Christopher Drake, "Conversational Standing: A New Approach to an Old Privacy Problem"
15 Everett Street #48, Cambridge, MA 02138 * Tel. (415) 205-9697 * cdrake@law.harvard.edu

Thank you very much for your consideration of the following article. The piece discusses the long-established shared privacy interest in conversations in American society, from the country's infancy up to the present day. Its core argument is as follows: (1) the protection of the Fourth Amendment should apply more broadly throughout remote conversations; (2) the extent of the protection should not depend on the means of the conversation's transmission, i.e. land line telephone, cellular telephone, instant message, text message, e-mail correspondence, FAX, etc.; (3) since there is a reasonable expectation of shared privacy in certain conversations, extending the coverage of the Fourth Amendment to conversations will bring search and seizure jurisprudence more in line with common customs, and would be more an affirmation of American society's general and rightful expectations than unfounded judicial policymaking.

Christopher M. Drake
J.D. Candidate, Harvard Law School, June 2007

Conversational Standing: A New Approach to an Old Privacy Problem

Despite the increasing complexity, accessibility,[1] and importance of communication technologies,[2] many characteristics of today's communication mirror those existing in the early days of the United States Constitution.[3] One of the most notable is the shared expectation of privacy in a conversation. In the remote communication context, despite differences between the various remote media in common use, it is the *conversation*[4] in which people expect privacy and in which such expectations are often objectively reasonable. Courts have nevertheless used a range of criteria to evaluate the objectively reasonable expectation of privacy, including means, place, time, content, and more. In most cases, including those the judiciary has not yet considered, this approach is likely to be both misguided and unnecessary.

Remote communication is a clear example of an institution[5] whose core precepts have not changed.[6] The Supreme Court has already acknowledged as much.[7] For instance, remote

[1] See Mulligan, Reasonable Expectations in Electronic Communications: A Critical Perspective on the Electronic Communications Privacy Act, 72 GEO. WASH. L. REV. 1557, 1572-76 (2004) (detailing the increasingly widespread use of the Internet in the United States).
[2] See Adler, Note, Cyberspace, General Searches, and Digital Contraband: The Fourth Amendment and the Net-Wide Search 105 YALE L.J. 1093, 1109 (1996) (describing an increasing reliance on computers and computer-based communication technology); Katopis, "Searching" Cyberspace: The Fourth Amendment and Electronic Mail, 14 TEMP. ENVTL. L. & TECH. J. 175, 177-78 (similar observation).
[3] Even so, some commentators have argued that interpretations of the Fourth Amendment should not be so rooted in expectations of the past and their applicability to modern-day fact patterns. See, e.g., Henderson, Nothing New Under the Sun? A Technologically Rational Doctrine of Fourth Amendment Search, 56 MERCER L. REV. 507, 563 (2005) (arguing that "the command of the Fourth Amendment is better served by adapting to changing circumstances than tenaciously hanging onto the past").
[4] Merriam-Webster's Online Dictionary defines "conversation" as an "oral exchange of sentiments, observations, opinions, or ideas," at http://www.m-w.com/dictionary/conversation. Here and throughout, for purposes of the argument, this definition of conversation will extend to any similar exchange, whether written or oral, in which at least two people are exchanging sentiments, observations, opinions, ideas, or other information.
[5] See Mulligan, *supra* note 1, at 1586 ("The change in form [between e-mail and 18th Century letters] should not override the shared nature of paper correspondence and electronic correspondence").
[6] Postal correspondence is, at least arguably, exactly one form of interaction the Fourth Amendment sought to protect. For analysis of the similarities between letters of the late 18th Century and e-mails of today, see Guirguis,

communication is the core purpose of personal letters, sometimes even involving interaction by way of back-and-forth letter writing. The Framers of the Bill of Rights would almost certainly have recognized privacy in letters due to their conversational nature. In the broader context, there is no meaningful difference between a letter and a facsimile or e-mail, [8] between cordless, land-based, and cellular telephone conversations,[9] or between a text message on a cellular phone and an instant message on a computer. All of these different communication tools share the same foundation: remote interaction with specific parties.[10] If the parties have taken reasonable steps to make their interactions private, then a presumption of objectively reasonable privacy expectations should prevail.[11]

The Constitution's Fourth Amendment[12] has long served as the anchoring constitutional privacy provision, recognizing certain spheres of life that the government may only infiltrate with good, sanctioned reason. The jurisprudence construing the Fourth Amendment is by now extensively developed. However, the change in communication capabilities has been so rapid that the judiciary has not been able to interpret the resulting privacy concerns consistently.[13] The key difficulty with the emerging jurisprudence has been a seeming arbitrariness, lack of clarity, or approach that is otherwise out of touch with common practice.[14] One example is the greater judicial protection for telephone calls made through land-based connections than for calls made

---

Electronic Mail Surveillance and the Reasonable Expectation of Privacy, 8 J. TECH. L. & POL'Y 135 (2003). See also id. at 155 (noting that "an overly broad warrant authorizing the police to monitor all sent and received e-mails repulses the Fourth Amendment as much as the general writs of colonial America the Framers expressly sought to ban").

[7] For instance, the Supreme Court has repeatedly established that letters and packages qualify as "effects" receiving constitutional protection. See, e.g., United States v. Jacobsen, 466 U.S. 109, 114 (1984) ("Letters and other sealed packages are in the general class of effects in which the public at large has a legitimate expectation of privacy; warrantless searches of such effects are presumptively unreasonable").

[8] Though courts and commentators have made numerous analogies between these forms of communication and others that do not carry particularly strong privacy protections. One such example is the comparison between an e-mail message and a postcard, where the postcard does not receive the same privacy recognition as a postal letter because it is not in a sealed container. See Note, 110 HARV. L. REV. 1591, 1597 (1997) (describing analogies between postal mail and communications in cyberspace).

[9] See id.

[10] Of course, many of them also have the same physical infrastructure. See Guirguis, *supra* note 6, at 136 (noting that many of the most common modern communication devices are "essentially based on the telephone and make use of the same underground cables, digital lines, radios, and satellite links to make connections between two or more users")

[11] See Reetz, Note, Warrant Requirement for Searches of Computerized Information, 67 B.U. L. REV. 179, 197 (1987) (arguing that "[a]n individual's expectation of privacy in computer records should be considered legitimate when, under similar circumstances, the person would have a reasonable expectation of privacy in records of another form").

[12] "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated..." U.S. CONST. amend. IV.

[13] See, e.g., Sergent, Note, A Fourth Amendment Model for Computer Networks and Data Privacy, 81 VA. L. REV. 1181, 1228 (arguing that "[t]he information stored on a computer is the same as that which could be stored in filing cabinets or desks, and should receive the same protection).

[14] See 1 WAYNE R. LAFAVE, SEARCH AND SEIZURE: A TREATISE ON THE FOURTH AMENDMENT § 2.1(d) (4th ed. 2004), *citing* Luna, Sovereignty and Suspicion, 48 DUKE L.J. 787, 827 (1999) (noting that "[the Court] (1) 'has interpreted privacy to be a question of fact rather than a constitutional value' and (2) is apparently 'out of touch with society's true expectations of privacy.'")

using cellular[15] or cordless phones.[16] That discrepancy demonstrates an errant focus not on the communication via telephone, but instead on the means of transmission. Similarly, while the Supreme Court has held that the Fourth Amendment protects the contents of letters and sealed packages,[17] lower courts have been inconsistent in their willingness to extend Fourth Amendment protection to e-mail. For instance, e-mails and records of conversations on computer hard drives generally receive greater protection when sent from personal computers at home[18] rather than from computers at one's place of work.[19] In using the reasonable privacy inquiry, the courts are using more factors as the complexity of the communication technology increases.[20] The factors determine not only whether certain communications are protected in the first place, but also the amount of protection they receive.[21] Courts will only make their task more cumbersome by adding greater detail to the inquiry,[22] both for members of the bar and for members of society in understanding whether their privacy expectations are constitutionally reasonable. Because the expectation of conversational privacy is as old as the country itself, the best way to validate its legitimacy is constitutional acknowledgment, namely its recognition in the coverage of the Fourth Amendment.[23]

Fourth Amendment protection is limited to those who have "standing" to assert it. Generally speaking, a claimant must establish that his or her own Fourth Amendment rights were violated

---

[15] Though there is some support for the notion that courts will find an explicit expectation of privacy in cellular phone communications. See Guirguis, *supra* note 6, at 139-40 (describing interpretations of the Third, Fifth, and Eleventh Circuit Courts of Appeals that might suggest Fourth Amendment protection for cellular phone conversations).

[16] Price v. Turner, 260 F.3d 1144, 1148 (2001) (no objectively reasonable expectation of privacy in a cordless conversation "readily susceptible to interception," nor did the Federal Wiretap Act cover the conversation, since cordless conversations were not protected until 1994); United States v. Smith, 978 F.2d 171, 181 (5th Cir. 1992) (as a matter of law, no Title III or Fourth Amendment violation to intercept cordless telephone calls, even if the speaker had a subjective expectation of privacy); McKamey v. Roach, 55 F.3d 1236, 1239-40 ("No reported decision has concluded that a cordless telephone user has a reasonable expectation of privacy in his cordless phone conversations under [the] Fourth Amendment")

[17] Ex parte Jackson, 96 U.S. 727, 733 (1877).

[18] Though Professor Kerr argues for computers being analogized to "homes and sealed containers[:] Just as an individual generally has a reasonable expectation of privacy in his home and his packages, so too should he have a reasonable expectation of privacy in the contents of his personal hard drive." Kerr, Searches and Seizures in a Digital World, 119 HARV. L. REV. 531, 549 (2005).

[19] United States v. Bailey, 272 F. Supp. 2d 822, 836-37 (D. Neb. 2003) (no standing in files on a work computer). But see Mancusi v. DeForte, 392 U.S. 364, 369 (1968) (finding Fourth Amendment standing to exclude contents of office files of which Defendant had custody, although the files were taken from a space Defendant shared with other employees).

[20] See Kerr, The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution, 102 MICH. L. REV. 801, 875-76 (2004) (noting judicial struggles to digest fact patterns involving developing technologies and a resulting greater likelihood of judicial errors).

[21] See, e.g., Simon, The Tangled Web We Weave: The Internet and Standing Under the Fourth Amendment, 21 NOVA L. REV. 941, 968 (1997) (concluding that, in the context of e-mail sent over a network, "it would seem that encryption of data is the only way a user can attain a legitimate expectation of privacy for purposes of standing under the Fourth Amendment").

[22] Though some say the judiciary should not be as involved in such policy definitions. For the argument that determining reasonable expectations of privacy in light of technological advancements is more appropriate for legislatures, not courts, see generally Kerr, *supra* note 20.

[23] See Katopis, *supra* note 2, at 205 (arguing that "Constitutional case law [and] statutory bases to protect all the components of e-mail from government searches [must] be broadly construed").

in order to have standing to challenge a violation.[24] From the beginnings of Fourth Amendment jurisprudence, standing often depended on possession of, or some other property interest in, the challenged item or place.[25] Since the 1967 *Katz* decision,[26] however, standing generally has turned on whether the claimant had a reasonable expectation of privacy in the challenged item or place.[27] Justice Harlan, concurring in that decision, laid out the familiar two-part test for this expectation of privacy: first, the defendant must have demonstrated "an actual (subjective) expectation of privacy;" second, that "expectation [must] be one that society is prepared to recognize as 'reasonable.'"[28] Society has long recognized the shared privacy interest in certain conversations, applying equally to all participants.[29] Therefore, the judiciary should affirm that parties to those conversations have standing to challenge unreasonable government intrusion on the conversation.[30] Moreover, in adjusting Fourth Amendment jurisprudence to the increasing number of remote communication technologies, the "standing" inquiry should focus solely on the conversation itself and should not depend on the means of transmission.[31]

In practice, conversational standing would constitutionally prevent the intrusion of the government, or its agents, on private communications, unless any of three exceptions applied. First, a properly issued and executed warrant authorizing interception of a conversation would

[24] See Rakas v. Illinois, 439 U.S. 128 (1978).
[25] See, e.g., Jones v. United States, 362 U.S. 257, 261 (1960) ("To establish 'standing,' Courts of Appeals have generally required that the movant claim either to have owned or possessed the seized property or to have had a substantial possessory interest in the premises searched")
[26] 389 U.S. 347 (1967).
[27] Professor Kerr contends that the shift in judicial inquiry has not been as significant as it might first appear. See Kerr, The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution, 102 MICH. L. REV. 801, 807 (2004) ("The Katz 'reasonable expectation of privacy' test has proven more a revolution on paper than in practice; Katz has had a surprisingly limited effect on the largely property-based contours of traditional Fourth Amendment law").
[28] Id. at 361 (Harlan, J., concurring).
[29] Following up on the principle announced in *Katz*, the Supreme Court suggested that both parties to a telephone conversation have standing to object to a warrantless wiretap of the phone line, but only if law enforcement is violating a clearly protected constitutional right, such as presence in one's own home. See Alderman v. United States, 394 U.S. 165, 176 (1969). Nevertheless, the Supreme Court and lower courts have yet to clearly establish, or even address, privacy protections for recorded conversations after they reach their recipients, or for conversations transmitted by means other than grounded telephone lines. For instance, the sender of a postal letter loses her expectation of privacy in the letter's contents upon delivery. United States v. King, 55 F.3d 1193 (6th Cir. 1995). The Supreme Court has stated that the Fourth Amendment does not protect against other parties to a conversation informing the police of wrongdoing. Hoffa v. United States, 385 U.S. 293 (1966); United States v. White, 401 U.S. 745 (1971). However, it has not indicated whether the sender retains standing in the conversation if the police obtain a copy of it without a proper warrant and after the recipient has already seen it, as with an opened letter found in a search of the recipient's house. See United States v. Dunning, 312 F.3d 528, 531-32 (1st Cir. 2002) (holding that the sender had neither a legitimate expectation of privacy in the letter to his girlfriend once it was delivered nor a legitimate expectation of privacy in his girlfriend's home).
[30] Commentators have suggested that just such a principle underlies Fourth Amendment jurisprudence generally. See Kerr, Digital Evidence and the New Criminal Procedure, 105 COLUM. L. REV. 279, 297 (2005) ("Fourth Amendment rules traditionally focus on the justification for entry into a space, not whether the item to be seized after the space is entered should be deemed public or private"). In this sense, the actual content of whatever conversation the government wants to access is immaterial. Rather, it is the government's act of intrusion on the conversation itself, regardless of content, that is the "entry into a space" and that courts might consider a constitutional infraction.
[31] See Katopis, *supra* note 2, at 199 (arguing that "[c]ontent is precisely what the Fourth Amendment strives to protect").

make that intrusion, and any information obtained from it, constitutionally reasonable.[32] Second, the government could defeat claims of conversational standing if exigent circumstances required the intrusion.[33] An example would be the imminent destruction of evidence in light of probable cause and not enough time to secure a warrant.[34] Finally, if any party to the conversation invited the government's participation,[35] then the government would become an equal participant in the conversation, and the original parties would have no standing to challenge the government's participation.[36] In other words, any invited participant in the conversation, meaning one at whom anyone already participating directed any communication pursuant to the conversation, could either inform the government of the conversation's content or allow the government to "listen in" without infringing any other party's rights. The rule would apply even without the knowledge or consent of any other party,[37] just as anyone can disclose any part of a conversation to a third party without the knowledge of any other direct participant[38] and without violating the Fourth Amendment. Generally speaking, the concept calls for protection from *uninvited* government intrusion on a conversation — that is, participation without any invited party's knowledge or consent.[39] The goal would be to protect conversational privacy from government intrusion only as much as we protect it in our ordinary social relations. That protection is precisely what reasonable expectation of privacy doctrine targets,[40] so the recognition of conversational

[32] Such a condition would not always invalidate standing, however. The party or parties could argue that the warrant did not properly issue, substantively or procedurally, and that the good faith exception to the exclusionary rule should not apply. If the challenge were successful, the court would then retroactively invalidate the warrant and could grant conversational standing unless it found either of the other two exceptions applicable.

[33] See Michigan v. Clifford, 464 U.S. 287 (1984).

[34] The government would still have the burden of proving that it had probable cause to make the intrusion, that it reasonably believed that the evidence sought was on the brink of destruction, and that it could not have obtained the evidence but for the warrantless intrusion

[35] Settled doctrine holds that one who sends or otherwise offers up a communication does not have a constitutional right to stop the recipient from turning that communication over to the government. Lopez v. United States, 373 U.S. 427 (1963); Hoffa v. United States, 385 U.S. 293 (1966); United States v. White, 401 U.S. 745 (1971); United States v. King, 55 F.3d 1193 (6th Cir. 1995); United States v. Lee, 359 F.3d 194 (3d Cir. 2004); United States v. Charbonneau, 979 F. Supp. 1177 (S.D. Oh. 1997); United States v. Jones, 364 F.Supp.2d 1303 (D. Utah 2005). See also Adler, *supra* note 2, at 1111 (noting that the risk of third parties disclosing information willingly revealed "in public or [to] others" is a "natural part of human interaction").

[36] Justice O'Connor, concurring in part and in the judgment in *United States v. Karo*, illustrated this principle nicely by analogizing a conversation to a jointly controlled container: "[T]wo people who speak face to face in a private place or on a private telephone line both may share an expectation that the conversation will remain private, but either may give effective consent to a wiretap or other electronic surveillance. One might say that the telephone line, or simply the space that separates two persons in conversation, is their jointly owned 'container.' Each has standing to challenge the use as evidence of the fruits of an unauthorized search of that 'container,' but either may also give effective consent to the search." United States v. Karo, 468 U.S. 705, 726 (1984) (O'Connor, J., concurring) (internal citations omitted).

[37] To reiterate: in most conversations, no one participant has direct control over whom any other participant invites to join the conversation, nor over what that participant chooses to disclose. Exceptions include conversations held under contractual agreements of confidentiality, in which case aggrieved parties' claims of standing would most likely survive.

[38] This kind of behavior is better known as "gossip," which happens often despite its negative connotation.

[39] "Knowledge and consent" subsumes the Fourth Amendment's provisions allowing governmental intrusion in certain instances. In other words, if the government has a warrant and/or probable cause, then it is assumed to be acting with the knowledge and/or consent of the parties.

[40] The Supreme Court has itself acknowledged the need to align judicial standards with societal expectations, particularly when Fourth Amendment privacy rights are at stake: a reasonable expectation of privacy must have "a source outside of the Fourth Amendment, either by reference to concepts of real or personal property law or to

standing would be not only a small departure from the established jurisprudence, but also a major step in favor of societal expectations.

While the first prong of the *Katz* test is less doctrinally puzzling because it is heavily fact-based, the second prong presents the greatest challenge to the judiciary because its legal interpretation now determines when a claimant has standing.[41] This prong is at the center of this Article's discussion because it calls for a close look at society's attitudes about privacy. Its language suggests that the judiciary should consider both societal attitudes that have changed with the growth of communication and those that have remained constant. The more simply courts apply the *Katz* standard, the more effective, consistent, and trustworthy their conclusions will be,[42] and the more they will avoid a clash with societal beliefs about privacy.[43]

The Article proceeds in three parts. Part I examines the history of Fourth Amendment standing and describes the doctrine's evolution into its present form. Part II explains the importance of recognizing standing throughout a conversation, equally applicable to all of the conversation's participants, as well as the limits and implications of conversational standing. Part III concludes with a discussion of modern-day interpretations of shared privacy interests and how they might apply to the concept of conversational standing as described throughout.

I. History & Overview of Fourth Amendment Standing

The Fourth Amendment traditionally only protects property — and now, in a broader sense, privacy — under specific circumstances. The one constant underlying all Fourth Amendment requirements is that anyone claiming the protection of the Fourth Amendment must have standing to assert it. The most significant characteristic of Fourth Amendment standing doctrine is that "Fourth Amendment rights … may not be vicariously asserted."[44] That is, parties only have standing to assert their own clearly defined constitutional rights, not those of others, even those constitutional rights in which they might have some legitimate stake.[45] This same principle holds for constitutional violations: in order to have Fourth Amendment standing, parties must show that the constitutional violations were directed against *them*,[46] such as police invasion of the violated party's home (but not that of a good friend or a neighbor), or wiretapping of the

---

understandings that are recognized and permitted by society." Minnesota v. Carter, 525 U.S. 83, 88 (1998), *citing* Rakas, 439 U.S. at 143-44 & n.12.

[41] See Rakas, 439 U.S. at 143 n.12 ("a 'legitimate' expectation of privacy by definition means more than a subjective expectation of not being discovered"); see also id. at 148 (petitioners' claim failed because they "made no showing that they had any legitimate expectation of privacy…").

[42] See Simmons, From Katz to Kyllo: A Blueprint for Adapting the Fourth Amendment to Twenty-First Century Technologies, 53 HASTINGS L.J. 1303 (2002) (arguing that the Katz test should be applied with only the results of the challenged intrusion in mind, not the method of intrusion).

[43] See, e.g., Mulligan, *supra* note 1, at 1592 ("Individuals consider their e-mail private, and the Court has consistently reiterated the importance of protecting the privacy of private communications").

[44] *Alderman*, 394 U.S. at 174.

[45] For a broad overview of the evolution of standing doctrine and its effect on enforcement of the exclusionary rule, see Steiker, Counter-Revolution in Constitutional Criminal Procedure? Two Audiences, Two Answers, 94 MICH. L. REV. 2466 (1996).

[46] *Alderman*, 394 U.S. at 171-72; United States v. Padilla, 508 U.S. 77, 81-82 (1993). See also United States v. Williams, 580 F.2d 578 (D.C. Cir. 1978).

violated party's personal phone line (but not that of a family member).[47] Likewise, parties may only challenge the admission of tainted evidence[48] against *them* in legal proceedings, not evidence that is admitted against another party but nonetheless implicates the would-be-contesting parties.[49] Judicial interpretation is critical because the concept is circular: standing is required to challenge constitutional violations, but a judicially-determined, constitutional stake in the violations is necessary to establish standing. The jurisprudence that has developed since *Katz*[50] and *Rakas v. Illinois*[51] has produced a much more compact doctrinal inquiry: Fourth Amendment protection only applies when the government has invaded the claimant's reasonable expectation of privacy.[52]

In order to enforce the protection of the Fourth Amendment, the United States Supreme Court adopted the now well-known exclusionary rule as a prophylactic measure.[53] The rule's development took place almost entirely during the 20th Century. It began with the case of *Weeks v. United States*,[54] which held that evidence obtained in violation of the Fourth Amendment was inadmissible in federal criminal trials.[55] The Court only extended the exclusionary rule to *state* criminal investigations many years later, in the 1964 case *Mapp v. Ohio*.[56] Throughout much of the 20th Century, an aggrieved party only had standing to challenge admission of certain evidence if the item at issue belonged to her, or if she otherwise had property rights in the invaded item or space rising to the level of constitutional protection.[57] The exclusionary rule became both a powerful tool for deterring government abuse in criminal investigations and a powerful means for defendants to retroactively suppress evidence against them. Nevertheless, its effectiveness in deterring law enforcement or protecting defendants depends almost exclusively on who has standing to assert the rule.

The 1967 *Katz*[58] decision solidified the role of the reasonable expectation of privacy in evaluations of standing. In *Katz*, the government taped a microphone to a telephone booth from which Charles Katz, suspected of involvement in an illegal wagering scheme, was known to

---

[47] See *Karo*, 468 U.S. at 725-26 (O'Connor, J., concurring) ("[A] third person, who never used a particular telephone line, could not suppress, at least on Fourth Amendment grounds, evidence obtained by an unlawful wiretap of conversations between two other persons").
[48] Evidence obtained pursuant to a Fourth Amendment violation.
[49] See *Alderman*, 394 U.S. at 179 (*citing* Silverthorne Lumber Co. v. United States, 251 U.S. 385 (1920); Johnson v. United States, 333 U.S. 10 (1948); Wong Sun v. United States, 371 U.S. 471 (1963)).
[50] 389 U.S. 347 (1967).
[51] 439 U.S. 128 (1978).
[52] See id. at 140.
[53] It is still worth noting that violations of the Fourth Amendment are generally only cognizable when the government commits them. Thus, the exclusionary rule does not apply when the government is not responsible for a privacy invasion that would otherwise violate the Fourth Amendment. Burdeau v. McDowell, 256 U.S. 465, 475 (1921) ("[The Fourth Amendment's] origin and history clearly show that it was intended as a restraint upon the activities of sovereign authority, and was not intended to be a limitation upon other than governmental agencies")
[54] 232 U.S. 383 (1914).
[55] Id. at 398.
[56] 367 U.S. 643 (1961).
[57] See United States v. Salvucci, 448 U.S. 83; Jones v. United States, 362 U.S. 257 (1960). See also United States v. Jeffers, 342 U.S. 48, 51-52 (1951) (holding that defendant had standing in narcotics seized from a hotel room to which his aunts had given him a key).
[58] 389 U.S. 347 (1967).

make regular phone calls.[59] The government recorded Katz's conversations in the booth, effectively eavesdropping on his phone calls without wiretapping the phone line. The evidence was admitted against Katz and used to convict him. The Supreme Court overturned the conviction,[60] holding that the Fourth Amendment protected Katz's privacy in the phone booth from the government surveillance.[61] Two often-quoted dicta from the opinions in *Katz* are arguably most responsible for the shift in standing doctrine. The first is Justice Potter Stewart's assertion in the majority opinion that "the Fourth Amendment protects people, not places,"[62] suggesting that the Court would look more closely at a broader set of personal concerns rather than confining itself to property or possessory interests.[63] The second assertion, from Justice Harlan's concurring opinion, has become the linchpin of Fourth Amendment privacy determinations. Justice Harlan focused solely on a person's privacy interests in a place or thing. He suggested two factors to determine a person's reasonable expectation of privacy for Fourth Amendment purposes: first, whether the person "exhibited an actual (subjective) expectation of privacy" in the place or thing; second, whether "the expectation [is] one that society is prepared to recognize as reasonable."[64] As courts have seized on Justice Harlan's language since *Katz*, defendants now have Fourth Amendment privacy if they demonstrate both subjective and objective expectations of privacy in challenged evidence.

Despite the impact of *Katz*, property and possessory interests remain key to Fourth Amendment standing inquiries.[65] The Supreme Court quickly reaffirmed that principle, holding in the 1973 *Brown* decision that there is no Fourth Amendment standing to suppress evidence seized from a place in which the challengers lack possessory or property interests.[66] In that case, defendants successfully conspired to steal merchandise from a warehouse.[67] They stored the stolen items at a co-conspirator's store.[68] The government invaded the store and seized the stolen goods, using them as evidence to convict defendants despite a violation of the co-conspirator's Fourth Amendment rights.[69] Defendants challenged the admission of the evidence, but the Supreme Court held that they did not have standing because they were not on the premises when the government seized the evidence and, most importantly, because they had no possessory or property interest in their co-conspirator's store. [70] The opinion did not explicitly address defendants' privacy interests, presumably finding them either irrelevant or overridden by their

[59] *Katz*, 389 U.S. at 347.
[60] Id. at 359.
[61] Id. at 353.
[62] Id. at 351.
[63] The opinion also quotes language from *Warden v. Hayden* declaring that "[t]he premise that property interests control the right of the Government to search and seize has been discredited." Katz, 389 U.S. at 353, *citing* Warden v. Hayden, 387 U.S. 294, 304 (1967).
[64] Id. at 361 (internal quotation marks omitted).
[65] See Simmons, *supra* note 42, at 1314.
[66] Brown v. United States, 411 U.S. 223, 229 (1973) (holding that defendants did not have standing because they "were not on the premises at the time of the contested search and seizure, alleged no proprietary or possessory interest in the premises, and were not charged with an offense that includes, as an essential element of the offense charged, possession of the seized evidence at the time of the contested search and seizure").
[67] Id. at 224-25.
[68] Id. at 225.
[69] Id. at 225-26.
[70] Id. at 229.

lack of proprietary interests in the store. It served as one clear example that the Court would not limit its evaluations of standing to the *Katz* privacy framework.

The Supreme Court's 1979 decision in *Rakas v. Illinois*[71] has become the leading case on Fourth Amendment standing over the past two decades. In *Rakas*, police stopped defendants, suspected of robbing a clothing store, as they escaped in a car.[72] Upon searching the car, the police found ammunition in the glove compartment and a sawed-off rifle under the front passenger seat,[73] which were admitted into evidence against defendants and used to convict them. Defendants argued that the search of the car in which they were traveling, and the seizure of the weapons found inside the car, violated their constitutional rights. Nevertheless, the Supreme Court held that they did not have standing to suppress the guns and ammunition as evidence because they neither owned nor had any recognized property interests in the car.[74] Such a property or possessory interest would certainly have existed if any of the defendants had owned the car, and would probably have existed if defendants had been allowed to borrow the car indefinitely. However, since the defendants did not have those interests, they did not have standing and their convictions were upheld.

Shortly after the Court decided *Rakas*, a government loophole to violate the Fourth Amendment in obtaining evidence entered the doctrinal scheme. *United States v. Payner*[75] involved a man indicted for falsifying his tax returns.[76] The evidence used to indict him was recovered through a private investigator's plan, designed to access bank records from a Bahamian bank that would demonstrate Payner's guilt.[77] In order to get the bank records, however, the investigator arranged a plan to steal a briefcase belonging to the bank's vice president, knowing that the briefcase contained the condemning evidence.[78] The Court held that Payner did not have standing to suppress the evidence seized from the bank's vice-president, both because he did not have a reasonable expectation of privacy in the bank records[79] and, implicitly, because he did not own the stolen briefcase.[80] In other words, since Payner and the bank vice-president did not share a privacy interest in either the briefcase or the records, Payner had suffered no constitutional

[71] 439 U.S. 128 (1978).
[72] Id. at 130.
[73] Id.
[74] Id. at 143, 149-50 & n.17.
[75] 447 U.S. 727 (1980).
[76] Id. at 728.
[77] Id.
[78] Id.
[79] Id. at 732, *citing* United States v. Miller, 425 U.S. 435 (1976) (holding that a bank customer had no reasonable expectation of privacy in checks, deposit slips, and other records of his banking activity).
[80] 447 U.S. at 733-34. The Court acknowledged "the District Court's commendable desire to deter deliberate intrusions into the privacy of persons who are unlikely to become defendants in a criminal prosecution," in this case the bank vice-president, and opined that "[n]o court should condone the unconstitutional and possibly criminal behavior of those who planned and executed this 'briefcase caper.'" Nevertheless, it justified lack of standing on a balancing test, weighing the value of excluding evidence "against the considerable harm that would flow from indiscriminate application of an exclusionary rule," concluding that the court should not have exercised such discretion in barring the evidence against Payner. Rawlings v. Kentucky, 448 U.S. 98 (1980), presents virtually the same justification, although its holding would have denied standing based on privacy in another person's effects. Thus, according to a *Rawlings* analysis, even if Payner had retained an expectation of privacy in his bank records, he would have lacked an expectation of privacy in the vice-president's briefcase and thus could not challenge the admission of the records as evidence.

violation. The judgment came over a lengthy and vigorous dissent by Justice Marshall, who crisply summed up the dangers inherent in the majority's interpretation: "[The] holding effectively turns the standing rules created by this Court for assertions of Fourth Amendment violations into a sword to be used by the Government to permit it deliberately to invade one person's Fourth Amendment rights in order to obtain evidence against another person."[81] Under *Payner*, despite serious concerns that even the majority itself acknowledged, almost any evidence against a third party is fair game for government seizure if the third party has no individual or shared privacy interest in the evidence or in the location of the evidence.[82]

Rakas indicated that privacy depends heavily on context. Defendants might have subjectively expected privacy from the government in the car, but the holding indicates that such an expectation was not objectively reasonable at the time. One common example of this subjective-objective conflict is government surveillance of workplace computers. Regardless of the likelihood of employer monitoring, any posted disclaimer removes any expectation of privacy the employee has in her actions on a workplace computer.[83] Strongly implied disclaimers, such as on computers that the employee knows others will be using, also defeat the privacy expectation.[84] However, if employees have control and authority over a space or items in a common workplace environment, they may have standing to challenge government intrusion on the space or items, based primarily on their possessory interest.[85] Overall, the privacy and proprietary interests have become intertwined. Although each is significant in determining a defendant's standing, the one generally implies the other, at least in some measure.[86]

Conversational privacy depends on the validation of shared privacy interests, but the judiciary's shared privacy recognition is murky even beyond the conversational context. For example, in *Minnesota v. Olson*,[87] defendant had standing because he was a designated overnight guest in an apartment and thus had an objectively reasonable expectation of privacy in his belongings kept there during his stay.[88] However, in the more recent *Minnesota v. Carter* decision,[89] defendants did not have standing as invited guests in an apartment because they were there only for a limited time and were there for a business purpose, albeit an illicit one.[90] Since their presence was only transitory and for such a narrow purpose, they had no objectively reasonable expectation of

[81] Id. at 738 (Marshall, J., dissenting).
[82] See Rawlings, 448 U.S. at 105-06 (holding that defendant lacked standing to challenge seizure of controlled substances from an acquiantance's purse because he had no reasonable expectation of privacy in the purse).
[83] See United States v. Angevine, 281 F.3d 1130, 1135 (10th Cir. 2002) (finding that a university professor had no reasonable expectation of privacy on workplace computer with clear disclaimers warning against misuse). See also Bailey, 272 F. Supp. 2d at 831; United States v. Simons, 206 F.3d 392, 398 (4th Cir. 2000); Monroe v. United States, 52 M.J. 326, 328, 330 (Court for the Armed Forces 2000).
[84] See United States v. Butler, 151 F. Supp. 2d 82, 84 (D. Me. 2001) (holding that there is no "generic expectation of privacy" on computers in a university computer lab).
[85] See O'Connor v. Ortega, 480 U.S. 709 (1987); DeForte, 392 U.S. at 369; Levanthal v. Knapek, 266 F.3d 64, 73 (2d Cir. 2001) (finding a reasonable expectation of privacy in an office computer not shared with other employees).
[86] See *Salvucc*i, 448 U.S. at 95; *Rawlings*, 448 U.S. at 105-06 (finding no reasonable expectation of privacy in items seized from a purse not belonging to defendant); Minnesota v. Olson, 495 U.S. 91, 98-99 (1990) (finding a reasonable expectation of privacy as an overnight houseguest); Minnesota v. Carter, 525 U.S. 83, 91 (1998) (finding no reasonable expectation of privacy as temporary houseguests for business purposes).
[87] 495 U.S. 91 (1990).
[88] Id. at 100.
[89] 525 U.S. 83 (1998).
[90] Id. at 91.

privacy from government intrusion, and their convictions were upheld.[91] The two cases set up an ambiguity in shared privacy interests:[92] Olson and the apartment owner had a shared privacy interest that the government unreasonably invaded, but the Carter defendants did not. Even in these situations, which could have been nearly identical more than 200 years ago, the Supreme Court has suggested that there are a number of varying factors to consider in determining shared privacy interests and relevant Fourth Amendment standing.[93] Not only will the multiplicity of factors make the judiciary's work much tougher, but it could also lead to ad hoc determinations of standing.

The combination of *Payner, Rakas, Olson*, and *Carter* gives at least some guidance as to which shared privacy interests the Supreme Court will now recognize. First, *Payner* and *Rakas* establish that claimants can only assert their own rights and not those of others — that is, they cannot argue that someone else's privacy was constitutionally violated and claim the same privacy right for themselves. On the other hand, *Olson* and *Carter* demonstrate that guests often do have shared privacy rights and, consequently, have Fourth Amendment standing in their capacity as guests. While *Carter* indicates that the right depends on the context of the visit,[94] the majority still acknowledged that guests often qualify for Fourth Amendment standing.[95] Property concerns were critical to the determination of privacy interests in all four cases, involving ownership itself or the rights implicated by granting access to certain property. The principle emerging from the cases appears to be that "legitimate" guests have constitutionally protected privacy interests in certain tangible property, including a home, a vehicle, or other effects. However, the applicability of this principle to intangible evidence remains to be seen.

The inquiry in cases of intangible evidence, and Fourth Amendment standing to suppress that evidence and its fruits, still focuses almost exclusively on the reasonable expectation of privacy. One of the most common examples of the judiciary's intangible privacy examination is the Internet chat room. Many of the criminal interactions on Internet chat sites involve child pornography. Generally, there is no reasonable expectation of privacy in public Internet chat

---

[91] Professor Weinreb was less than pleased with this outcome. See Weinreb, Your Place or Mine? Privacy of Presence Under the Fourth Amendment, 1999 SUP. CT. REV. 253, 256 (1999) ("[T]he decision in Carter is possibly the most clearly mistaken and the underlying jurisprudence the most inadequate of all the cases decided under the Fourth Amendment in the past thirty years").

[92] The disconnect between these two cases creates an even larger set of plausible inconsistencies. For example, if the defendant in *Olson* had been an overnight guest on a business trip, would he have had standing? What if he had not been a friend of the apartment's owner or tenant? If he had not initially planned to spend the night but were then invited to stay? Similarly, if the defendants in *Carter* had intended to spend the night after completing their illicit business, would they have had standing to object? What if the business were not facially illegal but were instead part of a larger conspiracy? And what if the case had been decided on different grounds, such as the defeat of defendants' privacy interests with the apartment's blinds left open wide enough for a police officer to see inside? Any of these hypothetical situations could easily take place, just as any of them could have been part of circumstances that the police could not have understood ex ante.

[93] See, e.g., Georgia v. Randolph, 126 S.Ct. 1515 (2006); Illinois v. Rodriguez, 497 U.S. 177 (1990); United States v. Matlock, 415 U.S. 164 (1973).

[94] *Carter*, 525 U.S. at 90 ("[A]n overnight guest in a home may claim the protection of the Fourth Amendment, but one who is merely present with the consent of the householder may not").

[95] See id. at 89 ("[W]e have held that in some circumstances a person may have a legitimate expectation of privacy in the house of someone else").

rooms, including from undercover government agents who participate.[96] Defendants who expose criminal activity in these chat rooms essentially run the risk that anyone will participate, placing the government on equal footing with any other participant and therefore making the surveillance reasonable under the Fourth Amendment. Even if defendants are not participating in public chat room conversations, instead maintaining written or otherwise recorded communications with one or a few people, the Fourth Amendment does not protect defendants from having the contents of the conversation disclosed to the government.[97] Further, if the government secretly participates while assuming a different identity, the contents of the conversation are still admissible and the Fourth Amendment does not shield them.[98]

Protection strengthens only if a tangible implement is involved. Thus, in *United States v. Carnes*,[99] defendant had standing to challenge admission of six audio tapes with recorded conversations between himself and his girlfriend.[100] The physical evidence containing the intangible evidence belonged to him and was found in his girlfriend's home, and he was found to have a possessory (and, by extension, privacy) interest in the seized tapes even though they were illegally made and he did not lawfully "own" them.[101] The case demonstrates that although privacy is the dominant inquiry, the evaluation has become so multi-faceted that it risks becoming even more cumbersome and nuanced as technological progress continues. Any clarity in the governing standards could soon become baffling, making the judiciary's job even more difficult.

Fortunately, there is a pre-emptive solution to the possible confusion on Fourth Amendment privacy concerns. Participants reasonably expect certain conversations to remain private. Even though the judiciary has not explicitly addressed Fourth Amendment standing in conversations *per se*, recognizing inherent privacy in conversations is a plausible approach. Moreover, adopting the concept of conversational standing would not only make future evaluations easier for the courts, but would also better align the jurisprudence with societal expectations of privacy. The following section describes how conversational standing would operate, how courts might apply it uniformly in cases invoking conversational privacy, and why it is particularly important to recognize conversational standing in today's increasingly complex communication landscape.

II. Conversational Standing

A. The Shared Privacy of Conversations

---

[96] See, e.g., *Charbonneau*, 979 F. Supp. 1177; State v. Evers, 815 A.2d 432 (N.J. 2003); State v. Townsend, 57 P.3d 255 (Wash. 2002); Commonwealth v. Proetto, 771 A.2d 823 (Penn. 2001); State v. Lott, 879 A.2d 1167 (N.H. 2005).
[97] *King*, 55 F.3d 1193; United States v. Mavroules, 813 F.Supp. 115 (D. Mass. 1993).
[98] *Townsend*, 57 P.3d 255; *Lott*, 879 A.2d 1167.
[99] 309 F.3d 950 (6th Cir. 2002).
[100] Id. at 959.
[101] Id. at 960. However, Carnes did *not* have standing to suppress a seventh tape, which was found in a tape recorder underneath his girlfriend's trailer home. The Court's reasoning conflicts somewhat with its rationale for Carnes's standing in the six other tapes seized: "Carnes never lived [in the trailer] and certainly was not present in it or in possession of the recorder or the tape when [his girlfriend] turned them over to the police. It would be unreasonable for him to claim an expectation of privacy with respect to something that he had no control or dominion over." Id.

The law currently grants Fourth Amendment standing to the party serving as the conduit for the government interception, such as the one whose telephone line is tapped or whose e-mail files are seized in transmission. Functionally speaking, the law officially recognizes only individual privacy interests in conversations, not shared privacy interests. Thus, in a private telephone conversation between two people, both in their homes, only the party whose phone the government wiretapped would have standing to challenge admission of any evidence based on the conversation.[102] The inquiry itself turns primarily on the invasion of the homeowner's explicit Fourth Amendment rights by tapping the telephone line.[103] This loophole opens the door for abusive government eavesdropping — not that this will actually take place,[104] but it certainly could.[105] When a commonly private conversation takes place, all parties to the conversation can reasonably expect that it will be free from governmental intrusion most of the time.[106] Particularly within the present array of remote communication possibilities, it is more important than ever to recognize the principle, implied in the Constitution, that certain conversations are presumptively private.

The judiciary's focus on fine technological distinctions and associated property rights has detracted from what should be its core focus: the nature of the relevant privacy interests. When it comes to conversations, privacy should not depend on technology. Without explicit statements to the contrary, such as disclaimers on computer screens or recorded disclaimers before phone calls begin, parties generally expect their remote communications to be free from warrantless government intrusion. Some parties might demonstrate a greater subjective expectation of privacy in the same conversation. For instance, someone walking down the street talking on a cellular phone does not demonstrate the same privacy expectation as someone on the other end of the call but alone in a soundproof room.[107] Regardless of the degree of privacy interests either subjectively demonstrated or objectively reasonable, one presumption remains clear: the parties to the remote conversation share a privacy interest in the conversation's contents.[108]

---

[102] *Alderman*, 394 U.S. at 176.
[103] See id. at 179-80.
[104] Although it is arguably taking place right now, with the National Security Agency's eavesdropping on domestic – international phone calls without warrants.
[105] The loophole gained explicit recognition in *Payner*, where the Court held that evidence the government *concededly* obtained in violation of the Constitution was admissible against a third party, since his constitutional rights were not violated. In essence, the Court cut back slightly on its post-*Katz* inquiry in Fourth Amendment cases, appearing to base the constitutional violation on interference with a possessory interest (one man's briefcase was stolen, and evidence obtained from it was used against a third party) and not on a third party's reasonable expectation of privacy.
[106] This does not mean that the conversation would be entirely immune from government participation. For instance, one participant could willingly turn over incriminating information from the conversation to the government. It only means that participants in private conversations reasonably believe that the government is not secretly listening.
[107] However, even though the one talking on the cell phone in public runs the risk that passers-by, even government agents, will overhear her, she can still expect to be free from the government intercepting her cell phone's transmission just as much as the speaker in the soundproof room can expect privacy.
[108] The Supreme Court's jurisprudence in this area is somewhat murky. In *Padilla*, the Court held in a *per curiam* opinion that co-conspirators do not automatically have standing to challenge government intrusion on jointly used property or a scheme in which they all play a significant role. *Padilla*, 508 U.S. at 82. But see United States v. Broadhurst, 805 F.2d 849, 852 (9th Cir. 1986) (holding that six defendants, all involved in marijuana cultivation, had standing to challenge the government's aerial search of the greenhouse where the marijuana was growing because "[p]articipation in an arrangement that indicates joint control and supervision of the place searched

Katz helped to establish the reasonable expectation of privacy standard, but it is now only helpful insofar as its formulation applies to shared privacy interests. Katz himself had standing to object to admission of his recorded conversations as evidence against him. However, those on the other end of the line did not, and the eavesdropping on Katz eviscerated any privacy interests they might have had. While the limited protection could deter incriminating statements in any kind of remote communication, its potential chilling effect on speech calls for judicial reevaluation. Unlike in *Katz*, there are now multiple remote communication methods in common use. The judiciary must avoid differentiating between the different methods, always beginning with a presumption of shared conversational privacy.[109] Doing so would not offend *Katz*. The only required change would be pluralizing the subject of Part I of the test Justice Harlan suggested. Consequently, parties to a conversation, with no explicit or implied disclaimers applied to its contents, would each only have to demonstrate a subjective expectation of privacy in their conversation.[110] *Katz* is the foundation for conversational privacy, and only a slight modification would substantially modernize even that decades-old case.

As complex as the judiciary's work will turn out to be in the wake of decisions like *Olson* and *Carter*, it will become far more difficult as more remote communication cases reach the docket. Because the Supreme Court has sanctioned the use of multiple factors in evaluating standing and shared privacy interests, every arrival or improvement of communication technology could present a new set of factors for the courts to consider. Despite this Article's contention that the conversations that are transmitted via remote communication technology are substantially the same, courts still treat the methods differently and use a hodgepodge of who, what, when, where, why, and how in their decisions that is wholly unnecessary and cumbersome. If anything, the courts must send out clear signals of which conversations are private and which are not for the benefit of society at large, not only for the government. Most importantly, society should be able to feel comfortable in judicial acknowledgment of its own long-settled privacy interests.

Besides codifying the shared expectation of privacy in a conversation, the judiciary must set out clear and uniformly applicable standards for how far the privacy protection will extend. The inquiry would focus on whom parties to a conversation usually expect to be privy to the

---

sufficiently establishes [a shared legitimate expectation of privacy]"). Though these two cases might appear to conflict, the Supreme Court has not actually struck down *Broadhurst*.

[109] One illustration of this difficulty appears in United States v. Maxwell, 45 M.J. 406 (A.F.Ct.Crim.App. 1996), which held that there was a "reasonable expectation of privacy, albeit a limited one, in [e-mail messages] sent and/or received on [America Online]." Id. at 417. Despite analogizing an e-mail to a sealed postal letter, the Court appeared to find an even lower expectation of privacy according to the number of people who might conceivably see the communication, even if unauthorized to access it. Thus, the expectation of privacy in an e-mail sent over a network would be lower than that sent in real time without an intermediate storage server. Since a central server stores all AOL e-mails, an AOL employee could conceivably access the server and read e-mails without the permission of the sender or the intended recipient. See id. at 418. Moreover, as in *King*, privacy in the e-mail terminates upon delivery, apparently without regard to who is reading the e-mail at that point. See Guest v. Leis, 255 F.3d 325, 333 (6th Cir. 2001), *citing King*, 55 F.3d at 1196. But see United States v. Most, 876 F.2d 191, 198 (D.C. Cir. 1989) ("*Rawlings* did not establish any general rule that an individual forfeits his reasonable expectation of privacy in his belongings simply by entrusting them to the care of another").

[110] The example given above provides a good point of reference. Someone talking loudly within earshot of strangers arguably does not exhibit a subjective expectation of privacy, whereas someone speaking in a private room, or through an e-mail or sealed letter, does.

conversation. Those who are invited into a conversation of any kind, whether a circle of friends at a cocktail party, participants in a conference call, or recipients of e-mail exchanges, are those who generally have full access to the contents of the conversation. The access comes by virtue of anyone already participating in the conversation inviting someone else's participation. Thus, the most sensible approach for the judiciary to use in determining conversational standing limits is to presume standing based on invited participation in the conversation.[111] Anyone invited to join any sort of conversation, including government agents, would have full access to any subsequent part of the conversation. An aggrieved party would have standing to challenge admission of any part of the conversation as evidence against him at trial, unless government agents were invited. On the other hand, those who eavesdropped on the conversation accidentally or deliberately would not qualify as invited participants in the conversation. Consequently, they would not have standing if they chose to participate without invitation. Finally, anyone who deliberately intruded on a conversation, acting on behalf of the government,[112] could not use any of the conversation's contents as criminal evidence against the participants.

In redefining its inquiry into the expectation of privacy, courts would streamline their own task by using fewer factors in their determinations. Although it is somewhat circular to say that the courts would only have to decide whether or not a conversation was private, the approach is reasonable because it calls for the recognition of common societal attitudes about conversational privacy. Again, the medium of communication is irrelevant.[113] That many of the new remote communication technologies have been available for a relatively short time does not indicate a substantial difference from long-existing communication methods.[114] Treating telephone calls, cell phone text messages, e-mails, etc. as the same, and treating the interaction that takes place through such media as a conversation in which there is a shared privacy interest, has at least two benefits for the judiciary. First, it would make the two-part test from *Katz* much more simple and straightforward. Second, and most importantly, the test would apply to any new type of communication technology that developed, while the evaluation scheme would stay the same. In sum, the proposed new approach to conversations would take a well-established test and societal

[111] The Ninth Circuit recently affirmed this very principle in United States v. Thomas, 447 F.3d 1191 (9th Cir. 2006), which held that the driver of a rental car lacked standing to challenge a government search of the vehicle because he was neither an authorized driver under the rental agreement nor had the authorized renter's permission to drive the car. Id. at 1199. Analogizing the rental car to a conversation, Thomas would then suggest that only those with permission to join the conversation — that is, with an invitation to join the conversation by any original or invited participant — would have Fourth Amendment standing to challenge government intrusion.

[112] For example, private citizens who hacked into e-mail accounts, discovered incriminating information, and then turned the information over to the government.

[113] Similarly, the method of intrusion is irrelevant to whether or not the judiciary should recognize certain government actions as an invasion of privacy. See Simmons, *supra* note 42, at 1326-27 (noting that Fourth Amendment protections deteriorate when courts examine the means of intrusion, and that this erosion will continue as technological advances create investigation methods that are less intrusive against their targets but obtain the same results).

[114] Justice Brandeis suggested as much in his dissent in *Olmstead v. United States*, noting that "[t]here is, in essence, no difference between the sealed letter and the private telephone message." Olmstead v. United States, 277 U.S. 438, 475 (1928) (Brandeis, J., dissenting) (internal citation omitted).

expectations from the past[115] and make them universally applicable in both the present and in the future.[116]

Even without arguments for judicial efficiency and recognition of society's expectations, there is another strong sense in which to view conversational privacy as a constitutional entitlement. Those who contend that the "papers and effects" language of the Fourth Amendment cannot extend to remote communications other than postal letters, since no modern-day communication technology existed in the late 18th Century, must still acknowledge that the Fourth Amendment precludes unreasonable government searches and seizures of any kind. *Katz* reiterated this principle in dictum almost 200 years later: "The Constitution protects people, not places." Without protection of conversations as papers and effects, the personal component of the Fourth Amendment still calls for stronger recognition of the intangible.[117] Much of a person's identity is intangible. One's personality, one's memories, thoughts, fears, and hopes expressed in words, and even one's unexpressed secrets, are just as fundamental to identity today as they have always been. A modern-day example of this recognized right to personal privacy appears in Congressional telecommunications legislation. Its purpose exceeds protection of property interests, such as ownership of a phone line, use of a computer, or rental of an apartment. Rather, it affirms that a conversation, as a type of connection between persons, is something that people can expect to remain confidential from impulsive governmental intrusion. Conversational privacy might thus be implicit in the "persons" language of the Fourth Amendment. The terms of the Fourth Amendment are all tangible, but the scope of their protective scheme undoubtedly extends to equally important intangibles that make up a person's life. Recognizing a right to a reasonable expectation of privacy in a conversation, and an expectation that all invited participants maintain, is fundamentally recognizing security in one's person.[118] Thus, even if the judiciary will not seize upon the policy arguments in favor of conversational standing, it can look to formalist grounds and find equally compelling justification for a new approach in the text of the Fourth Amendment itself.

B. Limits and Implications

Even if the recognition of shared privacy interests in a conversation becomes well-established in the jurisprudence, its judicial manageability requires clear limits on its extent. The argument, restated, is that all intended participants in a conversation have standing to challenge constitutional violations of privacy rights in that conversation. In other words, only those invited into the conversation by any of those already participating would have recognized shared privacy

[115] But see Simmons, *supra* note 42, at 1332 (arguing that it is both impractical and unnecessary to consider 18th century societal expectations).
[116] See id. ("[A] workable test must be flexible enough to change as society changes, but rigid enough to stay constant even as technology changes").
[117] The Supreme Court has consistently held that the Fourth Amendment protects both tangible and intangible evidence from unreasonable search and seizure. *See Hayden*, 387 U.S. at 305 (*citing Wong Sun*, 371 U.S. at 485-86).
[118] Moreover, technological change does not defeat this fundamental principle. See Simmons, *supra* note 42, at 1335 (contending that "[c]ourts must resist the temptation to conclude that just because a certain technology is available and the public could use it to render once-private realms public, that in fact it has been used to render them public" and without Fourth Amendment protection).

interests in the conversation.[119] Provided that any invited participant made a reasonable attempt to keep the conversation private,[120] her protected privacy interest would be equal to that of any other invited participant.

On the other hand, if any party chose to invite the government's participation, or to reveal information to the government that any participant disclosed in the conversation, then the aggrieved parties would have no standing to challenge any incriminating evidence thus exposed.[121] This principle reflects both current jurisprudence and the balancing of interests inherent in criminal investigations. While private parties have an interest in the government respecting their civil liberties, the government has a countervailing interest in solving and preventing crime.[122] The rule placing the government on equal footing with other invited participants would both preserve private citizens' Fourth Amendment rights and settled expectations of privacy *and* encourage their assistance in fighting crime. Consequently, the Fourth Amendment would protect invited participants in a conversation only from clandestine and unauthorized governmental intrusion. The change in current jurisprudence would be no more than subtle, as any information voluntarily disclosed to the government would remain fair game for a criminal investigation.

In practice, conversational standing would allow private citizens to ensure the privacy of conversations under their own control, including taking reasonable steps to shield the conversation from unauthorized participants. However, they would have no protection against any other participant volunteering information or inviting the government. Any criminal disclosures they made in the course of a conversation would enjoy more protection than in the current regime,[123] but only slightly more. Thus, a defendant who unknowingly conversed with a police informant or undercover agent,[124] or with a close confidante who then led police to incriminating evidence revealed in the conversation,[125] would not have standing to contest evidence from the conversation.[126]

The same would apply to messages either intended for, or easily accessible to, the public at large. A participant who posted a message on an electronic bulletin board would not have standing to

[119] The recognized shared privacy interest would only be the objectively reasonable expectation of privacy. Any failure to demonstrate a subjective expectation of privacy, such as talking on a cell phone in a crowded space and being overheard by an agent of the government, would defeat that particular party's privacy interest but not that of any other invited participant.
[120] Such action would satisfy step one of the test from *Katz*.
[121] See *Hoffa*, 385 U.S. 293; *White*, 401 U.S. 745.
[122] See Adler, *supra* note 2, at 1118-19 (arguing that the *Katz* standard should be reevaluated and applied, in the context of cyberspace, in order to balance competing governmental and societal interests).
[123] See Reetz, Note, *supra* note 11, at 200-01 (arguing that disclosure of information does not always amount to abandoning a privacy interest in that information).
[124] See *Hoffa*, 385 U.S. 293.
[125] See *King*, 55 F.3d 1193.
[126] This is not to say that standing to contest *all* evidence from the conversation would vanish. Assuming that the entire conversation were recorded, defendants could not challenge any evidence turned over directly to the government, as in words and phrases an informant reported. However, the government would then have to go through the usual procedures for complying with the Fourth Amendment, such as obtaining a warrant or establishing exigent circumstances, in order to access any other elements of the conversation. The government's invited participation in a conversation would give access to the entire conversation.

suppress evidence obtained from any such message. Even if the message were intended only for certain people or groups, easy access to the bulletin board would publicize the message and effectively make anyone who saw it an invited participant. Extending the hypothetical, a participant who posted a flyer on a streetlight pole would also lack standing to challenge incriminating evidence based on the flyer. Even if the posting were in a remote area, it would still be held out for any passers-by, a group over which the posting party would have little or no control.[127] Public exposure implies intent to publicize. Any passer-by would qualify as an invited participant, just as in the electronic bulletin board example. In sum, neither of the parties in the hypothetical would have standing to contest incriminating evidence arising from their postings because (a) the postings could presumably have been directed at anyone and/or (b) because the parties could have taken reasonable steps to exclude others from the conversation. Either example is akin to making an announcement using a megaphone in a public park: anyone passing by would have access to the contents of the message, including the police.

In terms of explicit invitation to the government, parties to the conversation would have no protected right to control invitees. Social custom and manners might dictate that all participants gain each other's approval, either express or implied, before inviting other participants. However, the Constitution is silent on habits and manners, only establishing the boundaries that govern the creation and enforcement of the laws. As an example, say good friends X and Y are having a conversation. Y invites his good friend Z to join the conversation, but without X's knowledge or consent. Z turns out to be a government agent. In practice, this scenario might take the form of X and Y having an e-mail conversation and Y deciding to blindly copy Z on e-mails to X.[128] Even if X reveals incriminating evidence to Y and asks Y not to tell anyone, the information is part of the conversation, and Z is an equal participant. Despite Y not being such a good friend after all, X has no standing to challenge the admission of that evidence against him if Z decides to use it.[129] Such a scheme promotes the balancing of civil liberties and criminal investigation by encouraging Y to implicate X, yet deterring Z from unauthorized intrusion.

Two critical issues come to mind in defining the limits of conversational standing as discussed here. The first involves the government trying to invite itself into the conversation. For instance, if a government agent makes a comment intended to be part of a conversation, and one participant responds to the comment in a way that suggests invitation, and no other party objects, then the government would be entering a conversation without an initial invitation. This practice would be tantamount to eavesdropping if the government sought invitation solely to access the conversation without a warrant. If the practice were sanctioned, then the government could try to invite itself into a number of conversations it believed *could* lead to incriminating information, regardless of the likelihood of such evidence actually surfacing. Its conduct would resemble indiscriminate profiling based on superficial characteristics, already viewed with disfavor. Moreover, defendants could assert an entrapment defense against the government, despite any rules on conversational standing. In such a situation, settled entrapment doctrine would most

[127] Of course, this situation can only apply to areas that are open to the public. Gated communities, or other fortified zones, would present a more complicated question of public openness, which might be enough to create standing if taken as a reasonable limitation on participants.

[128] Or, for an example that could have taken place before e-mail was common, suppose X and Y are talking on the phone and Y asks Z to pick up another receiver on the same phone line but in a different room.

[129] Nevertheless, if Z eavesdropped on the conversation without the knowledge or consent of either X or Y, then X *would* have standing to suppress incriminating remarks in spite of the close friendship between Y and Z.

likely apply — that is, the government would have to prove the defendant's predisposition towards committing the crime.[130] Since the government might try to circumvent conversational standing rules, including those that already exist, entrapment defenses based on what we might call baited-invitation techniques would effectively curb possible government abuse.

Second, and most importantly, the limits of conversational standing depend on the limits of a conversation itself. While these limits are harder to define, we might construe them as the traditional beginnings and endings of a conversation so that they would apply to all remote communications. The beginning of a conversation occurs when the original parties exchange a verbal or written greeting, or some gesture that implies greeting. The end is more complex and is the component that the government might easily attack without clear definition. Generally, one's participation in a conversation ends upon some indication that he or she no longer intends to take part. She can signal the indication by saying goodbye, hanging up the phone, or saying something indicating, from her perspective, that the purpose of the conversation has been fulfilled or that the business to be performed through the conversation is complete. Once any invited participant leaves the conversation, then she is no longer a party and must either initiate a new conversation or be invited again in order to regain access.[131] The greatest complication arises in the "ongoing conversation" context. The judiciary would do best to construe ongoing conversations narrowly. For instance, once parties have hung up the phone, the conversation is over, even if they intend to talk again. Once the business of an e-mail exchange is settled, that conversation has also ended. In the context of a dispute, determining the end of an ongoing conversation would be heavily fact-based if it were based on remote, recorded transmissions such as e-mail exchanges. Conversations without any clear, confined purpose would be considered ongoing, and thus any of their contents would be admissible into evidence, at least following the invitation to the government to join. As with any form of direct correspondence, when such a situation finally reaches the courts, the starting point should be well-established societal expectations, rather than the complex inquiries now used to evaluate conversational privacy.

III. Modern-day interpretations of shared privacy interests

While conversational standing has yet to gain explicit judicial recognition, it is useful to consider its application to a variety of current contexts, including both cases and other disputes that might reach the judiciary at some point. This section first considers how conversational standing might apply to the recently decided Supreme Court case of *Georgia v. Randolph*.[132] It then proposes a framework for reconciling conversational standing with the National Security Administration's monitoring of phone calls and e-mail exchanges between the United States and other countries.

A. Georgia v. Randolph

Randolph is the most recent Supreme Court case to address shared privacy interests, although on a more tangible level because it involved privacy interests in the home. Fourth Amendment

[130] Jacobson v. United States, 503 U.S. 540, 553 (1992) (holding that the "entrapment" defense is valid when the government cannot prove defendant's criminal predisposition).
[131] That is, for purposes of constitutional protection.
[132] 126 S.Ct. 1515 (2006).

jurisprudence has traditionally given the home more stringent protection than any other sphere of life, and *Randolph* generally followed the same line of justification. In *Randolph*, the police responded to a woman's call about a domestic dispute with her husband that culminated in his taking their child away with him.[133] The police did not have a warrant, but they attempted to access the house by asking for the wife's permission to search the bedroom, suspecting that the husband was keeping illegal drugs inside the house.[134] The wife consented to the search, but the husband, Randolph, who had recently returned and was standing nearby, immediately objected.[135] The police searched the home anyway. When they searched the bedroom, the police found a straw that Randolph had allegedly used to snort cocaine.[136] Randolph was tried and convicted on the basis of this and other evidence. He challenged the admission of the evidence on Fourth Amendment grounds. By the time the case reached the Supreme Court, the issue to be decided was whether one party's consent to a police search of an area or item could override the objection of another party with a shared privacy or property interest in the area or item, provided the other party was present to make the objection at the time of the consent.

Justice Souter's majority opinion held that the husband's objection defeated the wife's consent, rendering the police search and seizure unconstitutional and the challenged evidence inadmissible.[137] The majority had to distinguish *United States v. Matlock*[138] in justifying its holding. In that case, the defendant was not present to oppose a co-tenant's consent to a police search, locked in a squad car parked outside the house at the time the consent was given.[139] Thus, the holding depended on Randolph's presence at the time of the consent. Had he been elsewhere or given the objection at a different time, his wife's consent would have been valid under *Matlock* and the search and seizure would have been constitutional. Most importantly, however, Justice Souter supported the "presence" technicality by appealing to "social custom," which seemed to form the backbone of the entire majority opinion.[140] He mentioned that a guest invited to a house party by one person would generally not feel free to enter if a co-occupant objected upon her arrival.[141] In fact, according to Justice Souter, any time a guest thought of entering a home with the consent and objection of two parties with shared privacy interests in the home, the objecting party's wishes would usually carry the day.[142] The majority's care to note the shared privacy interest in the home might open the door for other explorations of shared privacy interests, but social custom was the deciding factor in holding the search and seizure unconstitutional.

Chief Justice Roberts, in dissent, highlighted problems with the majority's shared privacy analysis, particularly in the context of the home. The Chief Justice pointed out the ambiguity and arbitrary application of the majority's rule, emphasizing the dangers that could easily result. For instance, he persuasively mentioned that by the majority's rule, the husband's objection would

[133] Id. at 1519.
[134] Id.
[135] Id.
[136] Id.
[137] Id. at 1528.
[138] 415 U.S. 164 (1973).
[139] Id. at 179 (Douglas, J., dissenting).
[140] See 126 S.Ct. at 1526.
[141] Id. at 1522-23.
[142] Id. at 1523 ("Without some very good reason, no sensible person would go inside under those conditions")

have been invalid had he been sleeping in the next room,[143] allowing the wife to easily defeat any shared privacy interest he might have. Moreover, the Chief Justice addressed a concern that Justice Breyer had also raised during the proceedings, namely the possibility of domestic violence: in a similar situation, the husband could object as the wife consented, forcing the police to leave, after which the husband could immediately attack his wife.[144] In sum, the dissent exposed the instability of the rule the majority announced.

The application of *Randolph* shared privacy to conversational standing is difficult to reconcile, particularly because of the same-time requirement and the time frames of different conversations. Read broadly, *Randolph* holds that where shared privacy interests are implicated, objection trumps consent only if the two are simultaneous. If a party to a conversation were to cite *Randolph* in criminal proceedings, arguing that its principle applied to conversations in which one party invited government participation over another's objection, then at least two complications could appear. First, simultaneous consent and objection would be practically impossible, especially in remote communications not conducted in real time. For example, if a participant in an e-mail conversation offered to turn over recorded e-mails to the government over another's near-immediate objection, *Randolph*'s applicability would be difficult to determine.[145] The e-mail conversation might be nearly in real-time, but the objection would still not be contemporaneous, as it was in *Randolph*, or even as it would be if it were taking place on the phone. All would depend on the legal definition of simultaneity and its application to the factual timing. Moreover, the judiciary would have to make a controversial determination of how close in time a valid objection would be.

Second, even if the judiciary considered the objection contemporaneous, it would still have to contend with the presence rationale that was also critical in *Randolph*. The defendant was physically present to object to his wife's consent. Physical presence is necessarily impossible in remote communications. Taken literally, this complication would mean that no objection could ever defeat consent to join a remote conversation under *Randolph*. The only way a defendant could plausibly satisfy the presence requirement would be if the judiciary construed presence to mean invited participation in the conversation. Ultimately, the presence issue would turn on whether the judiciary wanted *Randolph* to apply to conversations or instead found *Matlock* more apposite, since presence is a necessary condition for satisfying the *Randolph* test. *Randolph*'s applicability to conversations is bound to be complex, perhaps even easier to manipulate than the majority's rule in *Randolph* itself.

As difficult as it is to square the shared privacy interests in *Randolph* with those in a remote conversation, the case appears somewhat inconsistent with conversational standing, which depends on invited participation. One of the requisite conditions for conversational standing as described thus far is that parties have no effective control over invitees. However, *Randolph*

[143] Id. at 1535 n.1 (Roberts, C.J., dissenting).
[144] Id. at 1537-38.
[145] The same would be true of conversations conducted by instant messaging and text messaging. However, even if *Randolph* did apply, the principle of *Hoffa* and *White* might control the outcome: parties are free to reveal any incriminating information to the government, even over the objection of those implicated. The clash between that principle and the holding in *Randolph* involves the reasonable expectation of privacy, which existed in *Randolph* but not in *Hoffa* and *White*.

suggests that when one party invites the government at the same time as another's objection,[146] that objection is valid. Even if the objection were given at the same time and place in conversation, as defined by the judiciary, any other party's consent would act as an invitation, which the objecting party could only defeat with another simultaneous objection. At that point, an objecting party's only recourse would be to drop out of the conversation.[147] Regardless of the objecting party's actions, the consenting party could manipulate the situation to invite government participation even more easily than in *Randolph*. In order to square the *Randolph* holding with the concept of conversational standing, same-time objection and consent would become the only instance in which a party could exclude an invitee from a conversation against another party's wishes. As pointed out, however, another party's consent at another time would still defeat the objection.[148]

Randolph's other distinguishing characteristic as applied to conversations is its setting. While the case focused on social custom, and in fact grounded its reasoning in what the majority considered common practice, it focused as much or even more on the location of the government intrusion: the home. The opinion eagerly mentioned the familiar house-as-castle metaphor. If future courts emphasize the shared privacy interest in the *home*, rather than the shared privacy interest in any particular area or item, then the justification for shared conversational privacy as a whole will be even weaker. Moreover, even reading *Randolph* to apply to any shared privacy interest, the specific interests addressed in the case – namely the interest in the home and the interest in effects within the home – would still be separable. The home was searched and effects were seized, despite the shared privacy interests. Thus, *Randolph* might apply strictly to shared privacy interests in, and within, the home. In fact, the Court in *Randolph* was probably more interested in affirming protection for the home than in privacy protection for the cocaine-laced straw. If it is the home that truly matters in evaluating shared privacy of the kind set out in *Randolph*, then litigants will struggle to apply it to conversations, which take place in almost every walk of life.

This is not to say that *Randolph*'s application beyond the home is entirely implausible. Just as there are different areas in which privacy interests are shared, certain conversations follow a similar track. Like the protection for the home, conversations between people in their capacities as members of certain categories,[149] such as doctors and patients, attorneys and clients, or clerics and penitents, generally receive much greater privacy protection than other kinds of conversations. The judiciary could decide to apply *Randolph* to any of these conversations if it found the degree of privacy protection for the home akin to the kind of protection given to certain privileged conversations.[150] Such an approach would even trump conversational standing,

[146] Again, the "same time" need definition for conversational purposes.
[147] The entire situation might be inconsequential, since the consenting party could always turn over evidence of the objecting party and could always "rat out" the objecting party after she decided not to participate.
[148] The court in *Randolph* left the question of consent at a later time unresolved. However, it strongly suggested that such consent would defeat the earlier objection, since the validity of the objection depended on both timing and presence. If Randolph's wife had given consent when Randolph was not at home, even after the encounter described in the case, the Court would probably consider any subsequent police search reasonable.
[149] If the persons in question are speaking outside of their protected capacities, then their privacy interests probably become less defensible.
[150] Put differently, objection to the government intruding or participating in any of these enumerated conversations should trump consent, but if the conversation does not fall within the set of defined privileged interactions, then the

since it could allow one party, after confiding incriminating information to a particular authority figure, to prevent the authority figure from revealing that information to the government.[151] Though preserving special privileges in conversations might be good policy, the judiciary would still have to be nuanced in its application of *Randolph*. For instance, the same-time and presence requirements would presumably still have to govern the inquiry in order for *Randolph* to map cleanly onto privileged conversations. Doing so, however, might call for the jumbled approach described above. In placing *Randolph* and shared conversational privacy side by side, their conflict depends on specific interpretations of *Randolph* itself. Though they might not stand on common ground, they might also peacefully coexist.

On a basic level, one standard could reconcile conversational privacy with a special version of *Randolph* applying outside the home but only to expressly privileged conversations. Although it would cut back slightly on the core concept of conversational standing, it might still give the judiciary a plausible and manageable policy. In sum, parties to a private conversation, regardless of the transmission medium, would be free to share their privacy interests in the conversation with whomever they chose, even over the objection of co-participants, *unless* the conversation were privileged. *Randolph* would then be available to defendants in privileged conversations even if conversational standing were not available, and the time and place requirements could be relaxed somewhat.[152] Even though critics might argue against this approach as giving defendants another way to use the exclusionary rule, *Randolph* would still have very narrow application, only applying to certain conversations in certain contexts.[153] Further, conversational standing itself, though an additional tool for defendants who otherwise would have fewer and less vigorously protected privacy interests, still invites the balancing of governmental and private citizen interests. The next section describes one such balancing approach in a particularly critical situation.

B. NSA Warrantless Eavesdropping

In December of 2005, the New York Times revealed that the Bush Administration had authorized government eavesdropping on communications between the United States and

---

consenter has the last word. For example, suppose the government joins an e-mail interaction without invitation and asks if it can see information a patient revealed in e-mails sent to a doctor. The doctor says she'll send the e-mails, but the patient objects upon finding out what the doctor intends to do. The patient's objection would bar the governments from using any evidence contained in the e-mails against him. For a contrary example, suppose two friends hatch a criminal conspiracy via unprivileged cell-phone instant messaging. The government asks one friend, via another instant message, to explain the conspiracy and implicate his co-conspirators. The friend is happy to comply, but the one who stands to be implicated objects. The objection against government intrusion is invalid.

[151] First, conversational standing would allow any party to invite the government's participation regardless of status, so sustaining one party's objection would have to be an exception. Second, the enforcement of conversational standing's invited participant concession in privileged conversations would be poor public policy. It would defeat the entire purpose of privileging certain conversations by making their confidentiality toothless: the trusted parties could readily turn over information to the government or allow the government to eavesdrop, and the confiding parties would not have standing to challenge the evidence thus obtained.

[152] Ironically, the parties who would want to use *Randolph* to protect their conversational privacy would be the same parties who would want to assert standing to exclude evidence from the conversation!

[153] For instance, a conversation between a doctor and a patient in that doctor's office relating to business between them would be protected. A conversation between the same two people but not in their capacities as doctor and patient, or entirely outside the scope of their doctor-patient relationship, would not be protected.

abroad,[154] hoping that the eavesdropping would help government agents to thwart planned terrorist attacks. The eavesdropping had been taking place without judicial approval, and the Administration had authorized it dozens of times since the terrorist attacks of September 2001.[155] The surveillance extended not only to telephone conversations, but also to Internet correspondence.[156] Public outcry over the warrantless eavesdropping was almost immediate. Critics pointed to its use as a violation of the Federal Wiretap Statute,[157] which requires an authorizing warrant or federal court order for each instance of wiretapping.[158] Beyond the statute, however, some said that eavesdropping on telephone calls was patently unconstitutional as a violation of the Fourth Amendment.[159] The Administration vigorously defended the legality of its strategy,[160] but the controversy did not disappear. The dispute highlights both the difficulty and the importance of balancing the government's interest in protecting its citizens from terrorist attacks, sometimes through questionable means, against the civil interest in protecting conversational privacy.

The concept of conversational standing could provide a healthy balancing approach to the NSA's technique. If applied, it would not require any exceptions to its present form, instead only limiting actions the government could take against suspected terrorists after the fact.[161] In such a regime, the government could continue its warrantless eavesdropping on domestic-international phone calls, allowing it to gain access to sensitive and otherwise unobtainable information it needed to thwart terrorist attacks. Even though citizens might want to maintain their privacy for modesty concerns — that is, even if the information obtained by the government is innocuous, people might rather have the information remain private for personal, emotional reasons that are difficult to explain — the critical factor in warrantless eavesdropping would be protection from prosecution for private information that the eavesdropping uncovered. Thus, despite the government's use of information gained from warrantless eavesdropping, the parties to the conversation would have standing to exclude any evidence obtained pursuant to the conversation. Their rights would be the equivalent of transactional immunity in a criminal prosecution: the government would not be able to punish them based on anything revealed in the conversation or any evidence that the government would not have discovered "but for" the eavesdropping. Of course, the government would still have all the usual tools available to defeat

[154] James Risen and Eric Lichtblau, "Bush Lets U.S. Spy on Callers Without Courts," N.Y. TIMES Dec. 16, 2005, at A1. Some eavesdropping also took place on purely domestic calls, although those incidents were apparently unintentional. See Eric Lichtblau, "Bush Defends Spy Program and Denies Misleading Public," N.Y. TIMES Jan. 2, 2006, at A11.
[155] See David E. Sanger, "In Address, Bush Says He Ordered Domestic Spying," N.Y. TIMES Dec. 18, 2005, at 1.
[156] Eric Lichtblau and James Risen, "Domestic Surveillance: The Program; Spy Agency Mined Vast Data Trove, Officials Report," N.Y. TIMES Dec. 24, 2005, at A1.
[157] 18 U.S.C. §§ 2510-22 (2006).
[158] 18 U.S.C. § 2518 (2006).
[159] Commentators had been attacking the constitutionality of other surveillance methods well before the New York Times exposed the NSA's eavesdropping. See, e.g., Lee, The USA Patriot Act and Telecommunications: Privacy Under Attack, 29 RUTGERS COMPUTER TECH. L.J. 371, 400 (2003) (arguing that the telecommunications provisions of the Patriot Act violate the Fourth Amendment and that "[t]he Act effectively snubs the judicial system in favor of executive power").
[160] See Sanger, *supra* note 155.
[161] In Justice Robert Jackson's view, "if we are to make judicial exceptions to the Fourth Amendment. .. it seems to me they should depend somewhat on the gravity of the offense." Brinegar v. United States, 338 U.S. 160, 183 (1949) (Jackson, J., dissenting in part).

the parties' standing, such as independent source and inevitable discovery. The government could punish the offending parties in other ways, such as using the press to sully their reputations and deporting them if they were foreign nationals illegally in the United States. Only one exception would uphold the constitutionality of eavesdropping without warrants by effectively protecting parties against unreasonable search and seizure:[162] evidence obtained without warrants and solely from conversations would be formally inadmissible at trial.

Standing to contest warrantless eavesdropping on conversations would represent good, judicially justifiable public policy for at least three reasons. First, it would avert the controversy that less stringent warrant requirements would generate. Although such a technique would place the eavesdropping clearly within the law by complying with the Federal Wiretap Statute and the plain language of the Fourth Amendment, it would also raise questions of whether obtaining such warrants were too easy, and thus whether the warrants were properly issued at all. Second, the policy would carve out a judicially manageable standard that would still be relatively straightforward to implement despite its vulnerability to attack on nuances and technicalities. Simply put, eavesdropping would be permissible, and the government could use information obtained from eavesdropping to fight terrorism, but the evidence would automatically be inadmissible at trial. Finally, it acknowledges that while citizens have an objectively reasonable expectation of privacy in telephone calls made to private parties, certain government interests are so important that not even the strict language of the Constitution should bar their fulfillment. Despite formal problems of constitutionalism and the limits the Constitution places on the government, exceptional circumstances reasonably require some constitutional protections to be relaxed, at least temporarily.[163] The application of conversational standing, and the compromise it creates in order to fit constitutional boundaries as closely as possible, could be the most workable and palatable solution for both the government and private citizens.

Beyond the policy rationale for using the balancing test, it is clear that avoiding such a test could lead to drastic results. The consequences of not balancing civil liberties and governmental interests, particularly in an area as sensitive as terrorism, provide ample justification on their own. For example, at one extreme, the government could wiretap domestic-international phone calls at will, justifying each wiretap as a critical security measure. While such an action would completely satisfy government interests in obtaining information through remote communication, it would suffer from two pitfalls. First, the approach would eventually prove ineffective or even counterproductive, since anyone who truly wanted to shield information from the government would find alternative means of transmission. Second, the approach would have a chilling effect on conversations between parties within and outside the United States. Innocent parties with no terrorist intentions might limit their expression, fearing the government's use of other information against them for some other reason.[164] Government freedom to listen to private conversations at will represents the same Orwellian state that the Federal Wiretap Statute, and even the Constitution itself, were designed to prevent.

---

[162] The protection is slightly different in that it takes place *ex post* as transactional immunity from prosecution, whereas the Fourth Amendment itself seeks to protect citizens from government abuse *ex ante*.
[163] For instance, the exigent circumstances exception to the Fourth Amendment, when the government need not go through constitutional procedures before obtaining evidence that is likely to be destroyed or capturing fleeing felons.
[164] It is questionable whether the government could even use information obtained from the intercepted phone calls unrelated to its primary purpose in eavesdropping: obtaining information to use in preventing terrorist attacks.

The opposite extreme is equally disturbing. If the judiciary enforced an absolute prohibition on wiretapping without warrants, then the government would struggle to legally obtain needed information. For instance, upon heightened suspicion short of probable cause, but without the ability to obtain a warrant, the government might be handcuffed in thwarting a likely terrorist attack. Imposing more aggressive procedural restraints would allow at least some terrorism planning information to escape government surveillance. The most obvious consequence of this extreme is also the most severe: attacks might occur that the government could have otherwise prevented. In fact, if the government were sure enough of its target but still could not obtain a warrant to investigate, it might choose to take preventive measures that would violate the Constitution.[165] With restrictions thus placed on the government, however, civil liberties would enjoy excessive protection, effectively impeding the government from doing its work under the most pressing of circumstances. While the situation described is a worst-case scenario, it remains a possibility.

Fortunately, the combination of conversational standing and transactional immunity strikes a healthy medium between the two extremes just described. Neither party has its interests fully satisfied, but the two sets of interests are not mutually exclusive. Generally speaking, the government seeks to protect its citizens from grave harm, while citizens seek to protect their privacy from capricious governmental intrusion. By establishing a system of carefully enumerated powers, along with checks and balances, the Constitution itself is geared toward a healthy relationship between citizens and government.[166] The proposed combination seeks a similar goal, and in a particularly pressing issue of modern times, it would do as much work as any other provision in ensuring the achievement of that goal.

Of course, the balance between conversational standing and transactional immunity must be constitutional to be plausible in the first place. Although warrantless wiretapping might appear to violate the plain language of the Federal Wiretap Statute and the Constitution itself, a number of reasons point to the proposed scheme's constitutionality.

First, transactional immunity for contents of conversations obtained without warrants would serve as a prophylactic measure against admitted violations of the Fourth Amendment. In theory, the only unconstitutional consequence of a Fourth Amendment violation is using the evidence in a prosecution of anyone whose constitutional rights were infringed. The exclusionary rule is the direct remedy for the violation, effectively placing the defendants – the conversants in this case – in the same position they would have been in had the government never violated their constitutional rights. At the same time, the government obtains the information it needs to

[165] Although the choice might not be universal, most would likely prefer an egregious constitutional violation to a devastating terrorist attack.

[166] More specifically, the Constitution applies to the relationship between citizens of the United States and the government of the United States. The Supreme Court has held, for instance, that the Fourth Amendment does not apply to searches and seizures, on behalf of the United States, of foreigner-owned property on foreign soil. See United States v. Verdugo-Urquidez, 494 U.S. 259, 274-75 (1990); see also id. at 265 (finding that "the people" in the language of the Fourth Amendment "refers to a class of persons who are part of a national community or who have otherwise developed sufficient connection with this country to be considered part of that community"). However, it has also assumed that Fourth Amendment protection can extend to undocumented foreign nationals living in the United States. I.N.S. v. Lopez-Mendoza, 468 U.S. 1032 (1984).

prevent terrorist attacks, using the information solely for criminal prevention, not for criminal prosecution.

The second argument for the scheme's constitutionality is more dubious and involves the wiretapping regardless of transactional immunity. Supporters of wiretapping suspected terrorists without warrants can argue that government eavesdropping is reasonable in such situations and that exigent circumstances allow the government to proceed without having to follow the usual protocol. There are two problems with this argument that make the first argument, presented above in favor of the entire scheme,[167] considerably more attractive. First, in passing the Federal Wiretap Statute to forbid unwarranted government eavesdropping, Congress has already strongly suggested that the eavesdropping is unreasonable.[168] Assuming that Congress reflects the will of the people as a popularly-elected legislature,[169] society then implicitly considers the warrantless wiretapping approach unreasonable. Second, a judicial determination that warrantless eavesdropping to prevent terrorist attacks were reasonable could amount to undesirable, content-based judicial policymaking. Courts would have to define when the government's interest in accessing a conversation were so substantial that the government should be allowed to proceed with what would otherwise be a constitutional violation. Aside from its interpretations being open to disagreement, whether the opposition originated in other government branches or in public opinion, the judiciary would have to create categories in which the government eavesdropping without a warrant would be presumptively reasonable. Such categories might include violent criminals, sex offenders, other felons who had been "clean" for many years, suspicious individuals deemed likely to immediately harm themselves or others, and many more.[170] The judiciary would have to explain each of these in turn. It would inevitably become mired in the kind of decisions it typically tries to avoid. The judicial complications that would stem from rationalizing warrantless wiretaps could easily become not only highly controversial, but possibly even intractable.

Even without the combination of conversational standing and transactional immunity, private citizens in the United States still have strong constitutional arguments against warrantless eavesdropping. In fact, even if the government does not recognize shared privacy interests in the conversations it is investigating, the constitutional privacy rights of at least the domestic party remain intact. They exist according to both the conversational standing approach and existing doctrine.[171] Under conversational standing, the domestic party has the right to prevent warrantless government intrusion on her conversation, by virtue of conversations receiving special status in the set of Fourth Amendment protections. In terms of the status quo, and even focusing on tangible property, the domestic party still has the constitutional right to keep her telephone and telephone line free from warrantless government intrusion. If the government

[167] That is, defendants' conversational standing and transactional immunity as a remedy for warrantless wiretapping.
[168] See Kerr, *supra* note 20, at 838 ("Additional privacy protections are needed to fill the gap between the protections that a reasonable person might want and what the Fourth Amendment actually provides[, and] those protections historically have come from Congress").
[169] Although there is concern that even members of Congress are out of touch with the privacy interests of their constituencies. See, e.g., Mulligan, *supra* note 1, at 1596-98 (calling for modifications to the Electronic Communications Privacy Act to more accurately reflect present-day privacy concerns).
[170] The government could probably obtain warrants for such wiretaps without much difficulty. The example only serves to illustrate what could result if warrants were not required to investigate certain categories of people.
[171] See *Verdugo-Urquidez*, 494 U.S. 259.

eavesdrops on a domestic phone line without a warrant, then the owner of the line has standing to exclude at least his own contributions to the conversation thus intercepted, according to *Katz* and its progeny. Thus, the domestic party can challenge the government's intrusion either way, whether or not conversational standing finds a place in Fourth Amendment jurisprudence. Regardless of the government's interpretation of warrantless wiretapping, domestic parties retain their own conversational privacy protection.

C. The Conversation as Private Property

The discussion of conversational standing thus far has focused on shared expectations of privacy in a conversation. However, there is also a justification for the concept based not on privacy, but on the original, critical component of Fourth Amendment standing: the property interest.[172] The core of the property right in Anglo-American jurisprudence is the right to exclude others from using the property. In the context of conversations, the right to exclude is not absolute for all parties involved, particularly if shared privacy interests are recognized. One party's desire to exclude does not always defeat another equally-situated party's desire to include, as demonstrated in a comparison of *Randolph* and *Matlock*. Nevertheless, any party to a conversation has a generally recognized right to exclude those who try to participate without invitation. With the right to exclude being the core characteristic of a private conversation, such a conversation is then arguably like the property of the participants. If so, it could be subject to constitutional protections for private property, most notably those of the Fifth Amendment's Takings Clause.

The Takings Clause provides that "private property [shall not] be taken for public use, without just compensation."[173] If a private conversation qualifies as private property, and if the government eavesdrops on the conversation and uses any information it contains, then the government has presumably performed a "taking" of the conversation. More specifically, the government's use of the information, for purposes such as thwarting a terrorist attack or uncovering another criminal conspiracy, is public in that it is done on behalf of all those within the government's jurisdiction — that is, the citizens who comprise the public.

While the government is allowed to take private property for public use, it must provide just compensation to the property owners in order for its action to be constitutional. How to provide just compensation to those whose conversations the government has intercepted is a challenging issue. How much compensation is "just" follows as another necessarily difficult issue. Fortunately, there is a relatively simple solution to the just compensation problem, and not one that involves money. In terms of the warrantless wiretapping analysis described above, an exclusionary rule guaranteeing freedom from prosecution based on a conversation would represent just compensation. Such an approach would compensate conversants by only allowing the government to use their conversations to prevent crimes, not to punish or deter. Moreover, just as in the NSA wiretapping example, the government could obtain important information and

[172] See Kerr, *supra* note 20, at 823 (noting that in *Katz*, "[b]y entering the phone booth and paying for a call, Charles Katz bought a temporary right to exclude others from the phone booth that was protected by the Fourth Amendment"); id. at 827 ("noting that "both before and after Katz, Fourth Amendment protections have mostly matched the contours of real property law")
[173] U.S. CONST. amend. V.

use it for public benefit while still deterring those thinking of committing similar crimes. Would-be criminals, understanding that the government could use information from their conversations to defeat their illicit objectives, might find such a privacy reduction dissuasive. The same balancing approach grounded in shared privacy concerns is thus equally applicable to shared property interests. In sum, both private citizens and the government have a range of theoretical and jurisprudential tools at their disposal to advance their own interests. Balance is the hallmark of the United States government and political system, just as it is the hallmark of conversational standing in every context.

IV. Conclusion

Certain conversations are private. Though recognized in varying degrees, the principle has been clear throughout the history of the United States Constitution. The judiciary has often recognized the privacy inherent in conversations. Nevertheless, *shared* privacy interests in conversations have been slower to gain recognition. Conversational privacy loses much of its force if it applies unevenly to participants in a conversation regardless of their subjective control. Participants in a conversation cannot always exclude others whom they do not wish to participate, much less prevent any other participants from sharing the contents of the conversation. But they all must be equally free from unchecked government intrusion if their privacy is to mean anything in modern criminal procedure. Moreover, their privacy must not depend on the medium in which they choose to communicate, since the purpose of remote conversation is the same regardless of the medium. With communication options constantly becoming more numerous and more advanced, it is particularly important to recognize shared conversational privacy interests at this juncture. Among other advantages, doing so will provide a judicially manageable standard applicable to any remote communication technology, past, present, and future, and it will square modern jurisprudence with society's established expectations of conversational privacy.

In terms of constitutional doctrine, shared privacy interests in a conversation fit best within the protection of the Fourth Amendment. The right to suppress evidence obtained in violation of one's Fourth Amendment rights — that is, standing to assert the protection of the Fourth Amendment and, if necessary, the exclusionary rule — is only available on one's own behalf. In other words, a search or seizure is unreasonable only as to the direct target of the government action. Only the targeted stakeholder has standing. Other parties, regardless of their interest in the matter, do not. As the doctrine currently operates, only direct targets of a conversational interception, such as those whose phone lines are wiretapped, can suppress evidence contained in the conversation. However, if the judiciary formally recognizes shared privacy interests in conversations, then an unconstitutional search and/or seizure against one party would also apply to all other parties. This concept of conversational standing calls for all invited parties to a conversation, regardless of the communication medium, to maintain recognized constitutional privacy rights in the conversation. Hence, so long as each has taken subjective steps to limit the conversation's participants, each has standing to claim Fourth Amendment protection. All other options remaining equal, namely the ability of any participant to involve the government without violating the constitution, the concept suggests only that shared privacy interests in a conversation receive constitutional status.

Far from being a dangerous principle, conversational standing instead allows the judiciary to affirm the widespread expectations of the people it serves. It requires that society continue to feel secure in its private conversations while addressing broader security concerns. It allows everyone to avoid getting lost in technicalities, as well as feeling unsure of which conversations are private and which are not based on minor details. Most importantly, it honors a human desire for privacy extending to some of the most intimate spheres of a person's identity, many of which appear in conversations with specified people. The concept has remained hidden in the background of Fourth Amendment jurisprudence for some time, and the shared privacy interests it connotes have gained at least mild recognition at the higher levels of the judiciary. The sooner its place becomes more solidified, the more streamlined criminal procedure will become in the remote communication arena. It is a healthy change, and its implementation will be good for both the conversationalists of today and the generations of tomorrow.