

THE YALE LAW JOURNAL

ANDREW J. DEFILIPPIS

Securing Informationships: Recognizing a Right to Privity in Fourth Amendment Jurisprudence

ABSTRACT. This Note argues for judicial recognition of a Fourth Amendment right to privity, conceived broadly as a right to make limited disclosure of one's personal information without surrendering the constitutional privacy interests that attach to it. In particular, this Note challenges the so-called third-party doctrine, which holds that when individuals disclose information to a third party, they retain no constitutional protection against government searches of that information. It argues that a privity right is essential for people to be secure in their "papers," particularly in a world increasingly defined by "informationships," or relationships formed around shared access to and exchange of personal information.

AUTHOR. Yale Law School, J.D. expected 2006. Princeton University, Woodrow Wilson School of Public and International Affairs, B.A. 2003. I would like to thank Marah Stith, my lead editor, for her tireless work and invaluable contributions. Thanks to Aaron Crowell, Justin Florence, Jack Balkin, Daniel Fernandez, and Charles Korsmo for their insightful comments on previous drafts of this Note. Most of all, thanks to my family, whose support is the reason for anything I do that is considered noteworthy.



NOTE CONTENTS

INTRODUCTION	1088
I. THE PITFALLS OF PRIVACY	1091
A. The Secrecy Paradigm	1091
B. Privity and Informationships	1094
II. A FLAWED THIRD-PARTY DOCTRINE	1097
A. Searches for Information	1097
B. Evaluating the Current Framework	1102
III. A PROPOSED FRAMEWORK	1108
A. A New Test	1109
B. Categories of Information	1111
1. Information Disclosed by Necessity	1112
2. Information Disclosed After Solicitation	1115
3. Information Created by Aggregation	1116
C. Practical Effects	1118
1. Enhanced Protection	1118
2. Outside the Fourth Amendment	1119
CONCLUSION	1120

INTRODUCTION

In a scene from Steven Spielberg's movie *Minority Report*, the main character walks into a clothing store and is greeted immediately by a pleasant voice. "Hello, Mr. Yakamoto! Welcome back to the Gap. How'd those assorted tank tops work out for you?"¹ Two things are striking about the scene. First, the pleasant voice comes not from a store clerk, but from a digital figure reciting information from the recesses of a vast computer database. Second, Yakamoto is not the name of the main character. Rather, in a gruesome twist, Mr. Yakamoto's eyes have been surgically removed and transplanted into the protagonist, who seeks to evade recognition of the eye-scanners that constantly record his identity. In Spielberg's imagined society, a seamless web of private- and public-sector databases aids the Department of Pre-Crime as it attempts to detect and prevent every illegal act.

Digital manifestations of identity, information, and surveillance—both on-screen and off—are rendering privacy a simplistic and incomplete lens through which to view problems of information control. The extent to which individuals may control the flow of data and information about themselves depends on relational norms governing the disclosure and use of that information. Yet privacy analysis as it has commonly been applied undercuts these relational components. The term privacy is little more than a convenient catch-all that courts and civil liberties advocates wave with frighteningly little precision.² To say that information should be "kept private" is to say very little.³ On the one hand, one can interpret such a statement to be synonymous with an expectation of total secrecy.⁴ On the other hand, one can construe it as conferring a more limited set of restrictions on the collection, use, and subsequent disclosure of information.⁵ The word itself is meaningless unless we ask "from whom" and "for whom" the information is being held.

1. MINORITY REPORT (Dreamworks Pictures & Twentieth Century Fox 2002).

2. For a full discussion of the linguistic inadequacies of current privacy terminology, see Daniel J. Solove, *A Taxonomy of Privacy*, 154 U. PA. L. REV. (forthcoming 2006). See also Tom Gerety, *Redefining Privacy*, 12 HARV. C.R.-C.L. L. REV. 233, 234 (1977); Judith Jarvis Thomson, *The Right to Privacy*, in PHILOSOPHICAL DIMENSIONS OF PRIVACY: AN ANTHOLOGY 272, 272 (Ferdinand David Schoeman ed., 1984); James Q. Whitman, *The Two Western Cultures of Privacy: Dignity Versus Liberty*, 113 YALE L.J. 1151, 1153-54 (2004).

3. See Whitman, *supra* note 2, at 1153-54.

4. See Solove, *supra* note 2 (manuscript at 35); see also Ronald A. Cass, *Privacy and Legal Rights*, 41 CASE W. RES. L. REV. 867, 867-70 (1991).

5. See, e.g., Jerry Kang, *Information Privacy in Cyberspace Transactions*, 50 STAN. L. REV. 1193, 1203 (1998).

This Note argues for recognition of a right to privity as a freedom implied by the Fourth Amendment's prohibition against unreasonable searches and seizures. In particular, it argues against the prevailing third-party doctrine, which holds that as long as information has been disclosed to a third party, individuals retain no constitutional privacy interest in it.⁶ Courts should abandon this paradigm in favor of a framework that affirms the right of individuals to make limited disclosure of their personal information (their "papers," in the words of the Fourth Amendment) without presumptively surrendering the protection of the Constitution's warrant requirement.

The proposed right to privity is grounded in the observation that we are moving toward a world of what I call "informationships," in which we frequently rely on others to act as custodians of our personal data, records, and communications. In such a world, any meaningful interpretation of the Fourth Amendment's guarantee against unreasonable searches and seizures must protect certain information that has been disclosed by its originator. Privity is ideally suited to describe the rights of individuals in this context, because it embodies notions of both confidential disclosure (in its common usage) and standing (in its usage in the law of contracts). Accordingly, this Note speaks of the "right to privity" in both senses. It conceives of the term first as a right of confidential disclosure protecting personal information held "in privity," and second, as a right of Fourth Amendment standing protecting a person's "privity to" an informationship as the basis for a valid constitutional claim.

As a whole, this Note challenges the literature's almost universal focus on privacy as the appropriate lexical/conceptual lens through which to analyze Fourth Amendment jurisprudence. It argues that privacy terminology undermines the protection of disclosed personal information in two major ways. First, privacy terminology limits information control by encouraging courts to conceive of informational transactions in dichotomous terms, as either private or public. This binary schema ignores the myriad ways in which sustaining constitutional values in an information technology age will require

6. While its doctrinal meaning is somewhat ambiguous, courts appear to use "third party" in the Fourth Amendment context to mean a party other than a charged defendant. See *infra* notes 55-58. In contrast, the common usage suggests, for example, that for the purposes of paying tuition, a school would constitute a "second party" (because it is the primary provider of the purchased good) whereas a loan company would constitute a "third party" (because it is merely enabling the desired transaction). The courts' preferred usage nonetheless accords with the legal definition set forth in *Black's Law Dictionary*: "A person who is not a party to a lawsuit, agreement, or other transaction but who is usu[ally] somehow implicated in it; someone other than the principal parties." *Third party*, in BLACK'S LAW DICTIONARY 1518 (8th ed. 2004).

maintaining a vibrant category of nonpublic information that is neither fully secret nor entirely exposed.

Second, the privacy paradigm undermines constitutional text and values by overemphasizing the negative liberty aspects of information control while giving short shrift to its positive liberty components. Privacy terminology encourages us to conceive of information control as essentially a right to remain silent with respect to one's own personal information. Such terminology naturally draws our attention to that which is hidden, secret, and presumptively salacious. Yet this exclusive construction misses the corollary affirmative freedom implied by information control—to freely express one's self and communicate information.⁷

This Note does not present privity as a wholesale replacement of privacy within the realm of Fourth Amendment searches. Rather, I intend for privity analysis to replace privacy analysis in cases involving information held outside the custody of its originator. In such cases, privity provides a more precise way of describing the potential harms that result from the government's seizure of personal data. Unlike privacy, privity is a highly intersubjective concept that would require judges to ask not only "whether the information has been exposed," but also "to whom" and "to what end." Put simply, privity describes a particular type of privacy interest that is affected when the government compels individuals to turn over others' confidential information or communications.

From the more textured analysis that emerges from the concept of privity, we can begin to build a suitable constitutional framework for information control in the twenty-first century. Part I lays out the theoretical need for a more intersubjective framework for analyzing information control. Part II traces the existing judicial doctrines and demonstrates how, despite the early promise of a privity-friendly jurisprudence, privacy concepts and terminology have hindered judicial analysis. Part III proposes and applies a new doctrinal framework with which we can analyze information control as it relates to the Fourth Amendment.

7. An early article conceptualizing privacy as information control is Charles Fried, *Privacy*, 77 YALE L.J. 475, 483 (1968). Subsequent scholars have continued to construe privacy as including control over information. See, e.g., Randall P. Bezanson, *The Right to Privacy Revisited: Privacy, News, and Social Change, 1890-1990*, 80 CAL. L. REV. 1133, 1135 (1992); Jed Rubinfeld, *The Right of Privacy*, 102 HARV. L. REV. 737, 740 (1989); Daniel J. Solove, *Conceptualizing Privacy*, 90 CAL. L. REV. 1087, 1131 (2002).

I. THE PITFALLS OF PRIVACY

In this Part, I outline the shortcomings of the existing privacy framework. First, I build upon Daniel Solove's critique of the so-called secrecy paradigm, a model that conceives of information as either wholly private or public. I argue that this model is inadequate to address the realities presented by informationships. I then describe my proposed concept of privacy in greater detail before assessing and evaluating current Fourth Amendment doctrine.

A. *The Secrecy Paradigm*

The Fourth Amendment, which establishes a right to be free from "unreasonable searches and seizures,"⁸ was crafted at a time when both the physical and metaphysical boundaries between public and private space were far easier to identify. A purely literal reading of the Amendment's enumeration of "houses, papers, and effects"⁹ could provide sufficient protection against government abuse in a world where such terms plausibly applied only to material things. Judges of the eighteenth and nineteenth centuries encountered few of the definitional challenges faced by judges today, who must classify amorphous items like e-mails, genetic profiles, biometrics, phone conversations, locational data, and computer databases into categories created over two hundred years ago. Invasive searches conducted by the English crown, authorized by general warrants, prompted the inclusion of the Fourth Amendment within the Bill of Rights as a means for limiting abuse of law enforcement powers.¹⁰ Yet the scope of warrants in the colonial era generally covered only the contents of a person's home or office. An equivalent warrant today likely would include vast quantities of digital information and records held outside the home by trustees of personal information, such as Internet Service Providers (ISPs), insurance companies, banks, merchants, phone companies, and private data brokers.

Thus, the technologically networked environment is introducing new interdependencies that arise from the limited disclosure of information. As

8. U.S. CONST. amend. IV.

9. *Id.*

10. See Akhil Reed Amar, *Fourth Amendment First Principles*, 107 HARV. L. REV. 757, 772-74 (1994); Tracey Maclin, *When the Cure for the Fourth Amendment Is Worse than the Disease*, 68 S. CAL. L. REV. 1, 8 (1994). General warrants lacked any requirement that the scope of the search be narrowed and frequently were used in connection with accusations of libel against the King. See, for example, *Huckle v. Money*, (1763) 95 Eng. Rep. 768 (C.P.), which was the first reported case involving a general warrant.

many scholars have pointed out, we live in an age of databasing.¹¹ Whether in the context of our purchasing habits, financial transactions, sexual tastes, reading choices, web browsing, genetic makeup, medical information, or political affiliations, we constantly disclose information about ourselves and entrust it to third parties.¹² Much of the information we disclose out of necessity is sensitive enough that we would prefer not to reveal it to others. Consequently, the holders of our information have increasing potential to wield significant power over us. We live in a world where “embarrassing material follows a victim for life.”¹³

The privacy implications of this transformation would be far more benign if such changes were merely the product of individual human choice. If it were truly the case that individuals’ preferences placed less emphasis on the ability to guard certain facts and information about themselves, then the loss of privacy might produce a welfare-maximizing result. Much of the distribution and recording of our information, however, is effectively nonconsensual. Such dissemination is both a part of the general informational architecture into which we are born and a requirement for living a normal modern life. For example, the sending of either an e-mail or a letter risks that an interloper will read its content. In the case of an e-mail, a single sending will save the message on at least three computer hard drives. In the case of a letter, no such recording takes place. But to ask a person to refrain from using e-mail for fear of its recordability is to ask him to live a premodern life.

In short, we are moving from a world defined primarily by conventional human relationships to one largely premised on informationships—relationships formed around shared access to, and exchange of, personal information. This world of informationships is fundamentally different from the society that existed at the time of the Founding—not only in the greater variety of informational goods exchanged, but also in the pervasiveness of those goods and the dependency they foster.

How should courts conceptualize privacy in a world of informationships? Previously, when there was less need for individuals to disclose information to third parties, conceptions of privacy could feasibly center around what Daniel Solove has called the “secrecy paradigm.”¹⁴ Under the secrecy paradigm, information is either private or public. In the Fourth Amendment context, this

11. See, e.g., James P. Nehf, *Recognizing the Societal Value in Information Privacy*, 78 WASH. L. REV. 1, 17-22 (2003).

12. See Kang, *supra* note 5, at 1226-30.

13. Daniel J. Solove, *The Virtues of Knowing Less: Justifying Privacy Protections Against Disclosure*, 53 DUKE L.J. 967, 969 (2003).

14. Solove, *supra* note 2 (manuscript at 35).

paradigm suggests that the various records and pieces of personal information individuals disclose to others are no longer “their . . . papers.”¹⁵ Courts have often implied as much by holding that information divulged to third parties is public and may be obtained by the government, no matter how narrow or limited the disclosure.¹⁶

Such a paradigm might have sufficed in a world where self-expression and the demands of daily life did not require frequent disclosure of highly sensitive information. This paradigm, however, cannot adequately describe the rights of individuals to exclude the government from their shared informational goods. As Mary Coombs has noted, “[m]uch of what is important in human life takes place in a situation of shared privacy. The important events in our lives are shared with a chosen group of others; they do not occur in isolation”¹⁷ Therefore, a key deficiency of the secrecy model is that it neglects the multitude of “ways in which privacy embodies chosen sharing.”¹⁸

Another problem with the secrecy paradigm is its tendency to cast privacy in preclusive terms. Imagine for a moment that every beach in a given area were to institute a “nude only” policy, whereby individuals were required to remove their clothes before entering the beach. Undoubtedly, such a policy would violate individuals’ preclusive privacy—their right to preclude others from viewing their naked bodies. More importantly, the policy would entail a violation of other rights that privacy enables. Without the freedom to cover their bodies, many people would not go to the beach at all. Therefore, a threat to the privacy right would undermine another fundamental right—the right to inhabit a public place. From this example, we can see how privacy not only allows individuals to preserve their dignity and autonomy, but also empowers them to engage in activities not obviously tied to privacy concerns.

In the information context, the enabling features of privacy have particular salience when they implicate freedom of speech. As Charles Fried and other scholars have noted, privacy often manifests itself as the power to control information.¹⁹ Information control lies at the core of human communication and relationships. In many situations, individuals robbed of shared privacy assurances would decline to speak or communicate at all. This realization underlies legal protections afforded to doctor-patient, lawyer-client, and

15. U.S. CONST. amend. IV.

16. See *infra* notes 46–58 and accompanying text.

17. Mary I. Coombs, *Shared Privacy and the Fourth Amendment, or the Rights of Relationships*, 75 CAL. L. REV. 1593, 1593 (1987).

18. *Id.*

19. See Fried, *supra* note 7, at 483.

clergy-parishioner communications.²⁰ Shared privacy cannot be dismissed, as some scholars have suggested, as an unnecessary burden on free speech.²¹ Rather, shared privacy provides a necessary precondition for the exercise of speech and the full development of the human personality. As Fried has aptly written:

[P]rivacy is not just one possible means among others to insure some other value, but . . . is necessarily related to ends and relations of the most fundamental sort: respect, love, friendship, and trust. Privacy is not merely a good technique for furthering these fundamental relations; rather without privacy they are simply inconceivable.²²

B. *Privity and Informationships*

In contrast to the simplistic and individualistic secrecy paradigm, I propose a privity framework to address the demands of information control in a technological era. A right to privity, as I define it for the purposes of this Note, incorporates two relevant conceptions of the word. The first, which derives from the nonlegal realm, centers on confidentiality. This conception speaks of privity in accordance with one of its dictionary definitions as “joint knowledge with another of a private matter.”²³ The confidentiality conception uses the term privity to reflect conditions of shared secrecy through limited disclosure. When people speak of information held “in privity” under this definition, they describe data that is divulged with an understanding that it will not be disclosed beyond a limited set of recipients. As one weblog aptly defines the term, privity often refers to information held “just between you and me.”²⁴

In the legal context, privity holds a different connotation. *Black’s Law Dictionary* defines privity as “[t]he connection or relationship between two parties, each having a legally recognized interest in the same subject matter (such as a transaction, proceeding, or piece of property).”²⁵ This conception of

20. See *Developments in the Law—Privileged Communications*, 98 HARV. L. REV. 1450, 1463, 1501, 1530–32, 1555 (1985). These protections arise not from Fourth Amendment doctrine but from the common law and the Federal Rules of Evidence. See, e.g., FED. R. EVID. 501.

21. See, e.g., Eugene Volokh, *Freedom of Speech and Information Privacy: The Troubling Implications of a Right To Stop People from Speaking About You*, 52 STAN. L. REV. 1049 (2000).

22. Fried, *supra* note 7, at 477.

23. *Privacy*, in WEBSTER’S THIRD NEW INTERNATIONAL DICTIONARY 1805 (1993).

24. Privity: Just Between You and Me, <http://www.cherylstephens.com/privity> (last visited Nov. 8, 2005).

25. *Privity*, in BLACK’S LAW DICTIONARY, *supra* note 6, at 1237.

privity is most frequently invoked, and is best understood, in the context of contract law. The term “privity of contract” has been interpreted to mean “roughly . . . that the only persons who are allowed to obtain benefits or to sustain burdens under a contract are the parties to it.”²⁶ While courts have recognized several exceptions to this broad principle,²⁷ the legal concept of privity remains a useful tool for identifying valid legal claimants.

Though primarily concerned with confidentiality, the right to privity discussed in this Note also implicates standing. In the Fourth Amendment context, a right to privity demands that when deciding whether the government has violated an individual’s “reasonable expectation of privacy,” courts must recognize the legitimate expectations of confidentiality that attach to data held by third parties. In this sense, confidentiality is paramount. Yet this confidentiality-based conception incorporates basic notions of standing, because a person who claims a violation of his reasonable privacy expectations must first prove that he has some cognizable interest in the seized information. For example, an individual alleging a Fourth Amendment violation in the seizure of his records from a bank must first establish that he has a sufficient interest in those records to be considered a party to the search. By recognizing the reasonable privacy expectation in a person’s records, a court would imply that the records are in fact his private records for the purposes of constitutional analysis. Thus, locating a right to privity in the Fourth Amendment necessarily implies a broadening of the class of relevant parties with a cognizable interest in data held by third parties.

Whereas privacy encourages us to conceive of information as either simply public or simply private, privity encourages us to define information in terms of human relationships. That is, we cannot describe information as being held in privity without conceiving of at least two people who share access. Therefore, rather than thinking of privity as creating metaphorical locked boxes for secret information, we can more appropriately view it as forging types of informationships that I will call “privity links” and “privity chains.” Privity links describe the direct individual connections we have with others on the basis of shared nonpublic information. For instance, my disclosure of credit card information to an online merchant can be seen as establishing a privity link. Both she and I have a common interest in each other’s access to the

26. Richard A. Epstein, *Into the Frying Pan: Standing and Privity in Telecommunications Law*, 4 COLUM. SCI. & TECH. L. REV. 1, 6 (2003), <http://www.stlr.org/html/volume4/epstein.pdf>.

27. GUENTHER TREITEL, *THE LAW OF CONTRACT* 594-618 (10th ed. 1999); *see also Privity*, *supra* note 25, at 1238 (“The requirement of privity has been relaxed under modern laws and doctrines of implied warranty and strict liability, which allow a third-party beneficiary or other foreseeable user to sue the seller of a defective product.”).

information. Privity chains, by contrast, describe the more indirect connections to others we forge through the use, aggregation, or subsequent disclosure of information. Thus, my doctor's disclosure of my medical information to a specialist for a second opinion would likely create a privity chain joining me, my doctor, and the specialist.

Privity links and chains have particular salience when discussing digitally networked environments. The construction of an information network demands the establishment of privity norms and safeguards. Networks must determine who may access the information they contain.²⁸ Moreover, individuals who make up the network—the “transacting parties” to whom Jerry Kang refers—must determine from whom and to whom they will receive and transmit data.²⁹ Proxies and protocols for identity, such as IP addresses, serve as a necessary component of successful network interfacing and allow individuals to connect over boundaries of geography.³⁰ Technological innovations such as passwords, encryption, and firewalls distinguish those who will be privy to a network's information from those who will not. To speak only of privacy in this context, in which information flows in many directions and networks give rise to exclusive and semi-exclusive subnetworks, would be akin to speaking only of cardinal directions in a three-dimensional universe.

Distinguishing privacy from privity becomes even more important when we consider the myriad ways in which personal information can be both collected and exploited without our knowledge or control. Concerns about security, crime, and terrorism ensure that the government will collect and analyze an increasing amount of personal information.³¹ At the same time, the government is just one of many parties—including commercial data brokers,

28. For a full discussion of the cyberspace informational architecture and its implications for privacy, see *Kang, supra* note 5.

29. *Id.* at 1224.

30. *See id.* at 1224-38, 1241-44.

31. For example, the Department of Defense's data-mining project known as Total Information Awareness sought to aggregate information from the public and private sectors for antiterrorist purposes, but was discontinued after intense criticism from civil liberties groups and privacy advocates. *See* TECH. & PRIVACY ADVISORY COMM., DEP'T OF DEF., SAFEGUARDING PRIVACY IN THE FIGHT AGAINST TERRORISM (2004), available at <http://www.cdt.org/security/usapatriot/20040300tapac.pdf> (presenting findings regarding the Department of Defense's data-mining efforts along with recommendations for future compliance with privacy principles). The Department of Homeland Security has similarly relied on private sector data for airline security purposes. *See, e.g.*, PRIVACY OFFICE, DEP'T OF HOMELAND SEC., REPORT TO THE PUBLIC ON EVENTS SURROUNDING JETBLUE DATA TRANSFER: FINDINGS AND RECOMMENDATIONS (2004), available at http://www.dhs.gov/interweb/assetlibrary/privacy_rpt_jetblue.pdf.

advertisers, credit agencies, and private investigators—who have an interest in amassing data about individuals. This explosion of information collection, and the resulting potential for the government to outsource its data collection efforts, raise a number of concerns that challenge a simplistic individual-versus-government understanding of the Fourth Amendment.

II. A FLAWED THIRD-PARTY DOCTRINE

A. Searches for Information

The right to privity of information—the idea that one may disclose personal information without granting the government presumptive access to it—finds little support in current Fourth Amendment doctrine. Courts have repeatedly upheld an opposite doctrinal principle known as the third-party rule or the third-party doctrine. The third-party doctrine holds that “a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties.”³² While some courts have recognized (in theory) the existence of a broad constitutional right to informational privacy, none has done so in the context of information disclosed to third parties.³³ Furthermore, a majority of the cases acknowledging such a right have found it to be overridden by competing governmental interests.

An examination of the current third-party doctrine’s roots in judicial decisionmaking shows why it cannot be sustained as a matter of law. The third-party doctrine has evolved in the context of the broader principles and doctrinal tests governing judicial interpretation of the Fourth Amendment. According to established doctrine, the Fourth Amendment requires that police obtain a judicially approved warrant supported by probable cause only when

32. *Smith v. Maryland*, 442 U.S. 735, 743-44 (1979).

33. See, e.g., *In re Crawford*, 194 F.3d 954, 958-60 (9th Cir. 1999) (holding that disclosure of a Social Security number on a bankruptcy form did not violate the constitutional right to privacy); *Walls v. City of Petersburg*, 895 F.2d 188, 192-95 (4th Cir. 1990) (holding that a government employee’s privacy rights did not preclude a requirement that she fill out a background questionnaire before beginning work); *Barry v. City of New York*, 712 F.2d 1554, 1558-64 (2d Cir. 1983) (upholding a financial disclosure requirement for public employment); *United States v. Westinghouse Elec. Corp.*, 638 F.2d 570, 577-80 (3d Cir. 1980) (holding that access to an employee’s medical records for the purposes of an Occupational Safe and Health Administration investigation was permissible because, among other factors, the benefit of the disclosure outweighed the harm, and adequate privacy safeguards were in place); *Plante v. Gonzalez*, 575 F.2d 1119, 1138 (5th Cir. 1978) (holding that compelled public disclosure of financial records by candidates for public office was constitutional).

the activity proposed constitutes a “search.” Information obtained through other means, by contrast, falls outside the scope of the Fourth Amendment’s protections,³⁴ and normally requires at most a subpoena. Subpoenas are the government’s most commonly used mechanism for seizing documents and records. Compared to warrants, they are far easier for law enforcement officials to obtain for two main reasons. First, unlike a warrant, a subpoena need not be supported by probable cause; rather, the records sought by a subpoena need only be “relevant” to an investigation.³⁵ Second, subpoenas often require no judicial approval whatsoever. Administrative subpoenas, for example, which can be used to investigate a number of federal crimes, require only the signature of an agency official.³⁶

Although most subpoenas require that the recipient have an opportunity to challenge the government’s demand for documents in court, successful challenges are rare.³⁷ As William Stuntz has observed, the relevance standard means in practice that “subpoenas require nothing, save that the subpoena not be unreasonably burdensome to its target. Few burdens are deemed unreasonable.”³⁸ In the federal grand jury context, for example, the Supreme Court has held that subpoenas are presumed relevant unless there is “no reasonable possibility” that the materials seized will produce relevant information.³⁹ A subpoena is therefore valid even if based on “nothing more than official curiosity.”⁴⁰

Nearly forty years ago in *Katz v. United States*, the Court articulated the test for whether a police action rises to the level of a search necessitating a warrant supported by probable cause.⁴¹ That case involved the wiretapping of an individual’s conversation in a public telephone booth by FBI agents without a search warrant.⁴² The Court overturned its previous decision in *Olmstead v.*

34. Christopher Slobogin, *Subpoenas and Privacy*, 54 DEPAUL L. REV. 805, 805 (2005).

35. *United States v. R. Enters.*, 498 U.S. 292, 306 (1991).

36. For a description of the administrative subpoena power and its recent implications, see CHARLES DOYLE, CONG. RESEARCH SERV., REPORT NO. RL32880, ADMINISTRATIVE SUBPOENAS AND NATIONAL SECURITY LETTERS IN CRIMINAL AND FOREIGN INTELLIGENCE INVESTIGATIONS: BACKGROUND AND PROPOSED ADJUSTMENTS (2005), available at <http://www.fas.org/sgp/crs/natsec/RL32880.pdf>.

37. Slobogin, *supra* note 34, at 806.

38. William J. Stuntz, *O.J. Simpson, Bill Clinton, and the Transsubstantive Fourth Amendment*, 114 HARV. L. REV. 842, 857-58 (2001).

39. *R. Enters.*, 498 U.S. at 301.

40. *United States v. Morton Salt Co.*, 338 U.S. 632, 652 (1950).

41. 389 U.S. 347 (1967).

42. *Id.* at 348-49.

*United States*⁴³ and found that the wiretap was a “search” under the Fourth Amendment even though it did not entail an intrusion into the subject’s physical property.⁴⁴ Concurring in the Court’s holding, Justice Harlan introduced two requirements for police activity implicating the Fourth Amendment’s warrant provision: “first that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as ‘reasonable.’”⁴⁵ The two prongs of this test—one subjective and the other objective—have become the lodestar of Fourth Amendment analysis in subsequent cases.

The possibility that *Katz* might lead to an expansive right to communicate private information was short-lived. Nine years after *Katz*, the Supreme Court held in *United States v. Miller* that no Fourth Amendment violation occurred when federal officers obtained an individual’s bank records (including microfilm copies of checks, deposit slips, and balance sheets) without a search warrant.⁴⁶ The officers obtained the information by issuing subpoenas to two of the banks where the defendant held accounts. The Court applied the “reasonable expectation” test set forth by Justice Harlan and found that the individual had no objectively reasonable expectation of privacy in the records held at the banks in which he kept his accounts.⁴⁷ In a rather sweeping refusal to extend the principle of *Katz* to information held by third parties, the Court set forth its first incantation of the third-party rule, stating that “the Fourth Amendment does not prohibit the obtaining of information revealed to a third party . . . 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.”⁴⁸

The *Miller* Court brushed aside concerns about individuals’ subjective expectations, focusing instead on its belief that the expectations were objectively unreasonable. The Court provided several arguments to support this conclusion. First, the bank records were not “private papers” held by their originator and thus were not protected by the text of the Fourth Amendment.⁴⁹ Second, a privacy interest in the information was precluded by the fact that all of the seized information had been “voluntarily conveyed to the banks and . . .

43. 277 U.S. 438 (1928).

44. *Katz*, 389 U.S. at 353.

45. *Id.* at 361 (Harlan, J., concurring).

46. 425 U.S. 435, 436-37 (1976).

47. *Id.* at 442-43.

48. *Id.* at 443.

49. *Id.* at 440.

to their employees.”⁵⁰ Finally, documents such as checks and deposit slips were not confidential communications, but rather “negotiable instruments” to be used in commercial transactions.”⁵¹

If *Miller* marked the first appearance of the third-party rule on the constitutional radar, *Smith v. Maryland*⁵² secured the rule’s permanent place in judicial doctrine. *Smith* involved a criminal investigation in which police—without a warrant—collected information from a pen-register, which records the numbers dialed from an individual’s telephone. The Supreme Court held that the phone company’s installation of the device at the request of police did not rise to the level of a “search” under the Fourth Amendment, both because the telephone company necessarily recorded such information anyway, and because the numbers were knowingly “conveyed” by their originator.⁵³

Since the *Miller* and *Smith* decisions, the rationale underlying the third-party doctrine has been applied to a wide variety of personal records, including information held by phone companies, lending institutions,⁵⁴ medical institutions,⁵⁵ auditors and accountants,⁵⁶ trustees in bankruptcy,⁵⁷ and ISPs.⁵⁸

Though *Miller*, *Smith*, and their progeny are often associated with the third-party doctrine, they also rely on a closely related Fourth Amendment doctrine known as assumption of risk. That doctrine was articulated more than a decade before *Miller* in *Hoffa v. United States*. There, the Supreme Court held

50. *Id.* at 442.

51. *Id.* at 440.

52. 442 U.S. 735 (1979).

53. *Id.* at 744.

54. *United States v. Payner*, 447 U.S. 727 (1980) (holding that a loan application disclosed to a bank did not fall within a reasonable expectation of privacy).

55. *Webb v. Goldstein*, 117 F. Supp. 2d 289, 295 (E.D.N.Y. 2000) (holding that a state official’s dissemination of a prisoner’s medical records upon presentation of a subpoena did not violate reasonable privacy expectations); *State v. Guido*, 698 A.2d 729 (R.I. 1997) (holding that the police’s seizure of a drunk driving defendant’s hospital records through a grand jury subpoena was constitutional); *Corpus v. State*, 931 S.W.2d 30 (Tex. App. 1996) (holding that the admission during trial of medical records, including results of a blood alcohol test, did not implicate a defendant’s Fourth Amendment privacy interests).

56. *Wang v. United States*, 947 F.2d 1400, 1403 (9th Cir. 1991) (holding that an individual possesses no reasonable expectation of privacy in information voluntarily turned over to his financial advisor).

57. *In re Lufkin*, 255 B.R. 204, 211-12 (Bankr. E.D. Tenn. 2000) (holding that a subpoena for records issued to a law firm’s receiver did not violate the Fourth Amendment).

58. *Guest v. Leis*, 255 F.3d 325, 336 (6th Cir. 2001) (“[P]laintiffs . . . lack a Fourth Amendment privacy interest in their subscriber information because they communicated it to the systems operators.”); see also *United States v. Kennedy*, 81 F. Supp. 2d 1103, 1110 (D. Kan. 2000).

that a defendant was not entitled to the Fourth Amendment's protections when he made statements to a government informant in his hotel room.⁵⁹ Reasoning that the informant "was not a surreptitious eavesdropper" because he was invited into the room by the defendant, the Court held that the defendant assumed the risk that any information gleaned would be shared with the authorities.⁶⁰

While *Miller* and *Smith* each embraced a similar logic as the court in *Hoffa*, their assumption of risk rationales can be distinguished. In *Smith*, the telephone company voluntarily complied with the police's request to install a pen register. Accordingly, the disclosure of the defendant's phone records occurred with the third party's full consent. In *Miller*, by contrast, the police compelled the disclosure of the defendant's financial records by issuing subpoenas to his banks.

Thus, while the assumption of risk rationale articulated in *Hoffa* lends support to the central holding of *Smith*, it remains distinct from the *Miller* Court's broader implication that individuals assume the risk not only of third-party betrayal, but also of government compulsion.

This distinction is vital in the context of privacy rights. When the government obtains personal information by compelling third parties to reveal it, the state asserts its authority to intrude upon an informationship. By contrast, when such access is gained through informants, the government establishes its own privacy to the information by gaining the consent of one of the existing parties to the informationship. While the use of informants or cooperators may be more deceitful, it is less detrimental to personal autonomy.⁶¹ In such cases, individuals ultimately retain the autonomy to control information by evaluating the trustworthiness of their friends and associates. They may seek to establish privacy links with only a limited group of associates with whom they have confidentiality agreements or in whom they place a high degree of confidence and trust.

In the case of third-party compulsion, however, the freedom to engage in such screening does not matter. Because the government's authority to seize information in this context applies to all holders of information, every disclosure to a third party risks a potential threat to privacy. Thus, the

59. 385 U.S. 293 (1966).

60. *Id.* at 302-03. Similarly, in *On Lee v. United States*, 343 U.S. 747, 753-54 (1952), the Court ruled that the subject of a criminal investigation had assumed the risk of disclosure when he spoke to an individual who was using a concealed transmitter that enabled the police to listen in on his conversation.

61. Moreover, the law often provides civil or criminal penalties for those who improperly disclose private information. See *infra* text accompanying notes 95-99.

assumption of risk doctrine as articulated in *Hoffa* poses a lesser threat to control of personal information than the blanket rule established in *Miller*.

B. Evaluating the Current Framework

The third-party doctrine has effectively denied standing to defendants who allege illegal government seizure of personal data held in an informationship.⁶² This sweeping denial of Fourth Amendment protection is at odds with the core principles set forth in *Katz*. Apart from its creation of a doctrinal test, the opinion in *Katz* was an admirable effort to adapt Fourth Amendment doctrine to the changing needs of a technological age. In particular, its assertion that the Amendment protects “people, not places” signaled a much-needed departure from the Court’s previous holdings that the Constitution limited only searches and seizures of tangible property.⁶³

Moreover, the *Katz* Court carefully avoided one of the fundamental flaws of privacy analysis: the tendency to view limited disclosure as tantamount to public display. Instead, the majority acknowledged the role that individual intent plays in distinguishing communications that are private from those that are public: “What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection. But what he seeks to preserve as private, *even in an area accessible to the public*, may be constitutionally protected.”⁶⁴

The Court’s analysis in *Katz* embraced an appropriately nuanced conception of the Fourth Amendment’s meaning. The Court refused to limit the right to privacy to objectively reasonable preclusive acts. Rather, it began to articulate an affirmative right to control one’s information by symbolic gestures and mutually recognized norms. The majority noted, for instance, that *Katz* entered a glass-enclosed telephone booth and closed the door to guarantee that his words “w[ould] not be broadcast to the world.”⁶⁵ Moreover, the opinion explicitly recognized the crucial role that such gestures play in facilitating our dialogic participation as human beings:

No less than an individual in a business office, in a friend’s apartment, or in a taxicab, a person in a telephone booth may rely upon the

62. The Supreme Court no longer considers standing as an explicit factor in its Fourth Amendment analysis, but rather considers the standing inquiry as an implicit part of the broader expectation of privacy test. See *Rakas v. Illinois*, 439 U.S. 128, 138-43 (1978).

63. *Katz v. United States*, 389 U.S. 347, 351 (1967).

64. *Id.* at 351-52 (citations omitted and emphasis added).

65. *Id.* at 352.

protection of the Fourth Amendment. . . . To read the Constitution more narrowly is to ignore the vital role that the public telephone has come to play in private communication.⁶⁶

In short, the *Katz* Court did not merely limit the government's ability to eavesdrop. It also underscored the crucial role that disclosed but nonpublic information plays in modern society. Although the privacy right enunciated by *Katz* entails the power to exclude individuals from conversation, the right also affirmatively enables conversation. The Court realized that the danger of denying a partially concealed domain for communication lies in the fact that without such a domain, people might not speak at all. Thus, the decision in *Katz* not only enforced the Fourth Amendment, but also upheld the broader values embodied by the First.

Admittedly, the decision in *Katz* is flawed in some respects. Most notably, the Court did not adopt a particularly sophisticated taxonomy, thus imposing a linguistic straitjacket on future decisions. The Court failed to acknowledge, for example, that privity, and not merely privacy, is central to any plausible understanding of *Katz*'s claims. After all, one cannot understand the need to protect the privacy of *Katz*'s phone conversation without first identifying the relevant privity links. On the one hand, analyzing the privity norms encourages us to view *Katz*'s affirmative actions of entering the phone booth, closing the door, paying, and dialing as shrouding his communication in a reasonable expectation that those standing outside the booth would not be privy to his communication. On the other hand, to the recipient on the other end of the phone, the placing of the call served not as a prohibition, but as an invitation to stand in privity with *Katz* as to the contents of the conversation. Conceiving of the conversation as part of a privity relationship makes sense of the key observation in *Katz* that telephones play a crucial role in fostering interpersonal relationships.⁶⁷ Privity is thus a useful term in this case because it emphasizes both the inclusive and exclusive functions served by the Fourth Amendment's protections.

Unfortunately, the Court's reasoning in *Miller* misapplied and betrayed the underlying privity principles of *Katz*. The *Miller* Court's contention that the documents at issue were not private papers rested on a proposition explicitly refuted by *Katz*—that the Fourth Amendment applies only to items physically held by their owners.⁶⁸ The Court in *Katz* had acted on a firm foundation when it recognized that privacy conceptions must go beyond pure property notions

66. *Id.* (citations omitted).

67. *Id.*

68. *Id.* at 353.

in response to modern technology.⁶⁹ Other decisions have validated *Katz's* insight, holding that physical property held remotely, or subject to shared use, is constitutionally protected. One federal court, for example, held in *United States v. Thomas* that an individual maintained a reasonable expectation of privacy with respect to the contents of his deposit boxes,⁷⁰ even though the boxes themselves were presumably the property of the bank. In *Jones v. United States*, the Supreme Court held that a drug-trafficking defendant had standing to challenge a police search of his friend's apartment when the defendant had been using the apartment with his friend's permission.⁷¹ In *Mancusi v. DeForte*, the Court held that a union employee had a reasonable expectation of privacy in union records kept in an office that he shared.⁷²

Although another Supreme Court decision, *Rakas v. Illinois*, appears at first glance to embrace a more property-based notion of privacy than these other decisions, the *Rakas* Court similarly rejected the idea that property notions should control Fourth Amendment analysis.⁷³ The Court held that defendants who were passengers in another person's automobile maintained no Fourth Amendment privacy interest in the contents of the car's glove compartment. However, the Court's holding was limited to the proposition that defendants could not prove a Fourth Amendment violation when they had neither a property-possessory interest nor a legitimate privacy interest in the searched property.⁷⁴ The opinion explicitly noted that defendants could challenge such evidence when they possessed a "legitimate expectation of privacy" (i.e., an "interest") in a third party's property.⁷⁵

Thus, the sweeping rule devised in *Miller* is at least partially at odds with other cases involving conceptions of shared privacy. This discrepancy derives largely from the fact that courts have viewed *Miller* and similar cases as involving "mere information," as opposed to tangible or exclusively held items.⁷⁶ Denying privacy protections purely on the basis of such a distinction is troubling, as it places vast quantities of modern digital communications outside the Fourth Amendment's purview. For example, the court in *United*

69. For a contrary viewpoint, see Orin S. Kerr, *The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution*, 102 MICH. L. REV. 801, 857-87 (2004).

70. No. 88-6341, 1989 U.S. App. LEXIS 9628, at *6 (6th Cir. 1989).

71. 362 U.S. 257 (1960).

72. 392 U.S. 364 (1968).

73. 439 U.S. 128 (1978).

74. *Id.* at 148-49.

75. *Id.* at 143.

76. U.S. DEP'T OF JUSTICE, SEARCHING AND SEIZING COMPUTERS AND OBTAINING ELECTRONIC EVIDENCE IN CRIMINAL INVESTIGATIONS 8 (2d ed. 2002).

States v. Charbonneau held that an e-mail message cannot be afforded a reasonable expectation of privacy once that message is received by its intended recipient.⁷⁷ Likewise, the Sixth Circuit in *United States v. Meriwether* held that an electronic message sent via pager did not receive Fourth Amendment protection because the message constituted “information” under the *Smith* standard.⁷⁸

Restricting constitutional privacy protections to protect only tangible items over which the defendant claims possession belies the logic underlying the Fourth Amendment’s protection of “papers.” Rather than merely prevent government seizure of the physical papers themselves, the Founders sought to prevent the broader harms associated with seizing the potentially sensitive information contained therein.⁷⁹ In an age of informationships, much personal and highly confidential information exists on paper and in machines that are not within their originator’s physical grasp. The fact that the government can seize such information without actually invading the originator’s physical space or property does not diminish the extent of the resulting intrusion. Thus, the *Miller* Court’s claim that the defendant could “assert neither ownership nor possession” provides a hollow justification for warrantless searches.⁸⁰ Courts should protect not only papers over which individuals claim possession, but also those in which individuals maintain an important but attenuated possessory interest as the originator of the information.

77. 979 F. Supp. 1177, 1184 (S.D. Ohio 1997). The court’s reliance on the distinction between received and unreceived e-mails is unconvincing. While it is true that the sender of an e-mail anticipates that the recipient may voluntarily share the message with others, it does not follow that he therefore anticipates compulsory disclosure of the e-mail to law enforcement. See, e.g., *United States v. Maxwell*, 45 M.J. 406, 418 (C.A.A.F. 1996) (“One always bears the risk that a recipient of an e-mail message will redistribute the e-mail or an employee of the company will read e-mail against company policy. However, this is not the same as the police commanding an individual to intercept the message.”).

78. 917 F.2d 955, 959-60 (6th Cir. 1990).

79. It would strain credulity to argue that “papers” received individual mention in the Constitution solely because of their property value when other unmentioned items (e.g., furniture) held greater monetary value. The notion that papers were enumerated on account of their informational content receives support from contemporaneous history. The Founders’ views on this subject were shaped largely by the mid-eighteenth-century controversy in England surrounding the indiscriminate seizure of papers by the British Crown. See Eric Schnapper, *Unreasonable Searches and Seizures of Papers*, 71 VA. L. REV. 869 (1985). Documentation of the debate from that period demonstrates that opponents of the Crown were concerned not only that the seizures entailed intrusions upon physical property, but also that such seizures entailed access to highly personal information and secrets. *Id.* at 882-84.

80. *United States v. Miller*, 425 U.S. 435, 440 (1976).

The *Miller* Court's reliance on the assertion that the bank records were conveyed voluntarily also belies Fourth Amendment principles. As Justice Brennan aptly noted in his dissent in *Miller*, "the disclosure by individuals or business firms of their financial affairs to a bank is not entirely volitional, since it is impossible to participate in the economic life of contemporary society without maintaining a bank account."⁸¹ Thus, it would be both unreasonable and unfair to assume that disclosure is tantamount to full consent when to withhold consent would be to live a premodern life.

Moreover, the assumption that the transactions were wholly volitional does not adequately explain the Court's refusal to grant Fourth Amendment protection. After all, the phone call made in *Katz* was similarly volitional and nonetheless received full Fourth Amendment protection. Those who disclose information to their banks anticipate that their information will be viewed by bank employees. However, they have no reason to expect it will be seen by strangers with whom they are not in privity, especially by the government.

Finally, the *Miller* Court's claim that bank records consist largely of "negotiable instruments" and are thus not confidential is significantly undercut by the fact that just two years after the Court's ruling in *Miller*, Congress passed the expansive Right to Financial Privacy Act.⁸² The Act, passed as a direct response to the court's reasoning in *Miller*, provided heightened privacy protections with respect to law enforcement access to financial information.⁸³ Specifically, it required that (1) notification be provided to customers before and after their information is seized,⁸⁴ (2) police obtain a subpoena or a warrant, or file a formal written request with the bank,⁸⁵ and (3) targeted individuals be permitted to challenge the requested disclosure.⁸⁶ In addition, at least one court has cited a rule that confidentiality "is an implied term of the contract between a banker and his customer."⁸⁷ In short, the *Miller* Court's logic rested on an unfounded assumption: that expectations of financial

81. *Id.* at 451 (quoting *Burrows v. Superior Court*, 13 Cal. 3d 238, 247 (1974)).

82. Right to Financial Privacy Act of 1978, Pub. L. No. 95-630, 92 Stat. 3697 (codified as amended at 12 U.S.C. § 3401 (2000)).

83. 12 U.S.C. § 3401 (2000). For a discussion of the *Miller* decision's influence on Congress's passage of this statute, see Matthew N. Kleinman, *The Right to Financial Privacy Versus Computerized Law Enforcement: A New Fight in an Old Battle*, 86 NW. U. L. REV. 1169, 1187-90 (1992).

84. 12 U.S.C. §§ 3405(2), 3407(2), 3408(4), 3412(b) (2000).

85. *Id.* §§ 3405-3408.

86. *Id.* § 3410.

87. *Peterson v. Idaho First Nat'l Bank*, 367 P.2d 284, 290 (Idaho 1961) (internal quotation marks omitted).

privacy are not, in the words of *Katz*, expectations “that society is prepared to recognize as reasonable.”⁸⁸

While the Court’s approval of warrantless pen-register surveillance in *Smith* is potentially defensible on the ground that the phone company in that case voluntarily installed the surveillance equipment at the government’s request, the *Smith* Court’s reasoning was equally problematic. The Court completely ignored the distinction between third-party compulsion and consent, and adhered instead to *Miller*’s blanket proposition that any information held by third parties receives no privacy protection. In denying such protection, the *Smith* Court (like the *Miller* Court) hopelessly entangled third-party and assumption of risk analysis, construing the latter doctrine to mean that individuals must assume the risk that the government will force access to their personal records.

The *Smith* Court also further eviscerated privacy rights by refusing to acknowledge a distinction between information turned over to people and information recorded by automated machines.⁸⁹ The Court dismissed the petitioner’s argument that because the automatic processing of information by machine does not require disclosure to a human being, individuals attach a greater privacy expectation to that information.⁹⁰ The refusal to acknowledge this distinction underscores the Court’s shortsighted and inadequate approach to information exchanges in the modern age.

Applying the Court’s logic to e-mail, for instance, would equate an individual’s expectation of privacy in a message he merely sends through an ISP’s server to his expectation of privacy in messages he intends to be read by ISP personnel. The implausibility of this notion suggests that people often retain greater expectations of privacy when their information is processed by machines as opposed to people. That is to say, individuals frequently form privacy links and privacy chains in which machines are the primary agents of interaction, and in which human access may be considered a violation of explicit or implicit agreements. Machines cover informational transactions with an additional cloak of privacy by allowing data to flow from sender to recipient without the necessary intervention of a middle-man. The Court’s refusal to acknowledge the significant difference between machines and human beings stands as one of *Smith*’s detrimental contributions to Fourth Amendment doctrine.

88. *Katz v. United States*, 389 U.S. 347, 361 (1967).

89. *Smith v. Maryland*, 442 U.S. 735, 744-45 (1979).

90. *Id.*

This analysis of *Smith* and *Miller* reveals the evisceration of the privacy-friendly principles underlying *Katz* in favor of a simplistic, “show one, show all” conception of privacy. We have yet to fully feel the detrimental impact of that crude conception. The “reasonable expectation of privacy” test, as applied in these two cases, conceives of privacy as an on/off switch, whereby an individual’s disclosure of information relegates his Fourth Amendment claims to the constitutional darkness. In reality, however, reasonable notions of information privacy are far more complex, and demand attention not only to disclosure, but also to the purposes for which the disclosure is made and the substantive nature of the information revealed. As the members of the Department of Defense’s Technology and Privacy Advisory Committee declared, “*Miller* and its progeny clearly conflict with American values concerning privacy.”⁹¹

III. A PROPOSED FRAMEWORK

This Part proposes a constitutional doctrine applicable to third-party information that protects informationships but recognizes the government’s need to collect information. As I argued above, the existing constitutional framework fails to adequately protect privacy in a modern world. Current law reveals a drastic asymmetry in privacy protections. Statutory and common law maintain a far more vibrant patchwork of privacy protections than does Fourth Amendment doctrine, suggesting that the Court’s doctrinal analysis has fallen behind the times. In tort law, for example, individuals can sue private parties for breach of confidentiality when others violate their privacy links.⁹² Thus, in *McCormick v. England*, the South Carolina Court of Appeals recognized a cause of action against a physician for unauthorized disclosure of medical information.⁹³ Even more relevant to privacy notions, several courts have held third parties liable when they induce a physician to disclose information about a patient.⁹⁴ Similarly, both federal and state laws protect against disclosure of certain kinds of information to private individuals, including video rental information,⁹⁵ cable service provider records,⁹⁶ medical records,⁹⁷ school records,⁹⁸ and drivers’ license information.⁹⁹

91. TECH. & PRIVACY ADVISORY COMM., *supra* note 31, at 23.

92. Solove, *supra* note 2 (manuscript at 36-37).

93. 494 S.E.2d 431 (S.C. Ct. App. 1997).

94. *Hammonds v. AETNA Cas. & Sur. Co.*, 243 F. Supp. 793 (N.D. Ohio 1965).

95. Video Privacy Protection Act of 1988, 18 U.S.C. §§ 2710-2711 (2000).

96. Cable Communications Policy Act of 1984, 47 U.S.C. § 551 (2000).

In sum, although legislatures have repeatedly affirmed the notion that individuals maintain strong expectations of privacy in countless facets of human life, courts have consistently ignored this fact when analyzing claims of unreasonable searches and seizures against the government. While legislatures can play a crucial role in protecting personal information from disclosure, courts still must determine which searches are reasonable under the Fourth Amendment. Courts do not fulfill this obligation when they deem reasonable acts that legislatures and the general public consider serious violations of basic privacy expectations.¹⁰⁰

A. A New Test

Because Fourth Amendment doctrine focuses on reasonableness, courts questioning the constitutional need for a warrant must engage in a balancing of opposing considerations. They must consider both the reasonableness of the asserted privacy interest and the reasonableness of the state's claim of a right to access information without a warrant.

In order to ensure that judicial doctrine fully addresses both of these considerations, I propose that courts apply a rebuttable presumption that a warrant is required in cases reviewing alleged illegal searches of information held by third parties. That presumption would apply whenever individuals show that they had an objectively reasonable expectation of privacy in their personal information. It could be overridden, however, with the showing of particular facts by the government. In determining whether a presumption had been established through a reasonable privacy expectation, the court would ask whether, at the time of his disclosure to a third party, the originator would have been reasonable in assuming:

- (1) that the third party would limit disclosure of the information;¹⁰¹ and

97. Health Insurance Portability and Accountability Act of 1996, 42 U.S.C. § 1320(d)(6) (2000).

98. Family Educational Rights and Privacy Act of 1974, 20 U.S.C. § 1232(g) (2000).

99. Driver's Privacy Protection Act of 1994, 18 U.S.C. §§ 2721-2725 (2000).

100. Cf. *Roper v. Simmons*, 125 S. Ct. 1183, 1192 (2005) (stating that legislative enactments regarding the applicability of the death penalty to minors provided "objective indicia of consensus").

101. The first two prongs of my proposed test bear some similarity to the framework proposed by Mary Coombs for determining whether searches and seizures implicate the Fourth Amendment when the claimant's privacy right is derivative of another's property interest. Her framework would allow a "derivative claimant" to challenge a search "when he can reasonably assume that (1) the primary rightholder would seek to exclude the public in general, including the government . . . and (2) the primary rightholder, in so acting, was

- (2) that the limited set of recipients would not include the government agent or agency.

An affirmative answer to both of these questions would establish a presumption in favor of a warrant, thus recognizing the originator's reasonable expectation that his information would be held in privacy. However, that presumption could be overcome—and the warrant requirement avoided—if the government could fulfill all three of the following conditions:

- (1) the government agent or agency had a need to know the information;
- (2) obtaining a warrant would have unreasonably hindered a government function or investigation; and
- (3) the methods used to obtain the information were reasonable.¹⁰²

This proposed framework injects a more nuanced conception of privacy into judicial decisionmaking by requiring courts to treat concerns about disclosure to the government as distinct from concerns about disclosure to other third parties. Accordingly, the two-pronged portion of the test draws special attention to the different reasons individuals may have for withholding the contents of an informationship from the government. For example, under this framework courts would recognize that having one's reading habits disclosed to a librarian via borrowing records does not violate privacy, but that having them disclosed to the FBI may amount to such a violation. Rather than speaking of privacy as a single on/off switch, the privacy test conceives of a series of switches, each conveying the individual's preferences and expectations regarding disclosure to particular third parties.

Furthermore, the three-pronged portion of the test provides an additional advantage over current doctrine by explicitly considering the interests of the government. In cases such as *Miller* and *Smith*, the Court remained noticeably silent on this issue. The Court's refusal to apply the warrant requirement stemmed from a perceived need for government access, yet the opinions focused almost entirely on defining the information itself as public or private. This proposed test would create a more realistic approach to Fourth

taking the claimant's interests into account." Coombs, *supra* note 17, at 1651. My test differs from this framework in that it applies exclusively to information and thus does not conceive of a primary rightholder upon whom the claimant must rely to "share with [the claimant] the umbrella of [the primary rightholder's] fourth amendment rights." *Id.*

102. For example, the police's seizure of an individual's phone number by surreptitiously breaking into her house and rifling through her phone bills would likely fail the test under this prong, despite the fact that the information itself is publicly available.

Amendment claims that would require courts to directly confront the government's asserted reasons for avoiding the warrant requirement.

A privity framework would not place undue burdens on law enforcement for two reasons. First, individuals raising Fourth Amendment challenges under this framework could not merely assert subjective expectations of privity as the basis for their attempts to exclude evidence. Rather, they would have to appeal to more objective indicia of privity (which I outline in Section C) to convince courts that their claims were reasonable. Moreover, just as Fourth Amendment doctrine in other areas recognizes instances in which warrantless searches of physical items may pass constitutional muster, so too my proposed test recognizes instances in which warrantless seizure of information held in privity may comply with the Fourth Amendment. Because the presence of a privity expectation merely establishes a rebuttable presumption, courts would evaluate the reasonableness of any given search on the basis of the particular facts of the case.

However, the proposed test would require the government to meet a relatively high bar to seize personal data that are held in an informationship. In essence, the test is based on the notion that such intrusions may entail affronts to personal dignity and security that are substantially equivalent to those caused by searches and seizures of one's physical papers. Thus, by requiring the government to demonstrate a need to know the information, the test forbids the type of pretextual searches that courts have repeatedly condemned in other strands of Fourth Amendment jurisprudence.¹⁰³ Further, the test's condition that obtaining a warrant must be an unreasonable hindrance mirrors the "exigent circumstance" exception that many courts have applied to uphold searches in the rare cases when securing a warrant is impracticable.¹⁰⁴ Finally, the requirement that the methods used be reasonable provides courts with a means to invalidate warrantless searches when they involve unnecessarily intrusive means for seizing information. In short, the test provides sound, specific, and well-grounded guidance to courts in an area currently bereft of doctrinal consistency or balance.

B. Categories of Information

Thus far I have discussed this proposed framework in the abstract. In the remaining pages – borrowing in part from previous scholarship – I will suggest three broad categories into which most seized personal information tends to

¹⁰³ See, e.g., *State v. Lair*, 630 P.2d 427, 434 (Wash. 1981).

¹⁰⁴ See, e.g., *United States v. Banks*, 540 U.S. 31 (2003).

fall. In each category, I will offer a concrete example that illustrates how my proposed test would affect the outcomes of judicial decisionmaking.

1. *Information Disclosed by Necessity*

The informationship at issue in *United States v. Miller* is a paradigmatic example of “functionally necessary”¹⁰⁵ disclosure. This category describes information that individuals share with third parties in order to perform necessary tasks or to obtain a service or product. Individuals make functionally necessary disclosures when they transfer data to third parties who in turn use the data for desired transactions. In *Miller*, for instance, the customer’s disclosure of his financial records to the bank was functionally necessary because the bank required that information to process his money exchanges. Likewise, in *Smith*, the recording of dialed telephone numbers by the phone company was functionally necessary because it allowed the telephone company to bill the customer for his usage.

Applying my proposed test to the facts of *Miller* shows how the test would expand the focus of a court to encompass a wider range of considerations. A court following my test would first ask whether Miller’s information was conveyed to his bank in privacy. Specifically, the court would ask whether it was conveyed with an expectation that the bank would “limit disclosure of the information.” One way the court might answer this question would be to consider the bank’s likely reaction if a random individual demanded access to Miller’s account information and transaction records. The court would conclude that no bank would comply with such a request. The bank’s refusal to distribute the personal information of its customer would be considered entirely prudent and reasonable, because bank records universally receive such basic protection. Thus, the *Miller* court would find that some privacy limitation attached to Miller’s bank records.

The court’s privacy inquiry would not end there, however, as the court would also have to consider whether the privacy expectation extended to the relevant government agency. The test specifically requires courts to discern whether the originator was reasonable in assuming that the government was not among the “limited set of recipients” with access to the information. Under this prong of the test, courts could find a plethora of reasons why individuals would reasonably wish to exclude the FBI from gaining privacy to their financial information. First and foremost, individuals’ financial transactions

105. Kang, *supra* note 5, at 1249. Kang refers to functionally necessary “use,” as opposed to disclosure. Thus, my phrase is an adaptation of his term.

may disclose intimate details of their lives, including their personal tastes, consumer habits, and associates. Furthermore, individuals may wish to prevent access to financial information by the government for the basic reason that disclosure to the bank itself is, in the words of Justice Brennan, “not entirely volitional,”¹⁰⁶ but rather a necessary activity for engaging in a modern financial system. In such a situation, further disclosure to other third parties would contravene the reasonable expectation of bank customers that the bank will distribute and access the information only when necessary to render its financial services. Consequently, my proposed rubric would recognize the strong privacy interest that remains attached to the data. The court would thus define the informationship in *Miller* as establishing a privacy link between the customer and his bank but not as creating a privacy chain among the customer, the bank, and the government.

One might challenge the right to privacy in *Miller* by arguing that the government can assert a unique right of access to the information due to the state’s role as a tax collector. Because individuals routinely disclose financial information to the federal government for tax purposes, bank customers arguably relinquish any expectation that banks will exclude the federal government from their account data. In other words, customers may have good reason to believe that the government stands in privacy with respect to their financial information.

This argument, however, embraces an overly simplistic conception of “the government.” Namely, it ignores the different privacy expectations that individuals hold with respect to various government entities. While most individuals realize that they must annually grant the IRS privacy to their financial information for tax purposes, few expect that such information will find its way into the hands of the FBI. For this reason, this Note’s proposed privacy test asks whether privacy expectations apply to the relevant “government agent or agency” and not simply to “the government.” Applying the test to *Miller*, a court would find that the account-holder had no reason to expect that his information would be subjected to warrantless access by a criminal law enforcement agency. Rather, the privacy expectation that attached to his financial information excluded the FBI from gaining privacy just as it would exclude an unspecified stranger from doing so.

Having recognized a presumption that a warrant was required, the court would then consider whether the government’s interests overrode the presumption. Looking to the first prong, the court would likely find that the government did in fact have a “need to know” the information sought from

106. See *supra* note 81 and accompanying text.

Miller. The facts of *Miller* reveal that, at the time federal agents seized Miller's bank records, law enforcement officials had already discovered significant evidence of Miller's involvement in the alleged crimes of "possessing an unregistered still" and "carrying on the business of a distiller without giving bond and with intent to defraud the Government of whiskey tax."¹⁰⁷ In particular, the evidence included a tip from an informant that Miller maintained an unregistered distilling operation, the discovery by police of distillery equipment and "raw material" in Miller's truck during a traffic stop, and the discovery by a sheriff, while responding to a fire in Miller's warehouse, of an actual distillery in that warehouse.¹⁰⁸ The state would rest on firm ground in arguing that Miller's financial information was necessary to confirm a likely crime.

Applying the second prong, however, would render the state's attempts to overturn the warrant requirement ineffective. The second prong requires government officials to show that obtaining a warrant would "unreasonably hinder" law enforcement functions. While requiring police to secure a warrant might have temporarily delayed the investigation of Miller, one could hardly argue that such delay would have imposed an unreasonable burden. After all, the state would have suffered no major harm or hindrance, especially when no danger existed that the evidence would be destroyed or that lives would be endangered. Thus, a court applying the proposed test to the facts of *Miller* would find that the presumption had not been overridden and that a warrant was constitutionally required in order to seize Miller's bank records.

This hypothetical application suggests that my proposed test would more frequently require a warrant for the seizure of information disclosed by necessity than does current privacy doctrine. Conceptualizing functionally necessary disclosure will be even more important when the information disclosed is highly content-laden, as opposed to largely transactional. This distinction most frequently arises in the context of the e-mail, voicemail, and web history files held by ISPs and telephone companies. In this context, the dividing line between content and transactional information is often unclear. This obscurity has been addressed by legislation such as the Electronic Communications Privacy Act (ECPA), which governs both private and law enforcement access to internet data.¹⁰⁹ Unfortunately, the ECPA resolves difficult questions regarding these distinctions in deeply unsatisfying ways. For example, as interpreted by the Department of Justice, the ECPA requires law

¹⁰⁷. *United States v. Miller*, 425 U.S. 435, 436 (1976).

¹⁰⁸. *Id.* at 437.

¹⁰⁹. 18 U.S.C. §§ 2510-2534 (2000).

enforcement to meet only the subpoena standard of “relevance” to access e-mail and voicemail that has already been opened by a recipient.¹¹⁰ If the voicemail or e-mail has not been opened, then a warrant is required only for the first 180 days, after which a mere subpoena will suffice.¹¹¹ This aspect of the ECPA ignores the important privacy interests that attach to information stored by third parties and rests on a wrongly conceived notion that privacy concerns will necessarily fade with time.

2. *Information Disclosed After Solicitation*

In contrast to information disclosed by necessity, information disclosed after solicitation has been provided voluntarily to third parties and does not have a service or transaction-enabling function. Common examples of this type of disclosure include the surveys that individuals complete at the request of particular vendors or other information collectors. In such cases, many of the assumptions that attach to information in the previous category do not apply, because individuals affirmatively consent to the disclosure without any functional necessity for doing so.

As a hypothetical example of information disclosed after solicitation, imagine the following scenario. Joe Smith is sitting down to enjoy his dinner when he receives a phone call:

“Good evening Mr. Smith, I’m Mary from XYZ-Marketing. We’re currently compiling a list of customers and their personal preferences to be shared with our affiliates. If you take just five minutes to answer some questions about your purchasing habits and preferences, we will gladly send you a free MP3 player.”

Remembering that his daughter recently asked for an MP3 player, Joe agrees to complete the survey. He answers a series of questions and, in so doing, reveals a wide range of information about himself. The information disclosed includes his preference for reading conservative magazines, his tendency to vote Republican, his opinions on gay marriage, his taste for Edy’s ice cream, his hunting and gun collecting hobbies, and his recent purchase of self-help tapes on how to get out of debt. Four months later, Joe falls under federal investigation for the illegal sale and transport of firearms across state lines. During the early stages of the investigation, the FBI compels the disclosure of Joe’s file by XYZ-Marketing without a search warrant. At trial, Joe challenges

110. U.S. DEP’T OF JUSTICE, *supra* note 76, at 103-04.

111. *Id.*

the FBI's warrantless access to his file and its use as evidence in trial as a violation of his Fourth Amendment rights.

Applying the proposed test to the facts of Joe's case, a court would likely find that no constitutional violation had occurred. After all, Joe would find it difficult to argue that he maintained any privity expectation whatsoever with respect to the information, given Mary's clear indication that it would be shared with XYZ-Marketing's "affiliates." Moreover, unlike the disclosure in *Miller*, Joe's providing of the information to Mary was wholly voluntary. Thus, the solicited nature of his disclosure would place Joe outside the protection of the Fourth Amendment's warrant requirement.

The example provided is admittedly an extreme case, and it does not fully illustrate the protections afforded by my proposed test. After all, solicited disclosures often do occur under reasonable explicit or implicit understandings that dissemination of the information will be limited. In such cases, recognizing privity expectations under my proposed test would not only be reasonable but required. Suppose, for instance, that Mary's initial offer had indicated that Joe's information would be shared "strictly with our trusted commercial affiliates" and then named the full list of those affiliates. In that case, Joe would have substantial and legitimate reason to expect that the FBI would be prevented from having unfettered access to his file. In such cases, courts applying the privity test to the Fourth Amendment issues at hand would be compelled to find that a presumption of a required warrant applied.

3. *Information Created by Aggregation*

The previous two examples do not address an additional complication that often arises in cases of solicited disclosure: aggregation. In choosing this as a relevant category, I borrow my terminology from Professor Daniel Solove. Solove defines aggregation as "the gathering together of information about a person."¹¹² More specifically, aggregation involves the piecing together of existing data about an individual to provide a fuller picture than any one piece of information would yield on its own.¹¹³

In order to illustrate the challenges presented by aggregation, let us return to our previous example involving Mary and Joe. This time, suppose Mary indicates that the information collected may be shared with "affiliates" (as in the first example above), but adds the following caveat to her previous solicitation: "You should know, however, that we will not record your name

112. Solove, *supra* note 2 (manuscript at 20).

113. *See id.*

anywhere on this list. Instead, our list will only include your telephone number along with any answers you provide.”

Suppose that Joe provides answers to this survey and, as before, he later finds himself under investigation by the FBI. This time, the FBI cannot identify Joe simply by searching XYZ-Marketing’s list, as his name does not appear on it. Therefore, the FBI contacts the local phone company to obtain Joe’s phone number, which enables the Bureau to compel XYZ-Marketing to hand over the appropriate file from its database.

In applying my proposed test to this variation of the example, courts will face a difficult challenge. They must conceptualize information which, in its original form, does not necessarily implicate privacy interests, but which nonetheless implicates such interests when aggregated with other information. In other words, the FBI’s collection of Joe’s phone number may not violate an informationship, because phone numbers alone have limited if any privacy expectations attached to them. Likewise, the FBI’s collection of XYZ’s anonymous data does not violate privacy norms, because Joe received warning that it might be shared with the company’s “affiliates.” However, the collection and use of both pieces of information almost certainly violates Joe’s privacy expectations, because such combination allows the FBI to attribute the information to Joe. As Daniel Solove has suggested, “[aggregation] results in revealing people in ways far beyond their expectations when giving out their data.”¹¹⁴

Thus, to construct a privacy paradigm that fully accounts for the reasonableness of seizing aggregated information, courts must account for what I will refer to as meta-information—information that establishes relationships or links that connect discrete pieces of data. For instance, the FBI’s knowledge that the number next to Joe’s information on the XYZ list corresponded to Joe’s name was a piece of meta-information because it allowed the government to make use of data that was previously anonymous.

When applying the various prongs of the proposed privacy test, courts should specifically examine the meta-information involved and decide whether privacy interests attach to it. To ignore such meta-information would deny the many ways in which piecing together discrete pieces of data can destructively impact dignity and privacy. A court examining the FBI’s seizure of Joe’s information would thus ask specifically whether the information linking his consumer preferences to his name violated reasonable expectations of privacy. The answer to that question would likely be yes, as Joe transferred his data to XYZ under the explicit understanding that the information would remain

¹¹⁴ *Id.* (manuscript at 21).

anonymous. The government's ability to link Joe's information with his name fundamentally altered the character of the data. Stripping the data of its anonymous quality magnifies the intrusiveness of an investigation. Courts should view such tactics as rising to the level of a Fourth Amendment search.

To draw an analogy, we might think of personal information given out in daily life as akin to the coins left in the "Take a Penny, Leave a Penny" trays common in convenience stores. Surely, taking a person's penny from the tray to make proper change does not violate the giver's expectations, as the penny is left precisely for that purpose. However, if one were somehow able to surreptitiously follow a person around for years, swiping his pennies every time he left them in a tray, such behavior would contravene the intended function of the tray and exploit the good intentions of the individual. Likewise, when the government amasses personal data without any particularized showing of guilt or suspicion, it engages in a similar betrayal of the trust of its citizens. Technology allows data to be exchanged and collected in such vast amounts as to create a potentially destructive force out of even the most ordinary and seemingly innocent transactions.

C. Practical Effects

1. Enhanced Protection

By drawing courts' attention not only to the presence of disclosure but also to the conditions that attach to such disclosure, my test would afford greater constitutional protection to much of the data exchanged by individuals. For example, when asking whether information has been disclosed in privacy under the first two prongs, courts are likely to import societal beliefs about which types of information are especially deserving of protection. Thus, customarily protected information such as medical histories, psychological counseling records, attorney-client conversations, and clergy-parishioner communications would likely trigger the rebuttable presumption of a required warrant.

Seized information that was protected by confidentiality agreements, devices, or protocols would also more frequently receive constitutional protection. For example, the existence of explicit contracts barring disclosure by the parties to an informationship would lead courts to recognize established privacy expectations under the test's first prong, because such contracts provide convincing and verifiable evidence of concerns about disclosure. Technological security measures such as encryption and password protection would also frequently trigger such recognition, as they tend to underscore the privacy expectations that attach to everyday communications such as e-mails and instant messages. Like the defendant's closing of the phone booth door in *Katz*,

such security measures serve as symbolic gestures that affirm the reasonableness of excluding others from the contents of our communications.

Courts applying my framework would also accord greater Fourth Amendment protection to information that, if disclosed, would implicate political- or speech-related freedoms. The test's inquiry as to whether the government was among the recipients in privity would prompt courts to examine the precise reasons individuals have for denying the government privity to various types of information. Courts could not fully analyze those reasons without considering the chilling effects of allowing law enforcement to easily pry into individuals' nonpublic opinions, or to enter confidential zones of candid, freewheeling communication. Thus, courts would likely recognize the need to afford heightened protection to informationships manifested in things such as library records, confidential communications with the press, logs of websites a person has visited, and nonpublicized membership lists of political groups.

2. *Outside the Fourth Amendment*

It is worth noting, as a final matter, which categories of information would not receive constitutional protection under the framework. My framework would not submit publicly available or nonsensitive data about individuals to the presumption of a warrant requirement. Data falling into these categories include those revealing, for example, whether individuals have visited a place open to the public, whether they subscribe to cable television, what school they attended (but not their grades), and the jobs they have held. Such information would escape the test's presumption because few if any individuals have reasonable justification for making such facts a secret to either the public or the government.

Nonpersonal information held by corporations would be treated similarly for this same reason. Thus, a company's balance sheets, employment lists, and many other documents could be obtained without a search warrant, so long as the documents did not contain records that, if disclosed, would contravene an individual's privity expectations. This treatment accords with the Supreme Court's distinction between the corporation as "a creature of the State" and the individual citizen who "owes no duty to the State . . . to divulge his business."¹¹⁵

Nor would my framework prevent police from requesting the voluntary cooperation of third parties. As explained earlier, the assumption of risk

115. *Hale v. Henkel*, 201 U.S. 43, 74 (1906).

doctrine—which allows police to obtain information with third-party consent—does not threaten privity in the same way as does the compulsory seizure of such data.¹¹⁶ Because informationships necessarily entail the mutually recognized obligations of two parties, each party retains the power to destroy or deny the informationship. Thus, law enforcement officials operating under this Note's framework would be able to seek the voluntary cooperation of third parties without running afoul of the Fourth Amendment. In particular, they could request documents or information from a third party while making clear that the production of such documents was not mandatory. This would then put the onus on the third party to evaluate whether it had any obligations as a party to an informationship. If the third party decided to withhold the information, the government could compel disclosure only by seeking a warrant (or subpoena).

Such a scheme may fail to protect privacy when third parties do not uphold the promises made to the originators of information. The ethical responsibility for a third party's disclosure in such cases, however, would appropriately be borne by the third party alone, and not by the government. Because the Constitution does not command respect for privacy by nongovernment individuals, this problem could more appropriately be addressed by statutory solutions.

Ultimately, shifting from a subpoena framework to a request-for-information framework could bolster privacy. The changed framework would give individuals and third parties an incentive to define carefully the terms of their informationships (either contractually or through privacy policies) in anticipation of possible law enforcement inquiries. Societal notions of privity and privacy would become more explicitly and frequently defined, further aiding the analytical work of judges and scholars.

CONCLUSION

This Note has reoriented discussion of the Fourth Amendment's protections for information exchanges around a privity framework. The information age has combined increasingly complex and powerful technological hardware with an ever-evolving set of multilayered social software. And yet courts continue to speak in the simplistic binary of the third-party doctrine. *Katz* offered a glimmer of hope for an adequate informational jurisprudence. That hope was later extinguished by *Miller* and *Smith*. Since then, few attempts have been made either in the Court's decisions or in the

116. See *supra* notes 58-59 and accompanying text.

academic literature to propose a feasible constitutional alternative to the “show one, show all” premise of the third-party doctrine.

The right to privacy as a mandate of our Constitution is not a new creation born of penumbral abstractions. Rather, such a right is directly implied by the Fourth Amendment’s guarantee that individuals be secure in their “papers.” The test proposed above offers a broad outline of how courts can respect the value of informationships. This Note has provided guidelines for courts to implement a more expansive, fair, and nuanced framework for Fourth Amendment violations involving information held by third parties.

Necessarily, the discussion has been largely theoretical and has focused on the rights of individuals as defined in the principles of the Fourth Amendment. To provide more specific guidance might contradict the premises and text of the Fourth Amendment, which center not on specific rules and concrete applications frozen in time, but rather on reasonable definitions of common words. In interpreting words such as “secure” and “search,” the task of legal thinkers and academics must be to provide courts with the appropriate conceptual tools for analysis, leaving precise meanings to the needs and shared values of particular times and settings. By pointing to the right to privacy as a textual command of the Fourth Amendment, scholars can help judges and practitioners recognize a highly useful tool for approaching problems of information control. In so doing, they can augment and modernize interpretations of the Fourth Amendment in order to better address problems that arise from a world increasingly defined by informationships.