually occurred as opposed to a mere potentiality of access. For example, the Northern District of California held in [Mehta v. Robinhood Financial](#) that allegations that the defendant allowed "unauthorized third parties ... to access approximately 2,000 Robinhood customers' accounts and deplete their funds" was sufficient to allege a security breach at the pleading stage. Similarly, in [Stasi v. Inmediata Health Group](#), the Southern District of California denied a motion to dismiss the plaintiffs' CCPA claim because the "plaintiffs repeatedly allege[d] their information 'was viewed by unauthorized persons'" rather than alleging inferred or presumed access.

In addition, the Los Angeles County Superior Court in [Lyman v. Kaufman Dolowich Voluck](#) granted the defendant's motion for summary judgment, in part because the plaintiff presented no evidence that his personal information on the defendant's website "was ever accessed by a third party."





Reasonable security procedures and practices

The private right of action also requires plaintiffs to allege that the security breach occurred because the defendant failed to "implement and maintain reasonable security procedures and practices appropriate to the nature of the information." This obligation is not retroactive. The court in *Gardiner v. Walmart* held that the duty to implement and maintain reasonable security procedures and practices is only applicable to conduct that occurred on or after 1 Jan. 2020.

While reasonable security is not defined in the statute, the California attorney general's office has put out nonbinding [guidelines](#) for businesses that describe these practices and procedures, including recommendations like strong encryption and multifactor authentication. Furthermore, some case law suggests that the simple fact of unauthorized access equates to deficient security. For instance, in [Kirsten v. California Pizza Kitchen](#), the Central District of California held that mere claims that the defendants allowed unauthorized parties to access the plaintiffs' PII amounted to a plausible allegation that they failed to maintain reasonable security procedures.

Other courts require more. In the case of [Eureka Casino Breach Litigation](#), the U.S. District Court for this District of Nevada found that the plaintiff's allegations met this burden. That is, the defendant failed to encrypt the plaintiffs' PII, adhere to Federal Trade Commission guidelines and industry standards, and monitor for suspicious activity or apply all available security updates, among other things. Likewise, in [In re LastPass Data Security Incident Litigation](#), the plaintiff plausibly alleged that LastPass violated the duty to implement and maintain reasonable security procedures where its password encryption algorithm fell below industry standards. In [Durgan v. U-Haul International](#), the U.S. District Court for the District of Arizona denied the defendant's motion to dismiss the plaintiff's CCPA claim in part because the defendant did not maintain adequate email filtering software, properly train its employees, implement multifactor authentication or encrypt personal information and delete it when it was no longer needed.

Furthermore, some courts indicate that conclusory statements will not suffice. In [Maag v. U.S. Bank](#), the Southern District of California found that the plaintiff failed to state a claim under the CCPA, where he simply "ma[d]e unsupported allegations that his PII was compromised because Defendant did not 'implement and maintain reasonable security procedures and practices.'" Likewise, in [Griffey v. Magellan Health](#), the District of Arizona rejected the plaintiffs' CCPA claim because they merely alleged that because there was a breach, the defendant's data security was inadequate.

Exceptions and exemptions

The CCPA contains exemptions from liability for certain entities and data, but these do not always overlap with the exemptions specific to the private right of action. For example, the defendant in [Florence v. Order Express](#) argued the CCPA did not apply to it because it is subject to the Gramm-Leach-Bliley Act; indeed, Section 1798.145(e) states that the CCPA does not apply to personal information subject to the GLBA. However, the Northern District of Illinois rejected this argument because the statute contains a clause that states this exemption does not apply to the private right of action.

Medical information and entities which are governed by the Confidentiality of Medical Information Act or HIPAA are specifically exempted from the CCPA, and plaintiffs have explored arguments surrounding these exemptions. In *Stasi v. Inmediata Health Group*, the plaintiffs alleged unauthorized access to both their medical and nonmedical information in violation of the CCPA. The Southern District of California agreed with the defendant that the alleged medical data was not subject to CCPA protection. However, it allowed the CPPA claim to proceed insofar as it was based on the nonmedical information, stating "Inmediata [did] not address the non-medical information that it admits was accessible on the internet." Inmediata did not address and the court did not decide whether the entity-level exemption applied.

Conversely, in [Lurry v. Pharmerica](#), the U.S. District Court for the Western District of Kentucky held that if a business maintains its nonmedical patient information in the same manner as its medical information, then all such information is exempt from the CCPA. The onus is on the plaintiff to allege otherwise. Similarly, the court in [Tate v. EyeMed Vision Care](#) declined to follow Stasi and dismissed the CCPA claim because the plaintiff failed "to provide specific allegations that EyeMed maintain[ed] non-medical patient information in a different manner than medical information — a fact required to establish the California statute covers EyeMed."

These cases suggest countervailing lines of jurisprudence. The analysis in Stasi implies that defendant Inmediata was responsible for claiming it maintained medical information in the same manner as nonmedical information. On the other hand, the courts in Tate and Lurry dismissed the CCPA claims because the plaintiff failed to make the inverse allegation, effectively flipping the pleading obligation to the other party.

Damages

A successful CCPA plaintiff may recover different types of compensation: statutory damages, which range from USD100 to USD750 per consumer per incident, or actual damages, which reflect the amount of money the plaintiff lost due to the breach. Actual damages can include, for example, the cost of identity theft protection or credit monitoring insurance. Plaintiffs can also ask for an injunction or other equitable relief.

Notice and cure

If a plaintiff wants to recover statutory damages, they must first provide the defendant with 30 days' notice to cure the alleged CCPA violation. For example, the court in *Lyman v. Kaufman Dolowich Voluck* granted summary judgment for the defendant because the plaintiff provided no evidence that he had ever given notice.

That said, courts disagree on the procedural consequences of this notice. For example, in *Griffey v. Magellan Health*, the District of Arizona found that the plaintiffs must provide this presuit notice at least 30 days before the initiation of a lawsuit rather than 30 days before some future amended complaint. Otherwise, it would defeat the objective of allowing the defendant an opportunity to cure the defect outside of court. As such, the case was dismissed with prejudice, preventing the plaintiff from curing his claim. However, the Western District of Washington in [Guy v. Convergent Outsourcing](#) dismissed the plaintiffs' CCPA claim without prejudice, allowing the plaintiffs to send notice to the defendant, wait for the required 30 days and then amend their suits to replead the claim if the defendant did not cure.

The District of Massachusetts in *In re LastPass Data Security Incident Litigation* analogized the notice requirement to a similar requirement in the California Consumer Legal Remedies Act, under which "some courts have held that notice sent thirty days prior to the operative complaint suffices," meaning the claim would not be barred as long as the plaintiff filed an amended complaint at least 30 days after sending notice. The court in the case of *Eureka Casino Breach Litigation* agreed with this reasoning and allowed a claim to proceed where the plaintiff provided CCPA notice and filed an action on the same day, then consolidated the complaint to include a CCPA claim several months later.

The Northern District of California in [In re San Francisco 49ers Data Breach Litigation](#) declined to hold one way or another because the issue remained "in question," instead directing the parties to come to an agreement amongst themselves as to whether the plaintiffs could argue the claim.

If the business "actually cures" the alleged violation within the 30-day notice period and informs the plaintiff of such in writing, the plaintiff cannot request statutory damages. As of 1 Jan. 2023, an amendment to the CCPA states that the implementation and maintenance of reasonable security procedures and practices only after notice is given is insufficient to qualify as a cure. However, this implementation and maintenance can constitute an actual cure for incidents involving information collected before 1 Jan. 2023.

Regarding what defendants can do to cure alleged violations for information collected after 1 Jan. 2023, the Northern District of California held in [Florence v. Order Express](#) that a bare assertion that one has enhanced their security measures is not enough. The defendant did not encrypt the plaintiff's PII nor delete that which it no longer needed to maintain its services, actions which presumably would have amounted to a cure. Likewise, in [Prutsman v. Nonstop Administration and Insurance Services](#), while the defendant said in its letter to the plaintiff that it had cured the CCPA violation, the court refused to dismiss the CCPA claim because this statement "[did] not render implausible the plaintiffs' allegations to the contrary."

Private right of action settlements

Cash settlements can vary from case to case depending on how severe the alleged violation was, how many people were affected and other factors. For example, some settlements have required defendants to implement improved security measures or pay for identity protection and credit monitoring after a data breach.

The first class-action settlement under the CCPA private right of action, [In re Hanna Andersson](#), saw the defendant company create a settlement fund of USD400,000. Class members were entitled to up to USD500 for a basic award and up to USD5,000 to reimburse losses like unauthorized charges and out-of-pocket expenses. The defendant also committed to "take reasonable steps to secure access to [its] e-commerce platform," which included conducting risk assessments, enabling multifactor authentication and hiring additional technical staff.

The settlement in the case of [California Pizza Kitchen Data Breach Litigation](#) saw similar terms: California class members could recover USD100 as statutory damages, members who incurred out-of-pocket expenses could recover up to USD1,000 and members who had monetary losses as a result of actual identity theft could recover up to USD5,000. California Pizza Kitchen also provided two years of credit monitoring and agreed to take remedial measures, again including multifactor authentication. This settlement stands out from the rest because it had no dedicated settlement fund; rather, it bore a "claims made" structure, meaning the only limit on the fees California Pizza Kitchen would pay depended on how many class members claimed their benefits.

After [In re T-Mobile Data Security Breach Litigation](#) settled, T-Mobile created a USD350 million settlement fund from which California class members could recover USD100 in statutory damages, and all members could recover up to USD25,000 for out-of-pocket losses and up to USD375 for lost time. All members were entitled to two years of identity theft protection and insurance, credit monitoring and restoration services, which included "access to US-based fraud resolution specialists who can assist with important tasks" related to identity theft and members' credit. The agreement also included a requirement for T-Mobile to spend at least USD150 million above its previous budget for 2022-23 on "data security and related technology."

Conclusions and takeaways

Plaintiffs, defendants and courts alike continue to test the parameters of the CCPA's private right of action. Notwithstanding six years of litigation and hundreds of cases filed across the U.S., this area of jurisprudence remains relatively underdeveloped. Still, some interpretative trends are emerging.

In terms of the scope of private right of action, it seems to be shifting over time. Based on a plain reading, the private right of action appears to strictly apply to security breaches, or what is traditionally understood as the unauthorized intrusion upon protected assets by a malicious actor. But courts are expanding that scope to encompass the website tracking context, denying motions to dismiss where plaintiffs have alleged that defendants disclosed their personal information without the plaintiffs' consent. This will be an extremely important development to watch since it broadens the circumstances which might prompt CCPA liability.

As for the parties, a plaintiff must be a natural person, not a company or business entity. They must also be in California for more than a temporary purpose or traveling elsewhere while also domiciled in California. On the other hand, a defendant cannot be a natural person or a labor union. Examples of in-scope businesses include data brokers and entities that use data to improve their services. Furthermore, while a service provider cannot be sued, an entity that is both a business and service provider can be in their capacity as a business.

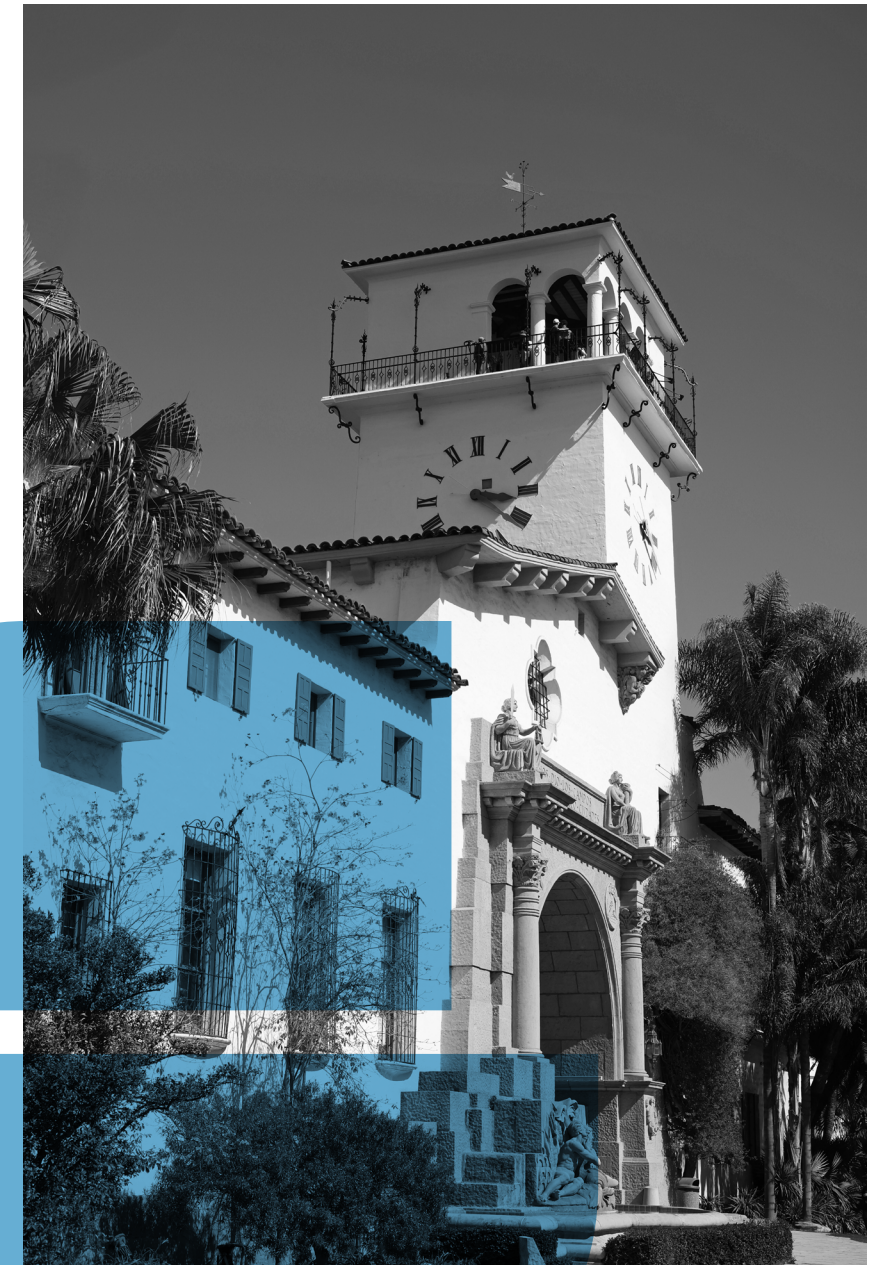
It's also important to remember that the definition of personal information in the private right of action context is borrowed from a different statute, not the definition found in Section 1798.140. Also, plaintiffs must be specific in their allegations of personal information, not state things in general terms such as "financial information" or "government documents."

Regarding the meaning of security breach, courts are clear that both unauthorized access and exfiltration, theft or disclosure must be alleged. Moreover, unauthorized access must be concrete, not speculative. And as for what level of security is reasonable, some courts hold that mere access amounts to unreasonable security, but conclusory statements that recite the elements of the law are likely insufficient. Even so, others require specific allegations that security fell below industry standards or failed to adhere to security best practices.

The exemptions applicable to the private right of action versus the broader CCPA are not one-to-one and require close reading. For example, the GLBA exemption does not apply in the private right of action context. Furthermore, exemptions for health information and entities can be complicated. Some courts say that a defendant must demonstrate that its nonmedical and medical information are treated in the same way in order to avoid liability altogether, while others require the plaintiff to allege that the two forms of information are maintained differently in order for liability to apply to the nonmedical form.

Finally, the private right of action provides for statutory damages, but these require presuit notice to cure of at least 30 days. Courts disagree as to whether this notice must come before a lawsuit is initiated or simply before the operative complaint. Furthermore, an actual cure after notice will prevent a lawsuit, but such a cure must be more than an empty statement that one has done so.

Even as jurisprudence under the CCPA's private right of action remains in flux, interested parties are building litigation strategies based on preliminary impressions. While definitive answers may be slow to materialize, understanding will nonetheless grow over time as more arguments and opinions shape what the private right of action means for individuals and businesses.



Part 6: Biometrics and consumer health data

There are various biometric and consumer health data privacy laws peppered throughout the nation. Most notable of these laws is the Illinois [Biometric Information Privacy Act](#), passed in 2008. After the Illinois Supreme Court held in [Rosenbach v. Six Flags](#) that an individual can sue under BIPA without alleging actual injury, private litigation under this law increased precipitously. Some private litigants alleging violations under BIPA have had success settling claims regarding the privacy of their biometric data.

BIPA requirements

Section 15 contains the core requirements for private entities' retention, collection, disclosure and destruction of biometric identifiers and information. Section 15(a) lays out requirements for covered entities, which possess biometric identifiers or biometric information, to develop publicly available, written policies that establish a retention and destruction schedule. Such biometric identifiers and biometric information must be destroyed when the initial purpose of collection has been met or within three years of the last interaction by the individual whom the information identifies with the private entity, whichever occurs first.

Section 15(b) prohibits private entities from collecting, capturing, purchasing, receiving through trade or otherwise obtaining an individual's biometric identifier or information, unless three conditions have been met:

- The subject has been informed in writing that a biometric identifier or biometric information is being collected or stored.
- The subject has been informed of the purpose and length of term for the collection, storage and use of the biometric identifier or information.
- The private entity has received a written release executed by the subject.

In [Salinas v. Arthur Schuman Midwest](#), the Appellate Court of Illinois held that Section 15(b) does not regulate entities that merely facilitate another entity's acquisition of biometric data. In addition, the third prong of this consent requirement for "written release" has been the subject of some debate. In August 2024, BIPA was amended to include "electronic signature" within the [definition](#) of "written release."

Furthermore, Section 15(d) prohibits private entities from disclosing, redisclosing or otherwise disseminating an individual's biometric identifier or information unless one of the following conditions is met:

- The subject consents to the disclosure.
- The disclosure completes a financial transaction authorized by the subject.
- The disclosure is required by state or federal law.
- The disclosure is required pursuant to a valid warrant or subpoena.

Section 15(c), meanwhile, puts a blanket prohibition on selling, leasing, trading or otherwise profiting from an individual's biometric identifier or information.

Lastly, Section 15(e) requires private entities in possession of biometric identifiers or information to store, transmit and protect from disclosure such data "using the reasonable standard of care within the private entity's industry" and "in the same as or more protective than the manner in which the private entity stores, transmits, and protects other confidential and sensitive information."

BIPA definitions and exclusions

Under BIPA Section 10, a biometric identifier is specifically defined as "a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry." By comparison, biometric information is any information "based on" one of these biometric identifiers that is then used to identify an individual. In [Martell v. X](#), the Northern District of Illinois reemphasized that biometric identifiers and information must be capable of identifying an individual to be subject to BIPA.

While the term biometric data does not appear in the text of the law, it has been used as an umbrella term to refer to both biometric identifiers and biometric information. Excluded from the definition of biometric identifiers are things such as written signatures, photographs and human biological samples used for valid scientific testing or screening. Demographics and physical descriptions such as height, weight, hair color or eye color also do not constitute biometric data nor do biological materials regulated under the Illinois Genetic Information Privacy Act or patient information regulated under HIPAA.

BIPA exemptions

Like other privacy laws, BIPA contains various exemptions, including for any "financial institution or an affiliate of a financial institution that is subject to Title V of the federal Gramm-Leach-Bliley Act of 1999 and the rules promulgated thereunder." In [Cisneros v. Nuance Communications](#), the plaintiff alleged the defendant unlawfully collected her voice print for identification purposes. The Northern District of Illinois dismissed the plaintiff's claim because the defendant engaged in a financial activity specified by the Federal Reserve Board — authenticating the identity of persons conducting financial and nonfinancial transactions — and was therefore a "financial institution" and exempt from BIPA. This issue was appealed to the Seventh Circuit.

Also appealed to the Seventh Circuit was a question about BIPA's government contractor exemption. This exemption states that "nothing in this Act shall be construed to apply to a contractor, subcontractor, or agent of a State agency or local unit of government when working for that State agency or local unit of government." In [Payton v. Union Pacific Railroad](#), the Northern District of Illinois denied the defendant's motion for summary judgement, where the defendant argued that it was exempt from BIPA under the government contractor exemption. The court reasoned that this exemption is not categorical; rather "it requires a nexus between the BIPA violation and the scope of the defendant's work with the government." Because the collection of the plaintiffs' fingerprints was not related to the defendant's government contracts, the district court found the exemption did not apply.

Furthermore, the plaintiffs in [Melzer v. Johnson & Johnson](#) alleged the defendant's AI face scanning technology used to diagnose and treat skin health issues collected digital copies of their unique facial geometries without consent in violation of BIPA. In its defense, Johnson & Johnson argued that it fell within BIPA's healthcare exemption, which excludes from the definition of "biometric identifier," "information captured from a patient in a healthcare setting or information collected ... for healthcare treatment ... under [HIPAA]." The U.S. District Court for the District of New Jersey denied the motion to dismiss and held that "patient in a healthcare setting" requires that the individual is awaiting or receiving medical care from a medical professional. Because the defendant's technology did not involve any medical professionals and was closer to a marketing strategy than informed medical care, it did not fall within the BIPA exemption.

Scope of BIPA's private right of action

Section 20 of BIPA contains its private right of action. This section provides "any person" aggrieved by a violation of the law with the right to file suit within a state circuit court or a supplemental claim within federal district court. Individuals may recover four types of relief:

- For negligent violations, the greater of liquidated damages of USD1,000 or actual damages
- For intentional or reckless violations, the greater of liquidated damages of USD5,000 or actual damages
- Attorney fees and other litigation expenses
- Other types of relief, including injunctions

Courts have previously ruled on the constructions of Sections 15(b) and 15(d) of BIPA, namely whether claims accrue every time a private entity scans a person's biometric identifier and every time a private entity transmits such a scan to a third party or only once upon the first scan and transmission. The Illinois Supreme Court in [Latrina Cothron v. White Castle System](#) construed that "a separate claim accrues each time a private entity scans or transmits an individual's biometric identifier or information in violation of section 15(b) or 15(d)."

Following this decision, the Illinois State Legislature passed Senate Bill 2979, which put a limit on BIPA claims. Now, individuals are entitled to at most one claim under Section 15(b) for any given biometric identifier or information regardless of the number of times it was collected, captured, purchased, received through trade or otherwise obtained. Likewise, they are now entitled to at most one

claim under Section 15(d) regardless of how many times the biometric identifier or information was disclosed, redisclosed or otherwise disseminated to a third party. In [Clay v. Union Pacific Railroad](#), the Seventh Circuit clarified that this amendment applies retroactively.

The statute of limitations on bringing a BIPA claim has also been decided through litigation. In [Tims v. Black Horse Carriers](#), the Illinois Supreme Court held that individuals can bring BIPA claims up to five years following an alleged BIPA violation.

Notable BIPA settlements

Several BIPA complaints with large technology companies have led to multimillion-dollar settlements and changes in the way companies collect, process and use consumers' biometric data.

In re TikTok Consumer Privacy Litigation

The settlement in [In re TikTok Consumer Privacy Litigation](#) stemmed from multidistrict litigation that combined 21 class-action lawsuits filed across California and Illinois. The BIPA claim, which was brought on behalf of the Illinois subclass, hinged on the allegation that TikTok extracted "a broad array of private data including biometric data and content" and that it allegedly tried to "ascertain users' race, gender and age by using biometric identifiers." In addition to TikTok agreeing to pay USD92 million, the [settlement](#) required TikTok to refrain from collecting or storing users' biometric identifiers or information and to hire a third-party firm to review their data privacy training for a period of three years.

Rivera v. Google

The protection of biometric information, a derivative of biometric identifiers, has been lauded as one of the most innovative aspects of BIPA. [Rivera v. Google](#) was a class-action lawsuit whereby members of the class alleged Google violated BIPA by collecting, storing and using their biometric data in connection with Google Photos without their informed written consent. It was settled in 2022 for USD100 million.

In its opinion, the court explained the definition and inclusion of the term biometric information "does important work" in BIPA, essentially preventing private entities from evading the law's scope "by converting a person's biometric identifier into some other piece of information, like a mathematical representation, or even simpler, a unique number assigned to a person's biometric identifier." Thus, the court found the "face templates" generated by Google qualified as biometric identifiers, specifically as a "scan of face geometry" under the statute.

Meta lawsuits

Hailed at the time as the largest privacy class-action settlement, Meta, then known as Facebook, reached a USD650 million agreement with Illinois Facebook users in the case of [Facebook Biometric Information Privacy Litigation](#) over its alleged use of facial recognition technology to collect and store users' biometric identifiers without consent.

More recently, a BIPA class-action lawsuit was dismissed in favor of Meta, this time on the issue of standing. Standing within privacy jurisprudence has been wrought with contention at least since the Supreme Court's decision in [Spokeo v. Robins](#) nearly a decade ago and in subsequent cases like [TransUnion v. Ramirez](#). A panel of the U.S. Court of Appeals for the Ninth Circuit found the plaintiff class in [Zellmer v. Meta Platforms](#) failed to demonstrate how they were harmed in a "concrete and particularized way" by the alleged BIPA violations and dismissed the claim.

Rogers v. BNSF Railway

The first jury trial under BIPA, heard in 2022, resulted in an order for Burlington Northern Santa Fe Railway to pay USD228 million to 45,600 truck drivers for collecting their fingerprints without consent. The amount of the settlement represented the maximum award, USD5,000 per individual. While a new trial was ordered so damages could be determined by a judge rather than a jury, BNSF and class members reached an [interim agreement](#) to settle the dispute for USD75 million. The lessons from BNSF will likely encourage BIPA defendants to continue to seek settlement agreements over jury trials.

In re Clearview AI, Inc. Consumer Privacy Litigation

Multiple class-action complaints were filed alleging that Clearview violated BIPA, among other consumer privacy laws. These actions were consolidated into a multidistrict litigation [lawsuit](#) in the Northern District of Illinois. [Clearview](#) settled with the plaintiffs in March 2025 to the tune of a 23% stake in the business. This unprecedented agreement balances the need for class members to be compensated with the fact that Clearview's widespread violations may have bankrupted the company under BIPA's private right of action, thus depriving injured parties of any redress.

Washington state's My Health My Data Act

Washington state's [My Health My Data Act](#) was signed into law 17 April 2023 with its provisions largely taking effect 31 March 2024. Small businesses — defined as those that collect, process, sell or share the consumer health data of less than 100,000 consumers annually or those that derive less than 50% of their gross revenue from the collection, processing, selling or sharing of consumer health data and control, process, sell or share the consumer health data of fewer than 25,000 consumers — had a delayed effective date of 30 June 2024.

Consumers must allege [actual damages](#) to bring lawsuits under MHMDA. In addition, the law will require plaintiffs to prove they suffered actual injury tied to data sharing. With this high threshold, it will be challenging to litigate due to the [requirement](#) that plaintiffs prove actual injury. But litigation could better define the scope of the law through court decisions.

On 10 Feb. 2025, almost a year after the law's entry into force, the first class-action lawsuit under MHMDA was brought against Amazon for alleged violations stemming from the use of the company's [software development kit](#) in third-party apps. The crux of the claim is that the location data Amazon's SDK collects could reveal sensitive health information that is protected under MHMDA.

New York's Biometric Privacy Act

The New York [Biometric Identifier Privacy Act](#), a proposed state bill that tracks closely to BIPA, has come close to passage. Like BIPA, it would prohibit the collection and sharing of biometric identifiers and biometric information without prior consent. Most importantly, the act would also include a private enforcement mechanism. Individuals could be awarded the greater of USD1,000 or actual damages for negligent violations and the greater of USD5,000 or actual damages for intentional or reckless violations.

Additionally, New York City's [Administrative Code](#) was amended to include notice requirements and disclosure restrictions for commercial establishments that collect customers' biometric data. Of note, Sections 22-1202 through 1203 provide a private right of action and prohibit commercial establishments from profiting from the transaction of biometric identifier information. In [Schottenstein v. Wakefern Food](#), the Southern District of New York granted the defendant's motion to dismiss the plaintiff's complaint, which alleged the defendant's use of third-party facial recognition technology to mitigate shoplifting in its grocery stores violated the code. The court declared the law does not prohibit any commercially useful application of biometric data; rather, it prohibits profits from the transaction of the data itself. In so holding, the court specifically distinguished the language in Section 22-1202 from that of BIPA Section 15(c).

Conclusion

Biometric privacy laws exist in over a half dozen states in the U.S. while state-level consumer health data laws — like Washington state's MHMDA and Nevada's SB 370 — are also becoming more numerous. Connecticut is among the states that have recently amended their comprehensive privacy laws, adding protections for health data. These laws fill an important gap by providing privacy protections for individuals' health and biometric data, including fingerprints, faceprints and voiceprints.

Moreover, BIPA and MHMDA are unique among state privacy laws as they contain private rights of action. By providing private individuals with the right to bring claims and join classes for alleged privacy violations, these laws have emerged as supplements to state and federal enforcement activities and magnify the compliance challenges for organizations that collect, use and store biometric and consumer health data.



Part 7: Daniel's Law and public officials' privacy

A state law aimed at protecting the personal information of public officials incidentally created a new era of data privacy litigation in the state and federal courts of New Jersey. Data brokers and other consumer-facing businesses now face rising litigation risks and exposure to financial and reputational damage as individuals assert their privacy rights under Daniel's Law.

New Jersey's Daniel's Law

Daniel's Law provides covered persons with the right to request that businesses remove their home addresses and unpublished telephone numbers from public databases and refrain from further publishing this information. Covered persons include federal and state judges, prosecutors, law enforcement officials and their family members. The law was passed in 2020 after an assassination attempt on U.S. District Court Judge Ester Salas resulted in the death of her son, Daniel Anderl, and critically injured of her husband.

In 2023, the New Jersey legislature amended the law to allow covered persons to assign their claims to a third party. This has led to hundreds of [lawsuits](#) filed against various defendants, including "online information services, traditional data brokers, enterprise software companies, real estate websites, and consumer reporting agencies." The law carries liquidated damages of USD1,000 per violation.

Many of these cases were brought by Atlas Data Privacy Corporation as an assignee of law enforcement officers with claims under the law. By May 2024, Atlas Data Privacy Corporation was the [assignee](#) of nearly 20,000 covered persons.

The U.S. Federal District Court of New Jersey consolidated 60 separate lawsuits filed by Atlas after the defendants removed the cases from New Jersey state court to federal court and filed motions to dismiss on First Amendment grounds. There, the defendants argued that the law is impermissibly overbroad and infringes their First Amendment rights. They also argued the law placed content-based restrictions on speech that could not survive the U.S. Supreme Court's strict scrutiny standard of review.

In November 2024, District Court of New Jersey Judge Harvey Bartle III denied the defendant's [motion](#) to dismiss the lawsuit after finding strict scrutiny was not the appropriate judicial standard of review. Instead, Bartle concluded that Daniel's Law is definitively a privacy law, and therefore, First Amendment challenges must follow the balancing test outlined in [Florida Star v. B.J.F.](#)

Under this Supreme Court precedent, a court must balance the right to privacy against the right of free speech using three factors: whether the defendant lawfully obtained information that is of public significance, whether the law "serves a need to further a state interest of the highest order," and whether the law serves the state's purported "significant interest" in a way that is not "underinclusive."

Bartle found the state's interest in protecting public officials' home addresses and telephone numbers outweighed any public significance arguments made by the defendants. Therefore, the court rebuffed the defendant's challenges to the law on its face and denied their motions to dismiss.

The defendants in these cases are not the first to challenge the law on First Amendment grounds. In [Kratovil v. City of New Brunswick](#), a journalist challenged the law in September 2023, arguing it violated his freedom of speech when he was barred from publishing the address of a New Brunswick public official. The state trial court ruled against the journalist and a panel of appellate judges affirmed the lower court's finding in April 2024. The New Jersey Supreme Court affirmed this holding in 2025.

Maryland passed a similar [statute](#) after a judge was killed outside his home in 2023. Florida, Georgia, Idaho, Minnesota, New York and Wisconsin have also passed their own judicial data privacy and security laws. Each of these state laws vary in their scope and available remedies.

Furthermore, Congress passed its own [version](#) of Daniel's Law with the James M. Inhofe National Defense Authorization Act for the Fiscal Year 2023, although it is more limited in scope. This [provision](#) of the defense bill prohibits data brokers from sharing the personal information of federal judges. It also allows federal judges to redact information provided by federal agencies. Related proposals from Congress also include [S 2144](#), which would provide similar protections for members of Congress, their staff and families.

How can entities comply with Daniel's Law?

Because Daniel's Law mandates the covered information must be removed within 10 days of receiving a proper request, entities that may collect data from covered persons under the law should create streamlined procedures for responding to potential takedown requests.

Businesses and individuals that receive takedown requests can take steps to prepare for compliance with this law. Businesses should maintain comprehensive data mapping or take inventory of existing data to properly map what information they may have. Businesses should also establish and maintain proper data governance within the organization to understand who will process and complete these takedown requests.

This law also requires businesses to sufficiently manage third-party vendors, develop proper data disposal protocols and retain records of compliance with takedown requests received by the organization. Importantly, New Jersey state and federal courts have not been persuaded by First Amendment challenges thus far. Barring any new defenses raised by entities subject to Daniel's Law, businesses must take appropriate steps to respect the rights of covered persons asserted under the statute.

Part 8: Shareholder actions

After a privacy incident, companies are often criticized for any conduct or missteps that hindsight suggests may have allowed the incident to occur. For public companies, shareholders — the individuals who own stock in the company — have a powerful way to seek accountability for alleged misconduct or inaction: a derivative action.

What is a shareholder derivative action?

Under U.S. business law, a public company's leadership has specific duties defined in the documents that created the company. For most publicly owned, for-profit companies, the C-suite and/or board of directors have fiduciary duties of care and loyalty to the shareholders. Although there are many exceptions and specific procedures that must be followed, generally speaking, any shareholder who alleges a company's leadership harmed the company — whether through negligence, bad decisions or outright misconduct — may file a derivative action against the leadership on behalf of the company to demand accountability if no other options have been or could be successfully pursued.

Shareholder derivative actions are based on the principle that a company's leaders must always act in the company's best interest. However, these lawsuits are not easy from a shareholder perspective. U.S. courts often give company leaders the benefit of the doubt, assuming they acted in good faith unless proven otherwise. To be successful, shareholders must bring forth strong evidence that the leaders acted irresponsibly or tortiously caused harm.

Even with these challenges, shareholder derivative actions can lead to significant changes. They can result in financial penalties for leaders, force companies to improve their policies and/or push them to strengthen their data protection practices.

Privacy, cybersecurity and digital governance remain enormous concerns for companies. When privacy incidents occur, they don't just hurt customers. Shareholders' stock value may drop or their dividends or returns could be impacted by loss of assets and hefty regulatory fines. Shareholder derivative actions have become an avenue through which shareholders attempt to ensure company leadership assumes responsibility for harm to shareholders, including in the privacy and security context.

Derivative actions based on privacy incidents

Although several shareholder derivative actions have been brought based on leadership's alleged role and conduct surrounding a company's privacy or cybersecurity incident, derivative actions rarely, if ever, obtain a successful trial judgment. However, by bringing actions and forcing leadership to respond to the allegations, shareholders can draw attention to past conduct and actions of leadership, seek remuneration through settlement and perhaps impact future conduct.

The Equifax data breach

In 2017, Equifax, a company that collects credit information, suffered a massive data breach that exposed the personal details of 147 million people. Shareholders filed lawsuits claiming Equifax's board of directors failed to protect the company from cybersecurity threats. They argued the board knew about weaknesses in the company's data systems but did not take proper action to fix them. The lawsuit

also highlighted how the breach damaged Equifax's reputation and financial stability.

The eventual settlement of the shareholder action exemplifies the impact of derivative suits. In addition to corporate governance reforms, enhanced cybersecurity measures and stricter board oversight on data security, Equifax was also required to appoint a new chief executive officer, chief information security officer, chief technology officer and other independent directors. Moving forward, the company agreed to allocate significant internal resources to prevent future breaches and mandate monitoring mechanisms in an effort to prevent or mitigate such incidents in the future.

The Facebook-Cambridge Analytica scandal

Facebook faced enormous backlash in 2018 after it was revealed political consulting firm Cambridge Analytica improperly accessed data from millions of Facebook users. Shareholders sued Facebook's leadership, accusing them of failing to prevent this misuse of data and misleading the public about how user information was handled. This lawsuit did not just seek financial damages; it also pushed Facebook to change how it managed and protected user data. The case ultimately settled for USD190 million and required Facebook, now Meta, to improve its privacy governance, bolster whistle blower protections and adopt a code of conduct that increases compliance and reduces conflicts of interest.

The Alphabet shareholder action

In 2018, Google discovered that its Google+ API was compromised, exposing the personal data of roughly 500,000 users to third-party developers. Noting the fallout from the Facebook-Cambridge Analytica scandal, shareholders alleged that Google opted not to disclose the breach for reputational reasons and in violation of the Securities Exchange Act of 1934. As news of the breach was eventually

disseminated, the company lost tens of billions of dollars in market value; a pension fund manager that held stock in Alphabet became the lead plaintiff in what eventually became *In re Alphabet Securities Litigation*. After a district judge dismissed the case for failure to allege a materially misleading misrepresentation or omission, the Ninth Circuit reversed, holding that two statements made in Alphabet's 10-Q omitted material facts necessary to make the statements not misleading. After remand, the case was settled for USD350 million.

A growing role

As technology evolves, so do privacy risks. Privacy and cybersecurity incidents are becoming more common, and shareholders are paying attention. Although these lawsuits are difficult to support and can be burdensome to bring, plaintiffs continue to bring these actions in order to recover lost value and incentivize responsible leadership going forward.

For shareholders, customers and companies alike, the message is clear: Neglecting privacy is not just bad for business, it's a breach of trust. Shareholders will continue to utilize every tool in their arsenal to demand companies prioritize privacy and protect sensitive and personal information. When a company fails to protect data or make good decisions, these lawsuits remind leaders that their actions or inactions have consequences.

Contacts

Connect with the team

Joe Jones

Director of Research and Insights, IAPP

jjones@iapp.org

Will Simpson

Former Westin Research Fellow, IAPP

Müge Fazlioglu

Principal Researcher, Law and Policy, IAPP

muge@iapp.org

The authors of the report and IAPP would like to express their sincere gratitude to the following experts who provided feedback on drafts of this report. Their contributions and insights were invaluable in bringing this report to completion.

Alphabetically by last name, they are:

Associate Attorney Kayla Bushey, CIPP/US

Data Privacy Attorney C. Kibby, CIPP/E, CIPP/US

Data Privacy and Cybersecurity Attorney Cheryl Saniuk-Heinig, CIPP/E, CIPP/US, CIPM

All responsibility for any remaining errors or omissions of fact resides solely with the report's authors.

Follow the IAPP on social media



Published August 2026.

The IAPP disclaims all warranties, expressed or implied, with respect to the contents of this document, including any warranties of accuracy, merchantability, or fitness for a particular purpose. Nothing herein should be construed as legal advice.

© 2026 IAPP. All rights reserved.