Privacy, Cybersecurity, and Data Breach Litigation: Key Laws and Considerations

A Practical Guidance® Practice Note by
Kristin Bryan, Jesse Taylor, and Shing Tse, Squire Patton Boggs

Kristin Bryan
Squire Patton Boggs

Jesse Taylor
Squire Patton Boggs

Shing Tse
Squire Patton Boggs

This practice note covers key legal issues in privacy, cybersecurity, and data breach litigation. Specifically, this note includes federal and state privacy laws often involved in such litigations, recent developments concerning U.S. Const. Art. III standing, the application of privilege to forensic reports prepared in the wake of a data event, and class certification considerations. Data privacy cases require retention of experienced counsel as this area of law is continually evolving and particularly complex, as illustrated in some detail below.

For related news, see Cybersecurity & Privacy Cases To Watch In 2022, State Privacy Law Compliance Has Ways To Go, Survey Shows, Google becomes latest tech giant stung by Illinois privacy law, agrees to $100 million settlement, and Facebook To Pay $90M To Settle Suit Over Tracking Users.

For more information on state privacy laws, see Data Breach Notification Enforcement and Penalties State Law Survey, Third-Party Disclosure of Personal Data State Law Survey, Protection of Personal Information in Government Records State Law Survey, Privacy Legislation Tracker: State Comprehensive Consumer Privacy Bills, and Consumer Data Privacy: State Law Comparison Charts.

Outside the scope of this note is biometric privacy litigation. For more information on biometric privacy, see How Ill. High Court Ruling May Further Evolve BIPA Landscape, Biometric Privacy: Mitigating Legal Risks When Using Biometric Technologies, and Biometrics and Data Privacy Podcast.

Common Federal Statutory Claims

A number of federal statutes commonly serve as the basis for data security and privacy litigation, including the Computer Fraud and Abuse Act, the Driver's Privacy Protection Act, the Electronic Communications Privacy Act, the Video Privacy Protection Act, the Telephone Consumer Protection Act, the Fair Credit Reporting Act, the Health Insurance Portability and Accountability Act of 1996, and others.

Computer Fraud and Abuse Act (CFAA)

The CFAA, passed in 1986, imposes criminal and civil liability on anyone who "intentionally accesses a computer without authorization or exceeds authorized access." See 18 U.S.C. § 1030(a)(2). The CFAA is largely considered to be the primary anti-hacking law and prosecutorial tool against outside actors who are accused of breaking into computer networks.

Application

The CFAA's prohibitions apply to every "protected computer," which includes computers:

- For use by or for the federal government or a financial institution –and–
- Used in interstate or foreign commerce, including non-networked computers and those connected to the internet

18 U.S.C. § 1030(e)(2).

The CFAA covers many types of fraudulent activity, including:

- Theft of trade secrets
- Hacking and data breaches
- Denial or interruptions of service –and–
- Other anticompetitive behavior

CFAA prohibitions that may form the basis for civil and criminal liability include:

- Intentionally accessing a computer without authorization or exceeding authorized access, obtaining:
  - Certain information from a financial institution
  - Information from any U.S. department or agency –or–
  - Information from any protected computer (18 U.S.C. § 1030(a)(2))
- Knowingly and with intent to defraud, accessing a protected computer without authorization, or exceeding authorized access and obtaining anything of value (18 U.S.C. § 1030(a)(4))
- Knowingly, intentionally, and without authorization causing the transmission of a program, information, code, or command, that results in damage to a protected computer (18 U.S.C. § 1030(a)(5)(A))
- Intentionally accessing a protected computer without authorization, resulting in damage and loss (18 U.S.C. § 1030(a)(5)(B))

Recent Decisions

Amidst a long-standing circuit split, the U.S. Supreme Court recently clarified the scope of "exceeds authorized access" within the meaning of the CFAA. The Court reversed the Eleventh Circuit's decision to uphold the conviction of a former police officer charged under the CFAA for searching a license plate in a law enforcement database for unofficial purposes. See Van Buren v. United States, 141 S. Ct. 1648 (2021). His conviction concerned a provision of the statute that made it illegal "to access a computer with authorization and to use such access to obtain . . . information in the computer that the accessor is not entitled so to obtain." The officer appealed, claiming that the CFAA did not cover unauthorized use of a database that he was otherwise authorized to access as part of his job.

The Court rejected broader interpretations adopted by the First, Fifth, and Eleventh Circuits that individuals may "exceed authorized access" when misusing information, they have permission to access when the misuse violates the terms of a policy or agreement. Ultimately, the Court concluded that the provision of the CFAA that plaintiff had been convicted under "covers those who obtain information from particular areas in the computer—such as files, folders, or databases—to which their computer access does not extend. It does not cover those who have improper motives for obtaining information that is otherwise available to them." Van Buren, 141 S. Ct. at 1652. Justice Barrett's opinion also focused on the statute's scope, noting that the government's broad interpretation would criminalize a "breathtaking amount of commonplace computer activity," including mundane activities such as using a work computer for personal purposes. Van Buren, 141 S. Ct. at 1661.

Prior to the Court's opinion, litigants often relied on the CFAA's "without authorization" or "exceeds authorized access" prohibition to reach other privacy-related conduct that violated a websites' terms of use or other agreements or policies, such as data scraping. The Supreme Court's opinion appears to have foreclosed such actions under the CFAA for the time being.

Indeed, the Ninth Circuit recently held that data scraping publicly available information is not actionable under the CFAA. hiQ Labs, Inc. v. LinkedIn Corp., 31 F.4th 1180 (9th Cir. 2022). Relying on the Supreme Court's "gates-up-or-down" inquiry (i.e., if authorization is required and has been given, the gates are up; if authorization is required and has not been given, the gates are down), the Ninth Circuit found that where information is on a publicly available website, "that computer has erected no gates to lift or lower in the first place." The Ninth Circuit articulated the following rule for CFAA liability:

> [T]he CFAA's prohibition on accessing a computer "without authorization" is violated when a person circumvents a computer's generally applicable rules regarding access permissions, such as username and password requirements, to gain access to a computer. It is likely that when a computer network generally permits public access to its data, a user's accessing that publicly available data will not constitute access without authorization under the CFAA.

hiQ Labs, Inc., 31 F.4th at 1224. In other words, only information that requires some prior authorization is encompassed under the CFAA. Publicly available information is generally not.

Driver's Privacy Protection Act (DPPA)

The DPPA, 18 U.S.C. § 2721 et seq., regulates the disclosure of personal information by state departments of motor vehicles and their officers, employees, and contractors.

The DPPA prohibits the release and use of certain personal information from a state's motor vehicle records except for reasons permitted by the statute. Under the statute's narrow private right of action, violators can be liable for:

- Actual damages not less than liquidated damages in the amount of $2,500
- Punitive damages upon proof of willful or reckless disregard of the law
- Reasonable attorney's fees and other litigation costs reasonably incurred –and–
- Other preliminary and equitable relief as the court finds appropriate

18 U.S.C. § 2724.

An increasingly common issue is whether an individual's driver's license, voluntarily given to a private person or entity during a commercial transaction, constitutes a "motor vehicle record" under the DPPA. Because driver's licenses are frequently used in private commercial transactions to verify identities, provide required personal information, and to collaterally secure goods and services, whether the scope of the DPPA encompasses licenses is a topic of debate among courts. See Garey v. Farrin, Nos. 21-1478, 21-1480, 2022 U.S. App. LEXIS 15391, at *15–16 (4th Cir. June 3, 2022); Allen v. Vertafore, Inc., 28 F.4th 613 (5th Cir. 2022).

Electronic Communications Privacy Act (ECPA)

The Electronic Communications Privacy Act of 1986 (ECPA) is comprised of the Electronic Communications Privacy Act and the Stored Wire Electronic Communications Act. It generally protects wire, oral, and electronic communications while those communications are being made, when they are in transit, and when they are stored on computers. The ECPA has two titles:

- **Title I: The Wiretap Act.** The Wiretap Act prohibits the intention actual or attempted interception, use, or disclosure, or obtaining another person to intercept or try to intercept any wire, oral, or electronic communication. 18 U.S.C. § 2511.
- **Title II: The Stored Communications Act (SCA).** The SCA protects the privacy contents of files stored and records held about the subscriber by service providers, such as name, billing records, or IP addresses. It authorizes claims when a service provider:
  - Allows for unauthorized, intentional access to the contents of stored communications
  - Intentionally discloses stored communications to any third party (18 U.S.C. § 2702)

The SCA distinguishes between content (e.g., the text of an email or message) and other information (e.g., identifying information, etc.), and only bars production of content.

Class action litigation may arise under the ECPA under several circumstances:

- Collecting information and data on users and selling it to third parties who send targeted ads to the users (In re Google RTB Consumer Priv. Litig., No. 21-cv-2155-YGR, 2022 U.S. Dist. LEXIS 115023 (N.D. Cal. June 30, 2022))
- Using a Javascript code maintained by a third party to collect and analyze data (e.g., IP address) of anonymous web users in order to identify who visits their website (Allen v. Quicken Loans, Inc., No. 17-12352, 2018 U.S. Dist. LEXIS 192066 (D.N.J. Nov. 9, 2018))
- Data breaches resulting in knowing disclosure of communications (In re Yahoo!, Inc. Customer Data Sec. Breach Litig., No. 16-MD-02752-LHK, 2017 U.S. Dist. LEXIS 140212, at *151 (N.D. Cal. Aug. 30, 2017); In re Pharmatrak, Inc. Privacy Litig., 329 F.3d 9 (1st Cir. 2003))
- Disclosing contents of a communication to advertisers through advertising banners (In re Facebook Privacy Litig., 791 F. Supp. 2d 705, 712 (N.D. Cal. 2011))

For more on the ECPA, see Electronic Communications Privacy Act (ECPA): Key Issues.

Video Privacy Protection Act (VPPA)

The VPPA, 18 U.S.C. § 2710, provides a private right of action against videotape service providers who knowingly disclose personally identifiable information concerning any consumer. 18 U.S.C. § 2710(c). "Video tape service providers" include any person engaged in the business of

rental, sales, or delivery of prerecorded video cassette tapes or similar audiovisual materials. 18 U.S.C. § 2710(a)(4).

Plaintiffs have relied on this statute to bring actions against a variety of entities, including television networks, website and app operators, and social media companies. See, e.g., Robinson v. Disney Online, 152 F. Supp. 3d 176 (S.D.N.Y. 2015) (dismissing VPPA claims against operator of streaming app where information was not PII within the meaning of the statute); T.K. v. Bytedance Tech. Co., Ltd., 2022 U.S. Dist. LEXIS 65322 (N.D. Ill. Mar. 25, 2022) (certifying VPPA class and settlement in suit against social media company).

Eichenberger v. ESPN, 876 F.3d 979 (9th Cir. 2017) addressed one such lawsuit. There, the plaintiff sued ESPN under the VPPA because ESPN disclosed his Roku device serial number and the titles of the videos he watched to Adobe Analytics. Adobe identified specific consumers by connecting this information with other data in Adobe's possession (such as email addresses, account information, or Facebook profile information, including photos and usernames).

Plaintiff argued that his Roku device serial number and the titles of the videos were personally identifiable information because Adobe would use them to identify him and, as such, ESPN violated the VPPA by disclosing such information. The district court rejected the argument finding such information did not constitute personally identifiable information within the meaning of the VPPA.

The Ninth Circuit found that the plaintiff's claims failed under the VPPA, because PII is the only information that "readily permits an ordinary person" to identify a particular individual as having watched a certain video. Since the disclosure of the device's serial number and titles of videos creates a large pool of possible individuals and did not identify a particular individual, the court held that such information does not constitute PII in this context. Furthermore, the court noted that the VPPA seeks to prevent services providers from "knowingly disclosing" a user's information and does not require the provider to consider how the recipient intends to use it. Consequently, even though Adobe could identify plaintiff by combining the data provided by ESPN with other data already in its possession, its ability to do so did not change the information shared by ESPN into PII under the VPPA.

The court's narrow reading of what constitutes "PII" and "knowingly disclose" may deter plaintiffs from relying on the VPPA. However, the precise meaning of "PII" under the VPPA will certainly be subject to further litigation—particularly in light of the unresolved circuit split. Compare Yershov v. Gannett Satellite Info. Network, Inc., 820 F.3d 482 (1st Cir. 2016) (finding that defendant, which operated the "USA Today Mobile App," disclosed PII when it shared with Adobe information about which videos the plaintiff-user watched on the smartphone application, along with GPS coordinates of the device when the video was viewed and certain identifiers associated with the user's device); with In re Nickelodeon Consumer Privacy Litig., 827 F.3d 262, 266 (3d Cir. 2016) (rejecting plaintiff's argument that his IP address and other information about his browser and operating system settings were PII on the grounds that PII only refers to "the kind of information that would readily permit an ordinary person to identify a specific individual's video-watching behavior").

Telephone Consumer Protection Act (TCPA)

The TCPA, 47 U.S.C. § 227, governs telemarketing calls and calls made using certain automated dialing equipment. While the TCPA, is not exactly a privacy statute in the traditional sense, courts have found that the injuries arising out of violations of the statute are based in consumers' privacy interests.

Application

The TCPA makes it unlawful to make any nonemergency, nonconsensual calls using any automatic telephone dialing system (ATDS) or an artificial or prerecorded voice to any telephone number assigned to a paging service, cellular telephone service, or any other service for which the called party is charged for the call. 47 U.S.C. § 227(b)(1)(A)(iii). Among other things, it likewise prohibits making telephone solicitation calls to any residential telephone number that is registered on the National Do-Not-Call Registry. 47 U.S.C. § 227(c); 47 C.F.R. § 64.1200(c).

Putative class action litigation is a common method of enforcing TCPA violations. State and federal courts have concurrent jurisdiction over private actions brought under the TCPA but, in practice, TCPA actions are most frequently litigated in federal courts. Mims v. Arrow Fin. Servs., LLC, 565 U.S. 368 (2012).

Recent Decisions

Prior to the Supreme Court's ruling in Facebook, Inc. v. Duguid, 141 S. Ct. 1163 (2021), TCPA plaintiffs frequently brought class action claims under 47 U.S.C. § 227(b)(1)(A), the restriction on using an ATDS to make nonconsensual calls. This is because courts interpreted the TCPA's definition of ATDS in different ways, often broadly. See, e.g., Marks v. Crunch San Diego, LLC, 904 F.3d 1041, 1043 (9th Cir. 2018). Some courts interpreted ATDS to encompass calls made using any equipment that could store telephone numbers to be called, which would include the vast majority of telephone systems in use today.

However, the Supreme Court clarified that dialing equipment is governed by the ATDS restrictions only if it stores or produces numbers using a "random or sequential number generator." Facebook, 141 S. Ct. at 1170. Thus, post-Facebook, it is not enough for equipment to store telephone numbers and dial such numbers automatically; it must actually use, in some manner, a random or sequential number generator. This is necessarily a high bar, resulting in a shift in focus in recent TCPA class actions.

Now, TCPA class actions are commonly brought under the TCPA's restrictions on calls made using an "artificial or prerecorded voice," 47 U.S.C. § 227(b)(1)(A). See, e.g., Williamson v. Irving K Motor Co. LLC, Civil Action No. 3:21-CV-1599-L-BH, 2022 U.S. Dist. LEXIS 101052, at *20 (N.D. Tex. June 7, 2022) (denying motion to dismiss prerecorded voice claims premised on alleged prerecorded voice marketing messages).

Plaintiffs are likewise bringing claims under the TCPA's implementing regulations prohibiting certain telemarketing and telephone solicitations, see 64 C.F.R. § 64.1200(c) and (d); Gill v. Align Tech. Inc., No. 21-CV-631-JPS, 2022 U.S. Dist. LEXIS 87464, at *5 (E.D. Wis. May 16, 2022), as well as the prohibition on making calls to residential phone numbers registered on the National Do-Not-Call (DNC) Registry. See 64 C.F.R. § 64.1200(c)(2); Visco v. Creditors Relief, LLC, No. 20-cv-12303-DJC, 2022 U.S. Dist. LEXIS 28908, at *3 (D. Mass. Feb. 17, 2022). Notably, calls are only actionable under Section 64.1200(c) and (d) if the subject calls were made to a "residential telephone subscriber," which the Federal Communications Commission has concluded covers calls made to cell phones. In re Rules & Reguls. Implementing the Tel. Consumer Prot. Act of 1991, 18 FCC Red. 14014, 14039 (2003). Neither the TCPA nor the implementing regulations define "residential telephone subscriber." Thus, a common issue in telemarketing, solicitation, and DNC claims is whether the subject phone number is, in fact, a "residential" number. See, e.g., Smith v. Vision Solar LLC, No. 20-2185, 2020 U.S. Dist. LEXIS 172224, at *8 (E.D. Pa. Sept. 21, 2020) (dismissing DNC claim where plaintiff failed to plead that the cell phone line in question was his residential phone, as required for a claim under Section 227(c)).

TCPA Standing

Another oft-disputed issue in TCPA actions is whether the class representatives satisfy Article III standing requirements, and there is no uniform answer among the circuits. Compare Cranor v. 5 Star Nutrition, LLC, 998 F.3d 686 (5th Cir. 2021) (finding that a consumer alleged a cognizable injury-in-fact sufficient to confer Article III standing based on receipt of a single unsolicited text message) with Salcedo v. Hanna, 936 F.3d 1162 (11th Cir. 2019) (finding that the receipt of a single unwanted text message does not constitute injury-in-fact under Article III). While the Supreme Court has yet to resolve the circuit split, its opinion in TransUnion LLC v. Ramirez, 141 S. Ct. 2190 (2021) may be helpful to guide courts in the meantime. Nonetheless, it is clear that the alleged harms caused by TCPA violations arise out of the invasion of privacy that animates other data privacy actions. See Krakauer v. Dish Network, LLC, 925 F.3d 643, 650 (4th Cir. 2019) (noting that Congress enacted the TCPA "to protect against invasions of privacy that were harming people").

Mini-TCPA Acts

Following the Supreme Court's ruling in Facebook, some states began passing their own "mini" versions of the TCPA. See, e.g., Fla. Stat. § 501.059. Such statutes tend to be broader than the TCPA insofar as they apply to a wider range of telephone equipment and have more stringent consent requirements. See Fla. Stat. § 501.059(8)(a) (prohibiting sales calls and texts placed using an "automated system for the selection or dialing of telephone numbers" without first obtaining prior express written consent). Given the breadth and vagueness of these TCPA state analogs, you can expect to see a significant increase in complaints filed under these statutes.

For more on the TCPA and mini-TCPA acts, see Telephone Consumer Protection Act (TCPA) Compliance and Telemarketing Privacy State Law Survey.

Fair Credit Reporting Act (FCRA)

The FCRA, 15 U.S.C. § 1681 et seq., governs the disclosure of certain information from a consumer's credit file. The FCRA prohibits consumer reporting agencies (CRAs) from disclosing information such as credit history, employment background, medical information, and financial status unless permitted by an express statutory exception, also known as a "permissible purpose," or with the consumer's consent. It also prohibits furnishers of credit information from providing inaccurate information and requires furnishers to conduct reasonable investigations into consumer disputes.

FCRA litigation arises from the myriad obligations CRAs, furnishers, and users of consumer information have under the statute, including the following:

- A CRA may provide a consumer report only for the reasons permitted by 15 U.S.C. § 1681b.
- Persons who procure an investigative consumer report must make the requisite disclosures to the consumer. 15 U.S.C. § 1681d(a)(1).
- CRAs have a duty to maintain reasonable procedures to avoid FCRA violations and ensure maximum possible accuracy of report information. 15 U.S.C. § 1681e.

- CRAs have a duty to timely reinvestigate consumer disputes. 15 U.S.C. § 1681i.
- Persons using information in consumer reports to take an adverse action against a consumer (such as denial of credit) must disclose the basis and source of the information used to support the adverse action. 15 U.S.C. § 1681m.
- Furnishers have a responsibility to provide accurate information, and to refrain from providing information if it knows or has reasonable cause to believe that the information is inaccurate. 15 U.S.C. § 1681s-2.

The FCRA imposes liability for both willful and negligent noncompliance. Willful noncompliance subjects a defendant to actual damages or statutory damages of $100 to $1000, punitive damages, and costs and attorney's fees. 15 U.S.C. § 1681n. Negligent noncompliance is limited to actual damages, costs, and attorney's fees. 15 U.S.C. § 1681o.

FCRA litigation has been on the upswing in recent years, both on an individual and class basis. One of the driving issues in recent FCRA litigation is whether a bare statutory violation of the FCRA, absent concrete harm, gives a plaintiff standing under Article III. The Supreme Court, in Spokeo, Inc. v. Robins, 578 U.S. 330 (2016), answered that question in the negative—but with a caveat. Specifically, the risk of real harm can provide standing, even if the harm may be difficult to prove or measure. Spokeo, 578 U.S. at 341. The Supreme Court carried this principle forward in TransUnion LLC v. Ramirez, 141 S. Ct. 2190 (2021), finding that individuals for whom inaccurate information was actually provided to third parties suffered a concrete harm, while those who had undisclosed inaccurate information in their reports suffered no harm and had no claim.

The FCRA was amended in 2003 by the Fair and Accurate Credit Transactions Act (FACTA), 108 Pub. L. No. 159, 117 Stat. 1952. Among its provisions, FACTA:

- Requires the three major CRAs (Equifax, Experian, and TransUnion) to provide consumers their credit reports without charge
- Permits consumers to place alert messages on their files if they suspect fraud –and–
- Limits the inclusion of payment card account numbers on receipts to the final five digits

A significant amount of FACTA litigation arises from technical violations of the account number limitation, and courts are generally in agreement that a noncompliant receipt is insufficient to establish a concrete injury. See, e.g., Thomas v. Toms King (Ohio II), LLC, 997 F.3d 629 (6th Cir. 2021); Muransky v. Godiva Chocolatier, Inc., 979 F.3d 917 (11th Cir. 2020) (en banc).

For more on the FCRA and state mini-FCRAs, see Fair Credit Reporting Act (FCRA) and State Mini-FCRAs: Step-by-Step Guidance for Compliance.

Health Insurance Portability and Accountability Act of 1996 (HIPAA)

HIPAA, Pub. L. No. 104-191, establishes national standards to protect certain health-related personal information from being disclosed without the patient's consent or knowledge. HIPAA is enforced by the Office of Civil Rights (OCR) within the Department of Health and Human Services, and OCR refers potential criminal violations of HIPAA to the U.S. Department of Justice. The range of potential civil fines for violations of HIPAA depends on the covered entity or business associate's degree of knowledge of the violation; the maximum penalty of willful violations is over $50,000 per violation with an annual cap of over $1.5 million for repeated violations.

Although HIPAA does not contain a private right of action, plaintiffs often use a business's alleged failure to comply with HIPAA standards to support state law claims, such as negligence or breach of contract. Plaintiffs in healthcare data breach actions also often argue that the disclosure of protected health information covered by HIPAA is sufficient to establish Article III standing. Moreover, HIPAA sets only minimum standards that must be followed when patient data is at issue. It does not prevent states from passing more stringent healthcare privacy laws, such as Minnesota's Health Records Act, Minn. Stat. §§ 144.291 through 144.298. And unlike HIPAA, these state laws permit patients to sue providers for violations.

In short, where patient health information is involved in data privacy litigation, HIPAA and state analogs may be invoked by plaintiffs to support their claims.

For more on HIPAA, see HIPAA Resource Kit.

Other Relevant Federal Privacy Laws

Certain other federal statutes provide no private cause of action to consumers, but still play an important role in data privacy litigation as the basis for state common law claims such as negligence per se, and as the subject of federal agency regulation and enforcement actions.

Gramm-Leach-Bliley Act (Financial Modernization Act of 1999)

The Gramm-Leach-Bliley Act (GLBA), 15 U.S.C. § 6801 et seq., requires financial institutions to respect consumer privacy to protect the security and confidentiality of customers' nonpublic personal information. 15 U.S.C. § 6801(a). It also requires federal agencies identified under 15

U.S.C. § 6805(a) to establish appropriate standards relating to administrative, technical, and physical safeguards. 15 U.S.C. § 6801(b).

The GLBA prohibits obtaining customer information by false pretenses, 15 U.S.C. § 6821, and imposes criminal penalties for violations. 15 U.S.C. § 6823. However, the GLBA provides no express or implied private right of action. See, e.g., Barroga-Hayes v. Susan D. Settenbrino, P.C., No. 10 CV 5298, 2012 U.S. Dist. LEXIS 47071, at *17 (E.D.N.Y. Mar. 30, 2012); Dunmire v. Morgan Stanley DW, Inc., 475 F.3d 956, 960 (8th Cir. 2007). Rather, the GLBA is enforced by the Consumer Financial Protection Bureau, federal functional regulators, state insurance authorities, and the Federal Trade Commission. 15 U.S.C. § 6805(a).

Significantly, some states have embraced negligence per se common law claims that permit consumers to borrow duties of care from consumer protection statutes and seek damages under state law. See, e.g., In re Experian Data Breach Litig., 2016 U.S. Dist. LEXIS 184500, at *9 (C.D. Cal. Dec. 29, 2016) (finding that New York's negligence per se cause of action permitted a plaintiff to rely on the GLBA to assert a state law claim). Other states, however, expressly bar consumers from relying on statutes like the GLBA to create duties under state law. See, e.g., Wells Fargo Bank, N.A. v. Jenkins, 293 Ga. 162 (2013) (holding that the GLBA could not create a duty under Georgia law in order to sustain a negligence cause of action).

For more on the GLBA, see Gramm-Leach-Bliley Act (GLBA) Privacy Requirements.

Securities and Exchange Commission Regulation S-P

Under its GLBA authority, the Securities and Exchange Commission promulgated Regulation S-P, 17 C.F.R. § 248.10(a). The scope of Regulation S-P is limited to financial institutions, including investment advisors, and prohibits the disclosure of nonpublic personal information about a consumer to nonaffiliated third parties without required notice and the ability to opt out. 17 C.F.R. § 248.10(a)(1). Regulation S-P applies only to transactions for "personal, family, or household purposes," 17 C.F.R. §§ 248(j), (k)(1); 248.3(g)(1), and does not apply to products or services obtained primarily for business, commercial, or agricultural purposes. 17 C.F.R. § 248.1(b). Because Regulation S-P was enacted pursuant to the GLBA, it does not provide for a private right of action. Rezende v. Citigroup Global Mkts., Inc., 2010 U.S. Dist. LEXIS 122349, at *14–15 (S.D.N.Y. Nov. 17, 2019); Dunmire v. Morgan Stanley DW, Inc., 475 F.3d 956, 960 (8th Cir. 2007) (collecting cases).

In practice, Regulation S-P is rarely invoked in litigation, primarily serving as the particular basis for the invocation of the GLBA in relation to a state common law claim. See, e.g., Furth v. Zanic, 2009 U.S. Dist. LEXIS 147985, at *61–66 (N.D. Ohio Feb. 2, 2009) (granting summary judgment with respect to breach of fiduciary duty claim premised in part on violation of Regulation S-P, where plaintiff was not a "consumer" or "customer" of the financial institution within the meaning of the Regulation). More often, Regulation S-P is invoked in discovery to ensure that consumer information is protected from improper disclosure. See, e.g., Murphy v. Schaible, Russo & Co., 2020 U.S. Dist. LEXIS 260740, at *6 (D. Colo. Feb. 3, 2020) (applying heightened protections to material sought in discovery and governed by Regulation S-P).

Section 5 of the Federal Trade Commission Act

Section 5 of the Federal Trade Commission Act (FTC Act) prohibits "unfair or deceptive acts or practices." 15 U.S.C. § 45(a). Section 5 permits the FTC to use both administrative proceedings and court actions to exercise its authority in regulating such acts and practices, including in data privacy matters. See FTC v. Wyndham Worldwide Corp., 799 F.3d 236, 240 (3d Cir. 2015). As recently as May 2022, the FTC expressly cautioned that "[r]egardless of whether a breach notification law applies, a breached entity that fails to disclose information to help parties mitigate reasonably foreseeable harm may violate Section 5 of the FTC Act." Significantly, despite the absence of a uniform federal data breach statute, the FTC is expected to continue enforcement efforts under Section 5 for unfair and deceptive practices in the cybersecurity context.

Section 5, however, does not provide a private right of action to consumers. See 15 U.S.C. § 57b. Whether Section 5 may serve as the basis for a private negligence or negligence per se claim in states that recognize such causes of action is dependent on each state's specific claim requirements. See, e.g., In re Marriott Int'l, Inc., 2020 U.S. Dist. LEXIS 200096, at *77–78 (D. Md. Oct. 26, 2020) (collecting cases finding that an "unfair practice" Section 5 can serve as the basis for a state common law negligence or negligence per se claim and that Maryland law permitted the same); but see In re Sonic Corp. Customer Data Sec. Breach Litig., 2020 U.S. Dist. LEXIS 114891, at *13–14 (N.D. Ohio July 1, 2020) (holding that Section 5 could not support a negligence per se cause of action under Oklahoma law because it does not impose "objective standards" as required to establish a duty based on an underlying statute).

For more on the FTC Act and enforcement, see FTC Data Security Guidance and Enforcement and Federal Trade Commission (FTC) Consumer Privacy Enforcement Tracker.

State Law Claims

A growing number of states, including California, Virginia, Colorado, Utah, and Connecticut, have enacted comprehensive consumer privacy laws. Although similar, they differ as to whether they provide a private right of action. Also, state common law claims are often premised on violations of statutory obligations.

Comprehensive State Privacy Statutes

In 2018, California became the first state in the United States to enact a comprehensive consumer privacy statute. The California Consumer Privacy Act (CCPA) went into effect January 1, 2020, and has since been amended through the enactment of the California Privacy Rights Act (CPRA). It provides a private right of action for unauthorized access, theft, or disclosure of un-redacted, unencrypted "personal information" as a result of a business's failure to implement and maintain reasonable security practices and procedures. See Cal. Civ. Code § 1798.150(a)(1). Beginning, January 1, 2023, it also provides a private right of action to consumers whose email addresses, with a password or security question and answer that would permit access to the account, are breached. In other words, the CCPA only provides for a private right of action under limited circumstances, such as security or data breaches. Damages available for a private right of action under Section 1798.150(a)(1) include:

- The greater of a statutory amount between $100 and $750 per consumer per incident and actual damages
- Injunctive or declaratory relief –and–
- Any other relief the court deems proper

Cal. Civ. Code § 1798.150(a). Generally, the CCPA covers all information so long as it relates to a California resident or California household. Aligning with the GDPR, the CCPA defines "personal information" to include "information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household." Cal. Civ. Code § 1798.140(o) (Cal. Civ. Code § 1798.140(v) after Jan. 1, 2023).

Not all "business[es]" are subject to the CCPA. The statute defines a "business" as a for-profit, private entity that:

- Collects personal information
- Determines the means of processing that personal information
- Does business in California –and–
- Meets one of the following criteria:
  - Has annual gross revenues exceeding $25 million
  - Annually sells/buys or receives/shares for commercial purposes the personal information of 50,000 (100,000 after Jan. 1, 2023) or more California consumers –or–
- Derives 50% or more of its annual revenue from selling (*or sharing* after Jan. 1, 2023) personal information

Cal. Civ. Code § 1798.140(c) (Cal. Civ. Code § 1798.140(d) after Jan. 1, 2023).

Despite its relatively narrow private right of action, the CCPA has driven a significant volume of consumer privacy litigation. In its first year, there were over 125 cases filed asserting CCPA claims. While most of the actions arise out of various data breaches, others have been animated by other data use implications mandated by the CCPA. For example, ovulation-tracking app Flo Health Inc. has been hit with a number of class action lawsuits alleging it secretly collected and shared users' personal information—including whether women were trying to get pregnant.

Several other states have followed suit and enacted similar comprehensive consumer privacy statutes. These states include Virginia (Virginia Consumer Data Protection Act, Va. Code Ann. § 59.1-575 et seq.), Colorado (Colorado Privacy Act, Colo. Rev. Stat. §§ 6-1-1301 through 6-1-1313), Utah (Utah Consumer Privacy Act, Utah Code Ann. § 13-61-101 et seq.), and Connecticut (CT SB 6). In contrast to the CCPA, however, these states' statutes do not provide for a private right of action—yet. States continue to propose similar comprehensive privacy laws similar to the CCPA, and therefore, you can expect that states will pass similar statutes providing for a private right of action.

Even in states where comprehensive privacy protection statutes have yet to be enacted, data claims are often brought under other consumer protection statutes. Nevada, for example, requires an operator (i.e., a person who owns or operates an internet website or online service for commercial purposes or collects and maintains certain information about Nevada residents) to establish a designated address through which a consumer may request that the operator not sell their covered information that the operator has collected. Nev. Rev. Stat. Ann. § 603A.345. The term "sale" is defined to include the exchange of covered information for monetary consideration by the operator to a third party to further license or sell the covered information. Nev. Rev. Stat. Ann. § 603A.333. The law also prohibits an operator who has received such a request from selling that consumer's covered information. Nev. Rev. Stat. Ann. § 603A.345(3). The attorney general may seek an injunction or a civil penalty for violations, but no private right of action exists at this time. Nev. Rev. Stat. Ann. § 603A.360.

For more on state privacy laws, see California Consumer Privacy Compliance (CCPA and CPRA), Colorado Privacy Act (CPA) Compliance, Virginia Consumer Data Protection Act (VCDPA) Compliance, Utah Consumer Privacy Act (UCPA) Compliance, and Consumer Data Privacy (CT).

Frequent Common Law Claims

In addition to statutory claims, privacy actions are often brought as common law claims, particularly where the relevant state has yet to adopt a CCPA analog and where existing privacy statutes do not provide a private right of action. Such actions include:

- Breach of contract / breach of implied contract
- Breach of fiduciary duty
- Invasion of privacy
- Intrusion upon seclusion
- Negligence
- Negligence per se
- Unjust enrichment

Common issues that arise when dealing with state common law claims include:

- Whether a federal statute may serve as the basis for state law causes of action for negligence and negligence per se
- Thorny choice-of-law issues created when class action plaintiffs assert state common law claims on behalf of nationwide classes, and whether failure to raise these issues at an early juncture waives reliance on non-forum law (see In re Brinker Data Incident Litig., 2020 U.S. Dist. LEXIS 247918, at *14–16 (M.D. Fla. Jan. 27, 2020))
- Whether the provision of sensitive personal information creates an implied contractual right to protect that information (see In re Brinker, 2020 U.S. Dist. LEXIS 247918, at *17–20 (M.D. Fla. Jan. 27, 2020); Lovell v. P.F. Chang's China Bistro, Inc., 2015 U.S. Dist. LEXIS 112101 (W.D. Wash. Mar. 27, 2015))
- Whether plaintiffs may rely on state law claims to avoid the jurisdiction of federal courts and plead around Article III standing to avoid removal

Standing

U.S. Const. Art. III imposes an "irreducible constitutional minimum of standing" on any claim asserted by a litigant in federal court. Lujan v. Defenders of Wildlife, 504 U.S. 555, 560 (1992). Standing contains three elements:

- The plaintiff must have suffered an "injury in fact"—an invasion of a legally protected interest which is:
  - Concrete and particularized –and–
  - Actual or imminent
- There must be a causal connection between the injury and the conduct complained of –and–
- It must be likely, as opposed to merely speculative, that the injury will be redressed by a favorable decision

Lujan, 504 U.S. at 560–61.

Plaintiffs must be able to satisfy the requirements of Article III standing to bring suit and maintain jurisdiction in federal court. Standing requires a "concrete" injury that is "real, and not abstract." TransUnion, 141 S. Ct. at 2204 (citing Spokeo, 578 U.S. at 340). Harms may be either tangible or intangible, but do not exist solely because "a statute grants a person a statutory right and purports to authorize that person to sue to vindicate that right." Spokeo, 578 U.S. at 341.

TransUnion addressed a class wide dispute under the FCRA in which a CRA reported inaccurate information on over 8,000 consumers' reports. However, only about a quarter of those plaintiffs had the inaccurate information disclosed to third parties. The Court ultimately held that the plaintiffs whose information was disclosed suffered a concrete injury as contemplated by the statute, but those who experienced no disclosure suffered no harm. Speculative future harm was not enough without a sufficient risk of future harm to support Article III standing. TransUnion, 141 S. Ct. at 2204, 2212.

TransUnion, however, did not create a clear line between "speculative" and "sufficient" future harm for the purposes of standing. Multiple courts have addressed the distinction in the data privacy context, with mixed outcomes:

- A plaintiff's fear of future harm and preemptive steps taken to ward off the anticipated consequences of a data breach were insufficient to confer standing. Tsao v. Captiva MVP Rest. Partners, LLC, 986 F.3d 1332 (11th Cir. 2021).
- Class action plaintiffs lacked standing where their data was compromised, but they failed to allege any certainly impending misuse of the data that would cause them harm. In re Practicefirst Data Breach Litig., No. 1:21-CV-00790(JLS/MJR), 2022 U.S. Dist. LEXIS 19272 (W.D.N.Y. Feb. 1, 2022).
- Class plaintiffs had standing because it could be assumed that the intent of hackers in accessing data was "not benign," and therefore a substantial risk of future harm existed. Pygin v. Bombas, No. 20-cv-04412-JSW, 2021 U.S. Dist. LEXIS 251118 (N.D. Cal. Nov. 29, 2021).

Other courts have addressed TransUnion and found it limited to standing involving statutory damages, or inapplicable at early stages of litigation. See Cotter v. Checkers Drive-In Rests., Inc., No. 8:19-cv-1386-VMC-CPT, 2021 U.S. Dist. LEXIS 160592 (M.D. Fla. Aug. 25, 2021); In re Blackbaud, Inc., Customer Data Breach Litig., No. 3:20-mm-2972-JMC, 2021 U.S. Dist. LEXIS 123355 (D.S.C. July 1, 2021).

As a reminder, Article III standing is only a requirement in federal court. Except in rare circumstances, state courts generally do not require that plaintiffs have Article III standing to maintain their claims. This can create complications on removal, where a plaintiff may assert state statutory or common law violations and seek damages but may avoid seeking the type of damages or alleging the kind of harm that would give rise to standing—even if federal court jurisdiction would otherwise be present.

Work Product and Attorney-Client Privilege

A growing number of federal courts have held that the attorney-client and work product privilege do not apply to internal investigatory reports and related communications. As these cases demonstrate, it is now routine for plaintiffs' counsel to seek data event incident reports. In re Rutter's Inc. Data Security Breach Litigation No. 1:20-CV-382, 2021 U.S. Dist. LEXIS 136220 (E.D. Pa. July 22, 2021); In re Capital One Consumer Data Security Breach Litigation, 2020 U.S. Dist. LEXIS 91736 (E.D. Va. May 26, 2020), aff'd, 2020 U.S. Dist. LEXIS 112177 (E.D. Va. June 25, 2020); Wengui v. Clark Hill PLC, 38 F.R.D. 7 (D.D.C. 2021).

Practical insight from recent instances of courts' refusal to apply privilege to forensic reports and related communications include the following:

- Compliance officers and counsel must be scrupulous to avoid blurring the lines between "ordinary course" factual reports and reports genuinely prepared for trial counsel for the purposes of assisting counsel in litigation.
- A litigation-consulting data breach vendor should not be the same vendor used for business purposes.
- Testimony given by a Fed. R. Civ. P. 30(b)(6) representative can be highly significant, if not dispositive, for a court when assessing assertions of privilege.

Class Certification and Considerations

Many data privacy lawsuits are brought as class actions. But for a class action to be proper, the class must be certifiable. To be certifiable, a class must satisfy all of the requirements of Fed. R. Civ. P. 23(a), and at least one requirement of Fed. R. Civ. P. 23(b). Rule 23(a) requires the following:

- **Numerosity.** The class is so numerous that joinder of all members is impracticable.
- **Commonality.** There are questions of law or fact common to the class.
- **Typicality.** The claims or defenses of the representative parties are typical of the claims or defenses of the class. –and–
- **Adequacy.** The representative parties will fairly and adequately protect the interests of the class.

Fed. R. Civ. P. 23(a).

Rule 23(b) also requires that at least one of the following is satisfied:

- Separate actions would result in consistent adjudications or nonparty interests would be substantially impaired.
- Final injunctive or declaratory relief is appropriate to the class as a whole. –or–
- Common questions of law or fact predominate over any questions affecting only individual members, and a class action is the superior method for adjudicating the controversy.

Fed. R. Civ. P. 23(b). Some jurisdictions impose an additional requirement that the class be "administratively feasible," that is, "a class definition must be sufficiently definite so that it is administratively feasible for the court to determine whether a particular individual is a member of the proposed class." In re Sonic Corp., No. 20-0305, 2021 U.S. App. LEXIS 25403, at *4 (6th Cir. Aug. 24, 2021).

Class certification is not proper if the class does not meet the above requirements. See, e.g., Dolmage v. Combined Ins. Co. of Am., No. 14 C 3809, 2017 U.S. Dist. LEXIS 67555 (N.D. Ill. May 3, 2017); S. Indep. Bank v. Fred's, Inc., No. 2:15-CV-799-WKW, 2019 U.S. Dist. LEXIS 40036 (M.D. Ala. Mar. 13, 2019). Class certification is also improper if the proposed class, as defined, is overbroad. See, e.g., In re TJX Cos. Retail Sec. Breach Litig., 246 F.R.D. 389, 392 n.2 (D. Mass. 2007).

Both plaintiff and defense practitioners should carefully consider the precise contours of the class definition to ensure that the class, as pleaded, is capable of being certified, and incorporate class certification issues as part of forming an overall case strategy.

Kristin Bryan, Partner, Squire Patton Boggs

Kristin Bryan is a litigator with deep expertise representing clients in complex bet-the-company data privacy, cybersecurity and data breach disputes in federal and state courts nationwide. She has obtained dismissals of numerous significant data privacy and cybersecurity litigations, in which plaintiffs collectively sought over US$280 billion in liquidated statutory damages for claims that her client's business practices violated federal and state privacy laws.

Kristin is a pragmatic litigator and integral member of the firm's privacy litigation team, which was ranked #2 in 2022 among all law firms by *Global Data Review*. She has broad experience defending data privacy, cybersecurity and data breach disputes across the country, including in the class action and multidistrict litigation context. Kristin has litigated cases brought under the Electronic Communications Privacy Act (ECPA), the Video Privacy Protection Act (VPPA), the Driver's Privacy Protection Act (DPPA), the Fair Credit Reporting Act (FCRA), the Computer Fraud and Abuse Act (CFAA), the California Consumer Privacy Act (CCPA) and the Illinois Biometric Privacy Act (BIPA), among others. Kristin has also efficiently resolved privacy and cybersecurity class actions concerning deceptive trade practice and breach of fiduciary duty claims.

Kristin has advised clients concerning privacy issues implicated by the use of facial recognition technology and AI. She is currently defending a case concerning an AI consumer-facing platform in federal court in Illinois and recently opposed class certification. Kristin has represented clients in data breach litigations regarding the alleged disclosure of personal information and protected health information regulated under the Health Insurance Portability and Accountability Act (HIPAA). As part of her litigation practice, Kristin also advises clients on their most sensitive business, cybersecurity/privacy diligence and data breach issues, and in state and federal regulatory investigations regarding their privacy practices. She is editor-in-chief of the firm's award-winning data privacy blog *Consumer Privacy World* and has published over 350 articles on developments regarding data privacy and cybersecurity.

Kristin is is a Certified Information Privacy Professional (CIPP/US) and a leader in the data privacy and cybersecurity community. She holds a number of executive positions with the International Association of Privacy Professionals (IAPP), including with the Privacy Bar Advisory Board, is co-chair of her local KnowledgeNet Chapter, and was selected to participate in the IAPP's 2022 Leadership Retreat. Kristin is also vice-chair of the American Bar Association's Cybersecurity and Data Privacy Committee and on the ABA's 11-member Technology and New Media Standing Committee.

Prior to joining the firm, Kristin practiced for five years at an international law firm in New York, specializing in data strategy and security.

Jesse Taylor, Senior Associate, Squire Patton Boggs

Jesse Taylor represents clients in a wide range of commercial litigation in state and federal courts. His experience includes Fair Credit Reporting Act (FCRA) and data privacy matters, insurance and real estate disputes, and complex class action and multidistrict litigation (MDL) disputes. Jesse is a focused, detail-oriented litigator who relishes the opportunity to counsel, advise and litigate complex disputes, and do so efficiently and effectively.

Prior to joining the firm, he worked as a litigation associate in another top 20 international law firm. Jesse also served as a law clerk to the Honorable Judith E. Levy, US District Court, Eastern District of Michigan, and to the Honorable James G. Carr, US District Court, Northern District of Ohio. In addition to his law firm experience and clerkships, Jesse worked as the online communications director for the Office of the Governor of Ohio. Jesse is also a member of the board of the Harmony Project, a Columbus-based nonprofit.

Jesse was named a 2022 Next Up Columbus honoree – an award that highlights bold, creative and socially conscious emerging leaders in central Ohio.

Shing Tse, Associate, Squire Patton Boggs

Shing Tse is an associate in our Litigation Practice, based in the Houston office. Shing has experience representing clients in a variety of complex litigation matters in state and federal courts.

Prior to joining the firm, Shing worked at a litigation boutique in Houston, where he represented both plaintiffs and defendants in a variety of different industries.