HINSHAW

Beyond Malpractice: The Rising Threat of Privacy and Statutory Claims Against Lawyers

Lawyers' Lawyer Newsletter | 10 min read

Jun 29, 2026

By: Matthew R. Henderson

The duty of confidentiality is one of the cornerstones of the legal profession, and lawyers have always faced civil liability and disciplinary exposure for violating that duty. But modern attorneys possess a dizzying array of sensitive materials**,** including personally identifiable information (PII) such as Social Security numbers (SSNs) and financial account numbers, protected health information (PHI) such as medical records and psychiatric evaluations, corporate confidences such as trade secrets and intellectual property, and a myriad of other electronically stored information (ESI).

As custodians of such sensitive information obtained from clients and other sources, lawyers and law firms face a wide variety of potential privacy-related claims that extend well beyond traditional legal malpractice actions. These claims arise from multiple sources, including federal and state privacy statutes that impose strict liability and statutory damages, common law torts that have been adapted to modern contexts, including social media, and traditional ethical obligations that carry increasing exposure to civil liability and lawyer discipline when breached.

The scope of potential exposure is substantial. Privacy violations can lead to significant compensatory damages stemming from the mishandling of sensitive client, employee, or third-party data. Key sources of liability include negligent law firm security practices and data breaches, violations of specific privacy statutes that can be asserted as class actions and can include statutory damages and attorney's fees, breach of confidentiality and fiduciary duty actions, and common law torts such as intrusion upon seclusion and public disclosure of private facts.

Statutory Claims

Attorneys may face privacy-related claims under federal and state confidentiality statutes that regulate specific categories of sensitive information, including mental health information, driver's license records, and confidential communications.

There is a wide range of federal and state privacy laws that can impose civil liability on lawyers if violated. For instance, personal injury attorneys and defense counsel are often in possession of a plaintiff's medical records, which could give rise to a claim under the Health Insurance Portability and Accountability Act (HIPAA). Attorneys are considered "business associates" under HIPAA when they receive, maintain, or transmit PHI. Lawyers may be sued under the Fair Credit Reporting Act (FCRA) for obtaining a copy of a debtor's credit report without a permissible purpose or for the misuse of background checks or credit information. They may also face claims under the Fair Debt Collection Practices Act (FDCPA) for disclosing a debtor's information to third parties. Attorneys likewise have liability exposure under the Telephone Consumer Protection Act (TCPA), which imposes restrictions on telemarketing practices, including calls, texts, and the use of auto-dialer systems. Lawyers may be liable for their own solicitation calls, which violate the statute or those of third-party vendors and lead generators.

Attorneys are frequently targeted under the federal Electronic Communications Privacy Act (ECPA) and its sub-statutes, including the Stored Communications Act (SCA), which focuses on privacy for communications and records held by third-party service providers (*e.g.,* emails, cloud storage, and social media messages). The federal Wiretap Act also prohibits lawyers from recording phone calls or intercepting electronic communications without the consent of all required parties (in "two-party" consent states) or for using information they know was illegally intercepted by a client.

Many states have enacted privacy laws that may likewise impose liability on attorneys if violated. California has taken the lead in this area. For instance, the California Consumer Privacy Act (CCPA) includes a private right of action, and a lawyer or law firm may be liable for a data breach resulting from a failure to implement "reasonable security procedures" regarding unencrypted personal information, such as client SSNs or driver's license numbers. The California Invasion of Privacy Act (CIPA) also targets unauthorized wiretapping and eavesdropping, which can include the use of artificial intelligence (AI) summaries and chatbots.

The Illinois Biometric Information Privacy Act (BIPA) is one of the strictest biometric privacy laws in the country. It restricts private companies from collecting, storing, or using biological identifiers such as fingerprints or facial scans. Law firms may become liable for violations in a number of ways, including using AI tools to record, transcribe, or summarize audio or video calls or meetings with clients and others where confidential or sensitive information is discussed. For instance, a personal injury law firm with an in-house or outsourced call center that uses AI applications that employ voiceprint technology to track interactions with potential clients may trigger a violation.

Many states also have data breach notification statutes, such as the New York SHIELD Act and the Florida Information Protection Act, and attorneys may be liable for failing to notify affected parties in the most expedient time possible after a data breach. Thus, it is imperative that attorneys be familiar with the privacy laws in the jurisdictions where they practice.

In *Doe v. Burke Wise Morrissey & Kaveny, LLC*., the plaintiff prevailed in a medical malpractice action arising from his suicide attempt in a hospital emergency room and was awarded a $4.2 million judgment.[1] But Doe subsequently sued his lawyer for allegedly violating the Illinois Mental Health and Developmental Disabilities

Confidentiality Act[2], for statements that the attorney made to the press after the trial about the case.[3] The Illinois Supreme Court ruled that Doe waived his claims of confidentiality under the Act by voluntarily and publicly disclosing his private health information in a public trial and that the defendants were not liable under the Act because the attorneys did not provide mental health services to the plaintiff.[4]

The US Supreme Court likewise weighed in on an attorney's privacy statute violation in *Maracich v. Spears*.[5] The Driver's Privacy Protection Act (DPPA),[6] is a federal law that prohibits state Departments of Motor Vehicles (DMVs) and their contractors from disclosing personal information in motor vehicle records without the individual's consent to prevent the misuse of personal data. In *Maracich*, attorneys obtained names and addresses of thousands of individuals from the South Carolina Department of Motor Vehicles in order to solicit clients for a lawsuit against a car dealership. The Supreme Court ruled this was not a permissible purpose covered by the litigation exception in the statute.[7] However, the decision preserved attorneys' ability to obtain protected information for legitimate investigatory purposes, such as research to support a complaint, locating witnesses for deposition or trial testimony, or contacting persons already involved in litigation.[8]

Common Law Claims

The attorney-client relationship is a fiduciary relationship of the highest character, and the lawyer is ethically obligated to safeguard the client's confidential information. The protections in ABA Model Rule 1.6 on confidentiality are significantly broader than the common law attorney-client privilege and extend "not only to matters communicated in confidence by the client but also to all information relating to the representation, whatever its source."[9] This includes a client's identity, billing information, the nature of the representation, and even information that may be available from public sources.[10] *In People v. Issac*, attorney Isaac was disciplined for disclosing confidential client information in responding to two negative online reviews.

Thus, a lawyer may be liable for legal malpractice or breach of fiduciary duty for violating the ethical duty of confidentiality.[11] In *Elkind v. Bennett*, the Florida Court of Appeals considered a legal malpractice claim where the client claimed that his former attorney had disclosed confidential information that caused the plaintiff to lose his job and concluded that an attorney's breach of a duty of confidentiality to his or her client, which causes damage to the client, may be enforced in an action for legal malpractice.[12]

Attorneys may likewise face liability for legal malpractice or breach of fiduciary duty for failing to exercise reasonable efforts to prevent the inadvertent or unauthorized disclosure of information relating to the representation of a client, including data breaches. For instance, in *Wengui v. Clark Hill, PLC*, the district court ruled that the plaintiff, a Chinese dissident, stated a claim that his law firm failed to maintain reasonable security measures to protect its computer systems from unauthorized access, where there was a cyber-attack and the plaintiff's asylum application and other confidential information were published on social media.[13]

A similar result was reached in *Hiscox Ins. Co. v. Grier*, where an insurer claimed that a law firm had failed to disclose a ransom payment made to hackers for over 16 months and forced the plaintiff to spend $1.5 million on investigations after it found its confidential information on the dark web.[14] A federal judge in Missouri allowed

the claim to move forward, though the law firm ultimately prevailed at a trial in 2022. It is recommended that when faced with a cyber incident, lawyers consult ABA Formal Opinion 483, which provides guidance on when an obligation exists for an attorney to communicate with current clients about a data breach.

Attorneys may likewise face civil liability from clients and third parties for traditional common law privacy torts, including intrusion upon seclusion, public disclosure of private facts, and false light.

Disciplinary Exposure

The consequences of confidentiality breaches can be severe and may extend to a lawyer's professional discipline.

In Dayton Bar Ass'n v. Daly, the Ohio Supreme Court imposed a conditionally stayed 18-month suspension against an attorney for disclosing confidential information to the police about a former client that he had learned during representation.[15] Daly's disclosure was particularly egregious because it was motivated by revenge–an effort to recover property he believed the client had stolen–and posed significant threats to the former client's liberty and custody of her child.

In the case of *In the Matter of Breault*, attorney Breault disclosed protected client information in court filings, including attaching a transcript of an audio recording of a meeting with his client's treating physician to a public filing.[16] The Special Master found that Breault violated Rule 1.6(a) by disclosing confidential information gained in his professional relationship in two public court filings and recommended that Breault be suspended for one month in addition to the federal court revoking his *pro hac vice* admission for six months.[17] The Georgia Supreme Court remanded for a more thorough analysis of the ethical rules that Breault violated, his mental state, and the potential and actual injury to the client from his misconduct.[18]

Defenses

The absolute litigation privilege is the most robust defense available to attorneys facing privacy claims arising from litigation conduct. This privilege provides complete immunity for statements and conduct made in connection with judicial proceedings, regardless of the speaker's motive or the unreasonableness of the conduct. In *Johnson v. Johnson & Bell*, the plaintiff alleged invasion of privacy, negligence, and negligent infliction of emotional distress against attorneys who had failed to redact her personal information from documents filed in a federal court case.[19] The appellate court affirmed the dismissal of all claims based on the absolute litigation privilege.[20] Critically, the appellate court held that the privilege extends beyond defamation claims to other tort theories, including those alleged by the plaintiff.[21]

Waiver of confidentiality is another cogent defense. In *Doe*, the Illinois Supreme Court ruled that an attorney could not be liable for discussing confidential mental health information that the client had voluntarily disclosed during public trial testimony.[22] The *Doe* court applied waiver principles, noting that "a public disclosure by [the plaintiff] of information protected by the Act took away its confidentiality."[23] (internal citations omitted). Once confidentiality is waived through public disclosure, it cannot be reasserted.[24]

Attorneys facing disciplinary proceedings for disclosure of client information often invoke a limited exception to Rule 1.6 that permits a lawyer to reveal information relating to the representation of a client to respond to allegations of wrongdoing concerning the lawyer's representation of the client. However, courts have consistently ruled that disclosure is permitted only "to the extent the lawyer reasonably believes necessary" to establish a defense or respond to allegations. An attorney may also disclose client information to prevent reasonably certain death or substantial bodily harm or to prevent a client from committing a crime or fraud where the client has used or is using the lawyer's services.

Risk Management Best Practices

Law firms and attorneys can substantially reduce their exposure to privacy claims through proactive risk management practices. Law firms should consider strictly limiting who at the firm has access to certain classes and types of information and encrypting sensitive information both in the office and when attorneys work remotely. This would necessarily include securing access to the law firm's server, email systems, and other databases, as well as establishing remote work protocols and strictly complying with HIPAA and other federal and state privacy laws.

Attorneys should carefully evaluate the source and permissible use of information obtained from government databases, ensuring that any use falls within clearly applicable statutory exceptions. Lawyers should establish and enforce protocols for redacting sensitive personal information from court filings and other documents. Law firms should likewise maintain appropriate oversight of third-party vendors who handle sensitive data, as firms may be held responsible for breaches occurring at those vendors.

Law firms of any size should seriously consider purchasing cyber liability insurance, which is separate from and in addition to a lawyer's professional liability insurance policy. Such insurance covers the costs of data breach response, forensic investigations, and client notifications, as well as regulatory fines or penalties. Some cyber policies offer a ransomware endorsement that covers negotiations, business interruption losses, and data restoration. Law firms should also develop an incident response plan to ensure timely notification of a breach.

Finally, law firms should take active steps to ensure the confidentiality of client information. Before disclosing any information relating to the representation of a client–even information that may be publicly available–attorneys should consider whether the disclosure is authorized and only disclose such information to the extent reasonably necessary. Through careful attention to these areas, practitioners can navigate the evolving landscape of privacy liability while continuing to provide effective representation to their clients.

---

[1] *Doe v. Burke Wise Morrisey & Kacveny, LLC,* 2023 IL 129097, ¶ 5.

[2] 740 ILCS 110/1 et seq. ("Act").

[3] *Doe*, 2023 IL 129097 at ¶ 7.

[4] *Id.* ¶ 23.

[5] *Maracich v. Spears*, 570 U.S. 48 (2013).

[6] Driver Privacy Protection Act, 18 U.S.C. §§ 2721–2725.

[7] *Maracich*, 570 U.S. at 52.

[8] *Id*. at 63-64.

[9] ABA Model Rule 1.6, Comment [3]

[10] See *People v. Issac*, 470 P. 3d 837, 840 (Colo. 2016).

[11] See *Elkind v. Bennett*, 958 So. 2d 1088, 1091 (Fla. 4th DCA 2007).

[12] *Id*. at 1092.

[13] *Wengui v. Clark Hill*, PLC, 440 F. Supp. 3d 30, 37-38 (D.D.C. 2020).

[14] *Hiscox Ins. Co. v. Grier*, 474 F. Supp. 3d 1004, 1006 (W.D. Mo).

[15] *Dayton Bar Ass'n v. Daly*, 179 Ohio St. 3d 331 (2025).

[16] *In the Matter of Breault*, 318 Ga. 127 (2024).

[17] *Id*. at 135.

[18] *Id*. at 141.

[19] *Johnson v. Johnson & Bell*, 2014 IL App (1st) 122677, ¶ 9.

[20] *Id*. ¶ 16-17.

[21] *Id*. ¶ 16.

[22] *Doe,* 2023 IL 129097, ¶ 42.

[23] *Id.* ¶ 29.

[24] *Id.*

Hinshaw & Culbertson LLP is a U.S.-based law firm with offices nationwide. The firm's national reputation spans the insurance industry, the financial services sector, professional services, and other highly regulated industries. Hinshaw provides holistic legal solutions—from litigation and dispute resolution,

and business advisory and transactional services, to regulatory compliance—for clients of all sizes. Visit www.hinshawlaw.com for more information and follow @Hinshaw on LinkedIn and X.

Related People

Matthew R. Henderson

Partner

312-704-3650

Related Capabilities

Consultants and Coaches for the Profession®

Counselors for the Profession

Cyber Security for Law Firms

Data Privacy, AI & Cybersecurity

Fair Credit Reporting Act (FCRA)

Fair Debt Collection Practices Act (FDCPA)

Lawyers for the Profession®

Professional Services

Telephone Consumer Protection Act (TCPA)