The Privacy Paradox – From "Let Alone" to "Share My Location"

By Turquoise S. Early and Amie Schoeppel Wilcox

About the Authors

Turquoise Early is an attorney with Kutak Rock LLP, where she specializes in technology transactions, privacy and data security.

Amie Schoeppel Wilcox is an attorney with Friday, Eldredge & Clark, LLP, where her practice focuses on healthcare regulatory and compliance matters.

In one hour of my Wednesday: I click through five online privacy policies while working. I check my sleep data from last night and get an update that my average heart rate is up this week. I order my favorite lunch, which is pre-saved on my app, and am pleasantly surprised that the nearest location of the restaurant was auto-populated to the area of town I am driving in. I check my spouse's location to see if they have already left the grocery store, because the Walmart app reminded me of an item I usually buy but forgot to put on the list this time. I decline a client's "follow" request on social media, because my privacy is very important to me.

These commonplace actions reflect a growing tension between convenience and control, raising a broader question: has the right to privacy been traded for convenience? More fundamentally, does a meaningful right to privacy exist?

The right to privacy was not directly addressed in the Declaration of Independence 250 years ago, but conceptually, the roots of it were there—the founders reflected that all men[1] are endowed by their Creator with certain unalienable Rights, and that among these are life, liberty, and the pursuit of happiness. The concept was more directly addressed when the Fourth Amendment was added to the Constitution in 1791, preserving "the right of the people to be secure in their persons, houses, papers and effects." However, this only prevented government officials from unlawfully intruding into homes or property, and did not do anything to prohibit invasions of privacy by private citizens or corporations.

The only legal tool available at the time for prohibiting the invasion of privacy by private citizens was trespass, which only prohibited physical intrusions on real property. For other types of invasions, the newly established courts struggled to make the limited framework in existence fit the rapidly evolving development of the new country, its citizens, and their industrial developments.

The Right to Privacy Emerges

The body of work that has received the most credit for first outlining and articulating the "right to privacy" was an 1890 Harvard Law Review Article authored by Samuel D. Warren and Louis D. Brandeis.[2] The article has been credited as both "perhaps the most influential law journal piece ever published" and "the best example of the influence of law journals on the development of law."[3] Brandeis and Warren describe the evolution from "very early times" where the law gave remedy only for trespass to the "right to life," which they describe as protecting the subject from battery or fear of injury, laying the grounds for the doctrine of assault and describing this evolution necessary to recognize "man's spiritual nature, of his feelings and his intellect." Later the law of nuisance developed from the need for protection against offensive noises and odors, dust and smoke, and excessive vibration, while the recognition of the value of human emotions came from the need for protection for a man's reputation through slander and libel doctrines.

Brandeis and Warren also described the growth of the legal conception of property from tangible to intangible property through the growth of intellectual property doctrines "in the products and processes of the mind as works of literature and art, goodwill, trade secrets and trademarks." They present the next step to be taken for protection of the person—"generally the scope of these legal rights broadened; and now the right to life has come to mean the right to enjoy life—the right to be let alone."[4]

The article was spurred from rapid developments in society following the rise of newspapers and the release of the Kodak Brownie becoming the first mass market camera in 1884.

> Instantaneous photographs and newspaper enterprise has invaded the sacred precincts of private and domestic life; and numerous mechanical devices threaten to make good the prediction that 'what is whispered in the closet shall be proclaimed from the house-tops.' For years there has been a feeling that the law must afford some remedy for the unauthorized circulation of portraits of private persons; and the evil of the invasion of privacy by the newspapers, long keenly felt, has been but recently discussed by an able writer . . . the press is overstepping in every direction the obvious bounds of propriety and decency.[5]

At the time, courts were struggling to establish a remedy for actions such as the publication of private letters or publication of photos without permission—often framing these actions as a breach of implied contractual terms or breach of private confidence. Brandeis and Warren argued these remedies were inadequate: "we must therefore conclude that the rights, so protected, whatever their exact nature, are not rights arising from contract or from special trust, but are rights as against the world."[6]

While not immediately adopted after publication, the privacy torts proposed by Brandeis and Warren became the modern trend in courts considering actions arising from the evolution of the media and technology. Over time, the proposals became so significant that the American Law Institute codified the right of privacy in the Restatement of Torts, later evolving into four separate torts: intrusion upon seclusion, public disclosure of private facts, false light of publicity, and appropriation.[7] Courts also began to recognize actions for breaches of confidentiality in special relationships, such as physicians and their patients.

Right to Privacy Expansion by Federal Actors

Just as the expansion of newspaper media and availability of cameras to consumers brought rapid changes and new concerns, so too did the introduction of telephones, computers, and the internet. The expanding role of the federal government required new tools. When the Social Security System was established in 1935, social security numbers were explicitly "NOT FOR IDENTIFICATION"—today, this information is one of the most economically valuable pieces of data in cases of data breaches and identity theft.[8]

The growth of telephone communication led to federal legislation against wiretapping telegraph messages and phone calls. But in 1928, The Supreme Court determined that the Fourth Amendment did not apply to wiretapping, because it did not involve physical trespass.[9] The dissent was written by none other than Louis Brandeis, then a Supreme Court Justice, who stressed the opinions outlined in his famous article nearly 40 years earlier:

> Subtler and more far-reaching means of invading privacy have become available to the

> government. Discovery and invention have made it possible for the government, by means far more effective than stretching upon the rack, to obtain disclosure in court of what is whispered in the closet.[10]

One year after *Olmstead*, J. Edgar Hoover prohibited wiretapping at the FBI, and the Federal Communications Act of 1934 prohibited the admission of communications gained by wiretapping in court. Ironically, reports after Hoover's death revealed that he was one of the largest abusers of wiretapping in history. The country saw a profound expansion of both wiretapping and more modern domestic electronic surveillance in response to domestic security threats during and after World War II, seizing upon fears of Communism in the McCarthy era.[11]

While the right to privacy was not explicitly included in the Declaration of Independence, and its textual inclusion in the Fourth Amendment was limited and only applied to government actors, the Supreme Court rooted the right to privacy as emanating from the "penumbras" of the Bill of Rights in *Griswold v. Connecticut* in 1965.[12]

The *Olmstead* decision would stand until 1967, when the Supreme Court fashioned the "reasonable expectation of privacy" test in *Katz v. United States*.[13] The *Katz* decision effectively adopted the reasoning of Justice Brandeis's *Olmstead* dissent. The Court determined that the right to privacy did exist where a person exhibits an actual or subjective expectation of privacy that society is prepared to recognize as reasonable. The right to privacy has since been expanded—and limited—by the Court many times.[14]

Modern Expansion of the Right to Privacy

While the right to privacy has been strengthened through the judicial system and through industry-specific Congressional action, the United States still has not enacted an overarching federal privacy framework.[15] The current privacy landscape has evolved to be a combination of sector-specific frameworks and various federal or state privacy laws. Some of the laws included in this framework focus on providing protections to data related to health, children and finances. For example, the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") is the first federal statute to directly address health privacy, while the Children's Online Privacy Protection Act of 1998 ("COPPA") focuses on the online privacy of children under the age of 13. Further, the Gramm-Leach-Bliley Act ("GLBA") introduced banking regulations that require financial institutions to explain their information-sharing practices and safeguard data.

The privacy landscape of the United States still does not fully provide strong protections for the right of privacy unlike the European Union's General Data Protection Regulation ("GDPR") that was enacted in 2018. The passing of GDPR forced the United States to examine the privacy rights it was providing its own citizens, which two years later in 2020 resulted in the passing of the California Consumer Privacy Act ("CCPA") followed by 19 additional state privacy laws granting consumers certain rights to their data. While many state laws are modeled loosely on the GDPR, they lack uniformity in scope and application.

We are far past Brandeis and Warren's outraged concerns based on the invasions of newspapers and photos of private citizens. Today, technology has engulfed our everyday so much that we overlook how integrated technology is in our lives only to realize its true significance when it stops working. Consumers have become accustomed to clicking "Accept" on terms and conditions, often selecting default options to bypass privacy notices—both from the fatigue of familiarity and the lack of meaningful opportunities to opt out. While 79% of Americans express concern about how companies use the data they collect about them, only 37% indicated at least some understanding about the laws and regulations currently in place to protect data privacy.[16]

Privacy Policies

When consumers use smartphones, smartwatches, wearables and voice assistants, they are often distracted by the convenience these products provide rather than the privacy tradeoffs involved. Only 22% of consumers say they often read a privacy policy before agreeing to it.[17] Ideally, privacy policies are supposed to work as a tool for companies to be transparent with consumers by outlining their data collection and data use practices.

The Federal Trade Commission ("FTC") encourages transparent privacy policies through enforcement actions under the FTC Act. The FTC's ultimate goals are to provide consumers with privacy protections, safeguard their personal information and stop abusive and unlawful data practices.[18] While the FTC provides this protection, this does not automatically prevent consumer's privacy protections from being violated. Over the past couple years, through public relations blunders, consumers are starting to become increasingly aware of the privacy sacrifices valuable technology may present.

Privacy in Health Data

Data security in the health industry is one of the country's most regulated areas. However, the right to privacy in health information is not as expansive as commonly thought. A common misconception is that any disclosure of health information constitutes a HIPAA violation. In reality, HIPAA only applies to certain types of actors (most often health care providers or insurers) and does not protect individuals from disclosure or discussion of their health information from other sources.[19]

This has contributed to widespread confusion regarding the privacy of health data, particularly with the rise of wearable technology. Most of the time, these wearables are created by companies that are not subject to HIPAA, and therefore the data the wearable collects is not subject to HIPAA either. In compliance with state privacy laws (or potentially GDPR) the wearable technology company provides both the privacy policy and terms and conditions to the consumer when the consumer creates their profile or account; however, these terms likely provide significantly less protection than the consumer believes, and may allow the company to sell the consumer's information to third-party companies.

The privacy policy, while still governed by the FTC to prevent unfair and deceptive practices, is not required to handle and protect the collected health data to the same level of confidentiality as a doctor's office. For example, Flo Health, a popular fertility-tracking app, collected sensitive health information but was not regulated by HIPAA. Flo Health promised to keep health information private, but the FTC discovered that Flo Health was disclosing user's sensitive health information including information about users' pregnancies to third-party analytic providers.[20] Flo Health is an example where even if the consumer were to read the companies' privacy policies, their privacy rights could still be violated—and the right to privacy the consumer believes is inherent may not actually exist. While the FTC provides some enforcement in protecting consumer's privacy rights, there still is room for error.

Privacy in Communication

Courts have increasingly addressed claims involving voice-activated devices capable of recording and storing user communications.[21] The consumer may use these devices to help with everyday tasks of playing a song or making a call, but these claims hinge on the fact that the device must listen to be able to know when to perform the task. These recordings could contain private data that the consumer does not want to have used for marketing purposes or to be used against them as evidence in a court of law. A common trend has been for authorities to try to obtain access to the recordings stored on these devices in their search for evidence of a crime.[22]

Consumers obtain these devices for convenience, without thinking that the device could be listening into the conversations held within the privacy of their home. While many times these companies do not hand the recordings over without a legally valid court order or they do not record without consumer's consent, it still highlights a gap in privacy protection that many consumers do not realize they are forfeiting when using these artificial intelligence assistants.[23]

Privacy in Location

Another example of the intersection of the right to privacy and technology can be found in *Chatrie v. U.S.* that will be heard this year by the Supreme Court.[24] This case examines the expectation that the Fourth Amendment protects from "unreasonable searches and seizures" by the government as it relates to geofence warrants.[25]

Geofence warrants can require companies to turn over location data for mobile devices they have tracked. Law enforcement then uses this information to reverse search the owner of a smartphone found in the area of interest.[26] The defendant in this case is seeking to suppress the evidence from the geofence warrant placing him in the vicinity of a robbery. The decision hinges on whether individuals have a reasonable expectation of privacy in the location history they have actively opted in to sharing with companies.

Privacy in Security

In a 2026 Super Bowl commercial, Ring promoted its new "Search Party of Dogs" feature that allows AI to help locate lost pets through the scanning of nearby user-enabled outdoor Ring cameras.[27] Many were surprised to learn the true capabilities home surveillance technology can have even if the owner is not actively using the services. At the surface, many viewers thought the capability would be helpful in the search of their own furry loved one. However, many understood the impact of mass surveillance that Ring was introducing with its partnership with Flock Safety.

The commercial made many aware of the future capabilities that were possible with home cameras. This surveillance could be introduced to everyone's neighborhood to look for more than just a lost German Shepherd. In reaction to the backlash, Ring announced that it was ending its partnership with Flock Safety and that the integration never launched, so no Ring customer videos were ever sent to Flock Safety.[28]

Conclusion

The right to privacy has transformed given the evolution of technology in today's society. Many consumers remain unaware of the extent to which modern technology implicates their privacy rights, or knowingly accept those tradeoffs in exchange for convenience. Despite legal precedent, the consumer right to privacy is still not strongly or uniformly protected and is often misunderstood by the individuals it is intended to protect. The right to privacy and society's opinion on privacy will continue to evolve, and we'll all need to answer for ourselves: what is the cost of privacy? The result is a paradox: privacy persists as a matter of legal doctrine, but its practical limits are increasingly defined by how readily it is surrendered. The question is no longer whether a right to privacy exists, but whether it retains meaningful protection in a world where participation often requires its compromise.

Endnotes:

1. Just as the right to privacy has evolved, fortunately, these self-evident truths have also been extended to women in the past 250 years.
2. Brandeis & Warren, *The Right to Privacy*, 4 Harvard L. Rev. No. 5 (Dec. 15, 1890).
3. *See* P. Dionisopoulos & C. Ducat, The Right to Privacy 20 (1976); I. Kramer, *The birth of privacy law: A century since*

Warren and Brandeis, 39 Cath. U. L. Rev. 703 (1990); H. Nelson & D. Teether, Law of Mass Communications 162 (3d ed. 1978).
4. Brandeis & Warren citing Cooley On Torts, 2d ed., p. 29.
5. Brandeis & Warren, supra note 2, at 195.
6. Brandeis & Warren, supra note 2, at 213.
7. Restatement of Torts § 867 (1939); Restatement (Second) of Torts (1977).
8. *See* Daniel J. Solove, "A Brief History of Information Privacy Law" in Proskauer On Privacy, PLI (2006).
9. *Olmstead v. United States*, 277 U.S. 438 (1928).
10. *Id.* at 473.
11. *See, e.g., Wilkinson v. United States*, 365 U.S. 399 (1961).
12. *Griswold v. Connecticut*, 381 U.S. 479 (1965).
13. *Katz v. United States*, 389 U.S. 347 (1967).
14. *See, e.g., Florida v. Riley*, 488 U.S. 445 (1989); *California v. Greenwood*, 486 U.S. 35 (1988); *New Jersey v. T.L.O.*, 469 U.S. 325 (1984); *O'Connor v. Ortega*, 480 U.S. 709 (1987).
15. GAO-19-621T, *Consumer Privacy: Changes to Legal Framework Needed to Address Gaps*, U.S. Gov't Accountability Off. (2019) (statement of Alicia Puente Cackley, Director, Financial Markets and Community Investment).
16. *Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information*, Pew Research Center (Nov. 15, 2019), https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/ (last accessed March 3, 2026).
17. *Id.*
18. 2023 *Privacy and Data Security Update* 3–4, Federal Trade Commission (2024), https://www.ftc.gov/reports/privacy-data-security-update-2023.
19. 45 C.F.R. §§ 160.102, 164.500 (2025); *Summary of the HIPAA Privacy Rule*, U.S. Dep't of Health & Hum. Servs., https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html (last visited Mar. 12, 2026).
20. Press Release, *FTC Finalizes Order with Flo Health, a Fertility-Tracking App that Shared Sensitive Health Data with Facebook, Google, and Others*, Fed. Trade Comm'n (June 22, 2021), https://www.ftc.gov/news-events/news/press-releases/2021/06/ftc-finalizes-order-flo-health-fertility-tracking-app-shared-sensitive-health-data-facebook-google.
21. *Lopez v. Apple, Inc.*, 519 F. Supp. 3d 672 (N.D. Cal. 2021).
22. *State v. Bates*, No. CR-2016-370-2 (Ark. Cir. Ct. Benton Cnty. Nov. 29, 2017) (dismissal order) (involving Amazon Echo recordings sought as evidence); *State v. Crespo*, No. 19-CF-009373 (Fla. 17th Cir. Ct. Broward Cnty. filed July 2019) (involving Amazon Alexa recordings sought as evidence).
23. *Data Privacy FAQs*, Amazon Web Servs., https://aws.amazon.com/compliance/data-privacy-faq/ (last visited Mar. 14, 2026); Press Release, *Our Longstanding Privacy Commitment with Siri,* APPLE INC. (Jan. 8, 2025), https://www.apple.com/newsroom/2025/01/our-longstanding-privacy-commitment-with-siri/.
24. *Chatrie v. United States*, No. 25-112 (U.S. argued Apr. 27, 2026).
25. *Id.*
26. LSB11274, *Geofence Warrants and the Fourth Amendment*, Cong. Rsch. Serv. (2025), https://crsreports.congress.gov/product/pdf/LSB/LSB11274.
27. Amazon Staff, *Ring's Search Party Helps Reunite More Than One Lost Dog a Day—Now Available to Everyone*, Amazon News, https://www.aboutamazon.com/news/devices/ring-search-party-for-dogs-united-states-missing-pets (last visited Mar. 14, 2026).
28. *Flock and Ring Cancel Announced Community Requests Integration*, Flock Safety Blog (Feb. 12, 2026), https://www.flocksafety.com/blog/an-update-on-ring-partnership. ■