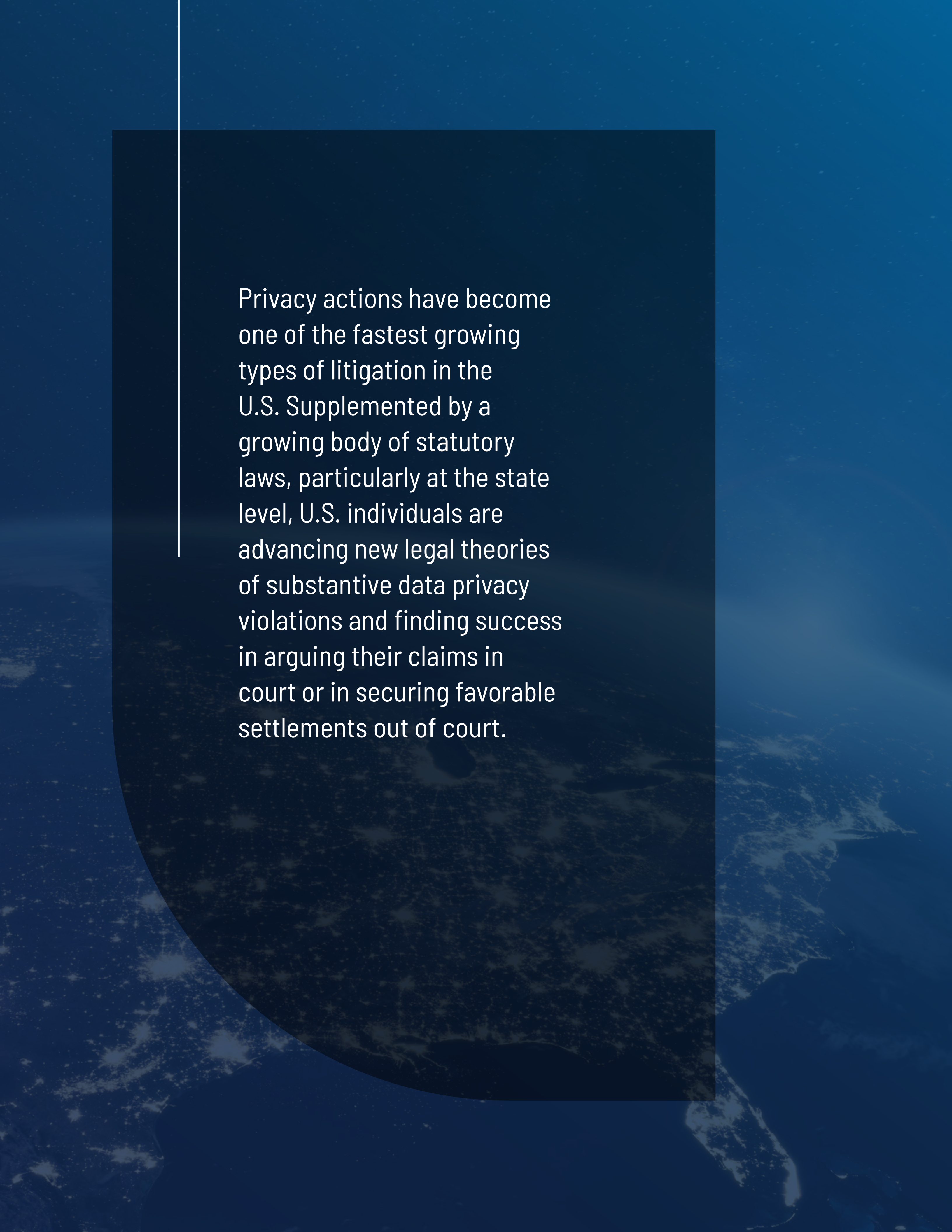
ARTICLE SERIES

US Data Privacy Litigation

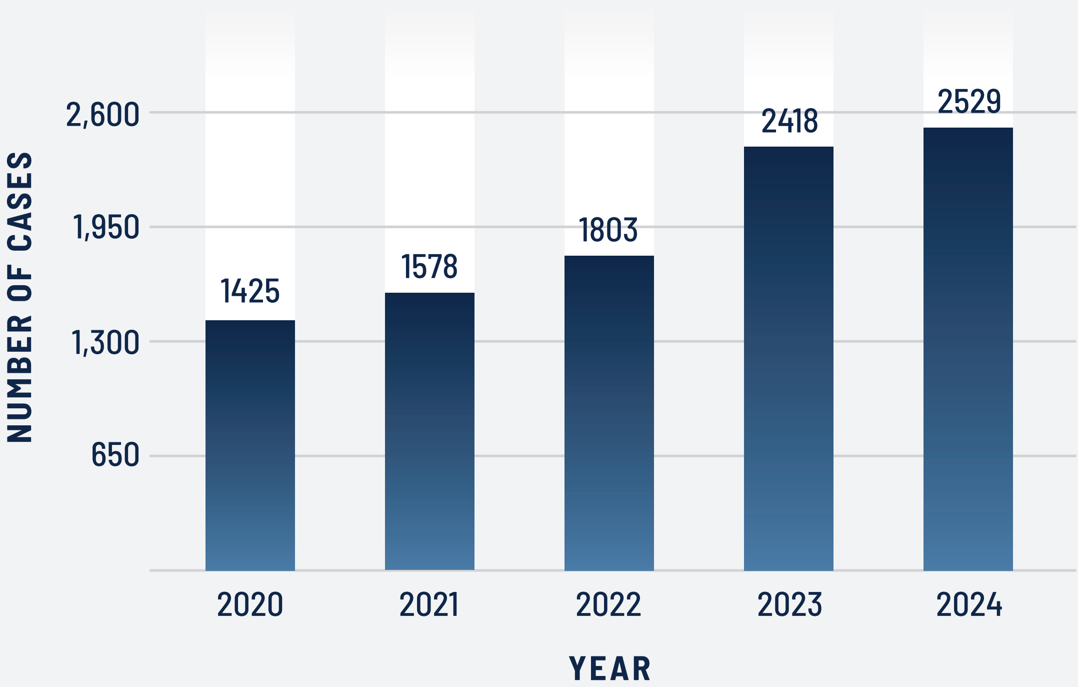
By:
Müge Fazlioglu, CIPP/E, CIPP/US
Cheryl Saniuk-Heinig, CIPP/E, CIPP/US
C. Kibby
Kayla Bushey, CIPP/US



Privacy actions have become one of the fastest growing types of litigation in the U.S. Supplemented by a growing body of statutory laws, particularly at the state level, U.S. individuals are advancing new legal theories of substantive data privacy violations and finding success in arguing their claims in court or in securing favorable settlements out of court.

Data privacy litigation in the U.S. is at an all-time high. By one count, nearly 2,000 lawsuits related to data privacy were brought to federal courts by litigants in 2024 alone. Across state and federal courts, class-action lawsuits related to data privacy have been on an upward slope over the past five years.

US Data Privacy Litigation, 2020–2024



Thomson Reuters / Westlaw Edge — Litigation Analytics, January 2025

When thinking about the enforcement of privacy laws, regulators such as the Federal Trade Commission and other agents of the government such as states' attorneys general come to mind. But individuals and certified classes of ordinary citizens have asserted their privacy rights around an assortment of digital issues, from web tracking to data breaches to biometric privacy. And while the enforcement capabilities of regulators and public authorities is capped by the number of such bodies that exist, as well as by their staff and budgetary resources, the number of citizens who may bring private actions in court is vastly greater and is always growing.

Moreover, as courts rule on issues at the emerging frontiers of digital governance, artificial intelligence and data privacy, there are many new precedents to be set that can cascade through the court system. As the court explained in Lopez et al v. Apple, "data privacy law is (a) developing area of law posing inherent risks that a new decision could shift the legal landscape as to the certifiability of a class, liability, and damages."

Thus, this series fills an important gap about how data privacy violations in the U.S. are contested through private litigation and class-action lawsuits. 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 statues like the California Invasion of Privacy Act against modern-day data uses.

Today, understanding how plaintiffs assert their privacy rights, how defendants contest them, 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.

Contents

Overview

In this six-part series, the first part, "Breach of contract and warranties litigation" by IAPP Research and Insights Analyst Cheryl Saniuk-Heinig, CIPP/E, CIPP/US, analyzes breach of contract and breach of warranty claims in the context of privacy. It examines when courts have allowed complaints to proceed and granted defendants' motions to dismiss, as well as when and how individuals have asserted privacy violations by leveraging a company's privacy notice, terms of service or other contractual arrangements.

The second part, "**Website tracking litigation"** by IAPP Westin Fellow Kayla Bushey, CIPP/US, analyzes litigation under the long-standing CIPA, originally passed to protect citizens against illegal wiretapping. The decades-old statute is now being repurposed by individuals to claim website tracking by third parties amounts to a form of digital eavesdropping.

The third part, "**Security breach litigation**" by IAPP Westin Fellow C. Kibby, analyzes the private right of action under the CCPA, which can be brought for unauthorized disclosures that are not cured and carries statutory damages between USD100-750 per consumer.

The fourth part, "**Biometrics and consumer health data litigation**" by IAPP Principal Researcher, Privacy Law and Policy, Müge Fazlioglu, CIPP/E, CIPP/US, examines litigation under the Illinois Biometric Information Privacy Act and the PRA in recently enacted and proposed consumer health data privacy laws like Washington state's MHMDA.

The fifth part, "**Data brokers and judicial privacy litigation**" by Bushey, focuses on lawsuits filed under Daniel's Law, a New Jersey privacy statute that protects the personal information of judges and other public officials, as well as the First Amendment challenges defendants have raised against it.

Finally, the sixth part, "**Litigating accountability through shareholder action**" by Saniuk-Heinig, examines how shareholders have sought to hold organizations accountable, through private litigation, for alleged misconduct or inaction around data privacy issues.

As the articles in this series demonstrate, the case law emerging from class-action litigation around data privacy violations adds a new dimension of depth to the operationalization of privacy rights by private individuals. Read comprehensively, the cases analyzed in this series articulate an elaborate web of obligations for businesses that collect, store and share personal information. With each new court settlement, dismissal and decision, data privacy continues to be a source of living law, reshaping our understanding of its boundaries, limitations and power.

1. Breach of contract and warranties litigation

By Cheryl Saniuk-Heinig, CIPP/E, CIPP/US

The data privacy litigation landscape in the U.S. has seen a rise in lawsuits brought by private individuals for privacy violations 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 or other public statements as contractual commitments or assurances.

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. This analysis will cover four types of claims — breach of express contract, breach of implied contract, breach of express warranty and breach of implied warranty — and discuss the strategies plaintiffs have used, both successfully and unsuccessfully, to advance these claims in court.

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 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 impacted patients have claimed breach of an implied contract when a health care provider advertised a commitment to keeping all patient data secure through "industry-leading practices" but inadequate security measures exposed patient data. They argued the provider implicitly promised to safeguard their data and, by collecting sensitive information, had an implied duty to protect it.

Breach of express warranty

Generally, a warranty is an assurance or promise regarding the existence or accuracy of facts, condition, quality, quantity or nature of a good or property. Express warranties derive from sales laws and 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 several 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	Contracts are formed based on conduct or circumstances, not written terms	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 are assumed based on the nature of the product/service, even if unstated	A cloud service implicitly promises secure storage, but data is leaked due to poor or outdated security practices

Successful strategies at preliminary stages: Unspoken promises, expected liability

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.

In 2019, Altice USA, a large media and telecommunications company, was the victim of a phishing attack through which several employees inadvertently divulged the credentials of their business email accounts. The stolen credentials were subsequently used to access and download emails and other data. In one of the accessed inboxes was a password-protected document that contained the personal information of 52,846 current and former employees.

According to the plaintiffs in McFarlane v. Altice USA, comprised of current and former employees' whose information was accessed, when Altice required them to disclose their personal information as a condition of employment, they entered an implied contract with the company to protect this data through the use of reasonable industry standards.

They further alleged examples of Altice's failure to perform its implied contractual duties included inadequate email filtering software, lack of sufficient cybersecurity training for employees with access to sensitive data, lack of encryption and the retention of personal identifying information of former employees years after they had left the company. At the motion to dismiss stage, the court agreed with the employees and the breach of implied contract claims proceeded to an eventual settlement in 2022.

This case follows the trend in some courts that emphasizes the reasonable expectations of privacy created by a company's own statements while simultaneously considering whether a reasonable consumer would interpret privacy statements as binding promises.

In In re BetterHelp Data Disclosure Cases, BetterHelp was operating a counseling service that connects customers with therapists and facilities. The company has several websites, some of which are aimed at specific groups and communities based upon religion, marital status, age, and sexual identity or orientation. At some point, BetterHelp delegated significant decision-making authority for advertising through its Facebook platform to a low-level employee who was a recent college graduate with no marketing experience, no experience in safeguarding health information and little training.

As a result, BetterHelp allegedly disclosed information of its customers and potential customers to various third parties for advertising purposes and the third parties' own purposes, which effectively revealed to the third parties that the customers were seeking and/or receiving mental health treatment. This disclosure occurred despite BetterHelp's privacy assurances throughout their website and interactive forms.

The U.S. Court of Appeals for the Ninth Circuit held that the plaintiffs sufficiently identified the particular promises they contend BetterHelp made, including assurances to keep customer information confidential, and facts that would constitute a breach of those promises. As such, the plaintiffs' breach of implied contract claim was allowed to proceed.

Decisions turn on the terms

The survival of a plaintiff's breach of contract claim will always turn on the specific language of the relevant statement, as well as the circumstances in which the defendant's breach allegedly occurred. Furthermore, even in courts that have determined a privacy notice can form an express contract, limitations within those policies can still preclude claims.

In Bass v. Facebook, multiple plaintiffs filed a data breach putative class-action lawsuit against Facebook in 2019. The plaintiffs claimed hackers exploited a coding vulnerability and stole the access tokens, which are "electronic object(s) embedded with all of a users' security information," of 69,000 users. These tokens were designed never to expire and allowed the information of connected users to be viewed. As a result, the stolen tokens of 69,000 users led to the theft of information from 29 million worldwide users.

Lawsuits claiming breach of contract and breach of implied contract, among other causes of action, were filed against Facebook. In its order on Facebook's motion to dismiss, the lower court determined, for the plaintiff with standing, that Facebook's data use policy and terms of service were construed as contractual promises to limit data sharing, and the plaintiff properly alleged such contractual promise was violated. However, the plaintiff's breach of contract claims ultimately failed because Facebook's terms of service included an accessible, procedurally fair and sufficiently clear limitation-of-liability clause.

Unsuccessful and unresolved strategies: No terms, no triumph

Breach of contract claims are often dismissed due to lack of specific, enforceable promises. In Anibal Rodriguez, et al. v. Google, the plaintiffs argued Google created a unilateral contract by providing a button to adjust a user's privacy settings. They asserted 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 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.

Additionally, some plaintiffs failed to adequately counter defenses, such as sufficient disclosures. In In re Google Gmail Litig., at the pleading stage, the district court declined to certify a punitive class. 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. Yet 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.

Vague loses the day

Regarding warranty claims, many complaints have been dismissed for either lack of specificity or because privacy notices are not typically seen as warranties. When examining the counts for breach of express warranty in In re Google Assistant Privacy Litigation, the court determined the plaintiffs had not identified terms of an express warranty within the provisions of the privacy notice. Additionally, service agreements often include disclaimers that negate implied warranties, which courts have upheld. 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.

Every word counts

Although courts have found collection of sensitive information can create an implied contract that imposes obligations on organizations, courts have also dismissed breach of contract claims when organizations have included clear limitation-of-liability clauses within their terms of service. This range of findings in the preliminary stages of cases suggests, as privacy incidents spur more private litigation, more and more circuit splits are likely to develop. Until comprehensive legislation or controlling precedent says otherwise, privacy professionals and attorneys alike must remain mindful of the ever-growing responses and novel arguments from plaintiffs in the wake of privacy incidents and develop responses to those risks accordingly.

2. Website tracking litigation

By Kayla Bushey, CIPP/US

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 spearheaded privacy class-action lawsuits against businesses using tracking tools on their websites and motivated plaintiffs elsewhere who seek to apply their states' wiretapping laws to digital tracking and analytics.

The CIPA

Since 2022, plaintiffs have filed hundreds of lawsuits alleging violations of the California Invasion of Privacy Act. CIPA 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 allege retail, insurance and manufacturing businesses, among others, use website tracking tools to collect consumers' data in a manner that violates CIPA. Many of these cases focus on Section 631(a), which prohibits intercepting communications while in transit to learn the contents of the communication, although Sections 632(a) and 638 have also been invoked in privacy-related complaints. Section 631(a) has four clauses that can give rise to liability.

The first part of the statute prohibits the intentional tapping of "any telegraph or telephone wire, line, cable, or instrument, including the wire, line, cable, or instrument of any internal telephonic communication system." Part two prohibits the unauthorized interception and reading of "the contents or meaning of any message, report, or communication while the same is in transit." The third portion of the statute prohibits use of the contents of the communication that was intercepted without authorization. Lastly, the fourth portion prohibits a party to the communication from aiding and abetting any third party attempting to complete any of the prohibited acts listed above.

Section 632(a) requires consent from all parties before recording any confidential communications, while Section 638.51(a) prohibits the use of a pen register without a court order or prior consent from the user.

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.

What is considered 'contents of a communication' under CIPA?

A CIPA claim follows the same analysis and definitions of the Electronic Communication Privacy Act of 1989, which updated the Federal Wiretap Act of 1968. 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 the metadata of a communication. The contents of the communication must be intercepted while the communication is being made and not at a later point.

Some district courts have allowed CIPA lawsuits to proceed and avoided motions to dismiss in which the complaints sufficiently allege the data points collected — such as the users' clicks, swiping, scrolling, mouse movements, geolocations, IP addresses and typing — were contents within the meaning of the statute. For example, the court in Saleh v. Nike found the plaintiff sufficiently pleaded the defendant's vendor had collected contents 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 the defendant's website.

However, other district courts have repeatedly found plaintiffs failed to allege that the tracking software collected contents at the pleading stage. Some of these decisions hinged on the bare allegations the plaintiffs included in their complaints. 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."

CIPA litigation leads to circuit splits

In the landmark case in CIPA litigation, Javier v. Assurance Ins., the U.S. Court of Appeals for the Ninth Circuit found Section 631(a) of CIPA covered internet communications and was not limited to traditional phone conversations. The court went further in finding prior consent is required before a consumer's communications with the website can be intercepted by an undisclosed third-party vendor in the form of a recording.

Here, the plaintiff alleged the defendant's use of a session replay software captured the "contents of his communication," which the court defined as his "demographic information and medical history." The court found the plaintiff properly alleged the third-party software company captured his actions in real time without his prior consent and allowed the claim to survive the defendant's motion to dismiss.

However, the Ninth Circuit is split on how to interpret other parts of Section 631(a).

Is the tracking software an extension of the defendant or an illegal third-party eavesdropper?

A circuit split emerged regarding whether a vendor that provides tracking technology is a third-party eavesdropper within the scope of CIPA. Section 631(a) holds third-party eavesdroppers and parties that aid and abet these eavesdroppers liable for intercepting a party's communications. Therefore, plaintiffs must allege the third-party tracking tools are illegal third parties under the statute.

Courts have differed on whether a third party's software acts as an extension of the defendant, as a tape recorder by only storing the consumer's data, or if it acts as a traditional eavesdropper. Courts have found tracking software that acts as a mere tape recorder does not intercept the consumer's communications with the defendant's website and, therefore, does not give rise to liability under CIPA.

For example, in Graham v. Noom, the court found the defendant's vendor, a session replay software company, did not use the data for its own benefit but instead collected information solely for the defendant's benefit. 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.

To survive a motion to dismiss at the early stages of litigation, plaintiffs must allege the tracking software acts as a traditional eavesdropper and has the capacity to utilize the collected data for uses other than reporting analytics to the defendant. Indeed, courts have found software that instead acts as an eavesdropper to the communications between the consumer and the defendant will give rise to liability under CIPA if the consumer has not provided prior consent.

In the Javier case, for example, the court found a defendant's vendor could be a third-party eavesdropper if it had the capacity to use the collected data for its own benefit and further uses. In another example, the court in Rodriguez v. Ford Motor Co. found the plaintiff sufficiently alleged the defendant's software as a 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.

Are tracking technologies unlawful pen registers under CIPA?

More recently, courts have been split in determining whether website tracking technology fits within the definition of a pen register under CIPA, and courts have allowed plaintiffs past the pleading stage.

In Greenley v. Kochava, the leading decision for CIPA pen register claims, the court found the plaintiff sufficiently alleged the defendant's embedded tracking software was a "process" under CIPA's definition of a pen register.

However, in Licea v. Hickory Farms, the district court rejected the plaintiff's argument that the defendant used a pen register to collect IP addresses from its website. The court granted the defendant's motion to dismiss because the plaintiff failed to allege what device or process operated by the defendant constituted a pen register. Further, the court distinguished this complaint against allegations in Greenley by stating the collection of IP addresses vastly differed from the unique digital fingerprint alleged by the plaintiff in the prior case. The court also emphasized 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, an interpretation that "would potentially disrupt a large swath of internet comm erce."

Yet, a month later in Daryl Levings v. Choice Hotels International, the same district court found the plaintiff sufficiently alleged the use of a pen register when the defendant used software to collect information transmitted from the plaintiff's device and install a tracking code. The court rejected the defendant's motion to dismiss by concluding the plaintiff met their burden at the pleading stage and "a detailed description of the software and precise mechanism it employs are evidentiary facts which need not be included."

In Gabrielli v. Insider, the court dismissed a CIPA pen register claim in February 2025 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.

Article III of the U.S. Constitution provides federal courts the power to hear only cases or controversies. To satisfy this requirement, plaintiffs must allege they have standing to bring a claim in federal court by showing they suffered from an injury-in-fact, meaning an injury that is concrete, specific and can be traced to the defendant's conduct. Under current U.S. Supreme Court jurisprudence, if a plaintiff bringing a privacy-related claim cannot show a concrete harm, in which the injury has a close relationship to a traditionally recognized harm, they do not have standing to bring a claim.

In a motion to dismiss, the defendant argued the plaintiff lacked standing because they failed to show how sharing IP addresses with third parties was a concrete harm. The plaintiff argued the disclosure of visitors' IP addresses to third parties for the defendant's profit is an invasion of privacy recognized at common law. The court rebuffed the plaintiff's arguments, concluding an IP address does not reveal personal information of a visitor but instead only provides general geographic information as specific as a zip code. The court concluded the general information provided by an IP address does not constitute an invasion of privacy and therefore is not a concrete harm. In doing so, the court dismissed the plaintiff's claim for lack of standing with prejudice, barring the plaintiff from amending or refiling this claim.

Although the judges in Gabrielli and Hickory Farms both dismissed plaintiffs' pen register claims that alleged tracking technologies merely collected IP addresses, the Gabrielli decision may have a further-reaching impact as courts may now dismiss CIPA pen register claims at the outset of a lawsuit with similar arguments. However, Gabrielli does not preclude future CIPA pen register cases in which plaintiffs can sufficiently allege detailed personally identifiable information was disclosed to a third party using tracking technology like the plaintiff in Greenley.

Ultimately, the new wave of CIPA pen register claims may have been hindered, but businesses should still be aware of the remaining strength of this claim.

Rise in CIPA lawsuits for consumer tracking technologies

Plaintiffs' lawsuits focus on the technical aspects of various tracking tools and how these tools allegedly provide third parties with confidential communications without the users' consent, in violation of CIPA. These tools include session replay software, chatbots and pixel trackers, among others.

Session replay software

Session replay software provides website operators with visual playbacks or video recordings of users' actions on websites. It is commonly used by businesses to seamlessly view how users interact with their webpages and to troubleshoot issues consumers may have while using the webpages.

Case study: Javier v. Assurance

In Javier, the plaintiff used the defendant's website, where he input the required personal information to receive an insurance quote. The defendant had installed session replay software from a vendor on its website, allowing it to record a visitor's entire interaction with the webpage.

Chatbots

Chatbot and chat software provide consumers with real-time virtual assistance in the form of written communications while browsing a business's webpage. However, chatbots are often created and operated by third-party vendors, leading to lawsuits for conversations that are transmitted to the third party in real time for the chatbot to answer the user's question or prompt.

Case study: Jones v. Peloton

The plaintiff in Jones v. Peloton challenged the defendant's chat feature on its website because it embedded third-party software into the chat function to intercept and transmit visitors' communications to the third-party. Here, the court found the plaintiff failed to allege that the third-party was an eavesdropper and therefore granted the defendant's motion to dismiss.

Pixel tracking

Pixel tracking provides website operators with the ability to track user events and actions throughout visits to websites. Pixel tracking is a unique piece of code that allows the business to customize what user actions, such as clicking a button or image on the webpage, it would like to track. Many pixel tracking codes are free and provide businesses the option to install the code manually or with a partnered software vendor.

Pixel tracking allows the business to see how many user actions occur and how users interact with the website to improve their advertising. The pixel also sends user actions to the company that originally wrote the pixel code and can allow it to customize the users' ad placements while using its platforms.

Case study: Griffith v. TikTok

In Griffith v. TikTok, the plaintiff brought a claim under Section 631(a) and Section 632 against TikTok for the pixel code it provided to various online websites. In the complaint, the plaintiff maintained she had never created a TikTok account or utilized the platform due to privacy concerns, but TikTok obtained her personal information through its pixel code installed by websites like Hulu and Etsy. The court rejected the defendant's motion to dismiss because it failed to show the information collected by the pixel was not confidential, to prove the code was not used as a tape recorder and to provide any legal authority on why it should not be a liable third party for its tool.

Email marketing tools

Email tracking tools allow consumer-facing businesses to track when a potential or returning customer clicks a link in an email advertisement sent by the business. By using a third-party software, the email's words and images contain unique and traceable links to the consumers' email addresses and their actions. These actions are transmitted to the third-party software vendor and then later to the consumer-facing business. This can provide the business and the third party with information about consumer actions, like placing items in a virtual shopping cart. This allows the business to email consumers to encourage them to finish completing their purchases or notify them when products in their carts reduce in price.

Case study: Ramos v. The Gap

At issue in Ramos v. The Gap was the defendant's use of an email tracking software that embeds code on the defendant's emails to past and potential customers. Here, the court rejected the plaintiff's argument that the tracking software could reveal any further information other than the record information for the email, ultimately dismissing the plaintiff's complaint.

Pen registers

Pen registers and trap-and-trace devices are traditionally physical devices that are attached to a telephone line to log all the telephone numbers of incoming and outgoing calls. Plaintiffs alleging violations of CIPA's prohibition on pen registers argue the tracking technology collects information like IP addresses, browser types and locations to create user profiles or fingerprints, which are later shared with the third-party vendor and fit within CIPA's definition of a pen register. Plaintiffs argue the digital profile that is collected and shared is akin to sharing the incoming and outcoming telephone numbers that a traditional pen register or trap-and-trace device would perform.

It is important to note the provision regulating pen registers is applicable to both contents of a communication and record information.

Case study: Greenley v. Kochava

As discussed above, the plaintiff in Greenley v. Kochava alleged the defendant, a data broker, installed unlawful pen registers in the form of its software development kits in violation of CIPA Section 638.51. Plaintiffs argued software developer clients of the defendant used the SDKs to develop their own apps and in exchange allowed the defendant to "surreptitiously intercept location data" from users of the apps and created a unique fingerprint from each device. The plaintiffs then alleged the defendant sold the surreptitiously intercepted data to other clients in consumer-facing industries.

The court in Greenley rejected the defendant's motion to dismiss, finding the plaintiff sufficiently alleged the defendant's SDK could be a pen register under the expansive language of Section 638.51 of the statute. The court reasoned, since the plaintiff had properly alleged the SDK kits collected users' location data, it fit the definition of a pen register. Further, since the SDK kits were installed without a court warrant, the pen register was unlawful and the claim could survive a motion to dismiss.

Notable settlements

In Katz-Lacabe et al v. Oracle America, the defendant software company settled a class-action lawsuit for USD115 million after a federal district court rejected its motion to dismiss the plaintiffs' CIPA allegations. The plaintiffs argued the defendant's proprietary JavaScript code, which was hosted on various third-party websites, surreptitiously collected their personal information to create a "digital dossier" or digital fingerprint, which it later sold to third parties, in violation of CIPA. The court found the plaintiffs sufficiently pleaded enough facts to allege a CIPA violation and avoid the defendant's motion to dismiss.

In July 2024, Oracle announced it reached a settlement agreement with the plaintiffs in which the company would pay USD115 million and agreed to implement specific privacy measures to its existing products, while denying any wrongdoing. The settlement was approved in November 2024; however, it has since been appealed. The software company ended its advertising business in September 2024, citing a fall in revenue.

How can entities comply with CIPA while using analytic tracking technologies?

Businesses can 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's website. The notice should also inform visitors of what data will be collected while using the website, along with a mechanism for users to opt out of the data collection.

Because the Ninth Circuit is split on what information may be "contents of a communication" under CIPA, 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.

Further, businesses should consider utilizing cookie banners to disclose the tracking software used on the website, note what data will be collected and provide an option for users to affirmatively consent to the data collection. Along with providing sufficient information in both cookie banners and privacy notices, these must be conspicuous and clear, and conform with state and federal laws.

Businesses should also consider configuring the settings of tracking software to limit or reduce the amount of personally identifiable information to collect only the data needed to provide necessary analytics. They should also consider discontinuing and deleting trackers that are unnecessary or redundant to avoid over-collecting data that could be interpreted as content under CIPA and other wiretapping laws. Although much of the information collected by these trackers may look like record data on its face, the court in Saleh v. Nike found the manner of collection can transform record data to contents and create liability under Section 631(a).

Another consideration for businesses using third-party tracking software is understanding what the third party intends to do with the collected information. As discussed in Graham v. Noom, third parties that do not use the collected data for their own benefit will not create CIPA liability for businesses. Nonetheless, businesses should closely review procurement contracts and monitor third-party vendors to ensure their conduct will not leave them at risk for litigation.

As litigation under CIPA continues, businesses using tracking technologies must closely monitor ongoing 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.

3. Security breach litigation

By C. Kibby

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 limited circumstances.

The CCPA is unique among its cohort of comprehensive state privacy laws for having a PRA. While every such law contains enforcement avenues for public authorities, such as attorneys general and government agencies, the CCPA is the only comprehensive state privacy law passed so far to include a PRA. Washington state's My Health My Data Act and Illinois' Biometric Information Protection Act both provide for PRAs, but they are limited to health data and biometric data, respectively. Vermont's legislature passed a bill containing a PRA, but Gov. Phil Scott, R-Vt., vetoed it partly due to the controversial inclusion of a PRA, "which would make Vermont a national outlier, and more hostile than any other state to many businesses and non-profits." This remains the only comprehensive state privacy bill to be vetoed.

So, how does the CCPA's PRA work? Which consumers can sue which businesses over what kind of data breaches, and when?

Jurisdiction

The proceeding analysis is based on cases filed in federal and state courts throughout the U.S., which means they are not all equally weighted. For example, a federal court's interpretation of the CCPA binds other federal courts and non-California state courts but not California state courts because it is a state law. Potential parties should pay careful attention to which authority is binding and which is merely persuasive in the court where they want to file suit.

Trial procedures

None of these cases have made it to a final judgment, which is when the parties go through trial and the judge issues a ruling on which party wins. Instead, they are settled or dismissed, meaning there is more information on the granting or denial of a motion to dismiss than on winning or losing a final judgment.

Requirements to file action under CCPA's PRA

To survive a motion to dismiss, the action must comply with the CCPA's many requirements. First, private plaintiffs may only file actions under the PRA and cannot allege violations of other sections of the CCPA. Second, to fall into the purview of the CCPA's PRA, each plaintiff must be a natural person who is a California resident.

Moreover, each defendant must be a business that collects consumer personal information, determines how and why that information is processed and meets threshold requirements. If the defendant only receives information from a business and processes it according to that business's instructions, then the defendant might be a service provider. Entities can be service providers and businesses at the same time, but people may only bring actions against businesses, not those that are service providers alone.

Third, the action must concern the plaintiff's unencrypted and unredacted personal information. Personal information has a different definition under the PRA than under the rest of the CCPA. For the purposes of the PRA, personal information only contains two categories of information. Under the PRA, personal information can be the plaintiff's first name or initial and last name in conjunction with "data elements" like financial information or personal identifiers. Only one of these, the name or the data elements, needs to be unencrypted or unredacted. Alternatively, personal information can be a way to access the plaintiff's online account, such as username and password or an answer to a security question.

The PRA only concerns allegations that the plaintiff's personal information was "subject to unauthorized access and exfiltration, theft, or disclosure." Some courts have dismissed plaintiffs' CCPA claims because they did not plead specific facts or provide evidence that such a security breach occurred, while others have allowed claims based on allegations that a third party accessed personal information without requiring supporting evidence. One court allowed an allegation of mere potential access and disclosure past a motion to dismiss, so this area is still somewhat murky.

The PRA also requires plaintiffs to allege their personal information was subject to a security breach because the defendant failed to "implement and maintain security practices and procedures," a term not defined in the statute. However, the California attorney general's office has put out nonbinding guidelines for businesses around these practices and procedures, which include recommendations like strong encryption and multifactor authentication.

Medical or health information, which has a specific definition in the statute, is specifically exempted from the PRA. Some plaintiffs filed actions that involve unauthorized access of both their medical and nonmedical information but only claimed violations regarding their nonmedical information. Courts do not agree on whether the CCPA applies to the nonmedical information, but the most recent authority puts the onus on the plaintiff to allege the business treated medical information differently than nonmedical information. One case held that, if a business treats both types as medical information, then it is exempt from the CCPA.

The plaintiff can recover different types of compensation: statutory damages, which are an automatic amount from USD100-750 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.

If the plaintiff wants to recover statutory damages, they must give 30-day notice to the business of the alleged CCPA violation. Courts disagree on the timing of this notice. Some courts have required plaintiffs to send the notice before filing lawsuits at all. In some instances when the plaintiff did not provide this notice beforehand, the courts dismissed it with prejudice, meaning the plaintiff cannot allege the same claim again. However, other courts dismissed claims without prejudice and allowed plaintiffs to send notice after filing the lawsuits, wait for the required 30 days and then amend their suits to put the claim back in when the business did not cure.

The plaintiff does not need to give this notice or wait for a cure period if they only want to recover actual damages rather than statutory damages.

During the 30-day notice period, if the business "actually cures" the alleged violation and lets the plaintiff know in writing that they cured it, the plaintiff cannot move forward with the claim for statutory damages. As of 1 Jan. 2023, an amendment to the CCPA went into effect that states implementing and maintaining reasonable security procedures and practices in the cure period is not enough to be an actual cure. However, this implementation and maintenance can be an actual cure for incidents involving information collected before 1 Jan. 2023.

Regarding what defendants can do to cure alleged violations, one court held that enhancing security measures is not enough for information collected after 1 Jan. 2023. In two cases, the defendants said they cured the violations, but the courts rejected the arguments because the defendants did not present evidence to back up those assertions.

What claims can plaintiffs allege?

The CCPA plainly states private plaintiffs may not file claims "based on violations of any other section of this title," only the PRA section.

In 2020, after news reports alleged the video communication platform Zoom improperly shared consumer PI, multiple California plaintiffs filed actions under other sections of the CCPA. These included, for example, allegations that Zoom had not provided consumers adequate notice before collecting or disclosing consumer information. Other plaintiffs alleged Zoom did not provide an opportunity for consumers to opt out of selling or sharing their information. The attorney general of California and the California Privacy Protection Agency are the only entities that may enforce other parts of the CCPA, so these claims were facially invalid and immediately dismissed.

What is personal information?

Most of the plaintiffs who brought CCPA PRA actions met the bar for what counts as personal information. However, a complaint regarding general financial information and credit card fraud that 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" was dismissed because it did "not sufficiently allege disclosure of Plaintiff's personal information."

Security breaches and deficient security management

Plaintiffs may only file lawsuits if their personal information is subject to unauthorized access and exfiltration, theft or disclosure by a third party. This security breach must also be due to a business's failure to implement and maintain reasonable security procedures and practices.

For the first requirement, plaintiffs must allege both components. In Rodriguez v. River City Bank, the court threw out a plaintiff's CCPA claim because he alleged exfiltration, theft or disclosure without alleging unauthorized access.

When plaintiffs do allege both components, courts have differed on what allegations are necessary to sufficiently plead a security breach. Some courts have held that allegations of potential access are enough, while others have held that plaintiffs need to allege that a third party accessed their information. Still others have held that plaintiffs need to provide evidence that a third party accessed their information.

Holdings on this subject have gone back and forth over time. Soon after the PRA came into effect, the court in Stasi v. Inmediata Health Grp., did not dismiss a CCPA claim because "plaintiffs repeatedly allege(d) their information 'was viewed by unauthorized persons'" instead of alleging potential or inferred access.

The court in Mehta v. Robinhood Financial agreed, holding that "alleging that thousands of customer accounts (were) accessed by unauthorized users in a matter of days" was sufficient to allege a security breach. Similarly, the court in M.G. v. Therapymatch did not dismiss the plaintiff's CCPA claim even though he did not allege a data breach, holding that allegations "that defendants disclosed plaintiff's personal information without his consent due to the business's failure to maintain reasonable security practices" was enough to survive. None of these cases required the plaintiffs to allege more specific facts or to provide concrete evidence of these claims at the pretrial stage.

In Kirsten v. California Pizza Kitchen, mere potential access was enough. The court refused to dismiss a claim specifically because "unauthorized parties can access Plaintiffs' (personally identifiable information) on the internet," without mentioning any allegations that this had or had not occurred. However, the court in Lyman v. Kaufman Dolowich Voluck granted summary judgment against the plaintiff partially because he presented "no evidence" that his personal information on Hightail.com, the defendant's website, "was ever accessed by a third party."

Many courts do not mention the security breach prong, or they gloss over it, instead focusing on the second part of this requirement: that the security breach is due to a business's failure to implement and maintain reasonable security procedures and practices.

There is a general trend so far of requiring plaintiffs to allege specific facts regarding what the defendants' security practices and procedures were and how exactly they were deficient. For example, in Maag v. U.S. Bank, Griffey v. Magellan Health, In re Waste Management Data Breach Litigation and Cruz v. Bank of America, the courts all rejected the plaintiffs' CCPA claims because they failed to make such factual allegations about the defendants' security practices and procedures.

Accordingly, courts tend to hold the plaintiff has satisfied the requirements for deficient security management when plaintiffs allege specific facts. In Durgan v. U-Haul International, which survived a motion to dismiss, the defendant did not have adequate email filtering software, train employees, implement multifactor authentication, encrypt personal information or delete it when it was no longer needed.

In In re Sequoia Benefits, the court agreed with the plaintiff's argument that the defendant failed to follow the U.S. Federal Trade Commission's cybersecurity guidelines or other industry standards. The plaintiffs in In re Eureka Casino Breach Litigation also convinced the court by citing FTC guidelines and alleging the defendant failed to monitor for suspicious activity or ensure its vendors had adequate security, among other things.

However, other courts have taken a more lenient stance toward alleging deficient security management, especially early on in litigation. The court in Eureka Casino above also rejected an argument that the plaintiffs did not "provide enough detail about the defendant's former security systems" because the case was still in the early stages of litigation before discovery. In Doe v. MKS Instruments the court similarly held that "in this early phase, Plaintiff's allegations regarding inadequate security procedures are sufficient to state a CCPA claim."

Exceptions and exemptions

The plaintiff in a CCPA PRA action must be a natural person and not a business, per Kostiv and Associates v. Payink, and the defendant must be a business and not a natural person, per Rosado v. Zuckerberg.

A business is an entity that collects consumer data and determines how and why it is processed. If the defendant processes information on behalf of another party and does not make decisions about how it is processed, then the defendant is not a business but a service provider, which is exempt from liability under the PRA per In re In re NCB Management Servers.

The plaintiff in In re Blackbaud adequately alleged the defendant was a business because, among other things, it offered "professional and managed services ... for each of its software solutions" and was registered as a data broker in California, the definition of which requires that the entity be a business. The court in Miller v. Nextgen Healthcare held that using "consumers' personal data ... to develop, improve, and test Nextgen's services' ... is sufficient to satisfy the second requirement."

The CCPA contains exemptions for liability for certain types of businesses, but these do not always overlap with the exemptions in the

PRA specifically. For example, the defendant in Florence v. Order Express tried to argue the CCPA did not apply to it because it is subject to the Gramm–Leach–Bliley Act, but the court dismissed this argument because the statute contains a provision that says this exemption does not apply to the PRA.

Plaintiffs have also explored arguments surrounding the exceptions related to medical information and health care providers. In Stasi v. Inmediata Health Group the court refused to dismiss a claim that involved both medical and nonmedical information. It acknowledged the medical information was exempt, but stated, "Inmediata (did) not address the non-medical information that it admits was accessible on the internet," which allowed the plaintiff's claim to survive. The court did not mention the entity-level exemption.

However, the court in Tate v. EyeMed Vision Care declined to follow Stasi's lead and dismissed the claim because the plaintiff failed "to provide specific allegations that EyeMed (maintained) non-medical patient information in a different manner than medical information — a fact required to establish the California statute covers EyeMed." The court in Lurry v. PharMerica agreed with Tate and dismissed a claim for the same failure to allege different treatment of medical and nonmedical information.

Because the Stasi court did not mention the entity-level exemption, this portion is dictum and does not bind future courts' decisions, but the structure of the analysis suggests defendant Inmediata had the responsibility to claim it maintained medical information differently than nonmedical information. The courts in Tate and Lurry instead dismissed their respective CCPA claims because the plaintiff failed to make the same allegation, effectively flipping the requirement to the other party.

Notice, cure period and timing

The court in Gardiner v. Walmart held the CCPA only applies to violations of the duty to implement and maintain reasonable security procedures and practices that occurred on or after 1 Jan. 2020.

To recover statutory damages, the plaintiff must give a 30-day notice and may only proceed with filing the claim for statutory damages if the defendant does not actually cure the alleged 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.

The court in Griffey v. Magellan Health Inst. dismissed a CCPA claim with prejudice because the plaintiff filed a complaint demanding both actual pecuniary and statutory damages without giving notice beforehand, holding that "if a notice filed before the 30-day deadline could be updated when an amended complaint is filed and satisfy the 30-day notice requirement, then having the pre-suit notice requirement would be pointless." Two other courts in Golden v. Onetouchpoint and Guy v. Convergent Outsourcing also dismissed the claims, but gave the plaintiffs leave to amend and put the claims back in after the notice-and-cure period passed.

A later court in In re LastPass Data Security Breach 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 plaintiffs have filed an amended complaint more than 30 days after sending notice. The court in In re Eureka Casino Breach Litigation agreed and allowed a claim where the plaintiff provided CCPA notice and filed an action on the same day, then amended the complaint to include a CCPA claim four months later.

Another court 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 among themselves as to whether the plaintiffs could argue the claim.

Even when a plaintiff provides notice, it is not yet clear what actions can sufficiently cure an alleged breach. As of 1 Jan. 2023, an amendment to the CCPA took effect, stating "the implementation and maintenance of reasonable security procedures and practices does not constitute a cure with respect to (a) breach" for which the business has received notice.

Few cases address this newer standard, but those that do have cut toward the plaintiffs. In Florence v. Order Express, the court refused to dismiss the plaintiff's claim based on the defendant's "bare assertion in the motion to dismiss that it 'cured all alleged violations within the requisite time period.'" The defendant in Prutsman v. Nonstop Administration also said in its letter to the plaintiff that it had cured the CCPA violation, but the court also refused to dismiss the claim because this statement did "not render implausible plaintiff's allegations to the contrary." The court in Sequoia Benefits agreed with this reasoning.

Settlements

So far, every case that has survived a motion to dismiss has been settled. Cash penalties vary from case to case depending on how severe the alleged violation was, how many people were affected and other factors, but other common themes have emerged. 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 PRA, 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 platforms," which included conducting risk assessments, enabling multifactor authentication and hiring additional technical staff.

The settlement in In re 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 implementing multifactor authentication. This settlement stands out from the rest because it had no dedicated settlement fund; the only limit on the fees California Pizza Kitchen would pay depended on how many class members claimed their benefits.

To date, the largest publicized settlement was in In re T-Mobile Data Security Breach Litigation. 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."

Conclusion

Plaintiffs, defendants and courts alike are still feeling out the edges of what the PRA does and does not allow. Five years of litigation and hundreds of cases filed across the U.S. still make this area of jurisprudence relatively underdeveloped compared to most other areas of the law.

Many factors contribute to the lack of consensus in CCPA PRA cases. Both sides feel the pressure to settle disputes quickly so defendants do not have to admit fault, plaintiffs can recover money quickly without waiting months or years for a verdict and both sides can avoid creating potentially disadvantageous precedent in the future. Even the text of the CCPA remains in flux as it receives amendments to keep it relevant to the blistering pace of technological development.

Even if litigation under the CCPA's PRA is unlikely to reach equilibrium for years, if not decades, parties and their lawyers in these early stages have built litigation strategies based on preliminary impressions. Developments may be slow to manifest, but understanding will grow over time as more arguments and opinions shape what the PRA comes to mean for individuals and businesses.

4. Biometrics and consumer health data litigation

By Müge Fazlioglu, CIPP/E, CIPP/US

Private litigants alleging violations under the Illinois Biometric Information Privacy Act have had success settling claims regarding the privacy of their biometric data. The largest per-member award to date, around USD1,000 each for a class with over 45,000 members, comes from the sole BIPA case that was decided by a jury.

BIPA requirements

BIPA 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 3 years of its last interaction with the individual, 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/information.
- → The private entity has received written release by the subject.

Similarly, Section 15(d) prohibits private entities from disclosing, redisclosing or otherwise disseminating, respectively, an individual's biometric identifier or information unless they have met those three analogous conditions.

The third prong of this consent requirement for "written release" had been the subject of some debate. In August 2024, BIPA was amended to include "electronic signature" within this definition.

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(d) requires private entities in possession of biometric identifiers/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.

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 the Health Insurance Portability and Accountability Act.

Scope of BIPA's PRA

Section 20 of BIPA contains its private right of action. This section provides "any person" aggrieved by a violation 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 injunction.

Courts have previously ruled on the constructions of Section 15(b) and 15(d) of BIPA, namely whether "claims accrue each time a private entity scans a person's biometric identifier and each time a private entity transmits such a scan to a third party, respectively, or only 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 BIPA 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 at most entitled to one recovery for a given biometric identifier or biometric information regardless of the number of times the biometric identifier/information was collected, captured, purchased, received through trade or otherwise obtained, per Section 15(b), and at most one recovery under Sec. 15(d) regardless of how many times the biometric identifier or information was disclosed, redisclosed or otherwise disseminated to a recipient.

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.

T.K. v. Bytedance Tech.

The settlement in T.K. v. Bytedance Tech. 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, also being one of those specified in the act as a "scan of face geometry."

Meta lawsuits

Hailed at the time as the largest privacy class-action settlement, Meta, then Facebook, reached an agreement with Illinois Facebook users in Patel v. Facebook for USD650 million over its alleged use of facial recognition technology to collect and store user's 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, as well as 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 — and only to date — jury trial under BIPA, heard in 2022, resulted in an order for BNSF 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 for the damages amount to be determined by a judge rather than a jury, an interim agreement was reached between BNSF and class members 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.

MHMDA

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, a subcategory of the act defined as those with the consumer health data of less than 100,000 consumers or that derive less than 50% of their gross revenue from the collection, processing, selling or sharing of consumer health data of less than 25,000 consumers, had a delayed effective date of 30 June 2024.

Consumers must allege actual damages to bring lawsuits under the 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.

Almost a year after the law's entry into force in March 2024, the first class-action lawsuit under MHMDA was brought on February 10, 2025, against Amazon for alleged violations by the company's software development kit embedded 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 Privacy Act, a proposed state bill that tracks closely to BIPA, has come close to passage. Like BIPA, it would prohibit collection and sharing of biometric identifiers and biometric information without prior consent, and, most importantly, it 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.

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 also 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 PRAs. 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 magnified the compliance challenges for organizations that collect, use, and store biometric and consumer health data.

iapp

5. Data brokers and judicial privacy litigation

By Kayla Bushey, CIPP/US

A new state law aimed at protecting the personal information of state and federal 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 under Daniel's Law, exposed to financial and reputational damage, as individuals assert their privacy rights under the law.

Daniel's Law of New Jersey

Daniel's Law provides covered persons the right to request businesses to 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 passed in 2020 after an assassination attempt on U.S. District Court for the District of New Jersey Judge Ester Salas tragically killed her son Daniel Alder and critically injured 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 fines of USD1,000 per violation.

Upon passage of the 2023 amendment, state and federal courts saw an influx of lawsuits brought under the law. 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. Here, defendants argued 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, U.S. District Court for the Eastern District of Pennsylvania 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 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 jurisprudence, the 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 " that is not "underinclusive."

Bartle found the state's interest in protecting public officials' home addresses and telephone numbers were not outweighed by any public significance arguments made by the defendants. Therefore, the court rebuffed the defendant's facial challenges to the law and denied their motions to dismiss.

The defendants in these 60 cases are not the first to challenge the law on First Amendment grounds. 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 district court ruled against the journalist and a panel of appellate judges affirmed the lower court's finding in April 2024. The plaintiff has petitioned to the New Jersey Supreme Court.

Maryland passed a similar statute after a Maryland judge was killed outside his home in 2023. Georgia, Florida, 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. The Florida, Idaho, Maryland, Minnesota and New York laws are already in effect, while the Georgia and Wisconsin laws will come into effect in July and April 2025, respectively.

Furthermore, Congress passed its own version of Daniel's Law, although it is more limited in scope, with the James M. Inhofe National Defense Authorization Act for the Fiscal Year 2023. 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.

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 take-down requests.

Businesses and individuals that receive take-down 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 take-down requests.

This law will also require businesses to sufficiently manage third-party vendors, develop proper data disposal protocols and retain records of compliance with take-down requests received by the organization. Although the existing class-action lawsuits have not reached final decisions on the merits of the law, New Jersey 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 steps to respect the rights of covered persons asserted under the law.appoint an authorized representative in the EU in accordance with Article 54.

6. Litigating accountability through shareholder action

By Cheryl Saniuk-Heinig, CIPP/E, CIPP/US

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.

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 leadership, such as the C-suite or board of directors, has fiduciary duties of care and loyalty to the shareholders, i.e., the owners of the company above all else. Although there are many exceptions and specific procedures that must be followed. Generally speaking, any shareholder who alleges a company's leadership — whether through negligence, bad decisions or outright misconduct — harmed the company, 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 its best interest. However, these lawsuits are not easy. 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 or push them to strengthen their data protection practices.

Privacy, cybersecurity and digital governance remain enormous concerns for companies today. 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 where shareholders attempt to ensure company leadership takes responsibility for failures to shareholders.

Derivative actions based on privacy incidents

Although several shareholder derivative actions have been brought based on leadership's alleged role and conduct prior to a company's privacy or cybersecurity incident, derivative actions rarely, if ever, obtain a successful trial judgment. However, by bringing actions and forcing companies to respond to the allegations, shareholders can highlight past conduct and action of leadership 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, mandate monitoring mechanisms, and hopefully 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.

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.

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 arsenals 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.

Contact

Müge Fazlioglu
Principal Researcher, Privacy Law and Policy
muge@iapp.org

Joe Jones
Director of Research and Insights, IAPP
jjones@iapp.org

For further inquiries, please reach out to research@iapp.org.

Follow the IAPP on social media

Published June 2025.

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.