Journal of Technology Law & Policy

Volume 7 | Issue 2 Article 7

December 2002

The Privacy Privilege: Law Enforcement, Technology, and the Constitution

Susan W. Brenner

University of Florida
Journal of Technology Law & Policy

Volume 7 December 2002 Number 2

THE PRIVACY PRIVILEGE: LAW ENFORCEMENT, TECHNOLOGY, AND THE CONSTITUTION

Susan W. Brenner[*]

I. INTRODUCTION 124

II. FIRST AMENDMENT 136

III. FOURTH AMENDMENT 150

IV. FIFTH AMENDMENT 182

V. THE PRIVILEGE OF BEING LET ALONE 190

"The Internet in its nature shocks real-space law."[1]

The movement of human activity into cyberspace must inevitably affect the law governing individual rights. Cyberspace creates new potentials for good and evil, for creative expression and criminal exploitation. This duality generates tension between our desire to encourage the freedom and autonomy that have thus far been the defining characteristics of cyberspace[2] and our obligation to ensure that it is not used for unlawful purposes. Courts, legislators, and society as a whole must decide how to balance this need for effective law enforcement against our historical respect for individual rights and liberties. This article considers how that balance should be struck with regard to what is perhaps the most amorphous of these rights — the constitutional guarantee of privacy.[3]

* Professor of Law, University of Dayton School of Law, Dayton, Ohio.

1. LAWRENCE LESSIG, THE FUTURE OF IDEAS 199 (2001).
2. *See, e.g., id.* at 264-68.
3. As Professor Gormly pointed out, there are many different definitions of "privacy":

I. INTRODUCTION

While the U.S. Constitution does not expressly grant a general right to privacy,[4] the U.S. Supreme Court has interpreted the U.S. Constitution as granting individuals a right to privacy that is incrementally derived from various constitutional guarantees.[5] The guarantees that are the most relevant to this discussion are the First Amendment's protection of free speech and freedom of assembly,[6] the Fourth Amendment's prohibition on unreasonable searches,[7] and the Fifth Amendment's privilege against self-incrimination.[8]

These three amendments protect privacy in different ways. The First Amendment protects the privacy of certain acts.[9] The U.S. Supreme Court held that when protecting free speech and freedom of assembly, the U.S.

> First, many scholars . . . have viewed privacy as an expression of one's personality or personhood, focusing upon the right of the individual to define his or her essence as a human being. Second, . . . are those . . . who have marked privacy within the boundaries of autonomy — the moral freedom of the individual to engage in his or her own thoughts, actions and decisions. A third cluster . . . have seen privacy . . . in terms of citizens' ability to regulate information about themselves, and thus control their relationships with other human beings. . . . Finally, a fourth cluster of scholars have taken a more noncommittal, mix-and-match approach, breaking down privacy into two or three essential components, such as Ruth Gavison's "secrecy, anonymity and solitude". . . .

Ken Gormly, *One Hundred Years of Privacy*, 1992 WIS. L. REV. 1335, 1337-38 (1992) (footnotes omitted). For the concept of privacy articulated in this article, *see infra* Section V.

4. *See, e.g.*, Alan H. Bomser, *Report: A Lawyer's Ramble Down the Information Superhighway*, 64 FORDHAM L. REV. 697, 739 (1995). One author maintains that as of 1890, "there existed no coherent notion of privacy at all in American law." Gormly, *supra* note 3, at 1343. *But see* Boyd v. United States, 116 U.S. 616, 630 (1886) (the Fourth and Fifth Amendments were intended to incorporate English common law principles into protecting privacy).

5. *See, e.g.*, Griswold v. Connecticut, 381 U.S. 479, 484 (1965). *See also* Bomser, *supra* note 4, at 739.

6. *See* U.S. CONST. amend. I. This section only considers free speech guarantees insofar as they impact upon the right to privacy. *Infra* Section II examines free speech in an on-line world.

7. *See* U.S. CONST. amend. IV. The Fourth Amendment also prohibits unreasonable "seizures," but because seizures implicate interests other than privacy, this aspect of the Amendment is not addressed in the discussion that follows. *See, e.g.*, Texas v. Brown, 460 U.S. 730, 748 (1983) (seizures threaten only the interest in possessing objects, not privacy).

8. *See* U.S. CONST. amend. V.

9. *See* U.S. CONST. amends. I, IV & V.

Constitution guarantees the right to speak anonymously and also the right to preserve the confidentiality of one's associations.[10] The Fourth Amendment historically has protected certain areas from unauthorized governmental intrusions based on their constitutional classification as "private."[11] The Fifth Amendment's contribution is more limited; while the U.S. Supreme Court has said that the privilege against compelled self-incrimination protects "personal privacy,"[12] it has "never on any ground,

---

10. *See, e.g.*, McIntyre v. Ohio Elections Comm'n, 514 U.S. 334, 341-42 (1995):

> [A]n author generally is free to decide whether or not to disclose his or her true identity. The decision in favor of anonymity may be motivated by fear of economic or official retaliation, by concern about social ostracism, or merely by a desire to preserve as much of one's privacy as possible. Whatever the motivation may be, . . . the interest in having anonymous works enter the marketplace of ideas unquestionably outweighs any public interest in requiring disclosure as a condition of entry. Accordingly, an author's decision to remain anonymous . . . is an aspect of the freedom of speech protected by the First Amendment.

(footnotes omitted). *See also* NAACP v. State of Alabama *ex rel.* Patterson, 357 U.S. 449, 462 (1958) ("This Court has recognized the vital relationship between freedom to associate and privacy in one's associations."). *See generally* Shawn C. Helms, *Translating Privacy Values with Technology*, 7 B.U. J. SCI. & TECH. L. 288, 307-08 (2001).

11. *See* Katz v. United States, 389 U.S. 347, 350 (1967). *See also* Warden v. Hayden, 387 U.S. 294, 304 (1967) ("the principal object of the Fourth Amendment is the protection of privacy"). *See generally* Olmstead v. United States, 277 U.S. 438, 478 (1928) (Brandeis, J., dissenting) ("every unjustifiable intrusion by the Government upon the privacy of the individual, whatever the means employed, must be deemed a violation of the Fourth Amendment"). The "intrusion" need not be a physical intrusion into a protected area. *See* Kyllo v. United States, 121 S. Ct. 2038, 2046 (2001) "(Where . . . the Government uses a device that is not in general public use, to explore details of the home that would previously have been unknowable without physical intrusion, the surveillance is a 'search' and is presumptively unreasonable without a warrant").

The extent to which the Fourth Amendment has evolved into a measure that protects more than private "places" is analyzed in Section III, *infra.*

12. Fisher v. United States, 425 U.S. 391, 399 (1976). *See, e.g.*, Murphy v. Waterfront Comm'n of N.Y. Harbor, 378 U.S. 52, 55 (1964):

> The privilege against self-incrimination . . . reflects many of our fundamental values and most noble aspirations: our unwillingness to subject those suspected of crime to the cruel trilemma of self-accusation, perjury or contempt; our preference for an accusatorial rather than an inquisitorial system of criminal justice; . . . our respect for the inviolability of the human personality and of the right of each individual "to a private enclave where he may lead a private life." . . .

(citations omitted) (quoting United States v. Grunewald, 233 F.2d 556, 581-82 (2d Cir. 1956), *rev'd* 353 U.S. 391 (1957) (Frank, J., dissenting). *See also* United States v. Couch, 409 U.S. 322, 327 (1973) (privilege "respects a private inner sanctum of individual feeling and thought"); Griswold

personal privacy included, applied the Fifth Amendment to prevent the otherwise proper acquisition . . . of evidence which . . . did not involve compelled testimonial self-incrimination of some sort."[13] Therefore, the only role the Fifth Amendment plays in this skein of privacy is to prevent the state from forcing people to divulge their guilty secrets.

Louis Brandeis and Samuel Warren recognized in 1890 that the essence of constitutional privacy guarantees, all of which were crafted to deal with conduct occurring in the physical world, established a right to be let alone,[14] a right to be ignored absent some demonstrable basis for official

---

v. Connecticut, 381 U.S. 479, 484 (1965) (privilege "enables the citizen to create a zone of privacy").

13. *Fisher*, 425 U.S. at 399 (footnote omitted). *See also id.* at 401:

> The Framers addressed the subject of personal privacy directly in the Fourth Amendment. . . . They did not seek in still another Amendment the Fifth to achieve a general protection of privacy but to deal with the more specific issue of compelled self-incrimination.

But see William J. Stuntz, *The Substantive Origins of Criminal Procedure*, 105 YALE L.J. 393, 418-19 (1995) (early privilege against self-incrimination concerned itself with protecting private information).

14. *See* Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 193 (1890) (defining privacy as "the right to be let alone"). Although the Warren-Brandeis article argued that violations of privacy should be cognizable in tort, the right to privacy they articulated had a constitutional foundation. *See, e.g.*, Gormly, *supra* note 3, at 1357:

> Many commentators have attempted to sever the "expectation of privacy" which has evolved in American jurisprudence under the Fourth Amendment, from the tort of privacy created by Warren and Brandeis in 1890 . . . . Such a sharp division is unfortunate, however, because history confirms that the various offshoots of privacy are deeply intertwined at the roots, owing their origins to the same soil. In the case of the Fourth Amendment, the same soil was Louis Brandeis, who laid the groundwork for the constitutionalization of his notion of privacy in *Olmstead v. United States*.

(footnotes omitted). *See also id.* at 1360 (noting that in his *Olmstead* dissent, Brandeis "borrowed heavily from his Harvard piece . . . weaving the 'right to be let alone' into a Fourth Amendment concept of privacy relating to searches and seizures"). For a discussion of Justice Brandeis' dissent in *Olmstead v. United States*, *see infra* text accompanying note 37.

Professor Lawrence Lessig divides privacy into three different concepts: privacy as a way to minimize the burden of state intrusions; privacy as dignity; and privacy as substantive. *See* LAWRENCE LESSIG, CODE AND OTHER LAWS OF CYBERSPACE 146-49 (1999). The first concept recognizes that the state has the right to interfere with our desire to be left alone but seeks to ensure that such interferences are kept to a minimum. *See id.* at 146 ("The test then is the burden of the

scrutiny, and the fulfillment of certain procedural requirements necessary for the implementation of such scrutiny.[15] This right to be let alone was "designed to balance the people's interests in privacy against the legitimate need for the government"[16] to collect information pertaining to criminal activity.[17]

---

state's intervention; when an intervention can be made less burdensome, the protection against it decreases as well"). The second concept postulates "that the very idea of a search of your possessions is an offense to your dignity. From this perspective, if the state wants to search your house, it had better have a good reason." *Id.* at 147. The third concept regards privacy "as a substantive limit on government's power." *Id.* at 149. "As a restriction on the power of government to enforce certain laws, it provides a substantive limit on the kinds of regulation that government can effectively impose." *Id.*

15. *See, e.g.*, William J. Stuntz, *Privacy's Problem and the Law of Criminal Procedure*, 93 MICH. L. REV. 1016, 1029 (1995):

> Law enforcement, civil or criminal, depends on information. That information is often "private" in the sense that it rests in the hands of someone who would like it kept secret. This description fits almost all incriminating evidence in the hands of a criminal defendant, information that sometimes cannot be extracted due to the Fifth Amendment. Much of the information the system needs is also "private" in a more meaningful sense. It is of a type that many people, not just a particular litigant, might care about keeping secret. . . .
>
> Fourth Amendment law purports to protect most information that is private in this second sense. Unless the police have a facially valid warrant or sufficient cause together with a valid exception to the warrant requirement, they may not search for evidence in places that are both (i) hidden from public view and (ii) likely to contain the sorts of things that ordinary people wish to keep to themselves.

The right to be ignored only applies to official, state action. The ability to escape private scrutiny has always depended on taking affirmative action to avoid such scrutiny. *See, e.g., Olmstead*, 277 U.S. at 478 (Brandeis, J., dissenting) ("The makers of our Constitution . . . conferred, as against the government, the right to be let alone — the most comprehensive of rights and the right most valued by civilized men").

16. Stuntz, *supra* note 15.

17. LESSIG, *supra* note 14, at 113. *See also* Anjali Singhal, *The Piracy of Privacy? A Fourth Amendment Analysis of Key Escrow Cryptography*, 7 STAN. L. & POL'Y REV. 189, 198 (1996) ("The Fourth and Fifth Amendments balance the individual's right to privacy against the government's responsibility to enforce this country's laws"). *See, e.g.*, Boyd v. United States, 116 U.S. 616, 630 (1886) (the Fourth and Fifth Amendments incorporated English common law principles that focus on protecting the individual from "the invasion of his indefeasible right of personal security, personal liberty and private property"). *See also Olmstead*, 277 U.S. at 473 (Brandeis, J., dissenting):

> When the Fourth and Fifth Amendments were adopted, ... [f]orce and violence were then the only means known to man by which a government could directly

The right to be left alone emerged as a reaction to activities conducted in the real world and manifested itself as a constraint on law enforcement's ability to effect real world intrusions.[18] Such intrusions not only included entering into and searching physical spaces, but also detaining, searching, and questioning individuals.[19] The first significant challenge to these concepts and constraints came with the appearance of technology,[20]

> effect self-incrimination. It could compel the individual to testify — a compulsion effected, if need be, by torture. It could secure possession of his papers and other articles incident to his private life — a seizure effected, if need be, by breaking and entry. Protection against such invasion of "the sanctities of a man's home and the privacies of life" was provided in the Fourth and Fifth Amendments by specific language.

See generally Frank v. Maryland, 359 U.S. 360, 376 (1959) (Douglas, J., dissenting) (First, Fourth, and Fifth Amendments are "closely related, safeguarding . . . 'conscience and human dignity and freedom of expression'"); Bram v. United States, 168 U.S. 532, 543-44 (1897) (noting the "intimate relationship" between the Fourth and Fifth Amendments, both of which attempt to perpetuate "principles of humanity and civil liberty").

18. *See, e.g., Boyd*, 116 U.S. at 626-30 (reviewing English common law, "every American statesman, during our revolutionary and formative period as a nation, was undoubtedly familiar" — barring government invasions of privacy and noting that these principles, which found expression in the Fourth and Fifth Amendments, "apply to all invasions on the part of the government and its employees of the sanctity of a man's home and the privacies of life").

The "real world" is our shared physical reality that provided the corporeal venue for the historical development of the criminal law and criminal procedure principles we apply today. *See, e.g.*, Brenner, *infra* note 121, ¶ 10. *See also infra* note 122 and accompanying text.

19. *See, e.g.*, LESSIG, note 14, 112-14. Lessig explains that the Fourth Amendment was written at a time when "the legal protection against the invasion of privacy was trespass law," and its warrant requirement aimed to protect officers from civil suits for trespass. *See id.* at 112-13. *See also id.* at 113-14:

> The Fourth Amendment focuses on trespass because that was the primary mode of searching at the time. If it had been possible simply to view the contents of a house without going inside, the restrictions of the Fourth Amendment would have made little sense. But the protections of the amendment did make sense as a way to draw the balance between the government's power to search and the people's right to privacy *given* the regime of trespass law and privacy-invading technologies that prevailed at the end of the eighteenth century.

(emphasis in the original).

20. Indeed, it was technology that produced an awareness of and a concern with the notion of "privacy." *See, e.g.*, Warren & Brandeis, *supra* note 14, at 193:

> Recent inventions and business methods call attention to the next step which must be taken for the protection of the person, and for securing to the individual what

namely, the telephone, which permitted instantaneous synchronous remote communication between individuals.[21] The proliferation of telephone technology in the early Twentieth Century compelled courts to consider how, if at all, traditional guarantees of privacy should be applied to mediated communication.[22]

> Judge Cooley calls the right "to be let alone." Instantaneous photographs and newspaper enterprise have invaded the sacred precincts of private and domestic life; and numerous mechanical devices threaten to make good the prediction that "what is whispered in the closet shall be proclaimed from the house-tops."
> . . . The intensity and complexity of life, attendant upon advancing civilization, have rendered necessary some retreat from the world, and man, under the refining influence of culture, has become more sensitive to publicity, so that solitude and privacy have become more essential to the individual; but modern enterprise and invention have, through invasions upon his privacy, subjected him to mental pain and distress, far greater than could be inflicted by mere bodily injury. . . .

See also Gormly, *supra* note 3, at 1336 (Brandeis & Warren argued for the recognition of a "new right," the right of privacy).

21. For the distinction between synchronous and asynchronous communication, see, *e.g.*, R.J. Slagter, *Visual Attention in Multiparty Communication* 6 (University of Twente, 1997), *available at* https://doc.telin.nl/dscgi/ds.py/Get/File (last visited Oct. 6, 2002):

> A face-to-face meeting is an example of *synchronous* communication. Synchronous communication is characterized by the fact that the cues sent by one person are instantly received by the other. If cues are first stored in some way, and the other person receives them later, the communication is a*synchronous*. Examples of asynchronous communication are: a letter, a voice mail and an e-mail message.

See also Karrie Karahalios, *Communication Systems: A Comparison Along a Set of Major Axes, available at* http://www.media.mit.edu/~kkarahal/generals/communication/ (last visited Aug. 23, 2002). *See generally* William J. Mitchell, *The City of Bits Hypothesis in* HIGH TECHNOLOGY AND LOW-INCOME COMMUNITIES (D. Schön et al. eds., 1996) (synchronous communication can take place in face-to-face interactions or via the telephone; asynchronous communication can take the form, either, of a letter, a voice mail message or an e-mail message); Mary E. Virnoche, *When A Stranger Calls: Strange Making Technologies and the Transformation of the Stranger* (1999), *available at* http://www.humboldt.edu/~mv23/STRANGER.PDF (last visited Dec. 18, 2002) (analyzing mediated and non-mediated communication strategies).

22. *See, e.g.*, LESSIG, *supra* note 14, at 111 (noting that by the 1920s telephones "had become a dominant mode of communication" and life had "begun to move onto the wires"). *See also* CLAUDE S. FISCHER, AMERICA CALLING: A SOCIAL HISTORY OF THE TELEPHONE TO 1940, 33-53 (1992).

The telephone was not the first technology to achieve instantaneous interchanges by applying "the natural phenomenon we call electricity to the processes of human communication." BRIAN WILSON, MEDIA, TECHNOLOGY AND SOCIETY – A HISTORY: FROM THE TELEGRAPH TO THE INTERNET 321-36 (1998). That honor belongs to the telegraph, which permits asynchronous

communication between people located at some geographical remote. *See, e.g.*, TOM STANDAGE, THE VICTORIAN INTERNET vii (1998) ("During Queen Victoria's reign, a new communications technology was developed that allowed people to communicate almost instantly across great distances"). After Samuel Morse formed his telegraph company in 1845, the "growth of the telegraph network was . . . nothing short of explosive." *See id.* at 56-91. As lines were installed around the world, the telegraph "revolutionized business practice, gave rise to new forms of crime, and inundated its users with information." *Id.* at vii.

But for practical reasons, telegraphy did not give rise to the privacy challenges associated with telephonic technology. It was a proprietary communication system in which all communications were necessarily revealed to agents of the telegraph company, who translated the messages into Morse Code and transmitted them to another agent, who then translated them from Morse Code and delivered them to the recipient. *See, e.g., id.* at 63-65. *See also* Arthur W. Grumbine, *The Era of Morse Telegraphy: Part 1, available at* http://www.faradic.net/~gsraven/telegraph_tales/grumbine/grumbine_1.html (last visited Sept. 9, 2002) ("Telegraphy. . . . was no different from opening everybody's mail and reading every word of it; then sending the contents across country by a peculiar code system invented by Samuel F. B. Morse"). It was simply not possible for those who employed telegraphic communication to claim that the privacy of their communications had been compromised by "outsiders." There were, in effect, no nonconsensual "overhears" in the telegraphic system. *See generally* Karahalios, *supra* note 21 (privacy was less of a concern with the telegraph because it "did not prevail in the home environment" and therefore tended to involve messages of a less personal nature). *But see id.* at 110-12 (telegraph patrons' concern about having their privacy compromised by the clerks who sent the messages gave rise to the widespread practice of sending telegrams in private code). *See, e.g.*, Primrose v. W. Union Tel. Co., 154 U.S. 1, 4-5 (1894) (suit seeking damages for mistake made in transmitting coded telegraphic message; Postal Telegraph-Cable Co. v. Louisville Cotton Oil Co., S.W. 843, 852-53 (Ky. App. Rptr. 1909) (suit for damages resulting from failure to deliver coded telegraphic message). Coded telegrams were sometimes used in criminal activity. *See, e.g.*, State v. Chapman, 6 Nev. 320, 1871 WL 3337, at *5 (Nev. 1871) (accomplice sent a "cipher telegram" advising robbers when a large shipment of coins would be arriving).

There were concerns that private messages might — by error or by intent — be delivered to the wrong parties or the contents otherwise revealed improperly. These concerns prompted some states to adopt statutes creating a cause of action for those whose messages went awry or were made public. *See, e.g.*, VA. CODE ANN. § 2900 (Michie 1900)

> (telegraph companies shall be liable for special damages occasioned in . . . delivering dispatches or for the disclosure of the contents of any private dispatch to any person other than to him to whom it was addressed, . . . the amount of these damages to be determined by the jury upon the facts in each case. Grief and mental anguish occasioned to the plaintiff . . . may be considered by the jury in the determination of the quantum of damages

(quoted in Connelly v. W. Union Telegraph Co., 40 S.E. 618, 622 (Va. 1902)). *See also* IND. REV. STAT. § 5513 (1894) (cited in W. Union Telegraph v. Bierhaus, 36 N.E. 161, 162 (Ind. App. 1894)). Some states made it a crime for a telegraph company or its employees to disclose the contents of a telegram to anyone but the authorized recipient. *See, e.g.*, MINN. GEN. STAT. § 6782 (1894) (cited in Peterson v. W. Union Telegraph Co., 77 N.W. 985, 987 (Minn. 1899); 13 WAGNER'S STATUTES

Mediated communication is communication that takes place via some artificial medium (such as the telephone); it is distinguishable from direct, or face-to-face, communication.[23] Mediated communication can be specifically directed at one or more known parties, as in a telephone conversation, or it can be disseminated generally to an unidentified audience, such as in radio or television broadcasts.[24] Mediated communication can also be interactive, like the telephone conversation, or it can be the unilateral transmission of information, such as with radio or television broadcasts.

---

§ 51 (cited in *Ex parte* Brown, 72 Mo. 83, 1880 WL 423, at *4 (Mo. 1880)). *See also* Little Rock & Fort Smith Tel. Co. v. Davis, 41 Ark. 79, 1883 WL 1201, at * 3 (Ark. 1883) (noting state statutes imposing civil liability and criminal penalties) (citing SCOTT & JARNAGAN, LAW OF TELEGRAPHS §§ 419-46).

In the Nineteenth Century, telegrams were far more private than telephone conversations. *See, e.g.*, Brashears v. W. Union Telegraph Co., 45 Mo. App. 433, 1891 WL 153, at *4 (Mo. App. 1891) ("[T]he use of telephonic connections in intra-urban service practically amounts to a collateral disclosure of the contents of a private telegram"). *See generally* FISCHER, *supra*, at 71.

23. *See, e.g.*, Prasad Boradkar, *The Object(s) of Communication*, Industrial Design Society of America — 2001 Proceedings, *available at* http://www.idsa.org/whatsnew/01ed_proceed/boradkar.pdf (last visited Oct. 28, 2002):

> The purest . . . form of interpersonal communication is executed face to face between two people without the use of any implement or instrument, and is called unmediated communication. . . . [M]ediated communication involves the use of a commodity/artifact/ technology, and is impure because the mere presence of a medium interferes with the process.

Id.; see also Robert T. Craig, *Communication in* ENCYCLOPEDIA OF RHETORIC, *available at* http://spot.colorado.edu/~craigr/Communication.htm (last visited Aug. 29, 2002) (one way of

> classifying communication is according to the . . . media . . . through which it occurs. . . . *Medium* (in current usage often confused with its Latinate plural form, *media*) refers to a particular configuration of physical, technological, and institutional characteristics that constitute a distinct form of communication such as face-to-face interaction, commercial television, or electronic mail).

24. An example of mediated communication directed at a "known" party is a telephone conversation. Absent obscene or harassing calls, the parties to such a conversation "know" each other in the sense that they each know the identity of the other, though they may not be personally acquainted. Television broadcasts, newspapers, or web sites are clear examples of mediated communications disseminated generally to an unidentified audience. In none of these examples does the speaker "know" the identities of all the persons who will receive the communication.

The first form of mediated communication was not telephonic, but rather used written symbols to record communications on paper. Unlike telephonic communication, which is necessarily interactive, written communication can either be interactive, as in an exchange of business or personal letters, or it can consist of unilaterally transmitting information, as with the publication of newspapers or other periodicals. The interactivity of telephonic communication and one-to-one written communication makes these types of mediated communications analogous to face-to-face communication. The analogy is more imperfect for written communication because the parties not only lack the opportunity to observe the body language of their correspondents,[25] but they also conduct a "conversation" that does not occur in real time.

Written one-on-one communication historically enjoyed the protections of existing privacy guarantees, at least while the writing was in transit.[26]

---

25. In face-to-face communication, "[l]anguage is closely linked with and supported by, non-verbal communication which adds to the meaning of utterances, provides feedback, controls synchronisation and also plays a central role in human social behaviour." Katerina Mania & Alan Chalmers, *A Classification for User Embodiment in Collaborative Virtual Environments, available at* http://www.cs.bris.ac.uk/Tools/Reports/Ps/1998-mania.pdf (last visited Oct. 28, 2002). *See also* Janet Bavelas et al., *Using Face-to-Face Dialogue as a Standard for Other Communication Systems*, 22 CANADIAN J. COMM. (1997). Non-verbal cues are communicated via facial expressions, gaze, gestures, posture, "self-representation," and bodily contact. *See* Mania & Chalmers, *supra*.

The parties to telephonic communication do have some opportunity to assess nonverbal cues, as they can analyze the tenor and other characteristics of the voice of each other. *See, e.g.*, Bavelas et al., *supra* (in telephone conversations "[t]here are . . . audible non-verbal features, such as the nuances of vocal inflection, tone of voice, and pauses — all of which can convey significant information" to the listener).

26. *See, e.g., Ex parte* Jackson, 96 U.S. 727, 733 (1878):

> [A] distinction is to be made between . . . what is intended to be kept free from inspection, such as letters, and sealed packages . . . and what is open to inspection, such as newspapers, magazines, . . . and other printed matter. . . . Letters and sealed packages . . . are as fully guarded from examination and inspection . . . as if they were retained by the parties . . . in their own domiciles. The constitutional guaranty of the right of the people to be secure in their papers against unreasonable searches and seizures extends to their papers, thus closed against inspection, wherever they may be. Whilst in the mail, they can only be opened and examined under like warrant, . . . as is required when papers are subjected to search in one's own household.

See also United States v. Jacobsen, 466 U.S. 109, 114 (1984) ("Letters and other sealed packages are . . . effects in which the public at large has a legitimate expectation of privacy"). As was

Conceptually, the protection derived from the fact that the transmitting correspondent took efforts to shield the content of the communication from outsiders, e.g., by sealing the message into an opaque envelope.[27] This was not true of other categories of written communication, which were made public or "published."[28]

The U.S. Supreme Court first addressed the privacy of telephonic communications in *Olmstead v. United States*.[29] The issue in *Olmstead* was "whether the use of evidence of private telephone conversations . . . intercepted by means of wire tapping, amounted to a violation of the

---

explained earlier, the structure of telegraphic communication meant that it did not produce the type of privacy issues associated with written and telephonic communication. *See supra* note 22.

27. *See supra* text accompanying note 26.

28. *See id.*

29. 277 U.S. 438 (1928). Prior to *Olmstead*, only a few reported decisions addressed wiretapping, mostly in the context of prosecutions under statutes that made it a crime to intercept telegraph or telephone messages. *See, e.g.*, State v. Behringer, 172 P. 660, (Ariz. 1918) (holding it was not a violation of Arizona Penal Code section 692 — which made it unlawful "by means of any machine, instrument or contrivance" to read or attempt to read "any message, or to learn the contents thereof, whilst the same is being sent over any telegraph or telephone line" — to place a dictograph over the transom of a room and thereby hear what was said over a telephone). *See also id.* at 479 n.13 (Brandeis, J., dissenting) (listing statutes that made it a crime to intercept telephone or telegraph messages).

Several of the reported cases indicate that wiretapping was far from uncommon, even before *Olmstead* was decided. In *State v. Nordskog*, 136 P. 694 (Wash. 1913), the Washington Supreme Court reversed the conviction of a former detective and "professional wire tapper" for "damaging" a telephone line. The Washington Supreme Court based the conviction solely on his having tapped the line to intercept a message. *See id.* at 694-95. The Washington Supreme Court found that the mere act of tapping the line inflicted no damage, but it also noted the need for legislation to prevent further such acts:

> [T]here has been altogether too much of this form of pilfering going on in this state, and the omission of the law now disclosed calls aloud for legislative action. . . . [T]he law should be so framed that the privacy of all citizens . . . may be protected, and that any tampering or interference, however slight, that is not done under the rules of the company and by its agents, or under some regulation of the public service commission, may be prohibited. . . .

Id. at 695. *See also* Robilio v. United States, 291 F. 975, 982-83 (6th Cir. 1923) (upholding the admissibility of evidence obtained by wiretapping the home of the defendant against evidentiary challenges as to its authenticity; no challenge was based on the act of wiretapping itself); People v. McDonald, 165 N.Y.S. 41, 44-45 (N.Y. App. Div. 1917) (refusing to suppress evidence obtained by tapping the home of the defendant on the grounds that under New York law it was immaterial how the state obtained the evidence and that the Fourth Amendment did not apply to the states, only to the federal government).

Fourth and Fifth Amendments."[30] The U.S. Government installed wiretaps on phone lines leading from the residences of Roy Olmstead, the suspected leader of a large bootlegging operation, and several of his associates.[31] The U.S. Government used the information so gathered to prosecute suspected bootleggers for violating prohibition laws.[32] The wiretaps connected to the phone lines as they ran toward the residences; therefore, there was no physical intrusion into the homes.[33] In an opinion written by Chief Justice Taft, a majority of the Court resolved the issue by simply transposing traditional Fourth Amendment[34] standards into this new context. The U.S. Supreme Court held that the intercepted conversations effected neither a "search" nor a "seizure" because there was no physical intrusion into a

---

30. *Olmstead*, 277 U.S. at 456-57.

31. *See id.* at 455-56:

> The evidence . . . discloses a conspiracy of amazing magnitude to import, possess, and sell liquor unlawfully. It involved . . . not less than 50 persons, . . . two sea-going vessels for the transportation of liquor . . . , the maintenance of a central office manned with operators, and the employment of executives, salesmen, deliverymen dispatchers, scouts, bookkeepers, collectors, and an attorney. . . .

Olmstead was the leading conspirator and the general manager of the business.

32. *See id.* at 455 ("The petitioners were convicted in the District Court for the Western District of Washington of a conspiracy to violate the National Prohibition Act . . . by unlawfully possessing, transporting and importing intoxicating liquors and . . . by selling intoxicating liquors").

33. *See id.* at 456-57:

> [I]nformation . . . was . . . obtained by intercepting messages on the telephones of the conspirators. . . . Small wires were inserted along the . . . telephone wires from the residences of . . . the petitioners and those leading from the chief office. The insertions were made without trespass upon any property of the defendants. They were made in the basement of the large office building. The taps from house lines were made in the streets near the houses.

34. The U.S. Supreme Court found there was no basis for applying the Fifth Amendment because there

> was no evidence of compulsion to induce the defendants to talk over their many telephones. They were continually and voluntarily transacting business without knowledge of the interception. Our consideration must be confined to the Fourth Amendment.

Id. at 462.

constitutionally protected area.[35] Justice Brandeis dissented, arguing that "in the application of a Constitution, our contemplation cannot be only of what has been, but of what may be."[36] Justice Brandeis maintained that in order to preserve the values the U.S. Constitution intended to protect, what is now known as a "technological-neutral" interpretation was necessary.[37]

It was not until 1967, in *Katz v. United States*,[38] that the U.S. Supreme Court recognized that the literal transposition of standards, developed to deal with the intrusions encountered in centuries past, was not a viable way by which to preserve and enforce privacy guarantees in an age of electronic communication. The issue was whether the government had violated Katz's Fourth Amendment rights by using a wiretapping device installed on the outside of a phone booth to record calls he made while inside.[39] The

---

35. *See Olmstead*, 277 U.S. at 466:

> The reasonable view is that one who installs in his house a telephone instrument with connecting wires intends to project his voice to those quite outside, and that the wires beyond his house, and messages while passing over them are not within the protection of the Fourth Amendment. . . .
> We think, therefore, that the wire tapping here disclosed did not amount to a search or seizure within the meaning of the Fourth Amendment.

The U.S. Supreme Court distinguished the interception of sealed mail. *See id.* at 465 ("the unlawful rifling by a government agent of a sealed letter is a search and seizure of the sender's papers of effects").

36. *Id.* at 474.

37. *See id.* at 473-74:

> When the Fourth and Fifth Amendments were adopted . . . [f]orce and violence were then the only means known to man by which a government could directly effect self-incrimination. It could compel the individual to testify . . . by torture. It could secure possession of his papers and other articles incident to his private life . . . by breaking and entry. . . . But "time works changes, brings into existence new conditions and purposes." Subtler and more far-reaching means of invading privacy have become available to the government. . . .
> The progress of science in furnishing the government with means of espionage is not likely to stop with wire tapping. Ways may some day be developed by which the government, without removing papers from secret drawers, can reproduce them in court, and . . . expose to a jury the most intimate occurrences of the home. . . . Can it be that the Constitution affords no protection against such invasions of individual security?

38. 389 U.S. 347 (1967).

39. *Id.* at 348.

Katz Court rejected *Olmstead* in favor of the approach Justice Brandeis had advocated forty-years before:

> [A] person in a telephone booth may rely upon the protection of the Fourth Amendment. One who occupies it, shuts the door behind him, and pays the toll that permits him to place a call is surely entitled to assume that the words he utters into the mouthpiece will not be broadcast to the world. To read the Constitution more narrowly is to ignore the vital role that the public telephone has come to play in private communication.[40]

Almost forty years after *Olmstead*, *Katz* broadened constitutional interpretation sufficiently to bring telephonic communication — Nineteenth Century technology — within the ambit of the privacy guarantees of the Fourth Amendment.[41] However, as the U.S. Supreme

---

40. *Id.* at 352. The shift in perspective was no doubt attributable to the increased use and sophistication of surveillance technology:

> By the 1950s, the technology that enabled government surveillance had grown by exponential leaps. Parabolic microphones, transmitters the size of cigarette packs . . . and miniature television transmitters made it possible . . . to watch, listen and record virtually any sound or movement. . . . Attempts by the states to . . . prohibit wiretapping were largely ineffective. The state statutes tended to create broad exceptions for police conducting eavesdropping . . . [and] the language of the statutes was rarely drafted to keep up with the swiftly-changing technology, rendering them quickly obsolete. . . .
> The 1960s soon witnessed a national uproar over the unchecked ability of government . . . to eavesdrop. Attorney General Robert Kennedy appeared before the Senate Judiciary Committee . . . in support of new legislation which would . . . authorize government interceptions only with court orders. . . .
> In his State of the Union address in 1967, President Lyndon B. Johnson . . . delivered the following message, amidst bipartisan applause:
>
> > We should protect what Justice Brandeis called the "right most valued by civilized men" — the right to privacy. We should outlaw all wiretapping . . . except when the security of the nation is at stake — and only then with the strictest governmental safeguards. And we should exercise the full reach of our Constitutional powers to outlaw electronic "bugging" and "snooping."

Gormly, *supra* note 3, at 1363-64.

41. Alexander Graham Bell patented the telephone in 1876, so it was more than fifty years old when *Olmstead* was decided. *See, e.g.*, WILSON, *supra* note 22, at 43-48. *See also* The History of the Telephone, *available at* http://inventors.about.com/library/inventors/bltelephone.htm (last

Court decided *Katz*, efforts were underway that would result in the invention of the Internet, and with it new and infinitely more complex varieties of mediated communication.[42] By the time the Twenty-First Century dawned, cyberspace had become an important new venue for mankind's activities, licit and illicit. The rise and proliferation of cybercrime raised new problems for law enforcement, both with the enforcement of existing substantive laws against conduct vectored through cyberspace and also in the gathering of evidence without violating the existing privacy standards.

II. FIRST AMENDMENT

The use of cyberspace offers criminals a number of advantages, despite the existing substantive laws. The most pertinent of those advantages to this discussion is anonymity.[43] A March 2000, report issued by the

---

visited Aug. 29, 2002); The Bell Patent, *available at* http://inventors.about.com/library/inventors/bltelephone1.htm (last visited Aug. 29, 2002).

42. *See, e.g.*, WILSON, *supra* note 22, at 321-36. *See also* Hobbes' Internet Timeline v5.4, *available at* http://www.zakon.org/robert/internet/timeline/ (last visited Aug. 29, 2002); Christopher D. Hunter, *The Real History of the Internet in* THE USES AND GRATIFICATIONS OF PROJECT AGORA, *available at* http://www.asc.upenn.edu/usr/chunter/agora_uses/chapter_2.html (last visited Aug. 29, 2002).

43. A distinction is often drawn between "anonymity" and "pseudonymity." Both involve shielding the true identity of oneself: pseudonymity is the use of a false name, an alias, to *disguise* the identity of oneself; anonymity consists of *concealing* the identity of oneself. *See, e.g.*, David G. Post, *Pooling Intellectual Capital: Thoughts on Anonymity, Pseudonymity, and Limited Liability in Cyberspace*, 11 U. CHI. LEGAL F. 139, 149-51 (1996):

> An "anonymous message" can be defined as a message that provides the recipient with no information . . . concerning the identity of the message originator. . . .
> . . . Assume . . . you receive a series of [untraceably anonymous] e-mails, all bearing the same signature. . . . As you come to associate certain characteristics with the . . . entity associated with the identifier "your friend" — grammar, spelling, style . . . and so on — it becomes increasingly useful to recognize that "your friend," whoever or whatever it may be, is the message originator. "Your friend," in short, has become a pseudonym.

See also id. at 152 (a "pseudonymous message" is "anonymous (in the sense that it provides no information concerning the identity of the . . . individual . . . responsible for . . . transmitting the message), but . . .contains some information about the identity of some cognizable entity that is" its originator).

The discussion which follows in the text uses the term "anonymity" to encompass both practices because it is concerned with the extent to which the First Amendment protects the right to shield the true identity of oneself regardless of the technique used to do so. *See, e.g.*, McIntyre

President's Working Group on Unlawful Conduct on the Internet noted many of the problems on-line anonymity poses for law enforcement:

> Anonymous e-mail accounts, which are e-mail accounts where subscriber information is not requested or verified, are the proverbial double-edged sword. Such accounts can protect privacy, but they add new complexities to identifying online lawbreakers, such as individuals who send child pornography, death threats, computer viruses, or copyright-protected works by e-mail.
>
> Similarly, "anonymous re-mailer" services, which are e-mail services that strip the source address information from e-mail messages before passing them along to their intended recipients, raise difficult privacy and law enforcement policy issues. On the one hand, anonymous re-mailer services provide privacy and encourage freedom of expression. . . . On the other hand, such services can plainly frustrate legitimate law enforcement efforts.[44]

The unique nature of cyberspace's mediated communication only exacerbates the problems anonymity poses, especially with regard to certain types of criminal activity:

---

v. Ohio Elections Comm'n, 514 U.S. 334, 341-43 (1995) (describing Madison, Hamilton and Adam's use of the pseudonym "Publius" in publishing the *Federalist Papers* as part of "a respected tradition of anonymity in the advocacy of political causes").

44. WORKING GROUP ON UNLAWFUL CONDUCT ON THE INTERNET, THE ELECTRONIC FRONTIER: THE CHALLENGE OF UNLAWFUL CONDUCT INVOLVING THE USE OF THE INTERNET § III(B)(2) (Mar. 2000), *available at* http://www.usdoj.gov./criminal/cybercrime/unlawful.htm (last visited Dec. 9, 2002). *See Testimony of Deputy Attorney General Eric Holder Before the Subcommittee on Crime of the House Judiciary Committee and the Subcommittee on Criminal Justice Oversight of the Senate Judiciary Committee (February 29, 2000), available at* http://www.cdt.org/security/000229justice.shtml (last visited Aug. 29, 2002) [hereinafter *Holder Testimony*]:

> It doesn't take a master hacker to disappear on a network. . . . [A] criminal using tools and other information easily available over the Internet can operate in almost perfect anonymity. By weaving his or her communications through a series of anonymous remailers; by creating a few forged e-mail headers with powerful, point-and-click tools readily downloadable from many hacker web sites; or by using a "free-trial" account or two, a hacker, online pornographer, or web based fraud artist can often effectively hide the trail of his or her communications.

See also Neal Kumar Katyal, *Criminal Law in Cyberspace*, 149 U. PA. L. REV. 1003, 1037 (2001); Jonathan I. Edelstein, Note, *Anonymity and International Law Enforcement in Cyberspace*, 7 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 231 (1996).

> Although prior communication methods permit anonymous communications, those services generally provide one-to-one communications. It would be both time-consuming and costly to use either the phone or mail systems to disseminate information wholesale, effectively preventing wide-scale malicious use and limiting the harm that can be caused. On the Internet, by contrast, there are no monetary or technical impediments to worldwide dissemination of communications.[45]

Anonymity, however, is part of the right to be let alone. As noted earlier, the U.S. Supreme Court has held, in decisions addressing conduct based in the real world, that the First Amendment guarantees the right to speak anonymously and to preserve the confidentiality of one's associations.[46] No one disputes that anonymity plays a legitimate role in on-line discourse.[47] The issue is how to translate rights devised to deal with

---

45. *Hearings on "Mayhem Manuals and the Internet" before the Subcommittee on Terrorism, Technology and Government Information of the Senate Judiciary Committee, available at* 1995 WL 293484 (Testimony of Robert S. Litt, Deputy Assistant Attorney General, Department of Justice, Criminal Division).

46. *See McIntyre*, 514 U.S. at 341-42; NAACP v. State of Alabama *ex rel.* Patterson, 357 U.S. 449, 462 (1958). In the discussion that follows, "anonymity" is used to encompass both the right to speak anonymously and the right to "associational privacy." The application of the two rights is clearly distinct in the real world because associations in the real world are face-to-face and therefore not anonymous; even if the parties involved in such an association use false names, the nature of face-to-face interaction means that they learn enough information to be able to identify each other by physical appearance. In the context of the real world, therefore, authorities can order someone to reveal the identities of those with whom they have associated, confident that the person possesses experiential or documentary information about what they at least believe to be the true identities of their associates. *See, e.g.*, Gibson v. Fla. Legislative Investigation Comm'n, 372 U.S. 539, 540-42 (1963); *Patterson*, 357 U.S. at 451-54. This is not necessarily true in the virtual world, where individuals can, and do, associate with a high level of anonymity. These anonymous associations pose a practical barrier to attempts to obtain information about associates. If, for example, law enforcement officials identified someone and directed them to reveal the names of those with whom they had associated with on-line, they could explain that this was impossible because the associations were anonymous. In this scenario, the right to remain anonymous in effect protects the right to maintain the confidentiality of one's associations. *See generally* People v. Aboaf, 721 N.Y.S.2d 725, 733 (N.Y. Crim. Ct. 2001) (statute did not prohibit wearing masks "for anonymity as a necessary corollary to freedom of association, both protected by the First Amendment"). And if the on-line association were not conducted anonymously, then they could simply invoke the right to maintain the confidentiality of those associations; the fact that the association occurred in the virtual world instead of in the real world would be irrelevant.

47. "[A]nonymity has sometimes been assumed for the most constructive purposes." Talley v. California, 362 U.S. 60, 65 (1960). *See* Post, *supra* note 43, at 139 ("By permitting individuals to communicate without fear of . . . retribution, anonymity permits information to be injected into

real world conduct into the on-line context, where greater degrees of anonymity are possible and where anonymity can more easily be exploited to illicit ends.

As Professor David Post points out, it is necessary to devise new approaches for dealing with anonymity in cyberspace "because there is not really any existing law regarding truly anonymous communications or transactions, for the simple reason that such communications or transactions are, by definition . . . beyond the reach of ordinary legal processes."[48] He uses the facts in *McIntyre v. Ohio Elections Commission*,[49] a recent U.S. Supreme Court decision on anonymous communications,[50] to illustrate why this is so. Mrs. McIntyre distributed leaflets opposing a proposed tax levy; since some of the leaflets did not identify her as the author, the Ohio Elections Commission fined her for violating an Ohio statute prohibiting the distribution of anonymous campaign literature.[51] The U.S. Supreme Court held that the statute violated Mrs. McIntyre's First Amendment right to anonymous speech.[52] Of course, the acts that caused Mrs. McIntyre to be fined

---

public discourse that might otherwise remain undisclosed"). *See also Surveillance by Design*, Scientific American (Sept. 2001), *available at* http://www.sciam.com/article.cfm?articleID=000B322D-294E-1C6F-84A909EC588ER21&pageNumber=1&catID=2 (last visited Oct. 28, 2002) ("critical for . . . whistle-blowers, political activists, those pursuing alternative lifestyles, and entrepreneurs who want to acquire technical information without tipping off their competitors"); *Hearings on "Mayhem Manuals and the Internet," supra* note 45 (lets whistle-blowers "come forward without fear of retribution" and lets individuals communicate "without sacrificing personal privacy — for example a group of rape victims might wish to communicate with each other without being personally identified"). *See, e.g.*, Anderson v. Hale, 2001 WL 503045, at *7 (N.D. Ill. 2001) (noting the chilling effect that would result from breaching the Internet anonymity of members of "one of the most despicable and hated organizations of this time"). For an analysis of legal and social conventions governing anonymity, see Saul Levmore, *The Anonymity Tool*, 144 U. PA. L. REV. 2191, 2192-95 (1996). *But see* LESSIG, *supra* note 14, at 80:

> Just as anonymity might give you the strength to state an unpopular view, it can also shield you if you post an irresponsible view. Or a slanderous view. Or a hurtful view. . . . Both utterances benefit from anonymity, but the community has good reason to resist utterances like the second.

48. Post, *supra* note 43, at 141.

49. *McIntyre*, 514 U.S. at 341-42.

50. The U.S. Supreme Court recently decided *Watchtower Bible and Tract Society v. Village of Stratton*, 122 S. Ct. 2080 (2002), in which it reiterated the importance of anonymous speech. *See* Watchtower Bible & Tract Soc'y v. Vill. Of Stratton, 122 S. Ct. 2080, 2089-90 (2001).

51. *See McIntyre*, 514 U.S. at 337-38.

52. *See id.* at 357.

> were not anonymous at all — she went to a meeting of her neighbors and, acting in a manner such that her identity was evident to all, distributed . . . literature without printed identification. There were . . . two elements to the offense with which Mrs. McIntyre was charged: (1) anonymous communication . . . and (2) some nonanonymous action sufficient to allow her to be identified and charged with the offense. Both were required . . . but only with respect to the first did the Ohio legislature make a choice; the second is a consequence of a more fundamental requirement that rules can only be enforced by identifying some party against whom to proceed.[53]

The Ohio statute at issue in *McIntyre*, like all criminal statutes, assumes that perfect anonymity[54] cannot be achieved and that the lack of perfect anonymity "can be counted on to resolve the enforcement dilemma."[55] Inherent in our legal system is the correlative assumption that society can and should allow a level of anonymity for its constructive benefits. The reasoning behind this assumption is that if the right to speak anonymously is abused for criminal or other undesirable purposes — descending into "destructive anonymity" — it is likely that the perpetrator can be identified and sanctioned for that conduct.[56] Anonymity as a component of the right

---

53. Post, *supra* note 43, at 143.

54. "Perfect anonymity is the absence of information related to the source of an action." Helms, *supra* note 10, at 301. Computer security expert Donn Parker describes what must be the ultimate in perfect anonymity.

> [A]n automated crime is a complete, fully automated, ready-to-use crime . . . packaged in a single computer program. . . . When the program is executed, it automatically commits the crime and removes any damning evidence . . . Theoretically, anyone could . . . send . . . an automated crime program over the Internet for execution in the victims' computers. Because the crime can be designed for bi-directional, perfect anonymity, the perpetrator need not know who the victim was, what crime occurred, what method was used or even the results of the crime. The victim, likewise, would not know the perpetrator, what method was used, and where his or her losses went. . . .

Donn Parker, *Automated Crime*, INFORMATION SECURITY (Sept. 1999), *available at* http://www.infosecuritymag.com/articles/1999/autocrime.shtml (last visited Aug. 30, 2002).

55. Helms, *supra* note 10, at 301.

56. These assumptions represent a pragmatic way of dealing with the issues Professor Lessig raises, e.g., that while society may want to indulge constructive anonymity, it has good reason to resist destructive anonymity. As long as these assumptions hold, society can tolerate anonymity without finding the bargain too costly.

to be let alone therefore comes with minimal costs. As long as these assumptions hold, constitutionally guaranteed anonymity does not pose a significant problem for law enforcement. Like Mrs. McIntyre who distributed leaflets anonymously, those who send death threats, distribute child pornography and steal intellectual property are likely to be identified by their actions in the real world, apprehended and punished.

Unfortunately, these assumptions do not hold in cyberspace, where perfect anonymity is achieved because of the complex types of mediated communication it allows. Any type of mediated communication, including snail mail correspondence and telephone calls, holds the potential for some level of anonymity since mediated communication by definition eliminates the opportunity for the personal observation that is inevitable in face-to-face interaction. In other words, cyberspace eliminates the ability to observe someone like Mrs. McIntyre distribute leaflets of information. But because snail mail correspondence and telephone calls only allow one-to-one communication, it is difficult, if not impossible, to communicate anonymously on a large scale.[57] Had Mrs. McIntyre wanted to distribute her leaflets anonymously, she would either have had to mail them to individual voters in unmarked envelopes or take advantage of the economies offered by bulk mail rates. Either option raises her risk of compromising anonymity: if she took the first, she might well be observed mailing the large quantity of leaflets in their envelopes; and if she took the second, she would have to interact with post office employees to arrange for bulk mailing.[58]

Maintaining anonymity would be even more difficult if she chose to communicate her message by telephone. Mrs. McIntyre would have to call each voter individually, and one or more might identify her voice. Using

---

57. *See, e.g.*, Katyal, *supra* note 44, at 1048 ("[I]n realspace, pay telephones, cell phones, and regular mail offer users some degree of anonymity, but these methods provide mostly point-to-point communications between sender and recipient. On the internet, however, one person can reach millions with a single message"). *See also* WILSON, *supra* note 22, at 60 ("Making it possible for one subscriber to talk to many others would have enhanced the telephone as a non-hierarchical means of communication" but "[i]t was not to be").

58. There are snail mail remailing services. *See, e.g.*, What's Interesting? Letter Postcard Remailing Service, *available at* http://www.whatsinteresting.com/remail.htm (last visited Aug. 30, 2002). For a fee, payable in cash, by check, or by credit card, these services will mail envelopes, postcards, or packages sent to them. *See id.* Payment by check or credit card obviously enhances the likelihood that the person using the service can be identified, but this is a possibility even for those who pay in cash, since the service tracks the ZIP codes of the items it sends. *See* What's Interesting? Tracking, *available at* http://www.whatsinteresting.com/tracking.htm (last visited Aug. 30, 2002).

a telephone on which caller identification had been disabled would prevent those she called from identifying the source of the call, but the telephone company would have records of the calls. These records could be used to identify the telephone she used and, perhaps, to identify Mrs. McIntyre herself. In none of these scenarios can Mrs. McIntyre achieve "threshold anonymity,"[59] let alone perfect anonymity.

Cyberspace eliminates these risks and gives Mrs. McIntyre the ability to contact hundreds or even thousands of people with perfect anonymity:

> [A] criminal using tools and other information easily available over the Internet can operate in almost perfect anonymity. By weaving his or her communications through a series of anonymous remailers; by creating a few forged e-mail headers with powerful, point-and-click tools readily downloadable from many hacker web sites; or by using a "free-trial" account or two, a hacker, online pornographer,

---

59. "Threshold anonymity" is the level of anonymity that "occurs when a person's actions cannot be observed, attributed or discovered." Helms, *supra* note 10, at 301. Unlike perfect anonymity, threshold anonymity cannot be equated to a complete absence of information about the source of a communication:

> Imagine a person receiving an "anonymous" letter in the mail. Even if the letter is unsigned, the content and form tell the recipient something about the author. . . . [I]f the letter is typed the originator had access to a typewriter or printer. If the letter uses English words, the originator speaks English. . . If the letter has a U.S. postmark, it likely originated from this country. If the letter has the recipient's correct address and the contents have some relationship to his life, the originator obviously knows the recipient in some way. These aspects . . . give the recipient information about the originator. Thus, . . . the letter is not perfectly anonymous.

Id. See also George F. duPont, *The Criminalization of True Anonymity in Cyberspace*, 7 MICH. TELECOMM. & TECH. L. REV. 191, 196-97 (2000-2001). Professor Michael Froomkin suggested that Mrs. McIntyre could achieve perfect, "untraceable anonymity" if she "drop[ped] an unsigned leaflet with no fingerprints on Bob's doorstep in the dead of night." Michael Froomkin, *Flood Control on the Information Ocean: Living with Anonymity, Digital Cash and Distributed Databases*, 15 J.L. & COM. 395, 418 (1996). If Mrs. McIntyre did this, she would no doubt achieve threshold anonymity, but she would not achieve perfect anonymity as long as there was any chance she could be linked to the leaflet. Bob might, for example, know Mrs. McIntyre was the advocate of the position set out in the leaflet, or he might know someone who worked at the Kinko's where she had the leaflets printed.

> or web based fraud artist can often effectively hide the trail of his or her communications.[60]

Cyberspace lets Mrs. McIntyre achieve a level of anonymity she cannot hope to achieve in the real world.[61] This creates questions as to whether the legal guarantee of anonymity, crafted in the context of real world conduct, and the limitations on that conduct, should encompass cyberworld conduct that is not subject to those limitations. Because technology alters the contours of the empirical environment in which the right to remain anonymous is exercised, it creates a tension between this aspect of the right to be let alone and the needs of effective law enforcement.[62]

How should this tension be resolved? One approach is to conclude that cyberspace is in fact a different place, and thus is not necessarily encompassed by the anonymity guarantees crafted for the real world. Logically, this solution offers to benchmark anonymity at the same level in the real world and the cyberworld. There are two problems with this solution. The first goes to the factual predicate upon which it is premised, e.g., the assumption that the real world and the cyberworld are empirically distinct places. This assumption is, as explained in Section III below, factually incorrect: Cyberspace is not a place. It is the accreted product of

---

60. *Holder Testimony, supra* note 44. *See also* Post, *supra* note 43, at 149:

> [E]veryone in cyberspace is connected to everyone else through the magic of interconnectivity protocols and can communicate instantaneously on a one-to-one, one-to-many, many-to-one, or many-to-many basis with a constantly shifting . . . population. . . . In the space of an afternoon, I can join a dozen (or a hundred) ongoing associations by subscribing to individual listservers or Usenet discussion groups, form a dozen new such associations myself with a few lines of code inserted in my Internet Service Provider's system, and set up a dozen aliases on my provider's mail system through which I can communicate. . . .

See also Helms, *supra* note 10, at 316-18 (describing privacy-enhancing technologies that can be used to ensure anonymity in cyberspace). Cyberspace also eliminates the practical and legal constraints that militate against anonymity in real world publishing. *See, e.g.*, April Mara Major, *Norm Origin and Development in Cyberspace: Models of Cybernorm Evolution*, 78 WASH. U. L.Q. 59, 99 (2000).

61. *See, e.g.*, Lawrence Lessig, *Reading the Constitution in Cyberspace*, 45 EMORY L.J. 869, 876-77 (1996): "[A]nonymity in cyberspace is not just different in degree from anonymity in real space. . . . [C]yberspace . . . gives an individual a kind of power that doesn't exist in real space. This is not just the ability to put on a mask; it is the ability to hide absolutely who one is."

62. "Perfect anonymity makes perfect crime possible." Lawrence Lessig, *The Path of Cyberlaw*, 104 YALE L.J. 1743, 1750 (1995).

complex varieties of mediated communication; that being the case, there is no empirical basis for creating a lesser set of First Amendment protections for activities that take place via these types of mediated communication.[63] The second problem is pragmatic; it would be extraordinarily difficult and time-consuming for courts to determine precisely what types of anonymity are comparable to those found in the real world and what types are not. For example, it seems that using an anonymous remailing system in cyberspace is comparable to using a postal remailing system in the real world.

There are two other possible approaches to dealing with the superseding level of anonymity one can achieve via cyberspace. One is to simply accept the incremental level of anonymity as an aspect of the types of mediated communication cyberspace makes possible. After all, for over a century, the telephone has created opportunities for anonymity that exceed those available in the real world. While caller identification may curtail some of those opportunities, many still exist, and yet there has never been any effort to outlaw this aspect of telephonic communication.[64]

The final alternative is to treat the problem for what it really is the use of anonymity for criminal purposes. While cyberspace concededly allows one to assume a level of anonymity exceeding that found in the real world, there are real world analogues for the uses of on-line anonymity that cause

---

63. *See, e.g.*, Doe v. 2TheMart.Com Inc., 140 F. Supp. 2d 1088, 1092 (W.D. Wash. 2001) ("The right to speak anonymously extends to speech via the Internet"). The U.S. Supreme Court rejected the notion of two First Amendment standards in *Reno v. American Civil Liberties Union*, 521 U.S. 844, 870 (1997) ("[O]ur cases provide no basis for qualifying the level of First Amendment scrutiny that should be applied to this medium").

64. States have outlawed the use of telephone anonymity for improper purposes, such as harassment or obscene phone calls. *See, e.g.*, ALASKA STAT. § 11.61.120(a)(4) (Michie 2001) (misdemeanor to make anonymous phone calls with the intent to harass or annoy another person); ARIZ. REV. STAT. ANN. § 13-2916(A) (West 2001) (unlawful to "disturb by repeated anonymous telephone calls the peace, quiet or right of privacy of any person"). *See also* DEL. CODE ANN. tit. 11, § 1311 (2001); IDAHO CODE § 18-6710 (Michie 2002); MD. ANN. CODE, CRIMES AND PUNISHMENTS § 555A; N.M. STAT. § 30-20-12(A); VT. STAT. ANN. tit. 13, § 1027 (2001). The telephone, of course, offers opportunities for both anonymous and pseudonymous communication.

For centuries, snail mail also created opportunities for anonymity that exceed those available in the real world. But while some states outlawed the use of anonymous letters for improper purposes, there has never been an effort to outlaw "postal anonymity." *See, e.g.*, NEV. REV. STAT. ANN. § 207.180(2) (Michie 2001) (misdemeanor to "write and send" "any anonymous letter . . . charging any person with crime; or . . . containing vulgar or threatening language, obscene pictures, or containing reflections upon his standing in society or in the community"); OKLA. STAT. ANN. tit. 21, § 1304 (West 2002) (misdemeanor to send anonymous letters designed to threaten or intimidate another). *See also* ARIZ. REV. STAT. ANN. § 13-3004 (West 2001); FLA. STAT. ANN. § 836.10 (West 2001).

concern for law enforcement. What causes this concern is the use of online techniques by criminals that either allow disguise of their identities (anonymity) or permit the assumption of false identities (pseudonymity). In the real world, the law has addressed the use of pseudonyms and the use of masks to conceal one's identity for criminal purposes. With regard to pseudonyms, states outlaw using false identities for certain purposes, such as: obtaining a credit card,[65] obtaining a firearms license,[66] practicing medicine,[67] or obstructing justice.[68] Some, including California, make it a crime to offer, display, or possess documents intended to conceal the true identity of oneself.[69] As for masks, some states make it a crime to wear disguises to conceal the identity of oneself for unlawful purposes;[70] others make the wearing of a mask or disguise an aggravating factor in the commission of an offense.[71]

Masks are a good real world analogue for anonymity achieved via cyberspace: Masks let someone conceal his or her identifying physical information in the real world just as remailers and other techniques let individuals conceal their identifying information in the cyberworld. The First Amendment protects the wearing of masks whenever the masks themselves have expressive content[72] or whenever "there is such a nexus between anonymity and speech that a bar on the first is tantamount to a

---

65. *See, e.g.*, ALA. CODE § 13A-8-194(a) (2002); R.I. GEN. LAWS § 11-49-2 (2001).

66. *See, e.g.*, IND. CODE ANN. § 35-47-2-17 (Michie 2002). *See also* GA. CODE ANN. § 16-13-76 (2002) (use of false name to obtain dangerous drugs).

67. *See, e.g.*, MICH. COMP. LAWS ANN. § 750.298 (West 2002).

68. *See, e.g.*, ARIZ. REV. STAT. ANN. § 13-2107(A) (West 2001); FLA. STAT. ANN. § 817.59 (West 2001).

69. *See* CAL. PENAL CODE § 529a (Deering 2001).

70. *See, e.g.*, CAL. PENAL CODE § 185 (Deering 2001) (unlawful to wear "any mask, false whiskers or any personal disguise" for the purpose of evading discovery, recognition or identification in the commission of any public offense); DEL. CODE ANN. tit. 11, § 1239 (West 2002) (wearing "a hood, mask or other disguise during the commission of any felony . . . is a class E felony"); D.C. CODE ANN. § 22-3312.03 (2002) (unlawful to wear "any mask, hood, or device whereby any portion of the face is hidden, concealed, or covered" while "engaged in conduct prohibited by civil or criminal law, with the intent of avoiding identification"). *See also* 18 U.S.C.S. § 241 (West 2002) (offense for "two or more persons [to] go in disguise on the highway, or on the premises of another, with intent to prevent or hinder his free exercise or enjoyment of any right or privilege" secured by the U.S. Constitution or laws of the United States).

71. *See, e.g.*, FLA. STAT. ANN. ch. 775.0845 (Harrison 2001) ("The felony or misdemeanor degree of any criminal offense . . . shall be reclassified to the next higher degree as provided in this section if, while committing the offense, the offender was wearing a hood, mask, or other device that concealed his or her identity"). *See also* N.M. STAT. ANN. § 30-3-2(B) (Michie 2002).

72. *See, e.g.*, Dayton v. Esrati, 707 N.E.2d 1140, 1144-45 (Ohio Ct. App. 1997).

prohibition on the second."[73] Courts have rejected First Amendment challenges to statutes that prohibit the wearing of masks for the purpose of committing crimes.[74] One approach to on-line anonymity would therefore

---

73. Aryan v. Mackey, 462 F. Supp. 90, 92 (N.D. Tex. 1978) (quoted in American Knights of Ku Klux Klan v. City of Goshen, Ind., 50 F. Supp. 2d 835 (N.D. Ind. 1999)). *See, e.g.*, Stephen J. Simoni, Note, *"Who Goes There?" — Proposing a Model Anti-Mask Act*, 61 FORDHAM L. REV. 241, 245-46 (1992):

> Challenges to anti-mask laws . . . . have alleged both the *direct violation* and *inhibition* of First Amendment rights. First, they have alleged that masks constitute a form of expressive conduct, stating that the visual effects of their masks assist in conveying their messages. Consequently, anti-mask laws directly violate First Amendment rights and must therefore satisfy the test provided in *United States v. O'Brien*. Second, individuals have alleged that masks are necessary for them to publicly speak and assemble, because the resulting anonymity reduces the risk of physical, economic, and social reprisals they would suffer if identified as holding the beliefs that they do. Because anti-mask laws thus inhibit exercise of First Amendment rights, they are also subject to the test in *NAACP v. Alabama ex rel. Patterson*.

(footnotes omitted). Anti-mask laws that directly violate First Amendment rights must be unrelated to the suppression of free expression; this is established if the law in question is concerned with the prohibited conduct itself, not with its communicative content. *See* United States v. O'Brien, 391 U.S. 367, 377, 381-82 (1968). A law that inhibits the exercise of First Amendment rights can be upheld only if it furthers a compelling state interest and that interest cannot be protected by methods that are more narrowly defined. *See* Shelton v. Tucker, 364 U.S. 479, 488 (1960); NAACP v. Alabama *ex rel.* Patterson, 357 U.S. 449, 463 (1958). *See also* McIntyre v. Ohio Elections Comm'n, 514 U.S. 334, 348 (1995).

74. *See, e.g.*, Church of Am. Knights of Ku Klux Klan v. City of Erie, 99 F. Supp. 2d 583, 590 (W.D. Pa. 2000). In *American Civil Liberties Union of Georgia v. Miller*, 977 F. Supp. 1228 (N.D. Ga. 1997), the District Court permanently enjoined the enforcement of a Georgia statute that made it a crime to "knowingly transmit any data through a computer network . . . for the purpose of . . . exchanging data with an electronic mailbox . . . or any other electronic information storage bank or point of access to electronic information if such data uses any individual name . . . to falsely identify the person." *Id.* at 1230 (quoting GA. CODE § 16-9-93.1). It found that the statute was a "presumptively invalid content-based restriction" because "the identity of the speaker is no different from other components of [a] document's contents that the author is free to include or exclude." *Id.* at 1232 (quoting McIntyre v. Ohio Elections Comm'n, 514 U.S. 334, 340-42 (1995)). The District Court also found that the statute was not narrowly tailored to further a compelling state interest; the state of Georgia claimed the statute intended to prevent fraud, but the District Court pointed out that

> the statute is not narrowly tailored to achieve that end and instead sweeps innocent, protected speech within its scope. Specifically, by its plain language the criminal prohibition applies regardless of whether a speaker has any intent to deceive or whether deception actually occurs. Therefore, it could apply to a wide

be to analogize it to the wearing of masks for the purpose of engaging in illegal acts in the real world, and thus criminalize on-line anonymity when it is used, or is intended to be used, for the purpose of engaging in illegal acts.[75] This could be done either directly, by adopting statutes that outlaw the use of on-line anonymity for unlawful purposes, or indirectly, by making the use of on-line anonymity during the commission of a crime an

---

range of transmissions which "falsely identify"the sender, but are not "fraudulent" within the specific meaning of the criminal code.

Id. at 1232. This differentiates the Georgia statute from anti-mask statutes that have been upheld against First Amendment challenges since the latter have explicitly tied the wearing of disguises to the achievement of some unlawful purpose. *See, e.g.*, Simoni, *supra* note 73, at 256 ("Anti-mask that prohibit mask-wearing only when the wearer possesses specified criminal intent permit virtually all First Amendment exercise by mask-wearers, requiring only that they possess no criminal intent. By not burdening speech substantially more than is necessary, these laws satisfy the narrowly tailored requirement") (footnote omitted). The U.S. Supreme Court's decision in *McIntyre v. Ohio Elections Commission* is also distinguishable since (a) it involved political speech which "occupies the core of the protection afforded by the First Amendment" and (b) Ohio's articulated interest was not narrowly tailored to meet the compelling state interest it asserted. *See McIntyre*, 514 U.S. at 346, 351-52.

75. To be workable, this approach requires that there be some way to identify those who have used anonymity for illegal purposes, and this is complicated by the fact that cyberspace creates the potential for perfect anonymity. *See supra* note 59 and accompanying text. If someone achieves perfect anonymity, then it is more likely than not that he will never be apprehended; and if he cannot be apprehended, he cannot be prosecuted for assuming anonymity for illegal purposes and for the crimes he committed while anonymous.

One solution to this problem is to assign Internet Protocol (IP) addresses; the IP addresses would be analogous to assigning Social Security or other identifying numbers, therefore not involving First Amendment speech guarantees. Some might argue that assigned IP addresses eliminate the possibility of remaining anonymous in cyberspace. How can you speak anonymously if your IP address gives you away?

It should, however, be possible to assign IP addresses and still allow for a level of on-line anonymity that is analogous to the anonymity available in the real world. Assume, for example, that someone in the real world wants to articulate their views on how the United States is treating Al Qaeda detainees in Guantanamo Bay, Cuba. In the real world, the caller phones the local talk radio station and without giving a name, and perhaps even using a disguised voice, gives an opinion anonymously. Comparable opportunities could be created on-line: services analogous to radio stations could be created to permit the expression of opinions (talk-cyberspace). The services would assign a unique identifier to visitors for each visit. The identifier would be valid within the service and the visitor's IP address would not be available to the other users; the service would know each visitor's IP address, just as radio stations can use caller identification technology to ascertain the names and phone numbers of those who call into the stations. The effect would be to achieve a level of anonymity on par with that currently available to those who patronize talk-radio.

aggravating factor in sentencing offenders.[76] Either tactic has the virtue of differentiating between licit on-line anonymity and illicit on-line anonymity and allowing the government to seek the imposition of sanctions against those who exploit on-line anonymity.[77] Criminalizing the use of on-line anonymity for unlawful purposes has the added virtue of permitting prosecution of those who purposely make anonymity available to individuals who use it for criminal purposes.[78] The anonymity-providers would be prosecuted as accomplices to the crimes their clients commit.[79]

---

76. *See, e.g.*, United States v. Fellows, 157 F.3d 1197, 1202 (9th Cir. 1998) (U.S.S.G. § 2G2.4(b)(3), which provides a two-level enhancement if a defendant used a computer to acquire child pornography. The statute "provides an extra deterrent to those inclined to pursue illicit pictures in the anonymity of the computer world"). *Fellows*, 157 F.3d at 1202.

77. This approach preserves "the right to read anonymously." The U.S. Supreme Court has held that the First Amendment guarantees a right to read anonymously because of "the likely chilling effect that exposure of a reader's tastes would have on expressive conduct, broadly understood — not only speech itself, but also the information-gathering activities that precede speech." Julie E. Cohen, *A Right to Read Anonymously: A Closer Look at "Copyright Management" in Cyberspace*, 28 CONN. L. REV. 981, 1010 (1996). Curtailing on-line anonymity, even if it is only to limit it to the anonymity that is available off-line, would infringe this right by denying individuals access to material that is only available on-line. This approach would allow individuals anonymous access to legitimate material that is available on-line, while imposing criminal liability on those who sought out illegitimate material such as child pornography. *See, e.g.*, Osborne v. Ohio, 495 U.S. 103, 108-10 (1990) (state could outlaw possession and viewing of child pornography).

78. *See, e.g.*, 1999 Revision of the Model State Computer Crimes Code § 8.06, Commentary ("if it can be shown that the provider [of anonymous remailing services] had actual or constructive knowledge of criminal activity being perpetrated through their system, then they could be held criminally responsible as aiders and abettors"). *See generally* COLO. REV. STAT. ANN. § 18-8-105(a) (West 2001) ("A person is an accessory to crime if, with intent to hinder . . . or prevent the . . . prosecution . . . of another for the commission of a crime, he renders assistance to such person," including providing the person with a disguise). *See also* State v. Thompson, 754 So. 2d 412, 417 (La. App. 2 Cir. 3/1/02) (defendant aided and abetted commission of crime by, *inter alia*, purchasing disguises used in committing it); Leigh v. State, 223 Ga. App. 726, 729 (Ga. Ct. App. 1996). In *People v. Lauria*, 251 Cal. App. 2d 471, 479 (Cal. App. 2d 1967), the *Lauria* Court concluded that "there is nothing in the furnishing of telephone answering service which would necessarily imply assistance in . . . illegal activities," e.g., prostitution, but an intent to participate in the illegal activity can be inferred from "knowledge, when the volume of business with the buyer is grossly disproportionate to any legitimate demand, or when sales for illegal use amount to a high proportion of the seller's total business." *Id.*

As to pseudonyms, the law has made it an offense for a hotelkeeper knowingly to let someone register under a false name. *See, e.g.*, Commonwealth v. Altenhaus, 57 N.E.2d 921, 922 (Mass. 1941) (reversing conviction under statute that made it a crime for an innkeeper to let someone register using a false name). *See also* ARK. CODE ANN. § 20-26-302(b) (Michie 2001).

79. *Id.*

This approach also alleviates the pragmatic objection to the first approach discussed earlier, e.g., the difficulty of ascertaining which types of anonymity are analogues to real world anonymity and which are not, so that the latter can be prohibited. The target of this endeavor should not be anonymity per se. Cyberspace should be encouraged to create new and more elusive types of anonymity that can enhance free speech and freedom of association. What cannot be tolerated is the use of anonymity for illegal ends. Treating on-line anonymity as analogous to the wearing of masks in the commission of criminal acts provides a clear standard for differentiating improper uses of anonymity from proper uses. To achieve a conviction under this approach, the prosecution would have to prove that the defendant purposely assumed anonymity, or sought anonymity, for the purpose of committing a crime.

III. FOURTH AMENDMENT

Anonymity is not the only area in which tension arises between individual rights and the needs of law enforcement. Cyberspace also raises difficult questions about how law enforcement should be allowed to gather evidence in cyberspace without violating the Fourth Amendment's constitutional guarantee of privacy.

The Fourth Amendment historically protected the privacy of certain physical spaces or areas from unauthorized law enforcement intrusion.[80] When the Fourth Amendment was adopted, the protection against invasions of privacy lay in trespass law: "If someone entered your property and rifled through your stuff, . . . [y]ou could sue that person for trespass, whether he was a police officer or private citizen. The threat of such suits gave the police an incentive not to invade your privacy."[81] The Fourth Amendment incorporated this common law notion of privacy and used the concept of a search warrant to balance the citizen's interest in spatial privacy against the state's need to gather evidence.[82] A warrant justified an intrusion into an area that was constitutionally-deemed private, such as a

---

80. *See supra* text accompanying note 35.

81. LESSIG, *supra* note 14, at 112 (footnote omitted). *See also* LESSIG, *supra* note 19.

82. *See* LESSIG, *supra* note 14, at 113 ("If the officer secured a warrant . . . before he made his search, the warrant immunized him against trespass liability"). *See, e.g.*, Humes v. Taber, 1850 R.I. LEXIS 26 (R.I. Sept. 1850) (warrant no defense to an action in trespass against a sheriff who searched the wrong house); Jones v. Gibson, 1818 N.H. LEXIS 32 (N.H. Oct. 1818) (action in trespass against an "inspector of revenue" for seizing goods without a warrant); Patcher v. Sprague, 2 Johns 462, (N.Y. Sup. Ct. 1807) (valid warrant is a defense to an action for trespass).

home. Areas that were not deemed private were outside the reach of the Fourth Amendment and law enforcement was not obliged to obtain a warrant to enter them.[83]

As explained earlier, this common law-derived concept of privacy first became problematic with the proliferation of telephone technology. In *Olmstead*, the U.S. Supreme Court held that federal agents did not violate the Fourth Amendment by using wiretaps to overhear conversations conducted from inside a home, the ultimate Fourth Amendment sanctuary, because they did not physically enter the home.[84] In *Katz*, the Court reversed its position in *Olmstead* and held that wiretapping that permitted officers to intercept conversations held in a phone booth was a search.[85] *Katz* was understood to articulate a different approach to Fourth Amendment privacy, one in which the "core value . . . was the protection of 'people, not places.'"[86]

> In the framers' context of 1791, protecting against trespass to property was an effective way to protect against trespass to privacy, but in the *Katz* context of the 1960s it was not. In the 1960s much of intimate life was conducted in places where property rules did not reach (in the "ether," for example, of the AT&T telephone network). And so a regime that made privacy hang on property did not protect privacy to the same degree that the framers had intended. Justice Stewart in *Katz* sought to remedy that by linking the [Fourth Amendment to a more direct protection of privacy.
>
> The link was the idea of a "reasonable expectation of privacy." . . . Where people have a reasonable expectation of privacy, the government cannot invade that space without satisfying the requirements of the Fourth Amendment.[87]

---

83. *See, e.g.*, United States v. Dunn, 480 U.S. 294, 301-05 (1987). In *Dunn*, the U.S. Supreme Court held that "open fields" are not encompassed by the privacy guarantee the Fourth Amendment accords "persons, houses, papers and effects." *See id.* at 300-01. The Court found, as it had found in earlier cases, that "open fields" are not protected as "private" because they do not harbor the "intimate activity" that is associated with the sanctity of the home and the privacy of one's personal life. *See id.*

84. *See* Olmstead v. United States, 277 U.S. 438 (1928). *See also supra* text accompanying note 35.

85. *See* Katz v. United States, 389 U.S. 347 (1967). *See also supra* text accompanying note 40.

86. LESSIG, *supra* note 14, at 117 (footnote omitted) (quoting Katz v. United States, 389 U.S. 347, 351 (1967)).

87. *Id.* at 117-18 (quoting Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring)). Justice Harlan actually articulated the "reasonable expectation of privacy" standard,

But as this quote illustrates, it seems quite impossible to operationally prohibit unreasonable searches without employing the concept of a place, a space, or an area that is being searched.[88] For that reason, the old privacy of place concept persisted even after *Katz*;[89] indeed, it provides the basis for the recent decision of the U.S. Supreme Court in *Kyllo v. United States*.[90] *Kyllo*, which considered the use of thermal imaging technology by police to detect heat escaping from a home,[91] was expected to be the new *Katz*, the decision in which the U.S. Supreme Court would explain how Fourth Amendment guarantees apply to Twenty-First Century technology. Many believe such a decision is necessary because of the impact technology has on the *Katz* formulation of privacy. According to *Katz*, to be within the protections of the Fourth Amendment, an area must be encompassed by a reasonable expectation of privacy. As technology gives rise to increasingly intrusive forms of surveillance, the reasonableness of subjective expectations of privacy diminish, thereby reducing the scope of Fourth Amendment protections.[92]

> first that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as "reasonable." Thus a man's home is . . . a place where he expects privacy, but objects, activities, or statements that he exposes to the "plain view" of outsiders are not "protected" because no intention to keep them to himself has been exhibited. . . . [C]onversations in the open would not be protected against being overheard, for the expectation of privacy under the circumstances would be unreasonable.

Katz v. United States, 389 U.S. 347, 362 (1967) (Harlan, J., concurring). The majority's formulation of the test was slightly different, e.g., "[w]hat a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection. . . . But what he seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected." *Id.* at 351 (citations omitted).

88. *See id.* at 361 (Harlan, J., concurring) (deciding what protection the Fourth Amendment provides "[g]enerally . . . requires reference to a 'place'"). *See also* Kyllo v. United States, 121 S. Ct. 2038, 2043 n.1 (2001) ("When the Fourth Amendment was adopted, as now, to 'search' meant to look over or through for the purpose of finding something . . . as, to *search* the house for a book").

89. *See, e.g., Leading Cases*, 115 HARV. L. REV. 346, 352 (2001).

90. *Kyllo*, 121 S. Ct. at 2046.

91. *Id.* at 2040-41.

92. *See, e.g.*, JEFFREY ROSEN, THE UNWANTED GAZE: THE DESTRUCTION OF PRIVACY IN AMERICA 61 (2000).

Two strategies identified by Professor Lawrence Lessig that the U.S. Supreme Court uses to interpret constitutional standards are predicated on presuppositions that have changed:[93]

> One strategy is focused on what the framers or founders would have done — the strategy of *one-step originalism.* The second strategy aims at finding a current reading of the original Constitution that preserves its original meaning in the present context — a strategy that I call *translation.*[94]

In *Olmstead,* Justice Brandeis unsuccessfully argued for translating Fourth Amendment protections "into a context in which the technology for invading privacy had changed."[95] The *Katz* Court sought to accomplish this translation, but many believe the test the *Katz* Court articulated has not dealt well with the deployment of technology in the real world; and while the *Kyllo* majority noted the problems with the *Katz* standard, the decision seems to be a regression, a return to the privacy of place approach that prevailed prior to *Katz.*[96] Indeed, the *Kyllo* Court closed by quoting *Carroll v. United States,*[97] a pre-*Olmstead* decision, for the proposition that the "Fourth Amendment is to be construed in the light of what was deemed an unreasonable search and seizure when it was adopted."[98]

---

93. *See* LESSIG, *supra* note 14, at 114.

94. *Id.*

95. *Id.* at 115; Olmstead v. United States, 277 U.S. 438 (1928).

96. *See Kyllo,* 121 S. Ct. at 2043.

> The *Katz* test . . . has often been criticized as . . . subjective and unpredictable. While it may be difficult to refine *Katz* when the search of areas such as telephone booths, automobiles, or . . . uncovered portions of residences are at issue, in . . . the search of the interior of homes . . . there is a ready criterion, with roots deep in the common law, of the minimal expectation of privacy that *exists,* and that is acknowledged to be *reasonable.* . . . [O]btaining by sense-enhancing technology any information regarding the interior of the home that could not otherwise have been obtained without physical "intrusion into a constitutionally protected area," *Silverman,* 365 U.S. at 512, 81 S. Ct. 679 constitutes a search . . . This assures preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted. . . .

Silverman v. United States, 365 U.S. 505 (1961) (a pre-*Katz* decision that applied *Olmstead*'s interpretation of the Fourth Amendment).

97. 267 U.S. 132 (1925).

98. *Kyllo,* 121 S. Ct. at 2046 (quoting Carroll v. United States, 267 U.S. 132, 149 (1925)).

So, where do things stand in terms of applying Fourth Amendment protections to cyberspace? Given the persistence of the privacy of place notion, the threshold issue must be whether or not cyberspace is a place in which the protections of the Fourth Amendment can be, though need not be, applied. There are two ways to approach this issue. The first is to consider whether cyberspace is analogous to real world places.

One can certainly argue that cyberspace is analogous in many respects to the real world.[99] Like the real world, cyberspace contains stores, government agencies, libraries, courts, universities, businesses, charities, churches, forums, and art galleries.[100] Cyberspace even has its own mail system. However, electrical signals construct these cyber-analogues of terrestrial institutions. They are not made from brick, stone, or wood. As a result, they tend to be more transparent, more permeable than their real world counterparts.

E-mail is a good example of the evanescence of cyber-constructs. E-mail is far more vulnerable to interception than traditional snail mail. Unlike snail mail, e-mail is not sealed (unless it is encrypted, a topic which is addressed later), does not travel as a single, discrete whole, and travels in a public domain where many types of information can be read by anyone with a certain level of technical expertise.[101] For this reason, it is

---

99. *See, e.g.*, An Atlas of Cyberspaces: Mapping Cyberspace Using Geographic Metaphors, *available at* http://www.cybergeography.org/atlas/geographic.html (last visited Aug. 30, 2002).

100. *See, e.g.*, Edward Ayers, *Cyberspace, U.S.A. in* AMERICAN PLACES: ENCOUNTERS WITH HISTORY (2001), *available at* http://www.oup-usa.org/sc/019513026X/019513026X_02.pdf (last visited Aug. 13, 2002):

> I write of a new American place, . . . "cyberspace." That place, simultaneously metaphorical and tangible, has touched every part of the United States. Information surges along networks . . . weaving ever tighter webs across the country and the world. Those networks define a space at once empty and densely populated, desolate and hopeful. . . .
> At one level, cyberspace is merely bits of electronic information, zeroes and ones, stored on computers and networks. At another level, it is more concrete, addresses and linkages whose names people know and can read. And at the sites where people interact with one another, cyberspace becomes physical, filled with color, sound, and image. Even though those places are merely projected on screens, people have fallen in love there, have cooperated, conspired, traded, and raged.

101. *See, e.g.*, Am. Civil Liberties Union v. Reno, 929 F. Supp. 824, (E.D. Pa. 1996), *aff'd*, 521 U.S. 844 (1997) ("Unlike postal mail, simple e-mail generally is not 'sealed' or secure, and can be accessed or viewed on intermediate computers between the sender and recipient"). When an e-mail message leaves the sender's computer, it is disassembled into packets of data, each of which carries the addresses of the sender and the intended recipient. The packets are sent

often compared to a post card, the contents of which can be read by anyone who comes into contact with it as it travels from sender to recipient.[102]

> from server to server across the Internet. As each packet reaches a new server, it is temporarily stored in that computer and then forwarded to another server until the packet reaches its destination. . . . A router analyzes each packet of information, determines the best available path, and passes the packet along to another router that sends it toward its final destination. . . .
> [T]he message eventually reaches the destination server and is stored on that computer. This destination server acts as a host for the receiver. . . . Here the packets are reassembled and the original document is recreated.

Christopher C. Miller, Note, *For Your Eyes Only? The Real Consequences of Unencrypted E-Mail in Attorney-Client Communication*, 80 B.U. L. REV. 613, 618-19 (2000) (footnotes omitted). Unencrypted packets can be intercepted in either of two ways.

> First, the system administrator of a router can access and read any message sent over its computer. Second, a cracker can use "sniffer" or "spoofer" software to intercept packets. . . . A sniffer program intercepts all data traveling through the server's network on the way to the destination computer.
> [A] spoofer program "emulates the intended recipient's computer and receives any mail intended for another machine." If a spoofer intercepts an entire message, it can then "retain the message, forward it to the intended recipient, forward it to others, or change the message."

Id. at 627 (footnotes omitted) (quoting Lucy Schlauch Leonard, Comment, *The High-Tech Legal Practice: Attorney-Client Communications and the Internet*, 69 U. COLO. L. REV. 851, 858-59 (1998)).

102. *See, e.g.*, "Privacy in the News," e-mail from Anonymizer (Jan. 9, 2002) (on file with author):

> Dear Anonymizer Customer,
> Did you know that sending unprotected email is like sending a postcard — ALMOST ANYONE between you and the recipient can read it!
>
> For that reason, we recommend using a strong and versatile program like ENSUREDMAIL to protect your sensitive electronic communications. Ensuredmail is easy to use and works with most email software and services, including Outlook, Outlook Express, Lotus, AOL, Hotmail, Yahoo Mail, and many others.

See also "The Carnivore Controversy: Electronic Surveillance and Privacy in the Digital Age," Senate Committee on the Judiciary (Statement of Dr. Vinton G. Cerg, Sept. 6, 2000), *available at* http://www.senate.gov/~judiciary/oldsite/962000_vgc.htm (last visited Oct. 28, 2002).

E-mail is also unlike snail mail in that private entities transport it themselves and not the government. This, however, should not be dispositive for Fourth Amendment purposes. Telephone communication is also in the hands of private entities, and *Katz* held that it enjoys a Fourth

Other types of communication found in cyberspace[103] include listservs and newsgroups,[104] which provide asynchronous one-to-many communication,[105] instant messaging, which allows synchronous one-to-one, one-to-many, many-to-many and/or many-to-one communication,[106] and "bulletin boards, online forums or conferences."[107] Newsgroups, bulletin boards and on-line forums are public discussion areas open to anyone who wants to participate; participants read messages posted on-line by others and can, if they wish, post responses. Listservs, which are essentially e-mail distribution lists, can be public or private; private listservs are closed to all but those who meet certain qualifications.[108] Like a private listserv, instant messaging lets members of a defined group

---

Amendment expectation of privacy. The same is true of sealed letters or packages entrusted to "private freight carriers" such as Federal Express. *See, e.g.*, United States v. Jacobsen, 466 U.S. 109, 114 (1984).

103. Internet telephony is another means of communication, but since it is essentially a variant on real world telephonic communication, it is not considered here. *See, e.g.*, Jeanne Lee, Internet Telephony, *available at* http://www.cc.ubc.ca/ccandc/nov-dec96/iphone.html (last visited Sept. 9, 2002) ("this technology allows point-to-point audio communication between two users in real time. In other words, you can use your computer like a telephone").

104. *See, e.g.*, E-Mail List General Information, *available at* http://www.uwex.edu/ces/wisplan/helpdesk/email/list/listgen.html (last visited Sept. 9, 2002):

> Lists make it easy for a group of people to have discussions via e-mail. Instead of each of you having to send the mail message to each of the people who want to have the discussion, you send the message to an e-mail address that identifies the list. The message is then redistributed (called "exploded") to everyone who subscribes to the list.

105. *See, e.g. Am. Civil Liberties Union*, 929 F. Supp. at 834-35. Listservs are primarily used in either of two ways, e.g., "for one-to-many communication like newsletters or for many-to-many communications where each member of a list can respond to the entire group." Nancy White, The Tools of Online Connection (Aug. 2001), *available at* http://www.fullcirc.com/community/connecttools.htm (last visited Sept. 9, 2002).

106. *See, e.g.*, NPTalk: Instant Messaging, *available at* http://www.ombwatch.org/article/articleview/322/1/96/ (last visited Oct. 28, 2002). *See also* White, *supra* note 105 ("Instant messaging applications such as ICQ, MSN Instant Messenger and AOL's Instant Messenger allow members of a group of users to see who is online at any moment, send instant messages and set up spontaneous small chats").

107. White, *supra* note 105. *See also* Ron Mader, Mastering the Web: Online Forums — Bulletin Boards, Listservs, Usenet and Chats (2002), *available at* http://www.planeta.com/ecotravel/period/master/online.html (last visited Sept. 9, 2002).

108. *See, e.g.*, Using Email Lists and More: The Power of Virtual Communities on the Net, *available at* http://www.ngflscotland.gov.uk/connectingcommunities/starting/hlists.asp (last visited Dec. 9, 2002).

exchange messages. Instant messaging software can also be used for real time chat.[109] On-line chat rooms allow people to enter cyberspace areas where they can use text messages to interact with whomever else is there. Most chat rooms are public because anyone who enters the chat room can read the messages posted there, but many sites also offer private chat rooms.[110]

These methods of communication are generally hosted by web sites. Simply put, they can be found at a specific web site. Web sites are the more or less stable areas built in cyberspace for the purpose of providing information and/or conducting various activities. Some web sites are extensions of real world endeavors, others are unique to cyberspace. Web sites host chat rooms and virtual worlds such as MOOs and MUDs.[111] They are the locus of on-line businesses, art galleries, professional firms, educational, charitable and religious institutions, libraries that offer text, video and music resources, hobby sites that provide information about a topic of interest to the creator of the site, and providers of news and entertainment, etc.[112] As with stores and other real world institutions, web sites are private in that specific persons or entities own them, and they are

---

109. *See, e.g.*, NPTalk, *supra* note 106.

110. *See, e.g.*, Other Chat Areas on the Internet, *available at* http://www.chatmag.com/help/others.html (last visited Sept. 9, 2002); Local Free Adult Chat Rooms, *available at* http://www.localfreeadultchatrooms.com/ (last visited Sept. 9, 2002). *See also* Vanessa Hwang, *Cable Modems and Privacy in the New Millennium*, 32 COLUM. HUM. RTS. L. REV. 727, 767-68 (2001) ("For chat rooms, the user first enters a 'lobby,' where s/he can then see other users participating in the 'conversation.' The user then has a choice: joining the current conversation, navigating to a 'public room,' or entering a 'private room'") (footnotes omitted).

111. *See, e.g.*, Ultima Online, *available at* http://www.uo.com/ (last visited Sept. 9, 2002). *See also* An Atlas of Cyberspaces: Multi-User Dimensions (MUDS) & Virtual Worlds, *available at* http://www.cybergeography.org/atlas/muds_vw.html (last visited Sept. 9, 2002).

112. *See, e.g.*, Ayers, *supra* note 100:

> Businesses quickly sprang up . . .; tens of millions of people "joined communities" by posting Websites reflecting their personalities, interests, and images of themselves. Those virtual communities soon became among the most heavily visited places in cyberspace; twenty million people have created Web pages in one virtual neighborhood or another, and the number of new arrivals continues to expand. . . . At GeoCities, one of the largest virtual communities, visitors are promised they can "meet people just like you." Websites are divided into neighborhoods, blocks, and houses.

See also Jonathan Weber, *Web Pioneers Lay Foundation for Cyber-Communities*, CNN.com (Sept. 11, 1997), *available at* http://www.cnn.com/TECH/9709/11/net.community.lat/ (last visited Sept. 9, 2002).

public in that they invite some portion of the cyber-populace to visit the web site to review its content and, often, to interact with its proprietors and other site visitors. Web sites are also private in that they may have off-line content which is not available to those who visit the public areas of the web site. Some web sites are private in a different sense; they require visitors to have a password to access the web site's content and to interact with the proprietors and other authorized visitors.[113]

As part of interacting with visitors, web sites, especially commercial web sites, engage in "monitoring,"[114] an activity that while analogous to conduct found in the real world, is far more sophisticated. Monitoring is not new; when the Fourth Amendment was adopted, and for centuries before, "most people lived in communities that constantly monitored everyone's behavior. Your comings and goings, who you were with, how

---

113. *See, e.g.*, Konop v. Hawaiian Airlines, Inc., 236 F.3d 1035, 1041 (9th Cir. 2001), *withdrawn*, 262 F.3d 972 (employee created password-protected web site where he posted material critical of his employer). Such sites may, of course, be vulnerable to outsiders who possess the skills necessary to crack the password protection and access the content they seek to preserve as confidential. *See, e.g., id.* at 1041 (official of company for which employee worked gained access to his password-protected web site). Indeed, all web sites are vulnerable, in varying degrees, to the efforts of those who would crack their security efforts in order to deface, alter or copy the information they contain. This, however, is not a factor that militates against Fourth Amendment protection: In the real world, law enforcement officers cannot enter someone's home without a warrant even though it is unlocked and the front door is standing open; the home's status as "private" for Fourth Amendment purposes derives from the societal understanding that it is "reasonable" to expect that homes are immune from government intrusion absent a warrant, not from the measures taken to make it difficult or impossible for such an intrusion to occur. *See, e.g.*, People v. Camacho, 23 Cal. 4th 824, 835, (Cal. 2000) ("we cannot accept the proposition the defendant forfeited the expectation his [home] would remain private simply because he did not erect an impregnable barrier to access"). *See also* Anthony G. Amsterdam, *Perspectives on the Fourth Amendment*, 58 MINN. L. REV. 349, 402 (1974):

> [A]nyone can protect himself against surveillance by retiring to the cellar, cloaking all the windows with thick caulking, turning off the lights and remaining absolutely quiet. This much withdrawal is not required . . . to claim the benefit of the Amendment because, if it were, the Amendment's benefit would be too stingy to preserve the kind of open society to which we are committed and in which the Amendment is supposed to function.

The same is true for businesses and other areas encompassed by Fourth Amendment protections. *See, e.g., In re* Search of Lucky Spot, No. 90-404M, 1990 U.S. Dist LEXIS 14936, at *13-14 (W.D.N.C. Oct. 30, 1990) (business had reasonable expectation of privacy in areas from which general public was regularly excluded).

114. *See* LESSIG, *supra* note 14, at 150.

much you spent at the market — all this was known by your neighbors."[115] This type of monitoring still goes on in the real world, though the urbanization of modern society has made it less intense. In cyberspace, monitoring is more intense than ever. As one floats through the virtual spaces of the cyberworld and interacts with web sites, automated systems collect every bit of personal information entered by the user.[116] The way this type of monitoring takes place in the public areas of cyberspace is analogous to the observations of nosy neighbors in a small real world community. However, the observations of those neighbors are certain to be erratic, imperfect, and transient;[117] unlike the machine-made observations in cyberspace, they cannot "be searched, or collected, or produced as records."[118] In modern society the use of observational technology is not limited to the cyberworld. While machine-made observations in the cyberworld are concededly more detailed and intense, they can be analogized to the use of real world monitoring technologies, such as video cameras in public areas.[119]

---

115. *Id.*

116. *Id.* at 153.

> If you search on "mortgage" in a web search engine, advertising for mortgages appears on your computer screen. The same for sex and for cars. . . . Data about the search are collected. . . .
>
> Data collection is the dominant activity of commercial web sites. Some 92 percent of them collect personal data from web users, which they then aggregate, sort, and use.

Id.

117. *See id.* at 150-51.

118. *Id.*

119. *See, e.g., Neighborhood Spycam Helps Catch Murder Suspect*, CNN.com (Feb. 9, 1999), *available at* http://europe.cnn.com/US/9902/09/big.brother/ (last visited Aug. 30, 2002):

> Police surveillance cameras are aimed at public streets in at least a dozen U.S. cities. And, by some estimates, another 200,000 video lookouts are in place in and around private homes. . . .
>
> Video cameras record people in banks, convenience stores, casinos, offices, day care centers, schools, buses and prisons. They monitor freeway traffic; they're atop buildings as television news skycams.

See also Seth Stern, *Security Trumps Privacy*, CHRISTIAN SCI. MONITOR (Dec. 20, 2001), *available at* http://www.csmonitor.com/2001/1220/p11s1-stct.html (last visited Aug. 30, 2002) (noting increased use of biometric scanners and facial-recognition cameras in public areas).

Because of the way cyberspace is currently configured, it is not only possible, but almost irresistible, to think of it as a virtual place, a contrived mirror of the real world. It is true, of course, that much of what we experience in the real world — streets, buildings, stores, vehicles, printed materials, electronic devices, etc. — is also contrived, the product of human intelligence and effort. In the real world, these contrivances must necessarily operate within certain externally-dictated constraints. Pool tables, for example, must have legs as well as tops. In the virtual world of cyberspace, however, these constraints no longer hold true. Pool tables in cyberspace do not require legs in this place where gravity does not exist.[120] Logically, therefore, even if cyberspace is a conceptualized place, there is no reason why that place should resemble the real world. The only reason why cyberspace currently mirrors the components of the real world is because those who originally settled the cyberspace frontier assumed that this virtual place should operate according to the same constraints that prevail in the real world. As cybercitizens grow more familiar with the virtual world, this assumption will diminish in force, if not disappear entirely, and cyberspace will come to resemble the real world less and less. This will only make even harder the already difficult task of trying to analogize the unsubstantial, transparent, permeable world of cyberspace to the fixed, bounded real world.

The problem is that cyberspace is not a conventional physical place. A person does not actually enter cyberspace, rather a person experiences cyberspace. It is "a domain that exists along with but apart from the physical world. It is a shared conceptual reality, a 'virtual world,' not a shared physical reality."[121] It is a new space, one that has its origins in

120. *See, e.g.*, NEAL STEPHENSON, SNOW CRASH 50 (1992) (in the virtual world known as the Metaverse, tables only have tops, not legs).

121. Susan W. Brenner, *Is There Such a Thing as "Virtual Crime"?*, 4 CAL. CRIM. L. REV. 1, ¶ 11 (2001). *See, e.g.*, MARGARET WERTHEIM, THE PEARLY GATES OF CYBERSPACE: A HISTORY OF SPACE FROM DANTE TO THE INTERNET 230-36 (1999).

physical reality but transcends that reality.[122] Consequently, while one can analogize cyberspace to real world places, the analogies are necessarily so imperfect that it is inadvisable to use them as the basis for importing the Fourth Amendment right to be let alone into cyberspace.[123]

Where does all the imperfect analogies leave the importation of the Fourth Amendment into cyberspace? One might, like the *Olmstead* Court, declare that since cyberspace is an artificial construct, comprised of virtual space rather than real space, the guarantees devised to protect us in the real world do not apply to activities undertaken in the virtual world we choose to visit. While this resolution has a certain straightforward simplicity, it ignores the reality *Katz* recognized. The reality that privacy is a construct which must transcend the methodological differences between the real world as it existed when the Fourth Amendment was adopted and the real world as it is shaped by technology since technology is an essential aspect of modern society.[124] The *Katz* Court based its holding on a recognition of the role telephonic communication came to play in Twentieth Century society.[125] Cyberspace already plays a far more integral role in Twenty-First Century society than the telephone did when the U.S. Supreme Court decided *Katz*,[126] and its importance will only increase. The information

---

122. *See* Brenner, *supra* notes 18 & 121; *see also* Richard A. Bartle, *The Pearly Gates of Cyberspace* (June 16, 1999), *available at* http://www.mud.co.uk/richard/tpgoc.htm (last visited Aug. 30, 2002) *quoted in* Brenner, *supra* note 18:

> When I "go" into cyberspace I leave behind both Newton's and Einstein's laws. . . . Traveling from Web site to Web site, my "motion" cannot be described by any dynamical equations. The arena in which I find myself online cannot be quantified by *any* physical metric; my journeys there cannot be measured by *any* physical ruler. The very concept of "space" takes on here a new . . . meaning. . . .

123. *See, e.g.*, United States v. Hambrick, 55 F. Supp. 2d 504, 508 (W.D. Va. 1999), *aff'd*, 225 F.3d 656 (4th Cir. 2000) ("Cyberspace is a nonphysical 'place' and its very structure, a computer and telephone network that connects millions of users, defies traditional Fourth Amendment analysis").

124. Even the *Olmstead* Court recognized that the Fourth Amendment protected sealed mail while it was in transit. *See supra* text accompanying note 26.

125. *See supra* text accompanying note 33. The decision also seems to have been prompted by concerns about the increased sophistication and proliferation of surveillance technology after World War II. *See* Gormly, *supra* note 3, at 1362-67.

126. *See, e.g., Hambrick*, 55 F. Supp. 2d at 508 ("Legal scholars and Congress have noted the ubiquity of cyberspace in the lives of all Americans. . . . The members of our society increasingly live important parts of their lives through the Internet"). *See also Hearing on "Fourth Amendment and the Internet" Before The Subcommittee on the Constitution of the Committee on the Judiciary of the House of Representatives (Opening Statement of Chairman Canady) (April 6, 2000),*

people previously kept in their homes, file cabinets, wallets, and purses is migrating to cyberspace.[127] Many of the activities formally conducted in the real world or through the telephone have also moved into cyberspace. This trend will only accelerate.

There is another way to interpret the privacy of place notion. If one can define the Fourth Amendment concept of place functionally — as the locus of human activities — instead of corporeally — as a physically-circumscribed area — then it becomes possible to extrapolate Fourth Amendment privacy protections to cyberspace.

Is it reasonable to translate the values incorporated in the Fourth Amendment into a context created and sustained by technology? This transfer of Fourth Amendment values into a technology context is consistent with the U.S. Supreme Court's approach to parsing the Fourth Amendment notion of privacy as place. The Fourth Amendment's origins in trespass law notwithstanding, the Court has never equated place with physical area.[128] Instead, the Court has looked to the nature of the activities one expects to conduct in a given location. This approach is evident in the Court's reverence for the home and the curtilage;[129] in its refusal to make

---

available at http://commdocs.house.gov/committees/judiciary/hju66503.000/hju66503_0.htm(last visited Aug. 30, 2002) [hereinafter *Canady Statement*]:

> [A] recent report by the White House working group . . . states that the . . . number of Internet users in the U.S. is projected to reach 177 million by the end of 2003 and the number of Internet users worldwide is estimated to reach 502 million by 2003.
>
> The Internet is not like the telephone system or the mail . . . [I]t combines a much broader range of functions serving not only the one-on-one functions of the telephone and the mail but also a wide variety of informational, artistic, political and sales and marketing functions. The development of the Internet as a network global communications medium, the expansion in the range of transactions that occur on line and the amount of information now stored with third party Internet companies . . . have produced a qualitative change in the nature of communications. . . .

127. *See Canady Statement, supra* note 126.

128. *See, e.g.*, Oliver v. United States, 466 U.S. 170, 183 (1984) (U.S. Supreme Court refused to find that "the government's intrusion upon an open field" is a "search in the constitutional sense because that intrusion is a trespass at common law," since the property rights "protected by the common law of trespass have little or no relevance to the applicability of the Fourth Amendment").

129. Curtilage refers to the land surrounding a home that is used to host intimate, personal activities. *See, e.g.*, United States v. Dunn, 480 U.S. 294, 300 (1987) ("central component" of Fourth Amendment "privacy of place" inquiry is "whether the area harbors the intimate activity associated with the 'sanctity of a man's home and the privacies of life'") (quoting Boyd v. United

Fourth Amendment protections coextensive with the acreage one occupies;[130] in its willingness to extend Fourth Amendment protections to temporary homes occupied by overnight guests;[131] and in its willingness to accord Fourth Amendment protection to employees' offices.[132] The theme that runs through these decisions is that the Fourth Amendment protects an individual's right to conduct certain activities privately, while secluded from others. The place is simply a necessary incident of this right to withdraw away from others as an aspect of the right to be let alone.

This approach shifts the focus of the Fourth Amendment from place to activity. Activity encompasses communication, both non-mediated and mediated. It does, for example, violate the Fourth Amendment for an officer to enter the curtilage of a home in order to eavesdrop on conversations that occur there.[133] Also, as explained earlier, the Fourth Amendment protects the privacy of telephone conversations and of sealed snail mail while it is in transit. Why is this important? It is important because what we call cyberspace is not actual space at all. It is, as William Gibson said, a "consensual hallucination experienced daily by billions.... A graphical representation of data abstracted from the banks" of computers around the world.[134] Cyberspace is not a thing; it is an activity,[135] a complex type of mediated communication, and as such, it is entitled to Fourth Amendment protection. We cannot, however, parse the extent to which this particular type of mediated communication is entitled to Fourth

---

States, 116 U.S. 616, 630 (1886). *See also* Kyllo v. United States, 121 S. Ct. 2038, 2046 (2001); *Oliver*, 466 U.S. at 180.

130. *See, e.g., Oliver*, 466 U.S. at 179 ("open fields do not provide the setting for those intimate activities that the Amendment is intended to shelter from government interference or surveillance"). *See also supra* text accompanying note 128.

131. *See* Minnesota v. Olson, 495 U.S. 91, 98 (1990) ("To hold that an overnight guest has a legitimate expectation of privacy in his host's home merely recognizes the everyday expectations of privacy that we all share"). *See also* Minnesota v. Carter, 525 U.S. 83, 90 (1998).

132. *See, e.g.*, O'Connor v. Ortega, 480 U.S. 709, 717-18 (1987). *See also Oliver*, 466 U.S. at 178 n.8; Marshall v. Barlow's, Inc., 436 U.S. 307, 311 (1978). While the Fourth Amendment was no doubt intended to outlaw the use of general warrants to search businesses, it is unlikely that the Framers would have contemplated protecting a government employee from searches conducted by her employer.

133. *See, e.g.*, United States v. Wilkes, 451 F.2d 938, 941 n.6 (2d Cir. 1971). *See also* United States v. Llanes, 398 F.2d 880, 883-84 (2d Cir. 1968), *cert. denied*, 393 U.S. 1032 (1969).

134. WILLIAM GIBSON, NEUROMANCER 51 (1984). Gibson, of course, coined the term "cyberspace."

135. *See, e.g.*, Albert Benschop, Peculiarities of Cyberspace: Building Blocks for an Internet Sociology, *available at* http://www.pscw.uva.nl/sociosite/websoc/indexE.html (last visited Oct. 1, 2002).

Amendment protection until we complete one more analytical step, namely, articulating how this approach fits into the structure of the Fourth Amendment and, indeed, into the general contours of the right to be let alone as derived from the First, Fourth, and Fifth Amendments.

The Fourth Amendment contains two clauses, the Unreasonable Searches Clause[136] and the Warrant Clause.[137] Together, these clauses are considered to create a right to be free from unreasonable searches and seizures. However, they actually function very differently and must therefore be analyzed separately. The Warrant Clause creates a set of procedural rights and thereby imposes certain obligations on the government, such as ensuring that warrants are based on probable cause, supported by oath or affirmation, and particularly describe the place to be searched, and the persons or things to be seized.[138] The Warrant Clause is functionally analogous to other procedural guarantees, such as the Due Process Clauses of the Fifth and Fourteenth Amendments[139] and the procedural rights the Sixth Amendment confers on defendants in criminal trials.[140] That is, it puts the onus on the state, rather than the individual, to carry out the requirements communicated in the amendment. Not only is the individual not required to invoke these rights, but an individual must take affirmative and unequivocal steps to surrender them.[141] The Warrant

---

136. The Unreasonable Searches Clause reads "[t]he 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.

137. The Warrant Clause states "no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized." U.S. CONST. amend. IV.

138. *Id.*

139. U.S. CONST. amend. V ("No person . . . shall be deprived of life, liberty, or property, without due process of law"); U.S. CONST. amend. XIV ("nor shall any State deprive any person of life, liberty, or property, without due process of law").

140. U.S. CONST. amend. VI,

> the accused shall enjoy the right to a speedy and public trial, by an impartial jury of the State and district wherein the crime shall have been committed, . . . and to be informed of the nature and cause of the accusation; to be confronted with the witnesses against him; to have compulsory process for obtaining witnesses in his favor, and to have the Assistance of Counsel for his defence.

141. *See, e.g.*, Hall v. Moore, 253 F.3d 624, 628 (11th Cir. 2001).

> [A]lthough a defendant may waive his Sixth Amendment right to . . . counsel . . . the defendant "should be made aware of the dangers and disadvantages of self-representation, so . . . he knows what he is doing and his choice is made with eyes

Clause, like other constitutional procedural guarantees, imposes a duty on the state.[142]

The Unreasonable Searches Clause, on the other hand, functions as a privilege, not as a right.[143] This clause does not specify obligations that are imposed on the state. Instead, it articulates an exemption, an immunity, from unreasonable searches.[144] In so doing, it gives rise to the notion of privacy of place, which is the contribution of the Fourth Amendment to the more general right to be let alone. The First Amendment contributes anonymity and the Fifth Amendment contributes an exemption from being required to testify against one's self.[145] Although the Fifth Amendment is the only one of the three that is commonly adumbrated as a privilege, all three, taken in isolation and as constituents of the right to be let alone, function as privileges because they put the onus of invoking privacy on the individual, not on the state. Unlike rights, privileges must be invoked to be honored.[146] Once an individual invokes a privilege, the state is obligated to honor it if the invocation is valid. It is reasonable to place the burden of implementing the Warrant Clause requirements on the state because the state controls the procedures involved in issuing and executing warrants. It is equally reasonable to make the state responsible for providing counsel and other procedural devices to defendants in criminal cases because the state controls the adjudicative process. It would be unreasonable to make the state the arbiter of privacy because the state does not have a vested interest in privacy. Indeed, privacy is in many respects antithetical to the state's interests since, if nothing else, the limitations imposed by privacy make it more difficult to investigate and prosecute crimes.

> open." . . . A defendant . . . must clearly and unequivocally assert his right to self-representation. The court must conduct a hearing to ensure that the defendant is fully aware of the dangers and disadvantages of proceeding without counsel.

(quoting Faretta v. California, 422 U.S. 806, 835 (1975)). *See also* Fuentes v. Shevin, 407 U.S. 67, 95 n.31 (1972) ("in the civil no less than in the criminal arena" courts indulge "every reasonable presumption" against the waiver of due process rights).

142. A "right" is something "due to a person by . . . legal guarantee." BLACK'S LAW DICTIONARY (7th ed. 1999). Rights create duties, so if there is "no duty there can be no right." *Id.*

143. A "privilege" is an exemption or immunity. *See id.* This is why the *Katz* Court said the Fourth Amendment "protects people, not places." Katz v. United States, 389 U.S. 347, 351 (1967).

144. *See* U.S. CONST. amend. IV ("the right of the people to be secure . . . against unreasonable searchers . . . shall not be violated").

145. As to the First Amendment Guarantee of Anonymity, see *supra* note 10. For the Fifth Amendment Guarantee, see U.S. CONST. amend. V ("no person . . . shall be compelled in any criminal case to be a witness against himself").

146. *See, e.g.*, United States v. Mandujano, 425 U.S. 564, 574-75 (1976).

The definition of the privacy privilege in the Fourth Amendment must therefore come from the people. Like evidentiary privileges, the U.S. Supreme Court derived the contours of the privacy privilege by balancing evolving societal expectations of privacy against the state's interest in information-gathering.[147] *Katz* made this explicit and, in so doing, made it clear that the privacy privilege can evolve to encompass new technologies, specifically, new forms of mediated communication.[148]

The *Katz* Court also made it clear that in order to be effective, the privacy privilege, like evidentiary privileges and the privilege against self-incrimination in the Fifth Amendment, must be invoked by the defendant. As the Court said, "[w]hat a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection. . . . [b]ut what he seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected."[149] Had Katz conducted his conversation while the door to the phone booth was open, so that the agents could overhear what he said without resorting to wiretaps, his comments would not have been protected because he would not have invoked the privilege. The same is true of someone who engages in illegal activity in their own home while in full view of anyone outside; the failure to draw curtains or otherwise invoke the privacy privilege

---

147. This is analogous to the process used to decide whether a new evidentiary privilege should be created. The factors considered in that calculus are as follows:

> (1) the importance to the community of the relationship sought to be protected; (2) whether community values would be offended by governmental intrusion into the privacy of the relationship; (3) the extent to which societal traditions . . . create a reasonable expectation of confidentiality in such a relationship; (4) whether the purpose of the relationship depends upon full and open communication; (5) the extent to which such communication would be impeded by non-recognition of a privilege; and (6) the . . . benefits to the public from . . . protecting the privacy of the relationship in comparison to the cost to the litigation process resulting from the loss of evidence.

2 C. MUELLER & L. KIRKPATRICK, FEDERAL EVIDENCE § 172 (2d ed. 1994).

148. It is important to note that, unlike evidentiary privileges, the Fourth Amendment's "privacy privilege" does not put information permanently beyond the government's reach; it can be overcome with a warrant. In this regard, the operation of this Fourth Amendment privilege is analogous to the operation of the Fifth Amendment's privilege against self-incrimination, which can be overcome with a grant of immunity.

149. *Katz*, 389 U.S. at 351-52 (citations omitted).

presumptively guaranteed by being present at home means that one is not protected by the Fourth Amendment.[150]

There are therefore two aspects to the privacy privilege in the Fourth Amendment: (a) the scope of the privilege, which is defined by the expectations of society as to what level of privacy is reasonable at a given historical moment; and (b) the invocation of the privilege by the individual, which the government must respect unless it obtains a search warrant. It is now necessary to consider how this privilege applies, if at all, to cyberspace.

The first question is whether the privacy privilege applies to cyberspace when cyberspace is construed as an activity, not as a place. As explained earlier, cyberspace is properly analyzed as a perceived reality that emerges from the interaction of multiple types of meditated communication.[151] The privacy privilege clearly applies to mediated communication. In the Nineteenth Century, the U.S. Supreme Court held that the Fourth Amendment privacy privilege protects sealed mail in transit,[152] and subsequently the Twentieth Century Court expanded the privilege to protect telephonic communication.[153] Given these precedents and the role cyberspace has come to play in society, there is no doubt that the Court will extend Fourth Amendment protection to cyberspace. The difficulty lies not in the decision to extend this protection to cyberspace but in how to define the protection. The types of mediated communication that have been protected thus far both involve simple one-to-one communication. The mediated communication that creates and sustains cyberspace involves one-to-one communication, one-to-many communication, many-to-one communication and many-to-many communication. Given the complexity of the types of activities involved in cyberspace, the Court cannot simply hold, as it did in *Katz*, that the Fourth Amendment protects this entire class of computer-mediated communication. It would not, for instance, be reasonable to hold that the Fourth Amendment categorically protects messages posted to a newsgroup.

The requirement that the privilege must be invoked to be effective is the solution to this problem. In extending this privilege to cyberspace, the

---

150. *See, e.g.*, United States v. $61,433.04 U.S. Currency, 894 F. Supp. 906, 910 (E.D.N.C. 1995), *aff'd*, 90 F.3d 903 (4th Cir. 1996) (not a violation of Fourth Amendment privacy for officers to look through blinds in dining room window that were not completely closed).

151. *See supra* text accompanying notes 134-35.

152. *See Ex parte Jackson*, 96 U.S. 727, 733 (1878); *see also supra* note 26.

153. *See Katz*, 389 U.S. at 352; *see also supra* note 40 and accompanying text.

U.S. Supreme Court must stress that, unlike the home,[154] cyberspace is not a context in which the Fourth Amendment presumptively applies. The Court must make it clear that the Fourth Amendment does not protect computer-mediated communications unless the parties to the communications affirmatively and effectively invoke the privacy privilege. One virtue of this approach is that emphasizing invocation gives courts a standard they can use when faced with the many varieties of computer-mediated communication. Privacy cannot encompass communications unless the parties took steps to ensure that they remained private, in effect, closing the telephone booth door.[155] The parties might rely on encryption, on the use of private, password-protected areas, or other security measures. However, they would not be able to claim the protections of the Fourth Amendment if they did nothing to preserve the privacy of the communications at issue.

Returning to the newsgroup example above, a court would reject a claim that someone had an expectation of privacy in messages posted to a newsgroup on the grounds that there had been no invocation of the privilege since the messages could be read by anyone who subscribed to that newsgroup. If a person posted the messages to a listserv, a court would have to determine if the listserv was open to the public or only accessible to a defined group of subscribers. With the latter situation, a court would then have to determine whether the subscribers had taken measures sufficient to limit access to the listserv, thereby invoking the "privacy privilege."[156] The content posted on publicly-accessible areas of a web site

---

154. *See* Kyllo v. United States, 121 S. Ct. 2038, 2046 (2001).

155. *Cf.* Kee v. City of Rowlett, 247 F.3d 206, (5th Cir. 2001). The *Kee* Court held that police did not violate a family's Fourth Amendment "privacy privilege" by putting a microphone in a funeral urn and taping what they said at a funeral for two murdered children.

> [M]ost damaging to Kee and Routier's argument is that they failed to present evidence demonstrating any affirmative steps taken to preserve their privacy. While it is apparent from their affidavits that they did not expect government agents surreptitiously to be recording their prayers, they also were aware that the service was being conducted in an outdoor setting. Kee and Routier fail to allege that they took any steps to ensure that unwanted individuals were excluded or that they did anything to preserve the private nature of the service. They point to no reasonable safeguards or common-sense precautions taken to preserve their expectation of privacy.

Id. at 216-17. The tapes came to light in the mother's trial for murdering the children. *Id.* at 208.

156. The "conversations" held on such a listserv can be analogized to the conversation at issue in *Katz*. Although they are written, not oral, the discussions among the participants are in effect a

would not be protected by the privilege. Content posted on controlled-access areas might be protected, depending on the steps that were taken to preserve its confidentiality.[157] The same would be true of messages posted in "chat rooms."[158] As to e-mails sent in the course of a one-to-one correspondence, the use of encryption would clearly serve as an invocation of the privilege, at least until the e-mails reached the intended recipient.[159]

It is relatively easy to identify the broad measures that, if taken, can qualify as an invocation of the privacy privilege. The difficult task is determining whether particular measures, once taken, are sufficient to constitute an invocation. Consider, for example, the use of encryption to

---

"conference call" involving multiple participants. As long as the participants have taken the steps necessary to invoke the "privacy privilege," their discussions would be protected.

157. *See, e.g.*, J.S. *ex rel.* H.S. v. Bethlehem Area Sch. Dist., 757 A.2d 412, 425 (Pa. Commw. Ct. 2000):

> [T]he creator of a web-site controls the site until . . . it is posted on the Internet. Once it is posted, . . . it may be accessed by anyone on the Internet. Without protecting the web-site, the creator takes the risk of other individuals accessing it. . . . [T]he trial court was correct in its determination that Student maintained no expectation of privacy in the web-site.

158. *See, e.g.*, United States v. Charbonneau, 979 F. Supp. 1177, 1185 (S.D. Ohio 1997):

> [W]hen Defendant engaged in chat room conversations, he ran the risk of speaking to an undercover agent. . . . Defendant could not have a reasonable expectation of privacy in the chat rooms. Accordingly, the e-mail sent by Defendant to others in a "chat room" is not afforded any semblance of privacy; . . . e-mail sent or forwarded to the undercover agents is not protected by the Fourth Amendment.

Accord Commonwealth v. Proetto, 771 A.2d 823, 831 (Pa. Super. Ct. 2001). *See also* United States v. Maxwell, 45 M.J. 406, 418 (C.A.A.F. 1996).

159. Encryption would overcome the argument that e-mail, like a postcard, is not encompassed by a reasonable expectation of privacy. *See* Note, *Keeping Secrets in Cyberspace: Establishing Fourth Amendment Protection for Internet Communication*, 110 HARV. L. REV. 1591, 1597 (1997). *See also* Smith v. State, 389 A.2d 858, 873 (Md. 1978) (Cole, J., dissenting), *aff'd*, 442 U.S. 735 (1979) ("any writing on the outside of an envelope or a postcard can be easily read by postal employees"). Some courts have found that there is "a limited reasonable expectation of privacy" in e-mail while it is in transit. *See, e.g.*, *Charbonneau*, 979 F. Supp. at 1184; *Maxwell*, 45 M.J. at 418.

The fact that officers can use technology such as keystroke loggers to capture encryption keys in no way undermines encryption's effectiveness as a way of invoking the "privacy privilege." *See infra* note 164. In the real world, a reasonable expectation of privacy encompasses one's home regardless of the measures taken to secure it. Even if the front door is standing unlocked and open, law enforcement officers cannot cross the threshold without a warrant or an applicable exception to the warrant requirement. *See supra* text accompanying note 113.

shield e-mail. If e-mail correspondents do not employ encryption, they cannot claim to have invoked the privacy privilege as they have done nothing to preserve the confidentiality of their communications. But, if they do employ encryption, what level of encryption will suffice to constitute an invocation of the privilege? Must they use the strongest level of encryption then available to invoke the privilege, or is it sufficient that they use any level of encryption?

The reasonable approach is not to invite an arms race by requiring that those who seek privacy employ the most recent, most sophisticated technologies to invoke the privilege. Predicating invocation on the sophistication of the countermeasures one employs is an unreasonable approach. First, it ultimately pits individual privacy against government technology, a battle the individual is destined to lose;[160] and second, it is inconsistent with the rationale behind the privilege. The Fourth Amendment privacy privilege protects individuals from government intrusions into activities that are not public, meaning that steps have been taken to shield those activities from observation by members of the general public.[161] The privacy privilege puts law enforcement officers in the same position as members of the general public. If one takes reasonable steps to

---

160. *See, e.g.*, United States v. Elkins, 95 F. Supp. 2d 796, 810 (W.D. Tenn. 2000) ("allowing the rights protected by the Fourth Amendment to fall victim to a technological race between the government and the people . . . is a race the people shall most certainly lose"). *See also* United States v. Cusumano, 67 F.3d 1497, 1504 (10th Cir. 1995), *vacated*, 83 F.3d 1247 (10th Cir. 1996) (en banc).

161. *See, e.g.*, California v. Ciraolo, 476 U.S. 207, 213-14 (1986):

> The Fourth Amendment . . . has never . . . require[d] law enforcement officers to shield their eyes when passing by a home on public thoroughfares. Nor does the mere fact that an individual has taken measures to restrict some views of his activities preclude an officer's observations from a public vantage point where he has a right to be and which renders the activities clearly visible. . . .
> The observations by Officers Shutz and Rodriguez . . . took place within public navigable airspace . . . ; from this point they were able to observe plants readily discernible to the naked eye as marijuana. . . . Any member of the public flying in this airspace who glanced down could have seen everything that these officers observed. On this record, we readily conclude that respondent's expectation that his garden was protected from such observation is unreasonable and is not an expectation that society is prepared to honor.

See also Kyllo v. United States, 121 S. Ct. 2038, 2046 (2001) (police's use of technology "not in general public use" to obtain information about the interior of a home violated a Fourth Amendment expectation of privacy).

shield an activity from observation by members of the general public, that activity is also protected from warrantless intrusions by law enforcement.[162]

The effectiveness of an attempt to invoke the privacy privilege therefore depends on whether the steps taken would reasonably shield activity from observation by members of the general public, not on whether or not the activity is shielded from observation by law enforcement officers equipped with the latest intrusion technology. So, if the utilization of fifty-six-bit encryption is an effective way to shield the content of e-mails from the general public, including the members of the general public who could otherwise review the e-mails as they travel from sender to recipient(s), it is effective as an invocation of the privacy privilege.

Emphasizing invocation also provides a way to deal with the type of monitoring discussed earlier, the cyber-analogue of the observations by nosy neighbors in the Eighteenth Century. Individuals who engage in transactions that allow the gathering of personal data will not be able to claim the benefits of the privacy privilege because they failed to invoke it. This is true regardless of whether they act knowingly or negligently. By entering cyberspace and engaging in transactions without taking measures to establish privacy, they assume the risk that those transactions are not private.

Another virtue of this approach is that placing the burden on the individual to establish a cognizable privacy interest gives an individual's control over the extent to which his or her activities are shielded by the privacy privilege. This is consistent with *Katz's* risk-analysis, e.g., its premise that "what a person knowingly exposes to the public . . . is not a subject of Fourth Amendment protection."[163] Those who employ the mediated communication of cyberspace without taking steps to ensure their privacy assume the risk that their communications will be read by outsiders, including law enforcement officers. The effect will be to encourage individuals to take steps to ensure the privacy of cyberspace communications, and to develop technology that can be used to invoke the privacy privilege.[164] Indeed, since cyberspace is an artificial construct, it

---

162. *See supra* text accompanying note 158.

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

164. One can see this dynamic developing with regard to keystroke loggers. *See, e.g.*, Robert Vamosi, *We Know What You're Typing*, MSNBC (Dec. 7, 2001), *available at* http://www.msnbc.com/news/669010.asp (last visited Aug. 30, 2002) ("a keystroke logging program is a memory application that records every keystroke a user makes on a given computer"). Since they record keystrokes as they are typed, loggers can be used to capture text before it is encrypted or to capture

should prove easier to do this than to counter surveillance technologies in the real world.[165]

This approach provides a way to apply Fourth Amendment protections to people engaged in computer-mediated communication. It is now necessary to determine if the Fourth Amendment encompasses data that contains the content of a communication or data that documents the

---

encryption keys. *See, e.g., id.* Late in 2001, the Federal Bureau of Investigation (FBI) confirmed that it was developing "Magic Lantern," technology that would let the FBI plant a Trojan horse keystroke logger on a target's computer by sending a computer virus via e-mail. *See, e.g., FBI Confirms "Magic Lantern" Exists,* MSNBC (Dec. 12, 2001), *available at* http://www.msnbc.com/news/671981.asp (last visited Aug. 30, 2002). *See also* Vamosi, *supra* (a friend or relative of the suspect could send the keystroke logger via e-mail). Earlier in 2001, the FBI used a keystroke logger to obtain the encryption keys of Nicodemo Scarfo, a suspected mobster; the logger was physically installed on the keyboard of Scarfo's computer during a surreptitious entry of his office. *See* United States v. Scarfo, Order Denying Motion to Suppress Evidence, (D.N.J. — Crim. No. 00-404) (Dec. 26, 2001), *available at* http://lawlibrary.rutgers.edu/fed/html/cr00-404-1.html (last visited Oct. 28, 2002). A search warrant authorized the entry and installation and the logger was configured to "minimize" the information it obtained, e.g., to obtain only data pertaining to the encryption key. *See* United States v. Scarfo, (D.N.J. — Crim. No. 00-404), Order Granting Application for Surreptitious Entry and Installation, (May 8, 1999), *available at* http://www2.epic.org/crypto/scarfo/order_5_99.pdf (last visited Dec. 9, 2002). *See also* United States v. Scarfo, (D.N.J. — Crim. No. 00-404), Affidavit of Randall S. Murch, (Oct. 4, 2001), *available at* http://www.epic.org/crypto/scarfo/murch_aff.pdf (last visited Sept. 30, 2002). The use of the "Magic Lantern" software to remotely install a keystroke logger would have to be authorized also, initially by an attorney general, later by a court. *See, e.g.,* Vamosi, *supra.* This is because the use of a keystroke logger certainly constitutes a search, as it invades an activity in which the individual has manifested a reasonable expectation of privacy; the acts of typing on the keyboard on which the logger is installed typically occur in the individual's home or office, both places presumptively encompassed by the Fourth Amendment's "privacy privilege." (The act of copying the key qualifies as a "seizure" of the information it contains. *See, e.g.,* United States v. Scarfo, Order Denying Motion, *supra*). The use of a warrant, or an alternative authorization approved by federal legislation, makes the installation of the logger "reasonable" under the Fourth Amendment, so the "privacy privilege" is not violated.

What is interesting, however, is that technology is developing in ways which lets individuals detect whether a keystroke logger has been installed on their computer(s); and if a logger has been installed, the software lets them disable it. *See, e.g.,* David Coursey, Keep Yourself Top Secret! How to Defeat Spyware (Part 2) (Jan. 4, 2002), *available at* http://www.zdnet.com/anchordesk/stories/story/0,10738,2836055,00.html (last visited Dec. 9, 2002). *See also* SpyCop, *available at* http://www.spycop.com/ (last visited Aug. 30, 2002). This dynamic illustrates how the "privacy privilege" may evolve in cyberspace; as law enforcement devises techniques to penetrate privacy, individuals respond with technology designed to make their privacy less impenetrable, a process analogous to building fences and taking other tangible measures to establish the privacy of an individual in the real world.

165. *See, e.g.,* LESSIG, *supra* note 14, at 160 (as to cyberspace, one can "imagine an architecture . . . that protects privacy rights in a way that real space cannot").

transmission of a communication. In analyzing these issues, it is helpful to compare the older forms of mediated communication, telephonic communication and written correspondence, to computer-mediated communication.

As to content,[166] telephone conversations, like conversations in the real world, are ephemeral. Unless a party to the conversation (or the government acting pursuant to a wiretap authorization) records what is said, the content dissipates except for what is left in the memories of the parties. The Fourth Amendment protects the sanctity of the conversation from intrusion by outsiders while it is in progress, but provides no recourse for the perfidy of a party to the conversation who tapes it and turns the tape over to the authorities or recounts the substance of the conversation to them.[167] Written correspondence sent by snail mail or private carrier in the real world does exist independently in a permanent, tangible form, and if a letter is sealed, it remains private until it reaches the intended recipient. Once it arrives, the Fourth Amendment, again, provides no recourse if the recipient decides to turn the letter over to the authorities.[168]

Communication in cyberspace differs from these older types of mediated communication in one important respect: There is no guarantee that the content of the communication will be transferred exclusively to the intended recipient(s). When someone receives an e-mail, it is read on the mail server or downloaded to the recipient's computer. Either way, a copy of the e-mail may remain on the server where it can be read by the network administrator or members of the staff.[169] Assume that a network

---

166. For a definition of "content," see *infra* note 182.

167. *See, e.g., Katz*, 389 U.S. at 363 n.** (White, J., concurring):

> When one man speaks to another he takes all the risks ordinarily inherent in so doing, including the risk that the man to whom he speaks will make public what he has heard. The Fourth Amendment does not protect against unreliable (or law-abiding) associates. . . . It is but a logical and reasonable extension of this principle that a man take the risk that his hearer, free to memorize what he hears for later verbatim repetitions, is instead recording it or transmitting it to another.

(citation omitted). *See also* Hoffa v. United States, 385 U.S. 293, 302-03 (1966) (one assumes the risk of being betrayed by an informer "whenever we speak").

168. *See, e.g.*, United States v. King, 55 F.3d 1193, 1195-96 (6th Cir. 1995); State v. Strickland, 683 So. 2d 218, 229 (La. 1996).

169. *See, e.g.*, Fraser v. Nationwide Mut. Ins. Co., 135 F. Supp. 2d 623, 633-34 (E.D. Pa. 2001); WARREN G. KRUSE II & JAY G. HEISER, COMPUTER FORENSICS: INCIDENT RESPONSE ESSENTIALS 36-37 (2002); Illinois Institute of Technology — How to Use Email, *available at* http://cns.iit.edu/howto/useineltools/index.html (last visited Dec. 9, 2002). *See also* Seth T. Ross, Attack of the Email Snoops, *available at* http://www.securius.com/Newletters/Attack_of_the_

administrator reads an e-mail, finds incriminating evidence, and takes it to the authorities.[170] How does this possibility fit into the Fourth Amendment? Is it reasonable to analogize the network administrator to the recipient of written correspondence or a party to a telephone conversation?[171] One can argue that it is in fact not reasonable to draw this analogy because the e-mail correspondents did not knowingly make the network administrator a party to their communication. The telephone and written correspondence decisions are based on the proposition that by intentionally making someone privy to a communication, one assumes the risk that the person will prove faithless and will share the content of the communication with others.[172]

The better approach, the Occam's Razor approach,[173] is to require that the privacy privilege be invoked to be effective. By failing to encrypt their e-mail, the parties to a correspondence fail to invoke the privilege and therefore cannot claim the protections of the Fourth Amendment. Their conduct is analogous to that of two individuals who conduct a telephone conversation on cell phones while each is located in a public place. Each fails to invoke the privilege by not taking steps to prevent bystanders from overhearing what is said.

The more difficult issue arises with regard to third-party records that document the transmission of computer-mediated communications. Again, it is helpful to begin by considering telephonic communication and terrestrial mail correspondence. In *Smith v. Maryland*,[174] the U.S. Supreme Court held that it was not a violation of the Fourth Amendment for police

---

Email_Snoops.html (last visited Oct. 28, 2002); Jim Gerland & Mark Winer, Internet Privacy and Security, *available at* http://www.internet-guys.com/display-article.php?article=31 (last visited Oct. 28, 2002).

170. *See, e.g.*, United States v. Maxwell, 45 M.J. 406, 418 (C.A.A.F. 1996) ("there is the risk that an employee or other person with direct access to the network service will access the e-mail").

171. The rule governing telephone conversations and written correspondence would apply to e-mail correspondence. *See, e.g., Maxwell*, 45 M.J. at 417-18 (like the party to a telephone conversation, an e-mail correspondent assumes the risk that another correspondent will share the communication with outsiders, including the authorities).

172. *See supra* text accompanying notes 167-68.

173. Occam's Razor is a principle of logic attributed to medieval philosopher William of Occam. *See, e.g.*, Occam's Razor, Principia Cybernetica Web, *available at* http://pespmc1.vub.ac.be/OCCAMRAZ.html (last visited Dec. 17, 2002). The principle is, basically, that the simplest explanation is the best. *See id.* ("the principle states that one should not make more assumptions than the minimum needed" to arrive at an explanation).

174. 442 U.S. 735 (1979).

to use a pen register[175] to record the numbers dialed on a telephone.[176] The pen register, which records only the numbers dialed, not the content of the calls, was installed by the telephone company at the police's request. They did not have a warrant authorizing the installation.[177] Smith argued that capturing the numbers was a search under the Fourth Amendment, but the U.S. Supreme Court disagreed:

> Petitioner can claim no legitimate expectation of privacy here. When he used his phone, petitioner voluntarily conveyed numerical information to the telephone company and "exposed" that information to its equipment in the ordinary course of business. In so doing, petitioner assumed the risk that the company would reveal to police the numbers he dialed. The switching equipment that processed those numbers is merely the modern counterpart of the operator who, in an earlier day, personally completed calls for the subscriber. Petitioner concedes that if he had placed his calls through an operator, he could claim no legitimate expectation of privacy. . . . We are not inclined to hold that a different constitutional result is required because the telephone company has decided to automate.[178]

With regard to mail covers, which are the "process by which a nonconsensual record is made of any data appearing on the outside cover of any sealed or unsealed class of mail matter," lower courts reached the same conclusion.[179] The U.S. Supreme Court held that inspecting the outside of mail in transit does not "disturb any privacy interest,"[180] and several circuits have held that the use of a mail cover does not violate the Fourth Amendment because the senders knowingly expose the outside of the mail, including address information, to "postal employees and others."[181]

---

175. A pen register is "a mechanical device that records the numbers dialed on a telephone by monitoring the electrical impulses caused when the dial on the telephone is released." *Id.* at 736 n.1. A pen register does not intercept the content of an oral communication. *See id.*

176. *See id.* at 745-46.

177. *See id.* at 737.

178. *See id.* at 744-45.

179. 39 C.F.R. § 233.3(c).

180. United States v. Hinton, 222 F.3d 664, 675 (9th Cir. 2000).

181. United States v. Choate, 576 F.2d 165, 177 (9th Cir. 1978) (en banc). *See also* Vreeken v. Davis, 718 F.2d 343, 347 (10th Cir. 1983); United States v. Huie, 593 F.2d 14, 14-15 (5th Cir. 1979).

Should the same rule govern information collected by Internet Service Providers, the channel by which one accesses cyberspace and sends e-mail? In answering that question it is necessary to consider the two types of non-content information generated by computer-mediated communication: subscriber data and traffic data.[182] Subscriber data is information held by an Internet Service Provider that can be used to establish "the type of the communication service used, the technical provisions taken thereto and the period of service;" "the subscriber's identity, postal or geographic address, telephone and other access number, billing and payment information"; and "any other information . . . . available on the basis of the service agreement".[183] Traffic data is "computer data relating to a communication by means of a computer system, generated by a computer system that formed a part in the chain of communication, indicating the communication's origin, destination, route, time, date, size, duration, or type of underlying service."[184] Of the two, traffic data is the most analogous to the types of information elicited by mail covers and by the pen register at issue in *Smith*. Like telephone numbers and postal address information, traffic data is necessarily exposed.[185] Most people probably do not understand the extent to which

---

182. *See, e.g.*, Council of Europe, Convention on Cyber Crime (ETS No. 185), Article 1, Article 21, & Explanatory Report ¶ 229, *available at* http://conventions.coe.int/Treaty/EN/cadre principal.htm (last visited Aug. 30, 2002) (content data is "the meaning or purport of the communication, or the message or information being conveyed. . . . It is everything transmitted as part of the communication that is not traffic data"). Content data is addressed above. *See supra* text accompanying notes 166-72.

183. Council of Europe, *supra* note 182, art. 18(3).

184. *Id.* art. 1(d).

185. Some distinguish traffic data from telephone numbers or postal addresses, arguing that traffic data can provide information about the nature of the communication itself. The size of a message can, for example, provide clues as to whether it is purely textual or includes graphics *See, e.g.*, Manton M. Grier, Jr., *The Software Formerly Known as "Carnivore": When Does E-Mail Surveillance Encroach Upon A Reasonable Expectation of Privacy*, 52 S.C. L. REV. 875, 886-87 (2001):

> [E-mail surveillance software once known as "Carnivore"] collect[s] the number of bytes transferred in the message. The software represents a unit of data with an "X" in the subject field. Thus, an e-mail sent containing seventeen bytes of data is represented by eighteen Xs, while an e-mail containing twenty-nine bytes of data is represented by thirty Xs. This data may seem insignificant, but consider the following hypothetical: A judge authorizes FBI agents to use Carnivore to capture e-mail addresses sent to and from a person suspected of violating child pornography laws. While the agents are viewing this information, they notice most

traffic data is exposed during the process of sending an e-mail. However, their understanding of this exposure is no doubt equivalent to the knowledge individuals have of the extent to which the telephone numbers they call are exposed to the telephone company.[186] Logically, therefore, traffic data is encompassed by the rule enunciated in *Smith*, that is, there can be no Fourth Amendment expectation of privacy in traffic data.

The same is true of subscriber data, but for slightly different reasons. In *United States v. Miller*,[187] the U.S. Supreme Court held that one does not have a Fourth Amendment expectation of privacy in "information voluntarily conveyed to . . . banks and exposed to their employees in the ordinary course of business."[188] The U.S. Supreme Court found that a person "takes the risk, in revealing his affairs to another, that the information will be conveyed by that person to the Government."[189] This holding is analogous to the holding in *Smith*, but the cases are factually distinguishable because of the extent to which the individual is aware that he or she is providing personal information to the third party. The information one reveals by making a telephone call, mailing a letter, or sending an e-mail is incidental to the act of engaging in mediated communication. The focus of the individual is on the communication itself, not on the information that the act of communicating adventitiously

---

> messages are small but some are extraordinarily large, perhaps indicating that illegal pictures are being transmitted. . . .

The size of the message, in other words, allows the agents to draw inferences about its content. This type of information is also available, however, for telephone calls and items sent through the mail. Telephone companies monitor the length of telephone calls for billing purposes; and postal workers necessarily obtain some information about the weight of the letters and packages they transport. *See also*, Parliament of the Commonwealth of Australia, *The Law Enforcement Implications of New Technology* 16 (Aug. 2001), *available at* http://www.aph.gov.au/senate/committee/nca_ctte/law_enforcement/law_enforcement.pdf (last visited Oct. 28, 2002) ("it is possible to build up quite a detailed picture of a person from traffic data").

186. *See supra* text accompanying note 178.

187. 425 U.S. 435 (1976).

188. *Id.* at 442.

189. *Id.* at 443.

> This Court has held repeatedly that the Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities, even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed.

Id.

reveals. This is not true when an individual actively shares personal information with a third party. With subscriber data, the level of awareness that one is exposing information and thereby assuming a risk that it will be disclosed to the government is necessarily higher. In *Miller*, the information concerned financial transactions between Miller and two banks.[190] For subscriber data, the information includes not only pedigree information such as one's name, address, and telephone number, but also financial information and information about the account the subscriber has with the Internet Service Provider.[191] Logically, therefore, subscriber data is encompassed by the rule enunciated in *Miller*, and again, there is no Fourth Amendment expectation of privacy.

Is this result to traffic data and subscriber data consistent with the premise advanced earlier, namely, that the Fourth Amendment prohibits unreasonable searches and should be construed as a privilege that must be invoked to be effective? This premise necessarily includes a corollary, namely, that one must be able to invoke the privilege. The discussion of content data concluded that one can invoke the privilege as to the contents of communications by encrypting those communications. If one chooses not to employ encryption, one assumes the risk that the content of a message will be read by an outsider who may share it with the authorities. The ability to choose privacy or to run the risk of non-privacy gives the individual the necessary element of choice. The element of choice is absent with traffic data and subscriber data.[192] If one wants to employ computer-mediated communication, one has no choice but to open an account with an Internet Service Provider and give them the information they require. Having done so, if the person wants to send e-mails, there is no choice as to the quantum of routing and identifying information those e-mails will reveal.

The *Smith* and *Miller* Courts found this acceptable, though in each instance Congress subsequently enacted legislation creating additional guarantees of privacy.[193] Superseding legislation is always an option, but the focus of this discussion is on the interpretation of constitutional guarantees. Legislation is transient; the U.S. Constitution endures.

---

190. *See id.* at 437-38.

191. *See* Council of Europe, *supra* note 182.

192. As, indeed, it is for the other types of mediated communication, the telephone, and the mail.

193. *See* Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848, 1868-73; Right to Financial Privacy Act of 1978, Pub. L. No. 95-630, tit. XI, 92 Stat. 3641, 3697-3710.

So, where does this leave the privacy of information held by a third party? If the assumption is that establishing such information as private is a desirable outcome, then there are several options that can be pursued. Secrecy havens[194] are a pragmatic solution. Secrecy havens are analogous to the bank secrecy havens that emerged in the 1980s, in that each guarantees the privacy of subscriber data.[195] This is an "outlaw"[196] solution that, aside from anything else, does not make it a desirable solution.[197]

Another option is to create a subscriber-provider evidentiary privilege that guarantees the privacy of subscriber data, and perhaps guarantees some measure of traffic data.[198] The difficulty with this approach is that while evidentiary privileges have been recognized as protecting information given to third parties, each of these privileges protects a relationship that society deems to be valuable for reasons beyond the information. The attorney-client privilege, for example, protects the need for full and free information sharing between an attorney and a client so that the attorney can effectively represent the client. The same is true of the doctor-patient privilege and the marital privilege in the way they both guard the sanctity of communications in a personal relationship that society deems significant enough to protect. As of now, there have been no purely informational privileges, which is not to say that such privileges cannot and should not be recognized. Perhaps they are a necessary concomitant of mediated communication as it is further extended by advances in technology. One possible concern with recognizing such a

---

194. *See infra* text accompanying note 195.

195. *See, e.g.*, Parliament of the Commonwealth of Australia, *supra* note 185 ("organised crime figures could establish ISPs, with obvious potential adverse consequences for law enforcement"). A secrecy haven would preserve the privacy of customer information and data against "any legal action" by a state or a private litigant. *See, e.g.*, About Haven Co., *available at* http://www.havenco.com/about_havenco/index.html (last visited Dec. 9, 2002).

196. "Outlaw" meaning "outside the law." *See, e.g.*, 3 W. HOLDSWORTH, A HISTORY OF ENGLISH LAW 46 (4th ed. 1936) (in Anglo-Saxon practice, an "outlaw" was "outside the law, and as a wild beast could be pursued and slain").

197. Subscriber data would be within the "outlaw" service provider's exclusive control, so privacy could be assured for this level of information. Since a service provider must inevitably interact with over service providers to transmit communications, it is difficult to see how an "outlaw" service provider could guarantee the absolute anonymity of a client's e-mail communications. At a minimum, the service provider's receiving and retransmitting of communications should be able to identify the service provider from which the communication came.

198. *See, e.g.*, Model Code of Cybercrimes Investigative Procedure, art. XI § 3(a) & Commentary to § 3 (recognizing Internet Service Provider-Client privilege), *available at* http://www.cybercrimes.net/MCCIP/art11.htm (last visited Aug. 30, 2002).

privilege is that like all evidentiary privileges, it effectively places the information in question outside the scope of law enforcement efforts. This is true in many cases despite the fact that the privileges incorporate exceptions for communications made to further criminal activities.[199]

A third option is to expand the scope of the Fourth Amendment privacy privilege so that it categorically encompasses a reasonable expectation of privacy in information given to third-party record holders. Procedurally, this approach would prove less of an impediment for law enforcement than creating an evidentiary privilege, because unlike evidentiary privileges, the privacy privilege can be overcome with a search warrant or an exception to the warrant requirement. The critical question is a matter of policy, i.e., whether this option strikes a sufficiently reasonable balance between law enforcement needs and individual privacy to justify such an expansion.

Ultimately, the answer must be that such an expansion simply cannot be justified as protecting the interests that the privacy privilege was intended to preserve. The Fourth Amendment does protect the privacy of communicative processes among individuals, but only under certain conditions; one of which is that the process involves known participants.[200] "Known" does not mean that the participants have a particularly close relationship with each other, nor does it imply the special type of relationships that are the predicate for evidentiary privileges. "Known" means that, at a minimum, the parties are acquainted and have some type of personal or professional relationship. It is a barometer of the extent to which society is willing to accept communications between these parties as private. Society accepts that conversations between personal friends or professional colleagues are private, if they have taken steps to invoke the privacy privilege, such as speaking in a room with the door closed. Society will not accept that a conversation between a cab driver and one who hires the cab is private because there is no empirical foundation for the mutual confidence that private implies; the cab driver and the customer interact as fungible, anonymous types.

Therefore, the first problem with expanding the privacy privilege to encompass traffic data and subscriber data is that there is no basis for assuming privacy in interactions between the customers and employees of an Internet Service Provider.[201] As to subscriber data, the customer knows that there are employees who process the account, but the customer has no

199. *See, e.g., id.* art. XI § 3(b).

200. *See* U.S. CONST. amend IV.

201. *See supra* text accompanying notes 185-91.

idea who they are nor is there continuity of personnel that would establish any kind of professional relationship.[202] Interchangeable employees will handle the account at different times throughout its life.

This lack of known parties is even more apparent as to traffic data. While the customer may have occasion to speak to one of the several employees who have access to their account, the customer will never interact with those who actually administer the account. Another problem, at least as to traffic data, is that it is not the product of a communicative process between the customers and employees of an Internet Service Provider. Traffic data is the product of what is really a series of mechanical processes, some involving the customer, such as addressing and sending e-mails, while others involve the technology used to send and monitor the course of e-mail.[203] For all these reasons, it would not be reasonable to expand the privacy privilege to encompass information given to third-party record holders.

A fourth option is to use technology itself to invoke the privacy privilege as to the content of subscriber data and traffic data. To the extent possible, technology seems the most attractive alternative, since it incorporates the notion of choice.[204] This solution leaves the decision of whether to invoke privacy or to risk losing it in the hands of the individual. Therefore, one can imagine a cyberspace in which it is possible to participate on several levels of diminishing privacy. The first level would offer channels that are highly secure for both personal data and traffic data, the second would offer channels that provide some level of security as to both, and the third level would offer channels that provide little security as to either. One objection to this approach is that although it preserves the choice option, it predicates the availability of choice upon the ability of an individual or entity to pay for privacy;[205] the tier system would certainly

---

202. To use an example drawn from the real world, one who lives in a smaller community may develop some familiarity with the postal employees who handle his mail, but it would be absurd to contend that conversations between the postal customer and postal employees are "private."

203. Traffic data in this regard is analogous to the information detected by pen registers. *See* United States v. N.Y. Tel. Co., 434 U.S. 159, 167 (1977) (a law enforcement official could not even determine from the use of a pen register whether a communication existed).

204. The use of technology as the means of invoking the privilege leaves the decision whether to do so or not in the hands of the individual. He or she can utilize technology to invoke the privilege and thereby gain its protections; or an individual can do nothing to invoke the privilege and thereby forfeit any claim to its protections.

205. *See, e.g.*, Kenneth Troiano, Comment, *Law Enforcement Use of High Technology: Does Closing the Door Matter Anymore?*, 24 CAL. W. L. REV. 83, 92 (1988) (claiming that only the wealthy and criminals can afford the measures needed to counter surveillance technology); *see, e.g.*, Ronald J. Bacigal, *Some Observations and Proposals on the Nature of the Fourth Amendment*, 46

cost more to subscribe to the channels with the highest security than to the lower security channels. However, while that may seem an unfortunate aspect of a tiered approach to privacy in cyberspace, it has always been a component of Fourth Amendment privacy. One cannot enjoy the fundamental level of Fourth Amendment privacy unless one is able to create and sustain a home. As technology has become increasingly pervasive, it has become impossible to invoke the privacy privilege in many aspects of life without having the financial ability to take certain countermeasures.[206] However debatable, the latter result may be, at least as to the real world, that anyone who ventures into the cyberworld bears the concomitant fiscal burden of ensuring privacy in that realm.

IV. FIFTH AMENDMENT

The Fifth Amendment privilege against self-incrimination plays a very modest role in protecting on-line privacy. Although the Nineteenth Century U.S. Supreme Court found that the Fifth Amendment privilege played an integral role in protecting "the privacies of life,"[207] the modern Court has reduced its role to bar the government from compelling someone to provide testimony that is "incriminating."[208]

The Fifth Amendment privilege only comes into play when all three elements are present, i.e., when someone is *compelled* to provide *testimony* that is *incriminating*.[209] Compulsion usually takes the form of a grand jury subpoena enforceable by civil contempt sanctions.[210] The compulsion must seek to extort testimony, or oral or written communications from an

---

GEO. WASH. L. REV. 529, 541-42, 542 nn.94-95 (1978) (suggesting that privacy only exists for the wealthy).

206. *See, e.g.*, Ensure Privacy, *available at* http://www.ensureprivacy.com (last visited Dec. 4, 2002) (purveyor of technological devices to prevent the use of wiretaps and other surveillance technology). Another example involves cell phones: the content of conversations on analog cell phones can easily be overheard by someone using a scanner; digital cell phone transmissions are scrambled and therefore provide more protection. *See, e.g.*, Cell Phone Security, Computing at Cornell, *available at* http://www.cit.cornell.edu/cellphone/security.html (last visited Dec. 18, 2002).

207. Boyd v. United States, 116 U.S. 616, 630 (1886).

208. *See, e.g.*, United States v. Braswell, 465 U.S. 605, 611 n.8 (1984); Fisher v. United States, 425 U.S. 391, 399 (1976). *See also* Andresen v. Maryland 427 U.S. 463, 472 (1976). The three requirements derive from the language the amendment uses to establish the privilege against self-incrimination, e.g., that "No person . . . shall be compelled in any criminal case to be a witness against himself". U.S. CONST. amend. V.

209. *See, e.g., Fisher*, 425 U.S. at 409.

210. *See, e.g.*, United States v. Mandujano, 425 U.S. 564, 571-72 (1976).

individual,[211] because the Fifth Amendment privilege does not encompass physical evidence per se.[212] But the act of producing physical evidence (i.e., documents, videotapes, etc.) in response to government compulsion can itself be a testimonial act encompassed by the privilege.[213] To be testimonial, the act of producing evidence must establish that the evidence exists, that it is within the control of the person being compelled to produce it, and that the evidence produced is evidence sought by the subpoena.[214] Finally, the third requirement is that the compelled testimony be incriminating.[215] The U.S. Supreme Court has held that the privilege "not only extends to answers that would in themselves support a conviction under a . . . criminal statute but likewise embraces those which would furnish a link in the chain of evidence needed to prosecute the claimant for a . . . crime."[216]

The requirement that all three elements be present accounts for the limited role the Fifth Amendment plays in guaranteeing on-line privacy. Actually, the primary obstacles are the first two elements, the requirements that the government must seek to compel someone to provide testimony.[217]

Because cyberspace is a perceived reality that emerges from communicative activity,[218] much of what comprises cyberspace qualifies as testimony that could be encompassed by the Fifth Amendment

---

211. Corporations and other artificial entities are not protected by the Fifth amendment privilege. *See, e.g.*, Braswell v. United States, 487 U.S. 99, 105-08 (1988).

212. *See, e.g.*, Schmerber v. California, 384 U.S. 757, 763-64 (1966) ("It is clear that the protection of the privilege reaches an accused's communications, whatever form they might take . . . but that compulsion which makes a suspect or accused the source of 'real or physical evidence' does not violate it" (citations omitted)). *See also, Fisher*, 425 U.S. at 408.

213. *See Fisher*, 425 U.S. at 409.

214. *See id.* at 409. *See also* United States v. Hubbell, 530 U.S. 27, 36-37 (2000).

215. *See supra* text accompanying note 213; *see also* U.S. CONST. amend. V.

216. Hoffman v. United States, 341 U.S. 479, 486 (1951).

217. *See supra* text accompanying note 213; *see also* U.S. CONST. amend. V.

218. *See* GIBSON, *supra* note 134, at 51; *see* Benschop, *supra* note 135.

privilege.[219] The problem is that this testimony was not compelled by the government.

The Fifth Amendment provides no protection for communications that are made voluntarily. All voluntary statements waive the privilege.[220] Therefore, any comments that are posted on-line are outside the privilege because the person responsible has voluntarily posted them, and thus is not compelled to "testify."[221] This is true regardless of whether the comments are posted in public areas such as web sites or newsgroups, or in private conversations in a chat room. Someone in a chat room chatting with an undercover officer is under no compulsion to have that conversation; indeed, one cannot be under any official compulsion because one is unaware that one is speaking to an agent of the state.[222] Therefore, as to the content of communications posted on-line, compulsion is lacking.

---

219. Testimony is an act that, "must itself, explicitly or implicitly, relate a factual assertion or disclose information." *See* Doe v. United States, 487 U.S. 201, 210 (1988). Most of the constituent elements of cyberspace, e.g., web sites, postings to newsgroups, conversations in "chat rooms," and e-mail clearly qualify as testimony under this definition because it involves making factual assertions and disclosing information. The facts asserted or the information disclosed may be false; however, testimony can be true or false. What is important in determining whether or not a discrete component of cyberspace satisfies this test is whether it communicates something factual. While much of what appears in cyberspace takes the form of textual communication, it is not the only form in which information can be communicated and thereby qualify as testimony. For example, it is possible to infer factual assertions from the graphical components of at least some web sites. Unlike the physiological processes which the U.S. Supreme Court have found to yield physical evidence instead of testimony, the intellectual process involved in designing the non-textual aspects of a web site can produce implicit testimonial communications. *See, e.g.*, United States v. Dionisio, 410 U.S. 1, 7 (1973) (suspect did not provide testimony by simply reading transcript; the purpose was to obtain a sample that could be used to measure the physical properties of his voice); *see also* Gilbert v. California, 388 U.S. 263, 266-67 (1967) (requiring suspect to provide samples of his handwriting by copying letters and symbols as directed did not elicit testimony).

220. *See, e.g.*, United States v. Mandujano, 425 U.S. 564, 571-72 (1976).

221. The U.S. Supreme Court has held that the rule governing voluntary statements applies to documents. By preparing a document, a person voluntarily gives the testimony it contains and therefore cannot claim the privilege as to its contents. *See* United States v. Doe, 465 U.S. 605, 610-11 (1984); *see also* Fisher v. United States, 425 U.S. 391, 409-10 (1976). The U.S. Supreme Court has indicated that diaries may be governed by a different rule. *See id.* at 401 n.7 ("Special problems of privacy which might be presented by subpoena of a personal diary . . . are not presented here") (citing United States v. Bennett, 409 F.2d 888, 897 (2d Cir. 1969)).

222. *See, e.g.*, Hoffa v. United States, 385 U.S. 293, 303-04 (1966) (a Fifth Amendment privilege is not implicated by the use of undercover agents before charges are filed because of the lack of compulsion).

The area in which the Fifth Amendment can come into play involves the use of encryption.[223] Section III of this Article explained that to invoke the Fourth Amendment's privacy privilege for the content of on-line communications such as e-mail, the correspondents must take steps to ensure that the content cannot be read by anyone other than the sender and the intended recipient. The solution is to use encryption:

> codes that convert information into a secret form. Cryptography has been used in one form or another since ancient times, but today, the widespread use of computers has enabled cryptographic techniques to become widely available and potentially very secure. Modern computerized cryptography uses encryption algorithms to keep digital information private, and the most complex of these algorithms can encode data so thoroughly that it would take millennia to decipher it with current technology.[224]

Encryption can also be used to protect data files stored in a computer or on other storage media.[225] Assuming files are encrypted with an unbreakable encryption algorithm,[226] the only way that law enforcement can access the content of those files is to use the password that can be used to decrypt the files.[227]

However, what if the owner of the files refuses to give up the password? If law enforcement officers ask for the password, the owner can refuse to give it to them and will face no consequences unless a statutory scheme requires the surrender of encryption passwords has been enacted.[228]

---

223. *See infra* text accompanying note 212.

224. D. Forest Wolfe, Comment, *The Government's Right to Read: Maintaining State Access to Digital Data in the Age of Impenetrable Encryption*, 49 EMORY L.J. 711, 712 (2000) (footnotes omitted). *See, e.g.*, Hushmail.com, *available at* https://www.hushmail.com/?PHPSESSID=612acb585080cf64c11c6e007408ee8b (last visited Oct. 28, 2002); VME Explained, *available at* http://www.meganet.com/Technology/explain.htm (last visited Aug. 30, 2002).

225. *See, e.g.*, Next-Generation Desktop/Laptop Data Security for the Enterprise, *available at* http://www.meganet.com/Products/VME2000/VME2000.htm (last visited Aug. 30, 2002).

226. *See, e.g.*, Christopher Wille, *Unbreakable Encryption Using One Time Pads*, AspHeute.com (Sept. 24, 2001), *available at* http://www.aspheute.com/english/20010924.asp (last visited Aug. 30, 2002).

227. *See, e.g.*, Bert-Jaap Koops, *What is Cryptography?*, *in* CRYPTO AND SELF-INCRIMINATION FAQ (1999), *available at* http://rechten.uvt.nl/koops/casi-faq.htm#1.2 (last visited Dec. 18, 2002); *see also* What is Public-Key Crytography?, *available at* http://www.rsasecurity.com/rsalabs/faq/2-1-1.html (last visited Dec. 9, 2002).

228. As Section III of this Article explained, officers can use a keystroke logger to seize the encryption key, which implicates Fourth Amendment concerns.

The viability of such a scheme is addressed below. On the other hand, if a grand jury issues a subpoena to the owner directing him to produce the password to the grand jury, this raises the possibility for invoking the Fifth Amendment privilege against self-incrimination.

The subpoena establishes compulsion and it is reasonable to assume, if only for the purposes of this analysis, that the contents of the encrypted files will incriminate their owner.[229] Therefore, the critical question is whether or not the subpoena compels the production of incriminating testimony. Answering this question requires considering two different scenarios. In the first, the owner of the files committed the password to memory and would have to appear before the grand jury and tell them what the password is. In the second scenario, the owner of the files recorded the password somewhere, in a diary, for example. In order to produce this password for the grand jury the owner would have to give the grand jury the entry in the diary.[230]

If the owner of the files committed the password to memory, then the Fifth Amendment privilege also privileges the owner to refuse to recite it before the grand jury as long as the contents of the files are incriminating. Reciting the password to the grand jury constitutes a factual assertion: the owner is being asked what password is needed to encrypt these files; if answered, the response is a factual assertion in the form of the password which establishes testimony.[231] Although the password itself may not be incriminating, it becomes a link in the chain of evidence needed to prosecute the file owner if the contents of the files are incriminating. The

---

229. More precisely, it is reasonable to assume that the contents of the files will incriminate their owner in some already completed criminal activity. *Cf.* United States v. Freed, 401 U.S. 601, 606-07 (1971) (Fifth Amendment privilege cannot be claimed to insulate one from liability for criminal activity yet to be committed).

230. There can be a third scenario: The owner of the files can encrypt them and throw away the encryption key but not before he "perform[s] a mathematical operation on the encryption key which produces a new [key] number. While this new number cannot be used directly to decrypt the [files], the original key can be recovered using this new number." James D. Miller & Lixin Gao, *Creating a Subpoena-Proof Diary: A Technological Solution to a Legal Problem*, 2001(3) J. INFO. L. & TECH., *available at* http://elj.warwick.ac.uk/jilt/01-3/miller.html (last visited Aug. 30, 2002). Since it will take some time to recover the original key, the files are effectively locked until that can be done. *See id.* The analysis presented in the text above encompasses this scenario, as well; the only difference is that the focus would be on requiring the owner to produce the number that can be used to recover the original encryption key, instead of on the original key itself.

231. *See, e.g.*, United States v. Hubbell, 530 U.S. 27, 43 (2000). *See* also United States v. Doe, 487 U.S. 201, 210 n.9 (1988). *See generally* United States v. Matos, 990 F. Supp. 141, 144 (E.D.N.Y. 1998) (asking witness "How do you spell drawers?" and having him spell the word would elicit testimony).

government cannot access the contents of those files unless the file owner identifies what the password is in testimony.[232] But while the privilege would protect someone from being compelled to recite a memorized encryption password, the government could override the claim of the privilege by granting the person immunity for the act of producing the password.[233]

Now assume the password was recorded as a diary entry.[234] The password itself is not testimony, it is an artifact, not a communication.[235] The government has the files, but their content is inaccessible without the password.[236] However, if the owner delivers the password to the grand jury, it can be used to produce the contents of the encrypted files. The issue therefore is whether the owner's act of giving the entry containing the password to the grand jury is a testimonial act of production encompassed by the privilege against self-incrimination.[237] If the act of providing the

---

232. *See supra* text accompanying note 216.

233. *See, e.g., Hubbell*, 530 U.S. at 39-42.

234. For the purpose of this analysis, it is irrelevant whether the entry was made in a paper diary or in a computer-generated diary. The type of record is not important; what is important is that the key has been transformed from mere memory into a tangible record.

235. *See, e.g.*, Wolfe, *supra* note 224, at 737-38 (An encryption key can be a legitimate word or sentence, but much more often it is a collection of unintelligible bits. Even if it were a sentence, it is unlikely that a criminal would make it an incriminating sentence (such as "IMGUILTY"). *But see* Greg S. Sergienko, *Self Incrimination and Crypto Keys*, 2 RICH. J.L. & TECH. 1 (1996) (key could be given "incriminating, testimonial content by making it a word or phrase that confesses to a crime" which carries little likelihood of prosecution "thereby triggering potential criminal liability and therefore the protection of the Fifth Amendment" with little risk).

Presumably, even if the content of a key were construed as "testimony," that testimony would not be protected by the Fifth Amendment because it would have been given voluntarily. *See supra* text accompanying note 220. The only question that could arise in the scenario given above is whether the fact the key was recorded in a diary matters. *See supra* text accompanying note 221.

236. The discussion above assumes the government already has the encrypted files because if it does not, then the owner would also be required to physically produce the files to the grand jury. The act of delivering the data files would be a testimonial act under the Fifth Amendment unless the government already knew they existed and knew the owner had them. The U.S. Supreme Court has held that if these issues are a "foregone conclusion," i.e., are already within the government's knowledge, then the act of producing evidence is not testimonial because it does not "tell" the government anything. *See, e.g.*, Fisher v. United States, 425 U.S. 391, 411 (1976). If the grand jury issued a subpoena that directed the owner to produce "any and all encrypted files that may be in your possession," his producing such files would "tell" the government something it apparently does not know; if, on the other hand, the subpoena directed the owner to produce encrypted files that were described with great specificity, his producing them would not "tell" the government anything it does not already know and would not, therefore, be testimonial.

237. If the government does not know that the owner has the key, then the act of handing over the recorded entry would itself be a testimonial act of production within the scope of the privilege.

password is testimony, the owner can claim the privilege because the elements of compulsion and incrimination are present. If the act of providing the password is not testimonial, the owner cannot claim the privilege.

While the U.S. Supreme Court has not addressed this particular situation, it has indicated that the act of producing the key to a strongbox containing incriminating documents is not testimony within the scope of the Fifth Amendment privilege, but the act of reciting the combination to a wall safe containing such documents is.[238] The distinction the Court draws is whether the act in question requires an individual to express "the contents of his own mind."[239] Handing over a tangible key is a purely physical act like the other acts the Court has found not to be testimonial.[240] However, reciting a combination does require the person to use one's mind to make a factual assertion, e.g., "the combination to the safe is . . . ."[241] When the encryption password was recorded, it assumed tangible form and became an artifact like the key to a strongbox. Since the password has an independent, external existence, the owner of the files can give the password to the grand jury without having to communicate the contents of his own mind. Consequently, the Fifth Amendment privilege cannot apply to this act.

The analysis thus far is based on scenarios in which a grand jury subpoenas an encryption password. What role, if any, does the Fifth Amendment play when law enforcement officers approach someone and ask him or her to surrender an encryption password? Another question that arises asks what role the Fifth Amendment plays when law enforcement officers approach someone and ask him or her to surrender the encryption password. If a password holder elects to comply, either by reciting a memorized password or handing over a recorded password, it would be a voluntary act outside the scope of the privilege against self-incrimination. The password holder can, on the other hand, decline to provide the

---

By giving the grand jury the key, the owner "tells" the state something it did not already know, e.g., that he has the key needed to encrypt the files. The scenario above, however, makes the logical assumption on the facts given, i.e., that the government already knows the owner has the key and is simply seeking possession of it. Under the "foregone conclusion" exception to the act of production doctrine, merely producing what the government knows you have is not a testimonial act. *See supra* note 224. *See also* Philip R. Reitinger, *Compelled Production of Plaintext and Keys*, 1996 U. CHI. LEGAL F. 171 (1996).

238. *See Hubbell*, 530 U.S. at 43; United States v. Doe, 487 U.S. 201, 210 n.9 (1988).

239. *See* United States v. Doe, 487 U.S. 201, 210 n.9.

240. *See supra* text accompanying note 219.

241. *See supra* text accompanying note 231.

password without consequence because officers currently cannot compel someone to comply with the request.[242] Could law enforcement be given that ability? Could a statute be enacted that makes it a crime to refuse to produce an encryption password to officers upon request?[243] Such a statute could certainly be adopted, but its application would be unconstitutional if the holder of a password could invoke the Fifth Amendment privilege as the basis for refusing to produce the password. The password holder would be faced with the alternatives of giving up the password and thereby providing incriminating testimony or refusing to give it up and being held criminally liable for refusing.

This dilemma violates the Fifth Amendment, which guarantees the right to refuse to provide incriminating "testimony."[244] Enforcing the statute would, in other words, be unconstitutional (a) when the password holder had memorized the password[245] and (b) when the government previously did not know that this specific person was actually the possessor of a password (in whatever form).[246] Enforcing the statute in these instances would not, however, violate the Fifth Amendment if the statute gave the password holder immunity for the act of producing the password.[247] Even absent a grant of immunity, enforcing the statute would not violate the Fifth Amendment if the government knew that the person possessed a password that had been reduced to tangible recorded form.

---

242. As Section III explained, the officers can bypass this step by using a keystroke logger to "seize" the encryption key. Because this involves a "search" and "seizure," it implicates the Fourth Amendment, not the Fifth Amendment's privilege against self-incrimination.

243. *See, e.g.*, Regulation of Investigatory Powers Act 2000, Part III — § 49 (Eng.) (judge can impose "a disclosure requirement" for an encryption key), *available at* http://www.hmso.gov.uk/acts/acts2000/00023--e.htm#49 (last visited Aug. 30, 2002). *See also* Regulation of Investigatory Powers Act 2000, Part III — § 53(1) (Eng.) (offense to knowingly fail to provide encryption key if directed to do so), *available at* http://www.hmso.gov.uk/acts/acts2000/00023--e.htm#53 (last visited Aug. 30, 2002).

244. *See, e.g.*, Gardner v. Broderick, 392 U.S. 273, 279 (1968) ("the mandate of the great privilege against self-incrimination does not tolerate the attempt, regardless of its ultimate effectiveness, to coerce a waiver of the immunity it confers"). This dilemma is not a problem in legal systems that do not have comparable protection against self-incrimination. *See, e.g.*, Criminal Justice and Public Order Act 1994, Part III — §§ 34-37 (inferences from silence), *available at* http://www.legislation.hmso.gov.uk/acts/acts1994/Ukpga_19940033_en_1.htm (last visited Dec. 18, 2002).

245. *See supra* text accompanying note 231.

246. *See supra* note 237.

247. Granting immunity for statutorily compelled disclosures has been found to satisfy the Fifth Amendment. *See, e.g.*, 26 U.S.C. § 4424(c)(1) (2002). *See also* Clifft v. Ind. Dep't of State Revenue, 660 N.E.2d 310, 317 (Ind. 1995); Zissi v. State Tax Comm'n of Utah, 842 P.2d 848, 857 (Utah 1992).

Instead of criminalizing the refusal to surrender encryption passwords, which does raise Fifth Amendment issues, another option is to require individuals to escrow their encryption passwords with the government or some trusted third party.[248] Such a requirement would not violate the Fifth Amendment because the escrowed password could not be used to produce evidence that would incriminate the owner in crimes that were already committed before the password was given to the escrow agent.[249] The owner could not invoke the Fifth Amendment for crimes committed after the password was sent into escrow because the Fifth Amendment provides no protection against incriminating oneself for crimes not yet committed.[250]

V. THE PRIVILEGE OF BEING LET ALONE

The right to be let alone postulated by Justices Brandeis and Warren at the end of the Nineteenth Century[251] became the privilege of being let alone in the Twenty-First Century. Unlike the right to be let alone, which was conceived as a civil remedy for invasions perpetrated by the media and other non-state actors,[252] the privilege of being let alone is of constitutional import that concerns state action. It is designed to maintain a fair balance

---

248. *See, e.g.*, H. Abelson et al., *The Risks of Key Recovery, Key Escrow and Trusted Third-Party Encryption*, Center for Democracy and Technology (Rev. 1998 version), *available at* http://www.cdt.org/crypto/risks98/ (last visited Sept. 3, 2002).

249. Since the key must be escrowed before it is used, it cannot have been employed to commit and/or to conceal the commission of past crimes. The key could, of course, be used to encrypt subsequently generated evidence pertaining to the commission of past crimes, such as a diary describing prior misdeeds. Assuming diaries are encompassed by the rule which dictates that voluntarily created documents are not protected by the Fifth Amendment, the use of the key to decrypt the diary would not violate the key owner's privilege against self-incrimination. *See supra* text accompanying note 221. The contents of the diary are not protected because they represent testimony that was given voluntarily; even if the key is considered "testimony," it is testimony which the key owner voluntarily gave to the escrow agent; and the act of production doctrine does not apply because law enforcement officers use a search warrant to obtain the key from the escrow agent — the owner is not compelled to produce it. *See, e.g.*, David B. Walker, *Privacy in the Digital Age: Encryption Policy — A Call for Congressional Action*, 3 STAN. TECH. L. REV. 59-65 (1999).

250. As noted above, even if the contents of the key are assumed to be testimonial, the key was created voluntarily and is not protected by the privilege; and since law enforcement obtains the key from the escrow agent, under the authorization of a search warrant, the owner of the key is not compelled to produce it.

251. *See supra* note 14.

252. *See, e.g.*, Gormly, *supra* note 3, at 1343-52.

between the interest of individuals in being free from official scrutiny and the need of the government to collect evidence of criminal activity.

The privilege of being let alone is an amalgam of privacy protections derived from the First, Fourth, and Fifth Amendments. The protection against self-incrimination from the Fifth Amendment is the only one of the guarantees that has traditionally been characterized as a privilege, not as a right. This characterization in no way diminishes the strength of the protection provided by the Fifth Amendment. Instead, it accurately captures the way the guarantee is operationalized. The Fifth Amendment puts the obligation on the individual to invoke the protection against self-incrimination.[253] Once invoked, the obligation shifts to the government, who then honors the invocation.[254] This aspect of the Fifth Amendment guarantee results because it functions in a manner analogous to evidentiary privileges. Like those privileges, the Fifth Amendment protects testimony, and also like them, it must be invoked to be effective. Requiring invocation gives people a choice: to maintain the confidences protected by the privilege or to waive the privilege and breach confidentiality.

This characterization has not traditionally been applied to the Fourth Amendment guarantee against unreasonable searches, which may not seem to be at all analogous to testimonial privilege. As Section III demonstrates, however, the privacy protections of the Fourth Amendment are properly cast as a privilege. The same is true of the guarantee of anonymity and confidentiality from the First Amendment. Unlike a right, which puts the onus of initiating the protection on the state, the protection of anonymity and confidentiality from the First Amendment must be invoked before the government will be required to take action to safeguard those interests. One must, in other words, don a mask in the real world or take measures to conceal one's identity in the cyberworld if one wishes to claim the "privilege of anonymity" of the First Amendment.[255]

These three guarantees are all correctly characterized as privileges because each protects privacy. The First Amendment protects the privacy of the identity and associates of an individual; the Fourth Amendment protects the privacy of the activities of an individual; and the Fifth Amendment protects the privacy of the thoughts of an individual. The degree to which they protect these different privacy interests has evolved significantly since Justices Brandeis and Warren wrote in 1890. This evolution is directly attributable to the increased sophistication and

253. *See supra* note 146 and accompanying text.

254. *See id.*

255. *See infra* Section III.

proliferation of technology. This evolution is also responsible for the shift from the *Olmstead* holding to the *Katz* holding. When the decision was made by *Olmstead* Court, wiretaps were in their infancy and were therefore an exceedingly uncommon event. By the time the decision was made by the *Katz* Court, surveillance technology had become very sophisticated, due in large part to advances made during World War II, and the ability of the government to spy on the activities of people had become a matter of public concern. In changing the focus of the privacy protections of the Fourth Amendment from places to people, the *Katz* Court sought to create a more dynamic standard, one that could be used to address the increasing invasiveness made possible by technology.

Prior to the development and proliferation of telephone technology, which proved very problematic for the *Olmstead* Court, privacy was a static concept solidly rooted in the real world. In that era, and for centuries before, ensuring the privacy of the activities of oneself was a matter of creating secure spaces — building walls and fences, closing and shuttering windows and retreating into the enclosures one thereby created. Telephone technology was the first mediated communication to transcend physical space. With the telephone, people separated by miles can engage in direct, synchronous communication. As the *Olmstead* Court failed to recognize, the transcendence of this communication required the formulation of a new approach to privacy, a dynamic approach that could evolve as technology evolved. That was what the *Katz* Court sought to do. By holding that the privacy guarantee in the Fourth Amendment "protects people, not places,"[256] the *Katz* Court took the first step toward recognizing the privilege of being let alone.

In the years since the *Katz* decision, technology has developed beyond the imagination of those who recognized that privacy must be defined by what people do, not by where they do it. New forms of mediated communication have emerged, creating the experiential world of cyberspace. New types of real world surveillance technology has developed, further threatening the privacy of life in the real world. Recasting the First and Fourth Amendment guarantees as privileges and then combining them with the Fifth Amendment to create a privilege of being let alone is the way to achieve a comprehensive, dynamic standard that can evolve as technology evolves.

Casting privacy guarantees as a privilege is appropriate because privacy is intrinsically an oppositional concept. Privacy is, by its very nature, an

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

antonym; it is prospective resistance to efforts to intrude where intrusion would be unwelcome. It is also a social construct. As the *Katz* Court recognized, the threshold level of privacy entitled to constitutional protection is defined not by Congress or the courts, but rather by what society is prepared to regard as reasonable. Although the *Katz* Court articulated this in the context of the privacy protections of the Fourth Amendment, it is also applicable to the protections provided by the First and Fifth Amendments. As to the First Amendment, this is apparent in the boundaries set on the uses of anonymity. Some uses are criminalized because it would not be reasonable to let anonymity be exploited to victimize others.[257] It is also apparent in the refusal of the U.S. Supreme Court to extend the Fifth Amendment privilege against self-incrimination to encompass statements voluntarily made to others, on the grounds that it would be unreasonable.[258]

The privilege to be let alone fashioned from these guarantees is an empirically grounded device that will allow the constitutional protection of individual privacy to evolve as technology evolves. It ensures the dynamism the *Katz* Court sought by first, requiring that the privilege be invoked to be effective and second, by using societal expectations to determine when such invocation is effective. This effectively imports contemporaneous technology into the interaction between individuals and the state. Nothing in the U.S. Constitution prevents law enforcement officers from monitoring the public areas of the real world and the cyberworld. Indeed, it is their duty.[259] If individuals want to maintain their privacy, therefore, they must use whatever technologies are effective to shield their identities, their activities, and their thoughts from the observant eyes of the state.

---

257. *See, e.g.*, Simoni, *supra* note 73, at 250 ("Few . . . would argue that preventing crime is not an important or substantial government interest" justifying the criminalization of anonymity).

258. *See, e.g.*, Illinois v. Perkins, 496 U.S. 292, 298 (1990) (Fifth Amendment does not protect someone from boasting about his criminal activities to those he believes to be sympathetic); Hoffa v. United States, 385 U.S. 293, 304 (1966).

259. "Police officers do not — indeed, the public would not want them to — close their eyes to obvious crime-related information placed in front of them". United States v. Waletzki, 1997 U.S. App. LEXIS 23697 (7th Cir. 1997).