LEAD ARTICLE

MORE THAN FRIENDS: A NEW THEORY FOR THE THIRD-PARTY DOCTRINE

EANG L. NGOV*

When a person gives information or something tangible to someone or a business, the Fourth Amendment's third-party doctrine allows the government to obtain that evidence without a warrant or probable cause. The third-party doctrine is premised on the rationale that we hold no reasonable expectation of privacy when we voluntarily expose information to others, that we assume the risk that the third party would share the information, and that we must deal with the consequences of that misplaced trust. The doctrine originated from a series of cases where law enforcement obtained information revealed by criminals through their mistaken trust of other criminals, snitches, or undercover agents posing as criminals, as seen in On Lee v. United States, Lopez v. United States, Hoffa v. United States, Lewis v. United States, *and* United States v. White.

---

* Professor of Law, *University of Oklahoma College of Law*. J.D., *University of California at Berkeley School of Law*; B.A., *University of Florida*.

I am indebted to Daniel P. O'Gorman, Christopher Slobogin, Michael Mannheimer, and the participants of the SMU Dedman School of Law Deason Criminal Justice Reform Workshop, ACS Constitutional Law Scholars Forum at Barry Law School, Southeastern Association of Law Schools Criminal Procedure Workshop, and Loyola Chicago University School of Law Constitutional Law Colloquium for their insightful comments. I thank Pamela Metzger and Kenitra Brown for the opportunity to present parts of this Article at the Criminal Justice Reform Workshop and for coordinating the Workshop. I am grateful for excellent research assistance and editing provided by Jade L. Grey, Andrew Grim, Darielena Lamastus, Catherine McCabe, Gianna Morgado, and Kathleen C. O'Gorman; help from Law Reference Librarians Diana Botluk, Jason Murray, and Louis Rosen; administrative help from Katherine Sutcliffe-Lenart and Lucinda Machado; and support through the summer research grant. I am also very grateful for the extraordinary and meticulous work of the *American University Law Review* editors and staff.

While the logic behind the impetus for third-party doctrine might appear sound, the doctrine's applications have been faulty. The third-party doctrine makes sense when applied to criminals and personal relationships, such as friends, family, and neighbors. But the third-party doctrine is incongruous when applied to legitimate commercial relationships, business transactions, or business records, as in United States v. Miller *and* Smith v. Maryland. *We have a reasonable expectation of privacy within legitimate commercial relationships and business transactions because that expectation is protected by contractual duties and rights, industry norms that ensure proper business conduct, assurances given by the business or an independent party to secure our confidence, and legal recourse to vindicate our expectations. Commercial relationships differ significantly from personal relationships because of the differences in trust and privacy expectations between friends and businesses. Legal norms support and reinforce our privacy expectations with businesses and commercial relationships. Our expectation of privacy within business transactions is ensconced in and recognized throughout the legal system—common law, statutes, constitutions, and international law.*

Based on the commonsense differences between commercial and personal relationships, this Article is the first to propose a new theory for the third-party doctrine by restraining its application only to the context of personal relationships. This theory is the most comprehensive model that has been proposed for refining the third-party doctrine and ensures that our privacy does not shrink as technology expands.

TABLE OF CONTENTS

Introduction 3
I. False Friends: The Right Starting Point 5
II. Taking the Wrong Turn: Business Records 8
III. Returning to False Friends: A Theory for the Third-Party Doctrine 11
A. Distinctions Between Trust and Expectations of Confidentiality and Privacy in Friends and Businesses 12
B. Trust, Expectations of Confidentiality, and Privacy Recognized by Law 22
1. Common law privacy protections 23
2. Legislative privacy protections 30
3. Constitutional privacy protections 36
4. International privacy protections 38
Conclusion 43

INTRODUCTION

When we think about relationships, we generally do not equate our relationships with friends as being synonymous with commercial relationships. Yet, interestingly, the U.S. Supreme Court saw no difference between the two types of relationships when it developed the third-party doctrine to determine reasonable expectations of privacy protected by the Fourth Amendment.[1] This Article is the first to disentangle the Court's conflation of friendships and commercial relationships to argue that there are reasonable expectations of privacy in commercial relationships that should be protected by the Fourth Amendment.

The Fourth Amendment's third-party doctrine, developed from a series of false friends cases in which criminals shared information with other criminals, informants, and undercover agents, is premised on the rationale that we hold no reasonable expectation of privacy when we voluntarily expose information to others and have assumed the risk that the third-party would share the information.[2] Subsequent cases, notably *United States v. Miller*[3] and *Smith v. Maryland*,[4] extended the doctrine to business records but took no notice of how the dynamics of trust change when you change the person receiving the trust. Whether a person has an expectation of privacy in the information shared should depend on with whom the information is entrusted and the context in which the information is shared.

This Article is the first to propose a new paradigm for the third-party doctrine by paring it back to the concept of false friends, which originally animated the doctrine. If we accept that one should bear the consequences of making false friends, then we should examine what is a false friend. A false friend is a person with whom you have misplaced trust. One may have the misfortune to misplace trust with friends, colleagues, neighbors, and family, and any one of them could rightly be placed in the "false friend" position. However, to attribute the appellation of "false friend" to businesses would be inappropriate because relationships with businesses are distinctly different from friendships. There is an expectation of privacy in the information

1. *See infra* Parts I–II for an in-depth discussion on the origins of the third-party doctrine and its evolution with business relationships being understood as synonymous to personal relationships, which poses a privacy law issue as business relationships are not viewed similar to personal relationship in the legal sphere.
2. *See infra* Part I.
3. 425 U.S. 435 (1976).
4. 442 U.S. 735 (1979).

conveyed to businesses because we reasonably rely on them to keep our information private. Our reliance is reasonable because the commercial relationship is bound by contractual duties and rights. Moreover, there are industry norms to ensure proper business conduct, assurances given by the business or an independent party to secure our confidence, and legal recourse to vindicate our expectations.[5]

Recent cases, particularly *United States v. Jones*,[6] *Riley v. California*,[7] and *Carpenter v. United States*,[8] show that the Court's perspective on privacy and the third-party doctrine is changing, signifying the recognition that too much privacy would be swallowed by the third-party doctrine and signaling that the time has come to rethink the doctrine.[9] The third-party doctrine should not be applied to commercial relationships or business transactions because trust and privacy expectations differ significantly between friends and businesses. It is natural and reasonable to have an expectation of privacy when transacting with a business because legal norms support and reinforce our privacy expectations with businesses and commercial relationships. We receive cues from a variety of places—common law, statutes, constitutions, and international law—that recognize our privacy expectations with commercial relationships and business transactions. Therefore, reformulating the third-party doctrine to encompass only disclosures made within personal relationships provides an elegant, simple solution that has intuitive appeal and provides broader protection for privacy than offered by other theories.

Part I of this Article traces the origins of the third-party doctrine to the false friends cases, involving evidence disclosed by informants and undercover agents. Part II argues that the doctrine's development to include business records in *United States v. Miller* and *Smith v. Maryland* is inappropriate because it conflates business relationships with personal relationships. Part III discusses the distinctions between commercial and personal relationships and the laws that protect the privacy expectations

5. *See infra* Section III.B.
6. 565 U.S. 400 (2012).
7. 573 U.S. 373 (2014).
8. 138 S. Ct. 2206 (2018).
9. *See, e.g.*, *Jones*, 565 U.S. at 404 (holding that the government's installation of a GPS-tracking device on the defendant's car and use of the device to monitor the defendant's movements violates the Fourth Amendment); *Riley*, 573 U.S. at 401 (holding that the search incident to arrest exception does not extend to a governmental search of a defendant's cellphone data); *Carpenter*, 138 S. Ct. at 2216–17, 2219, 2221 (holding that the third-party doctrine does not extend to governmental acquisition of a defendant's cell site location information and consequently, requiring a warrant for such information).

within commercial relationships. This Article concludes that restraining the third-party doctrine to personal relationships would be consistent with our intuition, industry norms, and laws.

I. FALSE FRIENDS: THE RIGHT STARTING POINT

The third-party doctrine's origin interestingly arose out of a series of cases focusing on the betrayal of trust and the criminal consequences of having false friends[10]: *On Lee v. United States*,[11] *Lopez v. United States*,[12] *Hoffa v. United States*,[13] *Lewis v. United States*,[14] and *United States v. White*.[15] These false friends cases are central to the third-party doctrine because they illuminate the doctrine's core: privacy is about trust and whether it is reasonable to trust or rely upon a third party.[16] As these cases show, it is unreasonable to rely on criminal collaborators—whether they are in fact criminals or undercover agents pretending to be criminals—to protect one's privacy interests.[17] Therefore, as a result of the false friends line of cases, when one unreasonably relies upon an individual, one assumes the risk of betrayal and must bear the consequences of choosing false friends.

In *On Lee*, the Court found no reasonable expectation of privacy existed because it was unreasonable for the defendant to trust a

---

10. Although some believe the third-party doctrine originated with *United States v. Miller*, *Miller* built upon the already-existing line of cases concerning false friends. *See Carpenter*, 138 S. Ct. at 2216 ("This third-party doctrine largely traces its roots to *Miller*."). *But see* United States v. Miller, 425 U.S. 435, 443 (1976) (citing United States v. White, 401 U.S. 745 (1971) (plurality opinion)); Hoffa v. United States, 385 U.S. 293 (1966); Lopez v. United States, 373 U.S. 427 (1963). In *Smith*, the Court similarly cited to the false friends cases—*White*, *Hoffa*, and *Lopez*—for the position that "[the] Court consistently has held that a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties." Smith v. Maryland, 442 U.S. 735, 743–44 (1979).

11. 343 U.S. 747 (1952).

12. 373 U.S. 427 (1963).

13. 385 U.S. 293 (1966).

14. 385 U.S. 206 (1966).

15. 401 U.S. 745 (1971) (plurality opinion).

16. *See, e.g.*, *Lopez*, 373 U.S. at 450 (Brennan, J., dissenting) ("It is not an undue risk to ask persons to . . . make damaging disclosures only to persons whose character and motives may be trusted."); *see also White*, 401 U.S. at 749–50 (discussing trust and privacy in the context of the previous decisions in *Hoffa* and *On Lee*).

17. *White*, 401 U.S. at 749 (emphasizing that "however strongly a defendant may trust an apparent colleague, his expectation [of privacy] in this respect [is] not protected by the Fourth Amendment," even "when it turns out that the colleague is a government agent regularly communicating with the authorities" (citation omitted)).

criminal collaborator.[18] In that case, a former employee and acquaintance visited the defendant's laundry.[19] During the visit, the defendant made incriminating statements to the acquaintance who was acting as an undercover agent and wearing a wire to transmit their conversations.[20] Although the acquaintance entered the defendant's place of business with the defendant's consent, the defendant argued that the acquaintance's wearing of an electronic transmitter during their conversations nullified the consent, thereby violating the defendant's Fourth Amendment protections against unlawful searches and seizures.[21] The Court dismissed the argument by analogizing the transmitted conversation to an eavesdropper overhearing a conversation and permitted evidence of the incriminating statements because the defendant "talk[ed] confidentially and indiscreetly with one he trusted" and made incriminating statements to a "confidante of shady character."[22] Thus, *On Lee* opened the door for evidence obtained through "informers, accessories, accomplices, false friends, or any of the other betrayals which are 'dirty business'"[23] and "the turning of state's evidence by denizens of the underworld."[24]

Lopez also involved a defendant's unreasonable reliance on a person whom he believed was part of his illicit scheme.[25] In *Lopez*, an Internal Revenue Service agent was investigating the defendant for delinquent taxes.[26] After the defendant offered the agent money to drop the case, the agent returned to the defendant's place of business on the pretense that he would cooperate with the defendant's scheme and wore a wire for their conversation to be transmitted and recorded.[27] Arguing for suppression of the recorded conversation, the defendant alleged an illegal seizure of the conversation through the agent's

---

18. 343 U.S. 747, 756 (1952). In the false friends cases, part of the reason the Court finds no reasonable expectation of privacy exists is the Court's view that individuals engaged in crime are inherently untrustworthy. *See, e.g.*, *id.* (intimating the unreasonableness of putting trust in "those who live by outwitting the law").

19. *Id.* at 749.

20. *Id.*

21. *Id.* at 750–52.

22. *Id.* at 753–54, 756.

23. *Id.* at 757.

24. *Id.* at 756 (balancing equities and reasoning that "[s]ociety can[not] . . . afford to throw away the evidence produced by the falling out, jealousies, and quarrels of those who live by outwitting the law").

25. Lopez v. United States, 373 U.S. 427, 431 (1963).

26. *Id.* at 428–29.

27. *Id.* at 430.

misrepresentation that he was taking part in the defendant's scheme.[28] The Court rejected the defendant's claim, reasoning that the defendant knew that the agent could have testified against him, even if the conversation had not been taped[29]: "[T]he risk that [the defendant] took in offering a bribe to [the agent] fairly included the risk that the offer would be accurately reproduced in court, whether by faultless memory or mechanical recording."[30] *Lopez* fits naturally within the false friends cases because it is unsurprising that the defendant maintains no privacy expectations in conversations with government agents, especially when he is aware of the agent's identity and purpose.[31]

Similarly, in *Hoffa*, the defendant's reliance upon a union colleague to keep his confidences was unreasonable.[32] The defendant, Hoffa, was a union president of the International Brotherhood of Teamsters, and while he was a defendant in an ongoing trial, he met with Partin, who was president of the local union.[33] During Partin's visits to Hoffa's hotel room, Hoffa confided in Partin his plan to bribe the jurors who were serving on his criminal trial where he was the sole defendant.[34] Partin, at the time, was facing criminal charges related to his union and agreed to report to federal officials any criminal misconduct relating to Hoffa.[35] Hoffa, like the defendant in *On Lee*, argued that Partin's role as a confidential informant vitiated Hoffa's consent for Partin's entry into Hoffa's hotel room and that Partin's listening constituted a search.[36] In upholding the government's conduct, the Court found that the Fourth Amendment does not protect "a wrongdoer's misplaced belief that a person to whom he voluntarily confides his wrongdoing will not reveal it."[37]

Lewis and *White* also fit neatly within the false friends line of cases because they reaffirm that when a defendant brings another into the fold of his criminal enterprise, he has no privacy interest when he unreasonably relies upon that person, even if law enforcement engaged in deception to lure the defendant's trust through the use of informants

28. *Id.* at 437.
29. *Id.* at 438.
30. *Id.* at 439.
31. *See id.*
32. Hoffa v. United States, 385 U.S. 293, 302 (1966).
33. *Id.* at 296.
34. *Id.*
35. *Id.* at 296–98.
36. *Id.* at 300; On Lee v. United States, 343 U.S. 747, 750–52 (1952).
37. *Hoffa*, 385 U.S. at 302.

or undercover police agents.[38] In *Lewis*, an undercover agent posed as a drug buyer and was invited into the defendant's home for a drug transaction.[39] The Court found that "[t]he pretense resulted in no breach of privacy; it merely encouraged the suspect to say things which he was willing and anxious to say to anyone who would be interested in purchasing marihuana."[40] In *White*, the deception was merely a replay of *On Lee*, where White's incriminating statements were transmitted by an informant and overheard by the police.[41] Because "one contemplating illegal activities must realize and risk that his companions may be reporting to the police," the Court reiterated that "the law gives no protection to the wrongdoer whose trusted accomplice is or becomes a police agent."[42] Thus, these cases laid the foundation of the third-party doctrine by establishing that a person assumes the risk of trusting others who could turn out to be unreliable.

II. TAKING THE WRONG TURN: BUSINESS RECORDS

In deciding whether a search is protected by the Fourth Amendment, the Court would later go on to adopt the test formulated in the concurrence of *Katz v. United States*[43]: police conduct constitutes a search if the defendant manifests a subjective expectation of privacy, and it is one that society is prepared to accept as reasonable.[44] The Court overlaid these false friends cases onto the *Katz* test to hold that there is no expectation of privacy in matters conveyed to third parties.[45] While this proposition seems sound regarding entrusting confidences to would-be criminals, the Court's jurisprudence took an unexpected turn by applying this notion to the loss of privacy in business records and information given within a commercial relationship. By inappropriately applying the earlier theory of false friends, the Court in two seminal cases, *United States v. Miller* and *Smith v. Maryland*, erroneously extended the third-party doctrine to businesses.

---

38. Lewis v. United States, 385 U.S. 206, 210 (1966); United States v. White, 401 U.S. 745, 752 (1971) (plurality opinion).

39. *Lewis*, 385 U.S. at 210.

40. *Id.* at 212 (quoting Brief for the United States at 25, *Lewis*, 385 U.S. 206 (No. 36), 1966 WL 100657, at *25).

41. *White*, 401 U.S. at 746–47 (plurality opinion).

42. *Id.* at 752.

43. 389 U.S. 347 (1967).

44. *Id.* at 361 (Harlan, J., concurring). Although the two-part *Katz* test "was not formulated by the majority, this test has been the main takeaway of the case." *Expectation of Privacy*, CORNELL L. SCH., https://www.law.cornell.edu/wex/expectation_of_privacy [https://perma.cc/59TJ-RKMA] (Dec. 2022).

45. *Katz*, 389 U.S. at 352.

Before examining *Miller* and *Smith*, it is important to note the influence of *Couch v. United States*[46] in propelling the third-party doctrine in the wrong direction. In *Couch*, as part of its investigation of the defendant's tax liabilities, the government subpoenaed the defendant's financial records from the defendant's accountant.[47] The Court upheld the government's acquisition of the records, reasoning that the defendant relinquished any Fourth Amendment expectations of privacy in the documents when she gave them to her accountant, knowing that the accountant would be under the obligations of the mandatory disclosure laws in filing her tax return.[48] Because much of the information being sought by law enforcement was required to be disclosed on the defendant's tax return, it would not remain private.[49] Although *Couch* can be limited because its rationale relies heavily on the existence of mandatory disclosure laws,[50] it precipitates the Court's third-party doctrine's divergence from the pure false friends circumstances to the realm of commercial and professional relationships and business records.

Building on *Couch*, the Court in *Miller* and *Smith* took the third-party doctrine further in the wrong direction.[51] In *Miller*, two banks under subpoenas provided checks, deposit slips, and financial statements relating to the defendant's accounts at the banks to federal agents.[52] Notwithstanding that the banks construed the records and information relating to customers' accounts as confidential,[53] the Court treated the checks as non-confidential communications and merely as "negotiable instruments to be used in commercial transactions [that] . . . contain only information voluntarily conveyed to the banks and exposed to their employees in the ordinary course of

46. 409 U.S. 322 (1973).

47. *Id.* at 323.

48. *See id.* at 335–36.

49. *Id.*

50. *Id.* (citing 26 U.S.C. § 7206(2) for the proposition that the accountant, too, would suffer criminal liability for assisting in the filing of a false return).

51. *See* United States v. Miller, 425 U.S. 435, 447 n.1 (1976) (Brennan, J., dissenting) (disagreeing with the extension of the third-party doctrine to *Miller* and distinguishing the expectation of privacy asserted in *Couch* by emphasizing that the accountant in *Couch* was obligated to abide by mandatory disclosure laws governing taxes, whereas Miller's banks "had no obligation to disclose the information voluntarily").

52. *Id.* at 437–38 (majority opinion).

53. *Id.* at 449 (Brennan, J., dissenting) (noting that "[r]epresentatives of several banks testified at the suppression hearing that information in their possession regarding a customer's account is deemed by them to be confidential").

business."[54] Relying on the false friends line of cases, the Court held that the defendant lacked any legitimate expectation of privacy in these disclosed documents because

> [t]he depositor takes the risk, in revealing his affairs to another, that the information will be conveyed by that person to the Government. This Court has held repeatedly that the Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities, even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed.[55]

Following *Miller*, the Court in *Smith* expanded the third-party doctrine to include telephonic information.[56] In *Smith*, the police installed a pen register at the telephone company's office without a warrant or court order.[57] Pointing out that pen registers do not reveal whether calls were completed, the content of the call, or the identities of the caller or recipient,[58] the Court held that the defendant lacked an expectation of privacy in the numbers that he dialed because he "voluntarily conveyed numerical information to the telephone company and 'exposed' that information to its equipment in the ordinary course of business . . . [, thereby] assum[ing] the risk that the company would reveal to police the numbers he dialed."[59]

Both *Miller* and *Smith* relied on the false friends cases.[60] However, in crafting the third-party doctrine in *Miller* and *Smith*, the Court neglected to recognize the distinction between a person's level of trust and expectation of privacy for friends or would-be criminals, on the one hand, and a person's level of trust and expectations of privacy in

---

54. *Id.* at 442 (majority opinion).

55. *Id.* at 443 (citation omitted). In response to *Miller*, Congress passed the Right to Financial Privacy Act of 1978, which prohibited nonconsensual disclosure of financial records to the government, except under limited circumstances: through a search warrant, administrative subpoena, judicial subpoena, or formal written request. 12 U.S.C. §§ 3401–08. If the government obtains the financial records through a search warrant, it "shall mail to the customer's last known address a copy of the search warrant" and must give the customer notice that the government accessed the financial records. *Id.* § 3406(b). If the government uses a judicial subpoena, administrative subpoena, or formal written request, the government must provide notice to the customer and an opportunity to be heard to quash the motion or enjoin the government. *Id.* §§ 3405, 3407–08.

56. Smith v. Maryland, 442 U.S. 735, 744 (1979).

57. *Id.* at 737.

58. *Id.* at 741.

59. *Id.* at 744.

60. *Miller*, 425 U.S. at 443; *Smith*, 442 U.S. at 743–44.

legitimate businesses, such as banks and phone companies, on the other hand.[61] *Miller* and *Smith* took no notice of how the dynamics of trust shift when you change the recipient of the trust. Whether a person has an expectation of privacy in the information shared should depend on with whom the information is entrusted and the context in which the information is shared.

III. RETURNING TO FALSE FRIENDS: A THEORY FOR THE THIRD-PARTY DOCTRINE

The third-party doctrine resembles a gangly, overgrown, and unwieldy bush that needs to be severely trimmed back to its stock to regain its form and utility. The stock is the original concept of false friends and trust. As established in *On Lee*, *Hoffa*, *Lewis*, and *White*, when a defendant assumes the risk of misplaced trust by confiding in others, he no longer has expectations of privacy in the information and is not protected by the Fourth Amendment.[62] Therefore, in the Court's view, privacy is fundamentally about trust. For criminals,

> those who do not accept morality, who are wicked and deceitful, the occasion for trust does not arise. We do not trust them, and they have no reason to trust us in the full sense of a relationship if mutual expectation, for our posture towards them is not one of cooperative mutual forbearance but of defensive watchfulness. Thus not only can a thoroughly untrustworthy person not be trusted; he cannot trust others, for he is disabled from entering into the relations of voluntary reciprocal forbearance for mutual advantage which trust consists of.[63]

It is confounding, however, that *Miller* and *Smith* relied upon a line of cases involving defendants who confided in other criminals as the basis for making the monumental leap that, going forward, no one can have a Fourth Amendment expectation of privacy in any third party—even with legitimate businesses.[64] The key differences between these false friends cases and *Miller* and *Smith* are the identity of the third-party—with whom trust was placed, the type of relationship, and the

---

61. *Miller*, 425 U.S. at 443 (citing the line of false friends cases—*White*, *Hoffa*, and *Lopez*—and lumping together all information "revealed to a third party" that was later "conveyed . . . to [g]overnment authorities," regardless of whether the information was conveyed to a false friend or a legitimate business).

62. On Lee v. United States, 343 U.S. 747, 757–78 (1952); Hoffa v. United States, 385 U.S. 293, 303 (1966); Lewis v. United States, 385 U.S. 206, 211 (1966); United States v. White, 401 U.S. 745, 751 (1971) (plurality opinion).

63. Charles Fried, *Privacy*, 77 YALE L.J. 475, 481 (1968).

64. *See generally Miller*, 425 U.S. 435 (discussing *White*, *Hoffa*, and *Lopez*); *Smith*, 442 U.S. 735 (discussing *Miller*, *Couch*, *White*, *Hoffa*, and *Lopez*).

context in which the information is shared. And it is these differences that should be at the heart of the third-party doctrine.

The third-party doctrine should be reformed based on the concepts of false friends—that there is no reasonable expectation of privacy in information revealed to friends because they can betray you—but that expectation is reasonable when the information is conveyed within a legitimate commercial or professional relationship or during a business transaction. A person's expectations of privacy with respect to information given within a legitimate business or commercial context is reasonable because a person's reliance on businesses to protect confidential information is rational and reasonable.[65] Legal sanctions, industry norms, and the business's reputation motivate businesses and professionals to maintain a person's privacy.[66] A person, therefore, assumes minimal risk of being betrayed by a legitimate business because there is legal recourse and ensuing damage to the business's reputation if it divulges a person's private information.[67] Thus, reformulating the third-party doctrine to encompass only situations involving false friends—personal relationships—and not commercial relationships best protects privacy interests. Reformulating the third-party doctrine will allow us to interact with businesses to further our emotional, physical, and social needs without fear of the government's warrantless access to our information.

A. Distinctions Between Trust and Expectations of Confidentiality and Privacy in Friends and Businesses

Because trust is integral to the third-party doctrine, it is important to understand what trust means. Trust can be defined in various ways. One definition of trust is "reliance without recourse"; when one trusts, one relies on the other person to hold that trust inviolate, even though one

---

65. *Cf.* J. H. Jennifer Lee, Kimberly B. Frumkin, Susan Tran & Nicolás Sánchez-Mandery, *Consumer Protection in the New Economy: Privacy Cases in E-Commerce Transactions or Social Media Activities*, 73 CONSUMER FIN. L.Q. 6, 23 (2019) (finding an increasing number of consumers believe companies have an obligation to and should take proactive steps to safeguard their personal information).

66. Avner Ben-Ner & Louis Putterman, *Trusting and Trustworthiness*, 81 B.U. L. REV. 523, 539 (2001) (listing incentives for companies to act as "safe custodians" of customer data, such as the risk of losing future business due to lack of trust).

67. *See* Lee et al., *supra* note 65, at 7 (explaining that consumers have statutory rights of action from acts such as the Electronic Communications Privacy Act, the Stored Communications Act, and the California Invasion of Privacy Act, which give consumers legal recourse).

has no recourse should that trust falter and harm ensue.[68] Trust can also mean "the willingness to rely on another even in the absence of binding external constraints."[69] While there is no universal definition of trust, most scholars agree that trust "embodies a willingness to accept vulnerability under conditions of uncertainty."[70]

Using these commonly accepted definitions of trust, it is easy to understand how the third-party doctrine developed through the false friends cases and should be restricted as such. In Aristotle's view, friendship entails "hav[ing] no need for justice"—likely to mean that friends must rely on trust alone instead of legal enforcement.[71] If a person trusts a friend, neighbor, or acquaintance with a secret and that secret is revealed, the person is unlikely to be able to avail himself of legal recourse.[72] Therefore, in the absence of legal recourse that would prevent the friend from gossiping or snitching, it makes sense that there is no reasonable expectation of privacy in the information given in a personal relationship. In situations involving friends, the reliance is arguably unreasonable or less reasonable than with businesses, which renders the expectation of privacy less reasonable.[73] Thus, there is

---

68. Justin (Gus) Hurwitz, *Trust and Online Interaction*, 161 U. PA. L. REV. 1579, 1584 (2013).

69. Larry E. Ribstein, *Law v. Trust*, 81 B.U. L. REV. 553, 555 (2001).

70. Rebecca M. Bratspies, *Regulatory Trust*, 51 ARIZ. L. REV. 575, 589 (2009). Countless definitions of trust have been formulated by scholars, many of which share common themes. *See, e.g.*, Margaret M. Blair & Lynn A. Stout, *Trust, Trustworthiness, and the Behavioral Foundations of Corporate Law*, 149 U. PA. L. REV. 1735, 1739–40 (2001) (defining trust to include "a willingness to make oneself vulnerable to another, based on the belief that the trusted person will choose not to exploit one's vulnerability (that is, will behave trustworthily)"). As one scholar has observed, "[f]or trust to be relevant, there must be the possibility of exit, betrayal, defection." Bratspies, *supra* (quoting DIEGO GAMBETTA, *Can We Trust Trust?*, *in* TRUST: MAKING AND BREAKING COOPERATIVE RELATIONS 213, 218–19 (Diego Gambetta ed., 1988)); *see also* Claire A. Hill & Erin Ann O'Hara, *A Cognitive Theory of Trust*, 84 WASH. U. L. REV. 1717, 1724 (2006) ("Trust experts all seem to agree that trust is a state of mind that enables its possessor to be willing to make herself vulnerable to another—that is, to rely on another despite a positive risk that the other will act in a way that can harm the truster.").

71. Ethan J. Leib, *Friendship & the Law*, 54 UCLA L. REV. 631, 653 (2007).

72. John Duffy, Huan Xie & Yong-Ju Lee, *Social Norms, Information and Trust Among Strangers: Theory and Evidence*, 52 ECO. THEORY 669, 670 (2013) ("[T]rust emerges among essentially anonymous agents who have little recourse to direct or immediate punishment.").

73. *Cf.* Shulman v. Grp. W Prods., Inc., 955 P.2d 469, 491 (Cal. 1998) ("[E]xisting legal protections for communications could support the conclusion that [an individual] possessed a reasonable expectation of privacy . . . .").

"reliance without recourse,"[74] the essence of trust, and nothing can be done legally when that trust is misplaced with friends. *On Lee*, *Hoffa*, *Lewis*, *Lopez*, and *White* involved this notion of trust.

On the other hand, the reliance upon third parties in *Miller* and *Smith* does not involve this same notion of trust—therefore, they are not cases about misplaced trust at all. The idea of misplaced trust connotes poor judgment,[75] but Miller's interaction with the bank and Smith's interaction with the telephone company lack this element. How can a person be faulted for sharing financial information with a bank, especially since banking services necessarily revolve around the exchange of financial information?[76] How can a person be criticized for exercising poor judgment in conveying phone numbers to a telephone company when those numbers are required to place the call?

Second, a person does not exercise poor judgment in trusting a business because there is the availability of legal recourse, the existence of institutional norms, the availability of the business's information, and the business's incentive to maintain its reputation, all of which contribute to a customer's logical decision to rely on or "trust" businesses.[77] The availability of legal recourse justifies a person's reliance on businesses and makes commercial relationships significantly different from friendships.[78] If a person gives financial information to the bank, the bank is not at liberty to publish this information.[79] But if

---

74. Hurwitz, *supra* note 68, at 1584.

75. Some definitions of misplace include "to put in a wrong or inappropriate place" or "to set on a wrong object or eventuality," as in "his trust had been misplaced." *Misplace*, MERRIAM-WEBSTER DICTIONARY, https://www.merriam-webster.com/dictionary/misplace [https://perma.cc/V9KL-7XYB]. Others define misplacing trust in someone to mean "to put trust in the wrong person; to put trust in someone who does not deserve it." *Misplace Trust*, FREE DICTIONARY, https://idioms.thefreedictionary.com/misplace+trust [https://perma.cc/39LG-74SH]; *see also Misplace*, DICTIONARY.COM, https://www.dictionary.com/browse/misplace [https://perma.cc/Q56T-EMFH] (defining misplace as "to place or bestow improperly, unsuitably, or unwisely: to misplace one's trust").

76. In their privacy notices, banks state, "All financial companies need to share customers' personal information to run their everyday business." *See, e.g.*, WELLS FARGO, WELLS FARGO U.S. CONSUMER PRIVACY NOTICE 1 (Oct. 4, 2023), https://www.wellsfargo.com/privacy-security/privacy/individuals.

77. *See* notes 65–67 and accompanying text.

78. Hurwitz, *supra* note 68, at 1597 ("The law offers a simple alternative to trust: remedies.").

79. *See* Gramm-Leach Bliley Act, Pub. L. No. 106-102, 113 Stat. 1338 (codified in relevant part primarily at 15 U.S.C. §§ 6801–09, 6821–27); *see also* FED. DEPOSIT INS. CORP., PRIVACY RULE HANDBOOK, https://www.fdic.gov/bank-examinations/privacy-rule-handbook [https://perma.cc/V9R2-8DDZ] (Aug. 11, 2023) (noting that "nonpublic personal information" is protected by the FDIC's privacy rules).

the bank's lapse of judgment leads it to share the financial information with the public, there is available legal recourse, such as a suit for breach of confidentiality or a contract claim.[80] "The law can clearly produce a decision to rely by enforcing contracts or imposing mandatory constraints that affect the parties' risk calculation."[81] The law enhances reliance by providing remedies and other means of recovery, which in turn reduce a customer's risk because they allow the customer to "hedg[e] against the risk" of unreliability.[82] This process of risk assessment makes reliance a cognitively rational decision.[83] As some trust scholars believe, "The law might help establish a *trustworthiness* norm, and thereby make promises more reliable. . . . [B]y penalizing disloyal behavior, the law expresses a social consensus concerning the type of conduct that constitutes cheating, and so concretizes the behavior that invokes emotional sanctions for violating internalized norms against cheating."[84] Such legal recourse includes breach of contract, breach of fiduciary duty, fraud, breach of confidentiality, conspiracy, theft, and unconscionable business practices, among others.[85] The availability of

---

80. *See infra* Section III.B (discussing common law remedies for privacy violations); *cf.* FED. DEPOSIT INS. CORP., *Gramm-Leach-Bliley Act (Privacy of Consumer Information)*, *in* CONSUMER COMPLIANCE EXAMINATION MANUAL VIII-1.1, VIII-1.4 (2021), https://www.fdic.gov/resources/supervision-and-examinations/consumer-compliance-examination-manual/documents/8/viii-1-1.pdf (describing the duties owed to consumers).

81. Ribstein, *supra* note 69, at 556 (emphasis omitted).

82. Frank B. Cross, *Law and Trust*, 93 GEO. L. REV. 1457, 1466 (2005). The association of law and risk assessment is widely recognized:

> Regarding the magnitude of risk, laws can both influence the likelihood that people will behave in a trustworthy fashion and signal to citizens that the community has adopted trustworthy norms of behavior. Both the expressive and the behavior-influencing effects of the law cause the trust evaluator to perceive a smaller risk of predation than would exist without the law. As to the costs of predation, to the extent a violation of the law yields partial compensation to the truster, she perceives a lower magnitude of harm from erroneously trusting.

Hill & O'Hara, *supra* note 70, at 1752–53.

83. Cross, *supra* note 82, at 1466–67. The rational choice perspective conceptualizes a person's behavior as "a function of his or her goals and the pressures and constraints the person perceives in the situation." Sirkka L. Jarvenpaa & Emerson H. Tiller, *Customer Trust in Virtual Environments: A Managerial Perspective*, 81 B.U. L. REV. 665, 672 (2001). In this view, "trust aris[es] from calculative decisions based on (1) the awareness of each party's motivations and goals, and (2) the ability to rely on laws and social norms, or creation of deterrence and control mechanisms by the parties themselves, to prevent opportunism." *Id.*

84. Ribstein, *supra* note 69, at 565.

85. *See* Hill & O'Hara, *supra* note 70, at 1755.

legal recourse and other formal sanctions,[86] which would generally be absent in trusts involving friendships, therefore facilitate interactions with, and reliance on, commercial entities.[87]

Additionally, reliance within commercial relationships is warranted because the existence of institutional norms, ordinarily unavailable with friends, guides a person's judgment in trusting a business. "When the content of the norms dictates cooperative behavior, social actors can use this information to develop expectations about the likelihood that others will cooperate, and then make a decision to act accordingly."[88] The institutional norms of an industry give the public a baseline to rely on for their expectations of proper business conduct.

> [G]eneralized trust is in important ways a function of everyday compliance with the prevailing social norms in a community. That is, general beliefs about the willingness of others to cooperate in mutually beneficial ways are in large part a function of our specific expectations about the willingness of others to comply with the prevailing social norms.[89]

For example, the fact that banks do not share nonpublic personal information and implement procedures to protect account holders' identity and information gives us the confidence to believe that our financial records within the bank are confidential,[90] negating any implications of poor judgment in trusting the bank. "In this way social norms generalize expectations beyond those of the actors whom we know personally."[91]

A business's motivation to protect its reputation also encourages a person to reasonably rely on the business. Businesses have incentives to earn our "trust" and to show that they are "trustworthy" through their reputation,[92] third-party enforcement, and providing information about themselves.[93] A company can build its reputation by establishing a corporate culture, identity, or character by applying consistent rules and best practices within and outside of the organization that surpass legal

---

86. See *infra* Part III for an in-depth discussion of laws that support an expectation of privacy in shared information.

87. Hurwitz, *supra* note 68, at 1599.

88. Jack Knight, *Social Norms and the Rule of Law: Fostering Trust in a Socially Diverse Society*, *in* TRUST IN SOCIETY 354, 359 (Karen Cook ed., 2001).

89. *Id.* at 360.

90. FED. DEPOSIT INS. CORP., *supra* note 80.

91. Knight, *supra* note 88, at 359.

92. Helen Nissenbaum, *Will Security Enhance Trust Online, or Supplant It?*, *in* TRUST AND DISTRUST IN ORGANIZATIONS: DILEMMAS AND APPROACHES 159 (Kramer & Cook, eds., 2004) (discussing reputation as a factor in forming trust).

93. Ben-Ner & Putterman, *supra* note 66, at 527–31.

obligations.[94] Because a company's reputation for unreliability will cause it to lose customers[95] and devalue its stock, the company has an incentive to not disappoint.[96] Because businesses are incentivized by the prospect of future dealings with customers, they seek to earn the customer's trust in all regards and give reassurances in the service they provide, as well as in safeguarding the customer's personal information, such as through privacy policies. Businesses provide privacy statements that enable consumers to make informed decisions about which company to trust, and, in turn, the businesses' transparency cultivates trust and goodwill.[97] Additionally, "direct assurances provided by third parties,"[98] such as through government endorsements or guarantees or

---

94. *Id.* at 535.

95. Reputation is essential in building customer reliance and confidence:

> For example, individuals and firms can bond future performance by investing time and money in developing a reputation that would be devalued by acts of disloyalty. The bond is self-enforcing in that misconduct diminishes the value of the trustee's reputation according to the public's perception of the seriousness of the misconduct.

Ribstein, *supra* note 69, at 569 (footnote omitted).

96. Ben-Ner & Putterman, *supra* note 66, at 536 ("Since a company stands to gain market share and the ability to sell at a higher price by maintaining favorable name recognition, a favorably viewed brand name is a form of intangible capital that can have marketable value in the millions or even billions of dollars.").

Trust scholars have observed that positions of trust are held in such high regard that an allegation of breach of trust, as opposed to a contract breach claim, carries with it a stigma that cannot be atoned with monetary compensation. Tamar Frankel & Wendy Gordon, *Introduction*, 81 B.U. L. REV. 321, 324 (2001). Thus, the cost of losing trust is great:

> The implication of this analysis for lawmakers is that if trustees are deemed part of the "crowd" wheeling and dealing in the market place, not only will they lose their unique elevated status, but the deterrence resulting from the threat of this loss will be eliminated as well. Not only will a valuable token of esteem that law can bestow on trusted persons will be lost, but the norm attendant to the status will be lost as well.

Id.

97. KAMALA D. HARRIS, CAL. DEP'T OF JUST., MAKING YOUR PRIVACY PRACTICES PUBLIC 1 (2014), https://oag.ca.gov/sites/all/files/agweb/pdfs/cybersecurity/making_your_privacy_practices_public.pdf (recommending companies draft privacy statements that are readable and informative regarding data collection).

98. Ben-Ner & Putterman, *supra* note 66, at 528; Russell Hardin, *Distrust*, 81 B.U. L. REV. 495, 519 (2001) ("[T]hird party guarantors of trustworthiness are especially important in commercial relations[hips] . . . ."). The Federal Deposit Insurance Corporation (FDIC), "an independent agency created by the Congress to maintain stability and public confidence in the nation's financial system," is one example of a third-party providing assurance. FED. DEPOSIT INS. CORP., 2022-2026 STRATEGIC PLAN:

through courts, might bolster a person's trust in a business.[99] Ironically, although the *Miller* Court found that Miller had no reasonable expectation of privacy in the information conveyed to his banks,[100] trust scholars often use banks as an example to illustrate when a customer would be justified in having confidence in the commercial relationship[101]:

> Indeed, banks are an instance of an organization that we might even think we understand well enough to be quite confident that its individual agents will perform their jobs in our interest as expected. They are so thoroughly and richly monitored in all their actions that systematic cheating is very difficult, even though it must sometimes happen.[102]

Additionally, the greater the availability of information about a business, the more it supports the trust placed upon the business.[103]

MISSION, VISION, AND VALUES 3 (2021), https://www.fdic.gov/system/files/2024-07/strategic-plan-2022-2026.pdf. Banks that are insured by the FDIC must adhere to FDIC policies, which include consumer protection.

> The FDIC directly supervises and examines more than 5,000 banks and savings associations for operational safety and soundness[, more than half of the institutions in the banking system]. . . . The FDIC also examines banks for compliance with consumer protection laws, including the Fair Credit Billing Act, the Fair Credit Reporting Act, the Truth in Lending Act, and the Fair Debt Collection Practices Act, to name a few.

What We Do, FED. DEPOSIT INS. CORP., https://www.fdic.gov/about/what-we-do [https://perma.cc/G8MP-92LX] (May 15, 2020).

99. Hardin, *supra* note 98, at 520 ("We rely on contract law and court enforcement to achieve successful cooperation in contexts in which, without such protective institutions, we would not risk cooperating with others.").

100. Several states protect bank records through their constitutions or statutes. *See, e.g.*, Commonwealth v. DeJohn, 403 A.2d 1283, 1291 (Pa. 1979) ("[U]nder . . . the Pennsylvania Constitution bank customers have a legitimate expectation of privacy in records pertaining to their affairs kept at the bank."); State v. Thompson, 810 P.2d 415, 418 (Utah 1991) (confirming that Utah's constitution protects the privacy of bank records). *Contra* State v. Schultz, 850 P.2d 818, 823 (Kan. 1993) (recognizing that privacy concerns in bank records are unprotected in the Kansas Constitution); State v. Adame, 476 P.3d 872, 876 (N.M. 2020) (applying the third-party doctrine to hold that the defendant relinquished his expectation of privacy in bank records shared with others).

101. *See, e.g.*, Ben-Ner & Putterman, *supra* note 66, at 531 (illustrating that better "formal information processing institutions like banks" can provide better information to develop greater trust).

102. Hardin, *supra* note 98, at 520.

103. Ben-Ner & Putterman, *supra* note 66, at 531 ("The better social networks, the media, and formal information processing institutions like banks work, the better the information individuals have about parties with whom they may transact, and the greater the trust they place in their transactions."). For example, banks insured by the FDIC must be compliant with a plethora of policies, which are available for the consumer to review.

Audits and monitoring by the government or independent entities contribute to the information that customers rely upon for evaluating trustworthiness.[104] For example, securities regulations on disclosures help to ensure the accuracy of the prospectus to help investors evaluate investment options.[105] Prospective customers may review the ratings and comments made by other customers,[106] such as on social media, before they engage with a business.[107] Particularly in the "gig economy," "sharing economy," or "peer-to-peer" markets,[108] "feedback is . . . [a] necessary ingredient for developing trust among diverse and

---

See, e.g., FED. DEPOSIT INS. CORP., CONSUMER COMPLIANCE EXAMINATION MANUAL (2019), https://www.fdic.gov/regulations/compliance/manual/index.html [https://perma.cc/2B35-SLT9].

104. Hill & O'Hara, *supra* note 70, at 1758.

105. *Id.* at 1756.

106. Epinions.com, the Better Business Bureau, Avvo.com, RateMyProfessors.com, and AngiesList.com are some examples of websites where customers can read reviews. Lior Jacob Strahilevitz, *Reputation Nation: Law in an Era of Ubiquitous Personal Information*, 102 NW. U. L. REV. 1667, 1706, 1710 (2008).

107. Ben-Ner & Putterman, *supra* note 66, at 542 ("[D]issatisfied consumers can post their grievances and warn other consumers about their dealings with those companies."); Hurwitz, *supra* note 68, at 1603 (discussing eBay's decision to allow customers to view other customers' feedback as enhancing trust); Abbey Stemler, *Betwixt and Between: Regulating the Shared Economy*, 43 FORDHAM URB. L.J. 31, 37 (2016) ("Modern trust is built on a feedback loop system of ratings and reviews, as first utilized effectively by eBay.").

For peer-to-peer markets, also known as "the gig economy," consumer feedback and a business's reputation are particularly important to offset risks:

> Peer review systems help consumers to make informed choices by giving them access to other peers' feedback on the peer provider and/or the product/service. Reputation systems, on the other hand, inform about the peer provider's reliability. In addition to having a trust-building function, review and reputation systems can also help regulate peer behaviour through peer-pressure, or help the platform monitor and enforce rules and minimum requirements.

PIERRE HAUSEMER, JULIA RZEPECKA, MARIUS DRAGULIN, SIMONE VITIELLO, LISON RABUEL, MADALINA NUNU ET AL., EXPLORATORY STUDY OF CONSUMER ISSUES IN ONLINE PEER-TO-PEER PLATFORM MARKETS FINAL REPORT 85 (May 2017).

108. These terms are often used interchangeably, but some distinguish them in that the sharing economy is considered a subset of the peer-to-peer market. The peer-to-peer market consists of buying or selling of goods and activities in the sharing economy (sharing or renting goods, sharing or renting accommodations, sharing or hiring rides, and hiring people for odd jobs). HAUSEMER ET AL., *supra* note 107, at 11; *see also* Michael Etter, Christian Fieseler & Glen Whelan, *Sharing Economy, Sharing Responsibility? Corporate Social Responsibility in the Digital Age*, 159 J. BUS. ETHICS 935, 937 (2019) (describing the sharing economy as "associated with the sharing or exchange of underused assets, such as properties, tools, or financial assets"); Stemler, *supra* note 107, at 57 (defining the features of the sharing economy market). Those engaged in peer-to-peer markets as "supply-side users" are considered microbusinesses. *See* Stemler, *supra* note 107, at 58 (discussing microbusinesses).

physically distant parties."[109] Therefore, given the measures employed by businesses to build and maintain their reputation by providing assurances and information to customers, and because of the availability of legal recourse, the type of trust a person holds with a friend is significantly different than the trust a person holds with a business.[110] For these reasons, the trust that lies at the core of a commercial relationship and the resultant expectations of privacy deserve greater protection.[111]

Finally, there is a difference in the voluntariness of sharing information with friends in *On Lee*, *Hoffa*, *White*, *Lopez*, and *Lewis* as opposed to with the businesses in *Miller* and *Smith*.[112] Friendship entails voluntariness, intimacy, trust, reciprocity, solidarity and exclusivity, warmth, mutual assistance, and equality.[113] Friends usually occupy equal positions without power differentials, which makes the sharing of information truly voluntary.[114] On the other hand, commercial relationships generally are marked by unequal positions and power, which makes the sharing of information with a business not entirely voluntary.[115] "Great power differences undercut the very possibility of

---

109. Stemler, *supra* note 107, at 45.

110. *See, e.g.*, *id.* at 53–54 (outlining how UberX instills trust between customers and drivers).

111. Ben-Ner & Putterman, *supra* note 66, at 539.

112. On Lee v. United States, 343 U.S. 747, 749 (1952); Hoffa v. United States, 385 U.S. 293, 296 (1966); United States v. White, 401 U.S. 745, 746–47 (1971) (plurality opinion); Lopez v. United States, 373 U.S. 427, 429 (1963); Lewis v. United States, 385 U.S. 206, 207 (1966); United States v. Miller, 425 U.S. 435, 437–38 (1976); Smith v. Maryland, 442 U.S. 735, 737 (1979).

113. Leib, *supra* note 71, at 642–46. Others have reflected that friendship includes "affection, admiration, intimacy, and vulnerability." Robert J. Condlin, "*What's Love Got to Do with It?" "It's Not Like They're Your Friends for Christ's Sake": The Complicated Relationship Between Lawyer and Client*, 82 NEB. L. REV. 211, 244 (2003) (quoting William H. Simon, *The Ideology of Advocacy, Procedural Justice and Professional Ethics*, 1978 WIS. L. REV. 29, 108 (1978)). "Most importantly, friendship is mutual and reciprocal, not hierarchical and unilateral." *Id.* at 296; *see also* Austen R. Anderson & Blaine J. Fowers, *An Exploratory Study of Friendship Characteristics and Their Relations with Hedonic and Eudaimonic Well-Being*, 37 J. SOC. & PERS. RELATIONSHIPS 260, 261 (2020) (discussing the types and characteristics of friendships); M. Neil Browne & Laurie A. Blank, *The Contrast Between Friendship and Business-Consumer Relationships: Trust Is an Earned Attribute*, 16 BUS. & PRO. ETHICS J. 155, 156 (1997) (describing differences between friendships and business relationships); Kent Grayson, *Friendship Versus Business in Marketing Relationships*, 71 J. MARKETING 121, 135 (2007) (describing four attributes of friendship).

114. Condlin, *supra* note 113, at 267.

115. In determining that the collection of data by a smart meter constitutes a search, the Seventh Circuit has recognized that it is not necessarily the case that the

agreement that is voluntary and uncoerced."[116] Customers are often in a less powerful position compared to the business and are unable to negotiate terms; the agreement reached is usually a take-it-or-leave-it situation.[117] For example, a customer has little power to limit a bank's internal use of a customer's information for marketing purposes and must accept a boilerplate privacy disclosure notice as written by the bank.[118] The power differential might be a byproduct of the business's specialized skills or knowledge, which explains why we trust

---

public voluntarily assumes the risk of the disclosure of its information when operating with some businesses.

> The third-party doctrine rests on "the notion that an individual has a reduced expectation of privacy in information knowingly shared with another." But in this context, a choice to share data imposed by fiat is no choice at all. If a person does not—in any meaningful sense—"voluntarily 'assume the risk' of turning over a comprehensive dossier of physical movements" by choosing to use a cell phone, it also goes that a home occupant does not assume the risk of near constant monitoring by choosing to have electricity in her home. We therefore doubt that *Smith* and *Miller* extend this far.

Naperville Smart Meter Awareness v. City of Naperville, 900 F.3d 521, 527 (7th Cir. 2018) (citations omitted) (quoting Carpenter v. United States, 138 S. Ct. 2206, 2219, 2220) (2018)).

116. Hardin, *supra* note 98, at 508 (describing professional relationships where business leaders need cooperation from subordinates to achieve organizational and personal goals, but power imbalances can often undermine trust in these relationships).

117. "The ubiquity of consumer SFCs [(standard form contracts)] cannot be exaggerated. One enters an SFC by opening a bank account, purchasing software on the web, renting a safe deposit box in a bank, or engaging in countless other day-to-day activities." Shmuel I. Becher, *Behavioral Science and Consumer Standard Form Contracts*, 68 LA. L. REV. 117, 119 (2007). Also, "[i]t can be daunting for an individual consumer to bargain with a distant [i]nternet merchant . . . about the desired level of privacy. To be successful, bargaining might take time, effort, and considerable expertise in privacy issues." Pamela Samuelson, *Privacy as Intellectual Property?*, 52 STAN. L. REV. 1125, 1127 (2000) (omission in original) (quoting PETER P. SWIRE & ROBERT E. LITAN, NONE OF YOUR BUSINESS: WORLD DATA FLOWS, ELECTRONIC COMMERCE, AND THE EUROPEAN PRIVACY DIRECTIVE 8 (1998)).

118. For many banks, their privacy notice makes clear that customers cannot limit the bank sharing the customer's information for marketing, though the customer can limit the ways the bank contacts the customer. Under its list of reasons for sharing a customer's information, the bank specifies that it will disclose "[f]or our marketing purposes—with service providers we use to offer our products and services to you (please see below to limit the ways in which we contact you)." *See, e.g.*, WELLS FARGO, *supra* note 76, at 1; *U.S. Consumer Privacy Notice*, BANK OF AM. (Jan. 2024), https://www.bankofamerica.com/security-center/consumer-privacy-notice [https://perma.cc/DR57-CZJ9]; SPACE COAST CREDIT UNION, PRIVACY POLICY 1–2 (Mar. 2020), https://www.sccu.com/SCCU/media/documents/Privacy-Policy_model-form.pdf; U.S. BANK, FINANCIAL SERVICE PLEDGE 1 (Mar. 2014), https://www.usbank.com/dam/documents/pdf/USBank_Dealer_Financial_Service_Pledge.pdf.

businesses.[119] Businesses possess specialized skills or knowledge that are helpful or necessary to our lives, and because we must turn to businesses for these specialized skills or knowledge, we have no choice but to trust them with the information provided within the commercial relationship.[120] Thus, because of the power inequities between the parties in *Miller* and *Smith*, it would be inaccurate to describe the defendant's sharing of information as voluntary.[121]

In sum, there is a stark distinction in the relationship between friends and commercial entities that affects whether the exposure of information in the relationship was truly voluntary and whether the reliance on the third party to maintain the privacy of the information was reasonable.[122] Therefore, the application of the third-party doctrine based on false friends is inapposite to the commercial entities.

B. Trust, Expectations of Confidentiality, and Privacy Recognized by Law

As previously mentioned, the availability of legal recourse is one significant reason for a person to "trust" commercial entities and disclose information during the commercial relationship.[123] Because commercial relationships are generally bound by law, a person's reliance on the confidentiality of information conveyed in that relationship is reasonable, and therefore, the expectations of privacy a person has in that information are reasonable.[124] Accordingly, the significance that law plays in supporting privacy expectations deserves further elaboration. The following Sections highlight the myriad ways in which a right to privacy has been incorporated into common law, legislation, and constitutions, reflecting the societal view that information shared with other parties is still confidential and private.[125]

---

119. Browne & Blank, *supra* note 113, at 162.

120. *Id.* at 163.

121. United States v. Miller, 425 U.S. 435, 442–43 (1976) (noting that there is no expectation of privacy when a customer deposits funds with a bank, a risk they must assume to conduct business); Smith v. Maryland, 442 U.S. 735, 744 (1979) (underscoring that customers assume the risk their information may be disclosed in the "ordinary course of business" when using a telephone line).

122. *See supra* notes 113–15 and accompanying text.

123. *See* Browne & Blank, *supra* note 113, at 157 (explaining that some scholars believe that the kind of trust that exists within friendships "is not necessary for business exchange because legally-binding written contracts preempt the need for trust to exist between buyer and seller").

124. *Id.*

125. For an excellent historical recount of the development of the right to privacy, see DAVID J. SEIPP, THE RIGHT TO PRIVACY IN AMERICAN HISTORY (1978).

An in-depth examination of each privacy measure is beyond the scope of this Article.

1. Common law privacy protections

Privacy is protected through a variety of legal sanctions and enshrined within many legal norms, whether one conceptualizes privacy as emanating from secrecy, property, confidentiality, the separation of the public from the personal, or autonomy.[126] If positive law supports a person's expectation of privacy, then how can that expectation be unreasonable? Common law has given birth to and sustained privacy expectations residing in evidence, contracts, and tort law.[127] "The common law secures to each individual the right of determining, ordinarily, to what extent his thoughts, sentiments, and emotions shall be communicated to others."[128]

Reliance on commercial entities is reasonable because they act as custodians, trustees, and fiduciaries of our information; they also guard our privacy and thereby, justify our cognitively rational

---

126. G. Michael Harvey, *Confidentiality: A Measured Response to the Failure of Privacy*, 140 U. PA. L. REV. 2385, 2403 (1992) (explaining that privacy is "essential to the preservation of 'individuality and human dignity,' 'an inviolate personality,' 'rules of civility,' or 'liberty, autonomy, selfhood, . . . human relations, and furthering the existence of a free society'" (footnotes omitted) (first quoting Edward J. Bloustein, *Privacy as an Aspect of Human Dignity: An Answer to Dean Prosser*, 39 N.Y.U. L. REV. 962, 1003 (1964); then quoting Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 211 (1890); then quoting Robert C. Post, *The Social Foundations of Privacy: Community and Self in the Common Law Tort*, 77 CALIF. L. REV. 957, 959 (1989); and then quoting Ruth Gavison, *Privacy and the Limits of Law*, 89 YALE L.J. 421, 423 (1980))); *see also* Anna Lvovsky, *Fourth Amendment Moralism*, 166 U. PA. L. REV. 1189, 1244–46 (2018) (discussing the value of privacy to include functioning "as a buttress for an individual's mental and psychological health"; "a precondition for intimate friendships and other valuable relationships"; "the bedrock of individual autonomy": "a precondition of personhood"; and "a safeguard of human dignity" (emphasis omitted)); Samuelson, *supra* note 117, at 1128 ("Those who conceive of personal data protection as a fundamental civil liberty interest, essential to individual autonomy, dignity, and freedom in a democratic civil society, often view information privacy legislation as necessary to ensure protection of this interest.").

127. Woodrow Hartzog, *Reviving Implied Confidentiality*, 89 IND. L.J. 763, 769 (2014) (explaining that "[o]bligations of confidentiality are found in multiple areas of the law, including contracts for confidentiality, the undeveloped tort of breach of confidentiality, evidentiary privileges regarding confidentiality, procedural protections like protective orders to prevent the disclosure of embarrassing personal information in court records, and statutes explicitly creating confidential relationships" (footnotes omitted)).

128. Warren & Brandeis, *supra* note 126, at 198.

expectation of privacy in the information entrusted.[129] These guardians are relied upon because they have specialized knowledge, training, or access to information.[130] One's expectation of privacy with information conveyed to custodians, trustees, and fiduciaries is justified because of the high regard given to those positions of trust[131]:

> Many forms of conduct permissible in a workaday world for those acting at arm's length, are forbidden to those bound by fiduciary ties. A trustee is held to something stricter than the morals of the market place. Not honesty alone, but the punctilio of honor the most sensitive, is then the standard of behavior . . . . Uncompromising rigidity has been the attitude of courts of equity when petitioned to undermine the rule of undivided loyalty by the "disintegrating erosion" of particular exceptions. Only thus has the level of conduct

---

129. Jack M. Balkin, *Information Fiduciaries in the Digital Age*, BALKINIZATION (Mar. 5, 2014), http://balkin.blogspot.com/2014/03/information-fiduciaries-in-digital-age.html [https://perma.cc/K5HH-NRDH] (arguing that those holding our information act as fiduciaries and have the concomitant duties of care and loyalty, which should constrain them from using our information to our detriment); Jack M. Balkin, *Information Fiduciaries and the First Amendment*, 49 U.C. DAVIS L. REV. 1183, 1186, 1204 (2016) (arguing that online service providers and cloud companies who "collect, analyze, use, sell, and distribute personal information" should act as information fiduciaries towards their customers); Kiel Brennan-Marquez, *Fourth Amendment Fiduciaries*, 84 FORDHAM L. REV. 611, 638, 647 (2015) (applying Jack Balkin's information fiduciary theory to Fourth Amendment disclosures). For example, courts have held that health insurers, hospitals, and physicians owe a fiduciary duty to keep a patient's records confidential. *See, e.g.*, Ingram v. Mut. of Omaha Ins., 170 F. Supp. 2d 907, 911 (W.D. Mo. 2001); Ari Ezra Waldman, *Privacy as Trust: Sharing Personal Information in a Networked World*, 69 U. MIAMI L. REV. 559, 600–01 (2015) (arguing that conceptualizing "privacy-as-trust, then, could create a relationship between sharers and recipients of personal data that is akin to a beneficiary-trustee, or fiduciary, relationship").

130. Hill & O'Hara, *supra* note 70, at 1759 (discussing the propensity of fiduciary duties arising when one party is dependent on another); Cross, *supra* note 82, at 1511 ("[P]rivate ordering has produced a host of guardians of trust, ranging from accountants to investment analysts and credit-rating firms.").

131. A fiduciary relationship occurs "where one person reposes special confidence in another, or where a special duty exists on the part of one person to protect the interests of another, or when there is a reposing of faith, confidence, and trust, and the placing of reliance by one person on the judgment and advise of the other." Alan B. Vickery, *Breach of Confidence: An Emerging Tort*, 82 COLUM. L. REV. 1426, 1459 (1982) (quoting 10 SAMUEL WILLISTON, THE LAW OF CONTRACTS § 1285, at 914 n.3 (1967)). Two elements are essential to a fiduciary relationship: "First, the fiduciary must have scope for the exercise of discretion, and, second, this discretion must be capable of affecting the legal position of the principal." Ernest J. Weinrib, *The Fiduciary Obligation*, 25 U. TORONTO L.J. 1, 4 (1975). Fiduciaries have the obligation to put their beneficiary's interest above their own, guard their beneficiary's confidences, act with good faith, and refrain from opportunism. Scott FitzGibbon, *Fiduciary Relationships Are Not Contracts*, 82 MARQ. L. REV. 303, 308–10 (1999).

> for fiduciaries been kept at a level higher than that trodden by the crowd.[132]

The high regard given to fiduciaries is due to the legal sanctions and strong ethical code imposed on them, which in turn reinforces our privacy expectations.[133] For example, the doctor-patient,[134] attorney-client,[135] and clergy-parishioner[136] relationships are guided by a mandate of confidentiality in matters divulged during the relationship.[137] This confidentiality is enforced by professional associations and state laws through privilege rules that restrict the introduction of evidence obtained during the professional

---

132. Frankel & Gordon, *supra* note 96, at 324 (quoting Meinhard v. Salmon, 164 N.E. 545, 546 (N.Y. 1928)).

133. "Fiduciary obligation is the highest order of duty imposed by law." Roy Ryden Anderson, *The Wolf at the Campfire: Understanding Confidential Relationships*, 53 SMU L. REV. 315, 317 (2000); Hill & O'Hara, *supra* note 70, at 1759–60.

134. The Hippocratic Oath requires a physician to swear to a duty of confidentiality: "Whatever I see or hear in the lives of my patients, whether in connection with my professional practice or not, which ought not to be spoken of outside, I will keep secret, as considering all such things to be private." *Ancient Greek Medicine*, NAT'L LIBR. OF MED., https://www.nlm.nih.gov/hmd/greek/greek_oath.html [https://perma.cc/YH8M-UGFL]. The American Medical Association additionally enforces a confidentiality code:

> Patients need to be able to trust that physicians will protect information shared in confidence. They should feel free to fully disclose sensitive personal information to enable their physician to most effectively provide needed services. Physicians in turn have an ethical obligation to preserve the confidentiality of information gathered in association with the care of the patient.

Opinion 3.2.1: Confidentiality, AM. MED. ASS'N, https://www.ama-assn.org/delivering-care/ethics/confidentiality [https://perma.cc/UVR5-8TZA].

135. The American Bar Association requires confidentially between lawyers and clients: "A lawyer shall not reveal information relating to the representation of a client unless the client gives informed consent . . . ." MODEL RULES OF PRO. CONDUCT r. 1.6 (AM. BAR ASS'N 2024). For additional discussions about the attorney-client confidentiality, see generally Geoffrey C. Hazard, Jr., *An Historical Perspective on the Attorney-Client Privilege*, 66 CALIF. L. REV. 1061 (1978), which examines the history and development of the attorney-client privilege, and Anne Klinefelter, *When to Research is to Reveal: The Growing Threat to Attorney and Client Confidentiality from Online Tracking*, 16 VA. J.L. & TECH. 1 (2011), which discusses the vulnerability of the attorney-client privilege when attorneys engage in online research.

136. "Clergy must exercise discretion and confidentiality in handling sensitive information and may not disclose confidential information to others not entitled to such information." *104 – Code of Conduct for Clergy*, ARCHDIOCESE OF SAINT PAUL & MINNEAPOLIS, https://safe-environment.archspm.org/100-ministerial-standardssafe-environment/104-code-conduct-clergy [https://perma.cc/NZ3E-9VBS] (Dec. 2016).

137. *Supra* notes 134–36 and accompanying text.

relationship.[138] "Perhaps the most signal recognition of the right of privacy is the spirit which underlies our positively declared and strictly enforced rule of law that no priest, lawyer, or physician can be compelled to testify as to matters confided to him in his professional capacity by another."[139]

The attorney-client confidentiality exists to encourage "full[] and frank[]" communications between attorneys and their clients in order for attorneys to represent their client's interest to the fullest and to foster "the trust that is the hallmark of the client-lawyer relationship."[140] Dating back to the sixteenth century when it was first recognized in common law, the attorney-client privilege is the oldest and most universally recognized privilege, spanning every state and federal jurisdiction.[141] Not only can a client depend on the attorney's

---

138. Florida, for example, provides a psychotherapist-patient privilege. FLA. STAT. § 90.503 (2024). For a history of the privilege's development, protections, and exceptions as applied to attorneys, physicians, and clergymen, see G.W. Field & John B. Uhle, *Privileged Communications*, 28 AM. L. REG. 1 (1889).

139. John Gilmer Speed, *The Right of Privacy*, 163 N. AM. REV. 64, 71 (1896) (explaining that the rule of confidentiality is not only limited to voluntary information but also covers all knowledge of a person and their affairs obtained within their professional relationship).

140. MODEL RULES OF PRO. CONDUCT r. 1.6 cmt. 2 (AM. BAR ASS'N 2024).

141. Field & Uhle, *supra* note 138, at 2 (referring to the Elizabethan era case of *Berd v. Lovelace*, 21 Eng. Rep. 33 [1577]); Hazard, *supra* note 135, at 1069; Klinefelter, *supra* note 135, at 22. In federal courts, Federal Rule of Evidence 501 protects privileges as follows:

> The common law—as interpreted by United States courts in the light of reason and experience—governs a claim of privilege unless any of the following provides otherwise:
> • the United States Constitution;
> • a federal statute; or
> • rules prescribed by the Supreme Court.
> But in a civil case, state law governs privilege regarding a claim or defense for which state law supplies the rule of decision.

FED. R. EVID. 501. The attorney-client privilege protects "legal research, legal research memoranda, and bills detailing cost and content of legal research," among other things. Klinefelter, *supra* note 135, at 25 (footnotes omitted); *see, e.g.*, *In re* Grand Jury Subpoena Duces Tecum Dated Sept. 15, 1983 v. United States, 731 F.2d 1032 (7th Cir. 1984) (protecting documents that relate to a company's request for legal advice); Kimberley-Clark Corp. v. Tyco Healthcare Retail Grp., No. 05-C-985, 2007 WL 1246411 (E.D. Wis. Apr. 27, 2007) (protecting information provided by a client to an attorney in seeking legal advice); BB&T of S.C. v. Pender, No. 2003-CP-32-0139, 2003 WL 25776071 (S.C. Ct. Com. Pl. July 16, 2003) (holding that the contents of a client's file are protected under the attorney-client privilege).

duty to keep his affairs confidential,[142] but the privilege extends to include that attorney's assistant or agent.[143] Nothing is more constant than the protection provided by the privilege for it waivers not even after a client's death.[144]

Similarly, patients have enjoyed a long history of protection for their communications with physicians as early as the 1800s.[145] Although not originating from common law, communications between physicians and patients have been afforded protection by states to encourage the flow of information necessary to allow the physician to perform her duties.[146] Like the attorney-client privilege, the patient's death does not waive the physician-patient privilege.[147]

Additionally, states began to preserve the confidentiality of clergy-penitent relationships around the 1800s, despite common law's failure to protect confessions to the clergy.[148] The clergy-penitent privilege arose from "the interests of religion, so 'that the guilty conscience may with safety disburden itself by penitential confessions, and by spiritual advice, instruction, and discipline seek pardon and relief.'"[149]

Related to privileges, privacy is also secured through confidential relationships, relationships that include a duty of nondisclosure. The

142. DeMassa v. Nunez, 770 F.2d 1505, 1508 (9th Cir. 1985) (per curiam) (holding that clients have an expectation of privacy in their client files maintained by their attorney).

143. Field & Uhle, *supra* note 138, at 4; *see also* Panasonic Commc'ns Corp. of Am. v. United States, 99 Fed. Cl. 422, 428 (2011) (extending attorney-client privilege to encompass the IRS's third-party independent contractor). "The common interest rule extends the attorney-client privilege to privileged communications revealed to a third party who shares a common legal goal with the party in possession of the original privilege." TIFD III-E, Inc. v. United States, 223 F.R.D. 47, 50 (D. Conn. 2004); *see also In re* Mortg. & Realty Tr., 212 B.R. 649, 654 (Bankr. C.D. Cal. 1997) (protecting a conversation between the debtor's executive officer and counsel and the creditor's counsel under the common interest rule for attorney-client privilege).

144. Field & Uhle, *supra* note 138, at 4. The attorney-client privilege also applies to a company's attorney and former employee, even after the employment relationship terminates. New York v. Salazar, No. 6:08-CV-0644, 2011 WL 13205947, at *5 (N.D.N.Y. June 23, 2011).

145. Field & Uhle, *supra* note 138, at 9.

146. *Id.* at 9, 16–21 (citing to cases and statutes dating back to the 1800s that provided for the physician-patient privilege).

147. *Id.* at 12.

148. *Id.* at 15, 16–21 (citing to cases and statutes dating back to the 1800s that provided for the clergy-penitent privilege).

149. *Id.* at 15.

precursor to fiduciary relationships,[150] confidential relationships, involve a person entrusting his interests to another.[151] The duty of nondisclosure imposed within confidential relationships extends broader security against protected information being divulged because it restricts disclosure to anyone, whereas privileges only preclude a witness's testimony in a judicial proceeding.[152] Physicians, psychiatrists, hospitals, attorneys, banks, insurance companies, social workers, accountants, school officials, and employees have been found to owe a duty of confidentiality.[153] Violations of the duty can give rise to a breach of confidentiality claim, which "focuses on the norms of trust"[154] that follows from a special relationship, fiduciary relationships, or an implied contract of confidentiality.[155]

In addition to the breach of confidentiality tort, expectations of privacy are supported by the invasion of privacy tort.[156] In their seminal article, *The Right to Privacy*, Samuel Warren and Louis Brandeis argued for an invasion of privacy tort,[157] drawing upon extensions in tangible and intangible property rights, spiritual rights,[158] and defamation laws.[159] Privacy, as Warren and Brandeis pointed out, is also secured

---

150. Fiduciary relationships generally imply a confidential relationship, but confidential relationships can exist without a fiduciary. 2 Ann Taylor Schwing, CALIFORNIA AFFIRMATIVE DEFENSES, § 46:3, Confidential and Fiduciary Relationships—Generally (2d ed. 2019).

151. Neil M. Richards & Daniel J. Solove, *Privacy's Other Path: Recovering the Law of Confidentiality*, 96 GEO. L.J. 123, 135 (2007).

152. *Id.*

153. Harvey, *supra* note 126, at 2399–400; Richards & Solove, *supra* note 151, at 157–58.

154. Richards & Solove, *supra* note 151, at 174.

155. *Id.* at 157 (citing Susan M. Gilles, *Promises Betrayed: Breach of Confidence as a Remedy for Invasion of Privacy*, 43 BUFF. L. REV. 1, 20–25 (1995)).

156. Warren & Brandeis, *supra* note 126, at 194.

157. *Id.* at 195 (quoting THOMAS M. COOLEY, A TREATISE ON THE LAW OF TORTS OR THE WRONGS WHICH ARISE INDEPENDENT OF CONTRACT 29 (2d ed. 1888)). Early support for Warren's and Brandeis's new tort of invasion of privacy came from notable scholars and future jurists, such as Augustus N. Hand. *See* Augustus N. Hand, *Schuyler Against Curtis and the Right to Privacy*, 45 AM. L. REG. & REV. 745 (1897) (discussing the right to privacy implications in *Schuyler v. Curtis*); SEIPP, *supra* note 125, at 76 (discussing Augustus Hand's endorsement of the right to privacy); Frederick Davis, *What Do We Mean by "Right to Privacy?"*, 4 S.D. L. REV. 1, 3 (1959) (discussing a New York Times article in favor of the right to privacy). By 1959, courts in approximately thirty states recognized the invasion of privacy tort as supported by common law, constitutional law, or natural law. Davis, *supra*, at 5. *But see* Herbert Spencer Hadley, *The Right to Privacy*, 3 NW. L. REV. 1 (1895) (arguing against the right to privacy and that Warren and Brandeis drew their theory from dicta); SEIPP, *supra* note 125, at 76 (discussing Herbert Spencer Hadley's rejection of Warren's and Brandeis's theory).

158. SEIPP, *supra* note 125, at 74.

159. Davis, *supra* note 157, at 3.

through intellectual property laws that protect information through trade secret law, patent law, and copyright law.[160] The invasion of privacy tort was created to secure "the right to be let alone" and "inviolate personality"[161] and now encompasses causes of actions against an intrusion upon a person's private affairs, disclosure of private facts, and misappropriation of a person's name or likeness.[162] States have nearly universally accepted the tort right of privacy.[163]

Tort and contract law provide several measures to protect a person's expectation of privacy and the "trust" or reliance placed with third parties. The tort of intrusion is one mechanism for enforcing privacy expectations.[164] Additionally, the breach of confidentiality tort buttresses an expectation of privacy in third parties.[165] The breach of confidentiality claim "focuses not on the *individual* or the nature of the information shared, but rather on the social *relationship* in which the information is shared."[166]

In contract law, privacy and trust are protected through a variety of measures, such as laws regulating good faith and fair dealing[167] and through an express or implied agreement of confidentiality,[168] which may overlap with the breach of confidentiality tort.[169] Courts have

---

160. Neil M. Richards, *Four Privacy Myths*, *in* A WORLD WITHOUT PRIVACY: WHAT LAW CAN AND SHOULD DO? 1, 9 (Austin Sarat ed. 2014).

161. David J. Seipp, *English Judicial Recognition of a Right to Privacy*, 3 OXFORD J. LEGAL STUD. 325, 328 (1983).

162. William L. Prosser, *Privacy*, 48 CALIF. L. REV. 383, 389 (1960).

163. Paul M. Schwartz, *Preemption and Privacy*, 118 YALE L.J. 902, 907 (2009) (attributing the root of the modern privacy law to Warren and Brandeis in their 1890 publication).

164. Waldman, *supra* note 129, at 613–14.

165. *Id.* at 622.

166. *Id.* at 617.

167. Eli Bukspan, *Trust and the Triangle Expectation Model in Twenty-First Century Contract Law*, 11 DEPAUL BUS. & COM. L.J. 379, 407 (2013) ("[C]ontract law strives to concretize the idea of interpersonal trust by means of the triangle of expectations created by each contractual promise—is clearly implicit vis-à-vis the principle of good faith."); Waldman, *supra* note 129, at 615.

168. Gilles, *supra* note 155, at 17.

169. Although torts and contracts law can intertwine when confidentiality issues occur, there are differences in how each tort arises:

> In theory, contract law enforces the expectations of parties settled in a bargained-for exchange. Tort law compensates injuries suffered at the hands of another. The obligations of the former arise from consent of the parties; the obligations of the latter are imposed by law irrespective of consent. The duty present in a confidential relationship and the injury suffered when that duty is

inferred an implied promise of confidentiality when confidential duties and contractual obligations exist in the same relationship and rely on "conduct of the parties and common usages, practices, and understandings at the time of the contracting" for making such inferences.[170] "When personal information is at issue, obligations of confidence arise out of the common notions of decency and social policy fostering the particular relationship, not out of bargained-for terms. . . . A contract, however, does frequently establish the relationship on which tort law imposes a duty of confidence."[171]

2. Legislative privacy protections

In addition to common law rights that buttress our privacy expectations, the government has passed a wide expanse of legislation to protect the privacy of information shared with others.[172] For example, early in the formation of our national government, Congress sought to instill sanctity in the privacy of letters by passing the "first organic law" of the U.S. Postal Office[173] and later levying fines against violators.[174] In 1850, the government provided for the confidentiality

---

> violated are characteristic of the duties and injuries associated with tort law and are foreign to contract law. When personal information is at issue, obligations of confidence arise out of the common notions of decency and social policy fostering the particular relationship, not out of bargained-for terms. Banks and doctors, for example, do not ordinarily offer lower rates if a customer or patient does not insist on confidentiality. A contract, however, does frequently establish the relationship on which tort law imposes a duty of confidence.
>
> The theoretical difference between contract and tort becomes especially important when there is no contract in which to imply an obligation of confidentiality.

Vickery, *supra* note 131, at 1444–45 (footnote omitted).

170. *Id.* at 1444; *see* Hartzog, *supra* note 127, at 768 (explaining that the obligation of confidentiality can be inferred from "customs, norms, and other indicia of confidentiality beyond explicit confidentiality agreements").

171. Vickery, *supra* note 131, at 1445.

172. For a historical discussion of privacy legislation, see Daniel J. Solove, *A Brief History of Information Privacy Law*, *in* PROSKAUER ON PRIVACY 1–3 (2006), http://scholarship.law.gwu.edu/cgi/viewcontent.cgi?article=2076&context=faculty_publications.

173. An Act to Establish the Post-Office and Post Roads Within the United States, ch. 7 (1792) (repealed 1810).

174. *Id.* § 16 (penalizing "unlawfully detain[ing], delay[ing], or open[ing] . . . any letter, packet, bag or mail of letters"); *see also* SEIPP, *supra* note 125, at 10, 12 (discussing the Organic Postal Act of 1825).

of information conveyed to census takers[175] and through the telegraph in 1918.[176]

The Privacy Act,[177] "a leading and influential example of a data protection law,"[178] is a prime example of legislation that recognizes people's privacy interests:

> The Privacy Act of 1974, as amended, 5 U.S.C. § 552a, establishes a code of fair information practices that governs the collection, maintenance, use, and dissemination of information about individuals that is maintained in systems of records by federal agencies. . . . The Privacy Act prohibits the disclosure of a record about an individual from a system of records absent the written consent of the individual, unless the disclosure is pursuant to one of twelve statutory exceptions.[179]

---

175. SEIPP, *supra* note 125, at 24. Confidentiality was necessary because the breadth of information collected on the census grew to encompass sensitive topics such as "capital invested, market value of products, contingent expense, wages, and composition of the labor force" and physical deformities, insanity, diseases, and debt, and the government had previously posted in public places the private facts contained in the census. *Id.* at 19, 20, 23, 44. As the following poem illustrates, people were skeptical of the census and feared governmental overreach into private spheres:

> I am a census inquisitor.
> I travel about from door to door,
> From house to house, from store to store,
> With pencil and paper and power galore.
> I do as I like and ask what I please.
> Down before me you must get on your knees;
> So open your books, hand over your keys,
> And tell me about your chronic disease.
> Are you sure you don't like it? Well, I'm not to blame;
> I do as I'm ordered. Wouldn't you do the same?
> I'm a creature of law, and work in its name
> To further the new statistical game.
> I nose from garret to cellar,
> With my last improved statistical smeller.
> If the housewife objects I loftily tell her,
> "I'm a socialistic government feller."

Id. at 27.

176. *Id.* at 65.

177. 5 U.S.C. § 552a.

178. David H. Flaherty, *On the Utility of Constitutional Rights to Privacy and Data Protection*, 41 CASE W. RSRV. L. REV. 831, 834 (1991).

179. *Privacy Act of 1974*, U.S. DEP'T OF JUSTICE, https://www.justice.gov/opcl/privacy-act-1974 [https://perma.cc/5JZQ-TVQG] (Oct. 4, 2022). *See generally Privacy Act of 1974, 5 U.S.C. § 552a*, U.S. DEP'T OF JUSTICE, https://it.ojp.gov/PrivacyLiberty/authorities/

Among its protective provisions, the Privacy Act restricts dissemination of information to others outside of the agency unless for routine use.[180] As one of the Privacy Act's cosponsors explained, "When

---

statutes/1279 [https://perma.cc/N9KV-L6JW] (providing background and summary on the Privacy Act).

> In 1974, Congress was concerned with curbing the illegal surveillance and investigation of individuals by federal agencies that had been exposed during the Watergate scandal; it was also concerned with potential abuses presented by the government's increasing use of computers to store and retrieve personal data by means of a universal identifier—such as an individual's social security number.
>
> Broadly stated, the purpose of the Privacy Act is to balance the government's need to maintain information about individuals with the rights of individuals to be protected against unwarranted invasions of their privacy stemming from federal agencies' collection, maintenance, use, and disclosure of personal information about them . . . . The Act focuses on four basic policy objectives:
> 1. To restrict disclosure of personally identifiable records maintained by agencies.
> 2. To grant individuals increased rights of access to agency records maintained on them.
> 3. To grant individuals the right to seek amendment of agency records maintained on themselves upon a showing that the records are not accurate, relevant, timely, or complete.
> 4. To establish a code of "fair information practices" which requires agencies to comply with statutory norms for collection, maintenance, and dissemination of records.

Privacy Act of 1974, 5 U.S.C. § 552a, supra. The Privacy Act provides the following exemptions: use of information by the Census Bureau and the Bureau of Labor Statistics, routine uses when sharing information outside the agency, archival purposes for records with historical value, law enforcement purposes, congressional investigations, and other administrative purposes. 5 U.S.C. § 552a(b); *Privacy Act of 1974, 5 U.S.C. § 552a, supra*. The Computer Matching and Privacy Act of 1988, 5 U.S.C. § 552a(b), amended the Privacy Act of 1974 to cover government use of automated matching programs and provide procedural protections. 5 U.S.C. § 552a(b); *Privacy Act of 1974, 5 U.S.C. § 552a, supra*.

180. 5 U.S.C. § 552a(b). On occasion, government disclosure does not satisfy the routine use exemption under the Privacy Act. *See* Swenson v. U.S. Postal Service, 890 F.2d 1075, 1078 (9th Cir. 1989) (invalidating the Postal Service's disclosure of a mail carrier's information to congressmen after the carrier sent a letter to the congressmen requesting an investigation); Covert v. Harrington, 876 F.2d 751, 756 (9th Cir. 1989) (invalidating the Department of Energy's disclosure of personnel security file to the Department of Justice); Britt v. Naval Investigative Serv., 886 F.2d 544, 550 (3d Cir. 1989) (holding that Naval Investigative Service's disclosure matters relating to an investigation of a special agent to the Immigration and Naturalization Service was improper); Tijerina v. Walters, 821 F.2d 789, 800 (D.C. Cir. 1987) (concluding that the Veterans Administration's disclosure to the Texas Board of Law Examiners was prohibited by the Privacy Act); Cooper v. Fed. Aviation Admin., 816 F. Supp. 2d 778,

personal data collected by one organization for a stated purpose is used and traded by another organization for a completely unrelated purpose, individual rights could be seriously threatened."[181] The Privacy Act was "intended to discourage the unnecessary exchange of information to another person or to agencies who may not be as sensitive to the collecting agency's reasons for using and interpreting the material."[182] By limiting the dissemination of information between agencies, the government acknowledges a privacy interest in the information that it—a third party—holds.[183] The Privacy Act provides a reasonable basis to form an expectation of privacy in one's information being held by the government because that information can be restricted from disclosure to others even though they are operating in the same branch of government.[184]

In addition to the broad privacy protections afforded by the Privacy Act, the government has passed agency-specific legislation that enhances the privacy of people's information held by each agency. For example, the Internal Revenue Code prohibits Internal Revenue Service (IRS) employees from disclosing people's tax returns: "Returns and return information shall be confidential, and except as authorized by this title—(1) no officer or employee of the United States . . . shall disclose any return or return information obtained by him."[185] Courts have sanctioned the IRS for violating the disclosure law, even when the

---

790 (N.D. Cal. 2008), *aff'd*, 566 U.S. 284 (2012) (invalidating the Social Security Administration's disclosure to the Department of Transportation that a certified pilot received disability payments). *But see* Pippinger v. Rubin, 129 F.3d 519 (10th Cir. 1997) (holding that the Treasury's disclosure of the plaintiff's romantic relationship with a subordinate detailed in his personnel files fell within the "need to know" and "routine use" exceptions to the Privacy Act); Long v. United States, 972 F.2d 1174 (10th Cir. 1992) (concluding that the IRS may disclose the tax return information of taxpayers who have received jeopardy assessments when sending liens and levies to financial institutions in efforts to collect the taxpayer's income tax); Ash v. United States, 608 F.2d 178, 180 (5th Cir. 1979), *cert. denied*, 445 U.S. 965 (1980) (validating the Navy's publication of the plaintiff's name, offense, and punishment in the daily bulletin of his command when the plaintiff was punished for possessing marijuana in an open nonjudicial proceeding as a "routine use" under the Privacy Act).

181. 120 CONG. REC. 36893–94 (1974) (statement of Senator Percy); Britt v. Naval Investigative Servs., 886 F.2d 544, 550 (3d Cir. 1989) (summarizing the legislative history of the Privacy Act).

182. Analysis of House and Senate Compromise Amendments to the Federal Privacy Act, *reprinted in* 120 CONG. REC. 40405–06 (1974).

183. 120 CONG. REC. 40406 (1974).

184. *Id.*

185. 26 U.S.C. § 6103.

IRS disseminated information that was already in public records, like criminal convictions.[186] Additionally, "Congress has declared that a taxpayer who . . . has placed his or her tax return information in the custody of a professional tax preparer retains an expectation of privacy in such information."[187]

More recent legislation also provides people with increased privacy protections. For example, in 2015, Congress passed the United and Strengthening America by Fulfilling Rights and Ensuring Effective Discipline Over Monitoring Act[188] (FREEDOM Act) to prohibit the direct collection and maintenance of phone records, a practice previously permitted under the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism[189] (PATRIOT Act).[190] The Electronic Communications

---

186. *See, e.g.*, Mallas v. United States, 993 F.2d 1111, 1120 (4th Cir. 1993) (relying on *Reporters Committee* to invalidate the IRS's republication of information previously disclosed in public records).

187. People v. Gutierrez, 222 P.3d 925, 935–36 (Colo. 2009) (en banc) (suppressing evidence obtained from the defendant's tax file that was seized from the tax preparer's office because "a taxpayer who entrusts his tax return to the care of a tax preparer for purposes of complying with federal and state tax law does not assume the risk that the tax preparer will voluntarily divulge the information to law enforcement").

188. Pub. L. No. 114-23, 129 Stat. 268 (codified as amended in sections 12, 15, 18, and 50 of the U.S.C.); Mary-Kathryn Takeuchi, *A New Third-Party Doctrine: The Telephone Metadata Program and* Carpenter v. United States, 95 NOTRE DAME L. REV. 2243, 2256 (2019) (explaining that the FREEDOM Act prohibits the government from "directly collect[ing] and maintain[ing] the phone records of U.S. citizens" without a warrant from the Foreign Intelligence Surveillance Court).

189. Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act, Pub. L. No. 107-56, 115 Stat. 287 (2001).

190. The FREEDOM Act came into existence

> [i]n 2014, [when] the Office of the Director of National Intelligence and the Department of Justice recommended to the President an approach that would end the National Security Agency's (NSA) bulk telephony metadata program conducted under Section 215 of the USA PATRIOT Act, while preserving key capabilities and strengthening privacy protections. That approach was enshrined in the USA FREEDOM Act of 2015, which directs that the United States Government will no longer collect telephony metadata records in bulk under Section 215 of the USA PATRIOT Act, including records of both U.S. and non-U.S. persons.

Fact Sheet: Implementation of the USA Freedom Act of 2015, OFF. OF THE DIR. OF NAT'L INTELLIGENCE, https://www.intelligence.gov/index.php/ic-on-the-record-database/results/787-fact-sheet-implementation-of-the-usa-freedom-act-of-2015 (last visited Oct. 5, 2024); Takeuchi, *supra* note 188, at 2256 (discussing the FREEDOM Act) (first citing Steven Nelson, *Senate Passes Freedom Act, Ending Patriot Act Provision Lapse*, U.S. NEWS & WORLD REP. (June 2, 2015); and then citing Robert Hackett, *No, NSA Phone Spying Has Not Ended*, FORTUNE (Dec. 1, 2015)).

Privacy Act of 1986[191] protects against monitoring online activity. Additionally, Congress has enacted privacy laws regulating information obtained by specialized markets and services: Health Insurance Portability and Accountability Act of 1996[192] (HIPAA) provides privacy for health care and medical information; Children's Online Privacy Protection Rule[193] (COPPA) protects children under the age of thirteen against the online collection of their personal information; Family Educational Rights and Privacy Act[194] (FERPA) enhances the privacy of students' information; Fair Credit Reporting Act safeguards consumers' credit information;[195] Gramm-Leach-Bliley Act protects financial information;[196] Right to Financial Privacy Act of 1978[197] overturned *Miller* by extending privacy to customers' records held by financial institutions;[198] Cable Communications Policy Act of 1984 ensures privacy for cable records and viewing habits;[199] Video Privacy Protection Act of 1988[200] provides privacy protection for video rental records; and Driver's Privacy Protection Act of 1994[201] prohibits selling drivers' motor vehicle records. Moreover, Congress passed a resolution designating January 28th as National Data Privacy Day.[202]

---

191. 18 U.S.C. §§ 2510–23, 2701–13, 3121–27. The Stored Communications Act (SCA), 18 U.S.C. §§ 2701–13, is Title II of the Electronic Communications Privacy Act and they are commonly referred to collectively as the Electronic Communications Privacy Act. The SCA amended a previous privacy law, which only covered the interception of telephone lines, but did not apply to the interception of online communications.

192. Pub. L. No. 104-191, § 264, 110 Stat. 1936 (codified as amended in scattered titles of the U.S.C.).

193. 15 U.S.C. § 6501.

194. 20 U.S.C. § 1232g.

195. 15 U.S.C. § 1681b.

196. *Id.* §§ 6801–09.

197. 12 U.S.C. §§ 3401–22.

198. FED. RSRV., RIGHT TO FINANCIAL PRIVACY ACT 1 (2006), https://www.federalreserve.gov/boarddocs/supmanual/cch/priv.pdf (explaining "[i]t was principally in response to this decision [*Miller*] that the Right to Financial Privacy Act was enacted"); United States v. Miller, 425 U.S. 435, 437 (1976).

199. 47 U.S.C. § 551.

200. 18 U.S.C.A. § 2710(b)(2)(B) (West Supp. 2013).

201. *Id.* § 2721(b)(12).

202. S. Res. 337, 113th Cong. (2014). "The Council in Europe first initiated Data Privacy Day in 2007. Their mission grew to a global platform. In 2009, the United States House of Representatives recognized National Data Privacy Day. The United States Senate later recognized Data Privacy Day in 2010 and 2011." *Data Privacy Day – January 28*, NAT'L DAY CALENDAR, https://nationaldaycalendar.com/data-privacy-day-january-28 (last visited Oct. 1, 2024).

Ironically, the government also prizes maintaining privacy and confidentiality in its own affairs.[203] While the National Security Agency (NSA) compiles vast databases of personal information regarding people in the United States and abroad, it demands privacy for its internal operations, which remained in the shadows until Edward Snowden leaked information about the NSA's surveillance.[204] The NSA achieved security and privacy in its affairs through the "secret FISA court, the 'gag orders' placed upon recipients of National Security Letters and orders pursuant to section 215 of the Patriot Act, and many other legal measures."[205]

Along with federal legislative efforts, states have adopted innovative privacy legislation that residents have come to rely upon for their privacy protection.[206] Forty-five states, Puerto Rico, the Virgin Islands, and the District of Columbia have enacted laws requiring notifications of data security breaches.[207] California has been a pioneer of privacy protection by passing the California Online Privacy Protection Act[208] (CalOPPA), "[t]he first state law in the nation to require commercial websites and online services to post a privacy policy."[209]

3. Constitutional privacy protections

Warren and Brandeis's visions of privacy laws are recognized in constitutional law as well. Beginning with *Griswold v. Connecticut*[210] and *Eisenstadt v. Baird*,[211] the U.S. Supreme Court affirmed that "the existence of a right of privacy against the state predat[es] the Bill of Rights."[212] The Court "has expanded the notion of privacy, in the area

---

203. Richards, *supra* note 160, at 10.

204. *Id.*

205. *Id.*; Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act, Pub. L. No. 107-56, 115 Stat. 287 (2001).

206. Schwartz, *supra* note 163, at 917.

207. *Id.*

208. CAL. BUS. & PROF. CODE §§ 22575–79 (West 2024). "The California Online Privacy Protection Act of 2003 (CalOPPA), the first law in the nation with a broad requirement for privacy policies, is a privacy landmark." HARRIS, *supra* note 97, at 1.

209. *California Online Privacy Protection Act (CalOPPA)*, CONSUMER FED'N OF CAL. EDUC. FOUND. (July 29, 2015), https://consumercal.org/about-cfc/cfc-education-foundation/california-online-privacy-protection-act-caloppa-3 [https://perma.cc/ Z9BJ-TUDU].

210. 381 U.S. 479 (1965).

211. 405 U.S. 438 (1972).

212. Flaherty, *supra* note 178, at 838 (discussing Justice Douglas's opinion in *Griswold v. Connecticut*).

of sexual freedom,[213] to be synonymous with individual autonomy 'or, indeed, with freedom itself'; moreover, the Court has characterized unreasonable searches, forced disclosure of membership in associations[214] and prohibitions on the possession of obscene matter[215] as invasions of privacy."[216] In *Whalen v. Roe*,[217] although it upheld the state statute requiring the collection of prescription drug information, the Court recognized a constitutionally protected interest in information privacy.[218]

Privacy considerations were also paramount in the early debates that sought to define the limits of government searches, which "emphasized an individual's interest in his commercial pursuits and personal papers more than his intimate or familial bonds."[219] These debates

> focused especially on *papers*, including business letters, as man's "dearest property": windows into an individual's "secret thoughts," the seizure of which was "least capable of reparation." What could be "more excruciating torture," demanded one widely read pamphleteer, than to have the government intrude upon one's "secret correspondences," whether between a husband and his wife, a "lawyer [and] his clients," or a "merchant . . . and his correspondents"?[220]

In addition to privacy protections recognized in the federal Constitution, eleven states—Alaska, Arizona, California, Florida, Hawaii, Illinois, Louisiana, Montana, New Hampshire, South Carolina, and Washington—have explicitly protected the right to privacy in their

---

213. Griswold v. Connecticut, 381 U.S. 479 (1965). Through *Griswold v. Connecticut* and *Eisenstadt v. Baird*, the Court has recognized sexual liberty and autonomy. But some have pointed out that these cases establish other types of liberty interests and do not fit within the scope of privacy based on information or intrusion into places. *See, e.g.*, Ronald A. Cass, *Privacy and Legal Rights*, 41 CASE W. RSRV. L. REV. 867, 875–76 (1991).

214. NAACP v. Alabama, 357 U.S. 449, 466 (1958) (protecting the NAACP's membership list against compelled disclosure).

215. Stanley v. Georgia, 394 U.S. 557, 568 (1969) (upholding a First Amendment privacy right to privately possess obscene material).

216. Seipp, *supra* note 161, at 330; *see also* Monu Bedi, *Facebook and Interpersonal Privacy: Why the Third Party Doctrine Should Not Apply*, 54 B.C. L. REV. 1, 39 (2013) (discussing the development of interpersonal privacy); Anna Lvovsky, *Fourth Amendment Moralism*, 166 U. PA. L. REV. 1189, 1197–98 (2018) (discussing development of the Court's "substantive privacy jurisprudence").

217. 429 U.S. 589 (1977) (deciding on the issue of whether New York may record personal information of all people who have obtained certain legal and illegal drugs, depending on the market, in a centralized computer system).

218. *Id.* at 599–600.

219. Lvovsky, *supra* note 216, at 1216.

220. *Id.* at 1213 (alterations in original) (footnotes omitted).

constitutions.[221] The California Constitution, for example, provides that "[a]ll people are by nature free and independent, and have certain inalienable rights, among which are those of enjoying and defending life and liberty; acquiring, possessing, and protecting property; and pursuing and obtaining safety, happiness, and privacy."[222] Florida affords "[e]very natural person . . . the right to be let alone and free from governmental intrusion into the person's private life" in its constitution.[223] Hawaii elevates the right to privacy to the highest order by requiring a governmental showing of compelling interest before it may be infringed.[224]

Thus, our expectations of privacy have been entrenched in the security afforded by common law and legislation and are justified by the rich history and accumulation of these common law and legislative protections. Common law and legislation provide the justifications for privacy in the Fourth Amendment, but they do not replace the need to have privacy guaranteed within the Fourth Amendment by placing information given to others beyond the third-party doctrine's boundary.[225]

4. International privacy protections

The need for and concern over privacy is not a uniquely American development. In fact,

> [p]rivacy is a fundamental human right recognized in the UN Declaration of Human Rights, the International Covenant on Civil and Political Rights and in many other international and regional treaties. . . . Nearly every country in the world recognizes a right of privacy explicitly in their Constitution. At a minimum, these provisions include rights of inviolability of the home and secrecy of communications. Most recently-written Constitutions such as South Africa's and Hungary's include specific rights to access and control one's personal information.[226]

---

221. JON L. MILLS, PRIVACY: THE LOST RIGHT app. II (2008). For the text of each state's constitutional privacy provision, see *id.*

222. Flaherty, *supra* note 178, at 837 (citing CAL. CONST. art. I, § 1).

223. FLA. CONST. art. I, § 23.

224. HAW. CONST. art. I, § 6 ("The right of the people to privacy is recognized and shall not be infringed without the showing of a compelling state interest.").

225. Michael W. Price, *Rethinking Privacy: Fourth Amendment "Papers" and the Third-Party Doctrine*, 8 J. NAT'L SEC. L & POL'Y 247, 247 (2018) (asserting "Congress has not stepped in to fill the void" regarding privacy protections of data processed by third parties).

226. David Banisar & Simon Davies, *Privacy and Human Rights: An International Survey of Privacy Laws and Practice*, GLOB. INTERNET LIBERTY CAMPAIGN, http://gilc.org/

The respect and protection afforded to privacy, in some respects, extends more broadly elsewhere in the world than in America. England, for example, has long recognized privacy in shared information through the breach of confidentiality.[227] Although England has not adopted the invasion of privacy tort as in America,[228] the English breach of confidence tort covers relationships where the duty of confidentiality is implied or situations where a person tells another that the information is being given "in confidence."[229] Aside

---

privacy/survey/intro.html [https://perma.cc/2K73-PEBU] (reporting the privacy protections afforded in fifty countries); *accord* Seipp, *supra* note 161, at 325 (acknowledging the international recognition of the right to privacy).

227. Harvey, *supra* note 126, at 2396.

228. Davis, *supra* note 157, at 4; Gilles, *supra* note 155, at 6; Harvey, *supra* note 126, at 2392–93 ("Though England has recognized a similar breach of confidence doctrine as the basis of privacy protection in that country, American courts and commentators have rejected such an approach primarily because it would be redundant with the invasion of privacy tort, it would present a myriad of practical and constitutional difficulties, and it would be under-protective of privacy interests.").

229. Harvey, *supra* note 126, at 2392; *see also* Gilles, *supra* note 155, at 10; Vickery, *supra* note 131, at 1453. Although Warren and Brandeis rejected the breach of confidence tort as being too narrow, the English approach to breach of confidence imposes liability where American courts have been reluctant to venture so far. Warren & Brandeis, *supra* note 126, at 211; Harvey, *supra* note 126, at 2392–93. American courts have limited the tort of disclosure of private facts, for example, by allowing the press to publish truthful information of significant public interest if the information was lawfully obtained, whereas the English courts would likely preclude publication through a breach of confidence claim. *See, e.g.*, Smith v. Daily Mail Publ'g Co., 443 U.S. 97, 103 (1979) (holding "if a newspaper lawfully obtains truthful information about a matter of public significance then state officials may not constitutionally punish publication of the information, absent a need to further a state interest of the highest order"). *Compare* Florida Star v. B.J.F., 491 U.S. 524, 533 (1989) (upholding a newspaper's right under the First Amendment to publish a rape victim's name obtained from a publicly released police report), *Smith*, 443 U.S. at 103 (vindicating a newspaper's First Amendment right to publish the name of a juvenile suspected for murder when the newspaper lawfully obtained the information), Landmark Commc'ns, Inc. v. Virginia, 435 U.S. 829, 838 (1978) (upholding a newspaper's publication under the First Amendment of details of a judicial disciplinary hearing that was considered confidential under state law and the Constitution), Okla. Publ'g Co. v. Dist. Ct. In & For Okla. Cty., 430 U.S. 308, 311–12 (1977) (allowing publication of a juvenile murder suspect's name and photograph that were obtained when reporters were permitted to be present at the hearing), *and* Cox Broad. Corp. v. Cohn, 420 U.S. 469, 491 (1975) (permitting publication of a rape victim's name that was obtained from public records against an invasion of privacy claim), *with* Stephens v. Avery [1988] 1 Ch. 477, 482 (Eng.) (applying a legally enforceable duty of confidence to protect discussion of sexual activities between friends). *See also* Harvey, *supra* note 126, at 2404 n.106 (discussing U.S. cases involving publication of private facts). The invasion of privacy tort's growth has been stunted because of countervailing First

from the typical confidential relationships between doctor-patient, attorney-client, clergy-penitent, and employer-employee, a breach of confidence claim reaches even information shared between friends when confidence has been requested and not explicitly refused.[230] English courts apply the breach of confidence tort to restrain not only the original party who received information in confidence, but also any third party who might have received the information innocently, as long as the third party knows the information was originally conveyed in confidence.[231] For example, English courts have protected the privacy of shared information by giving a right to someone who writes a letter to prevent the recipient from publishing the contents of the letter.[232]

The English courts have established boundaries providing privacy rights around private property, confidential communications, personal information, and the publication of embarrassing or annoying personal information.[233] In addition to the ability to exclude others from one's property, the English courts interpreted privacy to afford a person "'a right to keep his own sentiments' and 'a right to judge whether he will make them public, or commit them only to the sight of his friends.'"[234] Like in America, England enacted legislation to protect communications through the telegraph and telephone.[235]

Amendment concerns, but those First Amendment concerns are not implicated in cases involving the third-party doctrine. Even when the press has a First Amendment interest in obtaining publicly available information, such as the rap sheet that the FBI compiled based on prior public records in *U.S. Department of Justice v. Reporters Committee for Freedom of the Press*, 489 U.S. 749 (1989), the Court has recognized a privacy concern even in matters that had at one time been publicly disclosed.

230. Gilles, *supra* note 155, at 13 (citing Stephens v. Avery [1988] 1 Ch. 447, 479 (Eng.); Andersen Consulting v. CHP Consulting Ltd. 1991 Ch. (July 26, 1991) (LEXIS, Enggen library)); Harvey, *supra* note 126, at 2396.

231. Gilles, *supra* note 155, at 12 (citing Fraser v. Evans [1969] 1 Q.B. 349, 361 (Eng.)); *see also* COMMITTEE ON PRIVACY AND RELATED MATTERS, REPORT OF THE COMMITTEE ON PRIVACY AND RELATED MATTERS, 1990, Cm. 1102, ¶ 8.13–8.16 (UK) (surveying the practice of granting injunctions against third parties for the breach of confidence tort in England, Wales, and Scotland).

232. *See* Seipp, *supra* note 161, at 338 (discussing Thurston v. Charles (1905) 21 TLR 659); Speed, *supra* note 139, at 67 (citing Pope v. Curl, 1741); Wilbur Larremore, *The Law of Privacy*, 12 COLUM. L. REV. 693, 704 (1912) (discussing *Baker v. Libbie*); Baker v. Libbie, 210 Mass. 519 (1912) (prohibiting copies of a letter from being reproduced and recognizing the rights held by the writer but permitting the recipient to sell the actual letters).

233. Seipp, *supra* note 161, at 333.

234. *Id.* at 334, 338.

235. *Id.* at 339.

Through its 1984 Data Protection Act,[236] and later amended 2018 Data Protection Act, England imposed strict rules on information and data collection, retention, and processing.[237]

Other European countries also fortify privacy protections through their regulations and constitutions.[238] The European Union, for example, adopted the General Data Protection Regulation.[239] According to the Human Rights Watch organization, "The European Union General Data Protection Regulation (GDPR) is one of the strongest and most comprehensive attempts globally to regulate the collection and use of personal data by both governments and the private sector."[240] The GDPR requires companies to obtain consumers' consent for the collection of their personal data, restricts the collection to only necessary information, mandates that information be deleted when it is no longer necessary to maintain it, and imposes hefty penalties of up to twenty million euros or 4% of annual global revenue, whichever is greater.[241] Additionally, the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data,[242] instituted by the Committee of Ministers of the Council of Europe, prescribes restrictions on collection of personal information through automated processing.[243]

Apart from the privacy recognized and protected by the European Union collectively, various countries have also incorporated such measures within the country's specific laws.[244] "Germany has a scheme of integrated privacy and data protection laws at the federal and state

---

236. Data Protection Act 1984, c.35, http://www.legislation.gov.uk/ukpga/1984/35/pdfs/ukpga_19840035_en.pdf; Flaherty, *supra* note 178, at 834.

237. Data Protection Act 2018, c.12, https://www.legislation.gov.uk/ukpga/2018/12/enacted [https://perma.cc/ZPP5-747J].

238. *See* Samuelson, *supra* note 117, at 1142 ("[T]he civil right conception of personal data protection is predominant in Europe.").

239. Council Regulation 2016/679, On the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), 2016 O.J. (L 119) 1; *see also The EU General Data Protection Regulation*, HUM. RTS. WATCH (June 6, 2018), https://www.hrw.org/news/2018/06/06/eu-general-data-protection-regulation [https://perma.cc/FSG4-SQYF] (providing answers to common questions about the EU's General Data Protection Regulation).

240. *The EU General Data Protection Regulation*, *supra* note 239.

241. *Id.*

242. Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, Jan. 28, 1981, E.T.S. No. 108.

243. Seipp, *supra* note 161, at 353.

244. Flaherty, *supra* note 178, at 841.

levels, based on constitutional language and judicial decisions, that is a model for federal systems offering protection for personal privacy."[245] The German Constitution provides that "'[e]veryone has the right to the free development of his personality,'" which the German courts have affirmed includes a right to privacy.[246] "The law of France, which follows the rule of the Roman Code, has explicitly declared the right of privacy."[247] Switzerland "unequivocally guarantee[s] privacy."[248] Since the nineteenth century, Scotland has recognized a right against invasion of privacy.[249] In Canada, Quebec, Ontario, Alberta, British Columbia, Manitoba, and Saskatchewan have accorded privacy rights through civil law and statutes.[250]

Thus, the need for privacy is universal, and people have come to rely on the privacy protections given to them through constitutions, the common law, and legislation. These protections are evidence that an expectation of privacy in shared information is a reasonable one that society is prepared to respect. History is replete with examples of laws and norms across the world reflecting societal expectations of privacy in shared information.[251] Just as Warren and Brandeis argued "for the recognition of the right of privacy as a mere extension of principles already fully engrafted upon the law—principles which are themselves departures from the crude notions of our unenlightened ancestors,"[252] the extension of the right to privacy in information shared with others to the third-party doctrine is a natural extension of that right as currently recognized throughout common law, legislation, constitutions, and societal norms. The third-party doctrine is a grievous departure from the privacy rights long embedded in common law, legislation, constitutions, and societal norms that recognize "[t]he laws of the land are intended not only to preserve the person and material property of every citizen

245. *Id.* For more information about the German and European Union approaches to privacy laws, see Schwartz, *supra* note 163, at 909–11.

246. Flaherty, *supra* note 178, at 841.

247. Speed, *supra* note 139, at 66; *see also* Flaherty, *supra* note 178, at 843–52 (discussing the development of privacy laws in Canada).

248. Spiros Simitis, *Privacy—An Endless Debate?*, 98 CALIF. L. REV. 1989, 1990–91 (2010).

249. Seipp, *supra* note 161, at 366.

250. *Id.* at 367.

251. Matthew Tokson & Ari E. Waldman, *Social Norms in Fourth Amendment Law*, 120 MICH. L. REV. 265, 274 (2021) (discussing how the Supreme Court often applies social norms in determining the Fourth Amendment's scope of privacy protections).

252. W. M. Lile, *Editorial*, 5 VA. L. REG. 709, 711 (1900).

sacred from intrusion, but to secure the privacy of his thoughts, so far as he sees fit to withhold them from others."[253]

CONCLUSION

The third-party doctrine developed from cases about false friends, where criminals are betrayed by other criminals or duped by undercover agents, but its application to commercial relationships and business transactions has unmoored it from these origins. The doctrine's extension to business records is oblivious to the obvious dichotomy between commercial and personal relationships and the trust and expectations of privacy that reside within these distinct relationships.

A third-party doctrine based on the concept of false friends, that there is no expectation of privacy in what we share with friends, is consonant with our commonsense understanding of personal relationships. The fact that one cannot always rely on friends to keep his information private is a lesson learned as early as kindergarten, when a child first experiences the betrayal of his friend who has "tattle taled" or "told on him." Additionally, the false friends paradigm would work to discourage trust where needed—among criminals. Under a false friends paradigm of the third-party doctrine, the trust between criminals would enjoy no protection because there is no reasonable reliance on criminal cohorts to keep the information private. This application would also comport with our commonsense notion that one cannot trust a criminal.

At the same time, a false friends paradigm where commercial and professional relationships are not subject to the third-party doctrine and where the privacy of information shared in commercial and professional relationships is protected would be consonant with our understanding of business interactions and relationships. The availability of legal recourse, institutional norms, and the incentive of businesses and professionals to uphold their reputation buttress a person's reasonable reliance on businesses and professionals and expectation of privacy in the information disclosed during the relationship. Commercial relationships operate with a higher expectation of privacy between the business entity and person because these relationships are protected by regulations, institutional norms, and independent auditors. We enter commercial relationships with a reasonable expectation of privacy because such expectations are enforceable through legal recourse. Common law, constitutions, and

253. SEIPP, *supra* note 125, at 13 (quoting a Postal Office special agent).

federal, state, and international law support our expectations of privacy within commercial relationships and business transactions. The third-party doctrine's treatment of commercial relationships as consonant with personal relationships ignores common sense, and the doctrine should be applied strictly to personal relationships because we know, intuitively and legally, that businesses are more than friends.