DePaul Law Review

Volume 54
Issue 3 *Spring 2005: Symposium - Privacy and Identity: Constructing, Maintaining, and Protecting Personhood*

Article 9

Doors, Envelopes, and Encryption: The Uncertain Role of Precautions in Fourth Amendment Law

Lee Tien

DOORS, ENVELOPES, AND ENCRYPTION: THE UNCERTAIN ROLE OF PRECAUTIONS IN FOURTH AMENDMENT LAW

*Lee Tien**

INTRODUCTION

We conventionally understand the Fourth Amendment as securing our privacy against arbitrary or unreasonable government searches.[1] Searches of the home usually require a judicially issued warrant based on probable cause that evidence will be found. Searches that infringe privacy by capturing the content of communications, like eavesdropping on conversations and wiretapping of phone calls, are (at least in theory) tightly regulated.

But does the Fourth Amendment secure a right to *protect* our privacy? We normally produce privacy by taking precautions: We whisper to confidants or confide only in people we trust, enclose letters in envelopes, close bathroom doors, and draw curtains. If I wanted to make an untraceable, anonymous phone call, I would probably use a coin payphone. We take for granted that we may and can do these things to protect our privacy against prying ears or eyes. Do we actually have a right to do these things?

Think for a moment of the various ways that the law could restrict precautions-taking in order to make surveillance easier. The government could directly target precautionary acts, such as requiring us to use postcards or subjecting us to criminal liability if we use envelopes. The government could restrict the resources needed for precautionary acts, like envelopes (paper or digital) or doors.

Precautions are crucial to modern Fourth Amendment search law. As the Supreme Court said in *Katz v. United States*:

> [A] person in a telephone booth may rely upon the protection of the Fourth Amendment. One who occupies it, *shuts the door behind*

* Lee Tien is a Senior Staff Attorney with the Electronic Frontier Foundation, which specializes in free speech law, including intersections with intellectual property and privacy law. This Article grew out of a presentation made during the Symposium: *Privacy and Identity: Constructing, Maintaining, and Protecting Personhood*, held on March 13, 2004 at DePaul University College of Law.

1. This Article does not address Fourth Amendment seizures or searches incident to seizures, such as arrests.

> *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.[2]

At the very least, *Katz* means that one may be able to create a legally cognizable reasonable expectation of privacy by taking a precaution like closing a door. In short, the possibility of Fourth Amendment privacy has been closely tied to the taking of privacy precautions ever since *Katz*.[3] But what privacy precautions are actually possible, and how many of these precautions are protected, is unclear. After all, Katz could only "shut the door behind him" because there was a door to close.[4]

The Supreme Court understood that when Katz closed the phone booth door, he created a temporary zone of personal privacy that society recognizes. What if there had been no door? How much did the door really matter, doctrinally speaking?

In *United States v. Muckenthaler*,[5] the defendants, relying on *Katz*, contended that the arrest warrant was based on unconstitutionally gained evidence: A police officer positioned himself so as to overhear parts of a telephone conversation.[6] The United States Court of Appeals for the Eighth Circuit distinguished *Katz* partly because the defendant "was talking on a telephone attached to a post around which were three other telephones . . . and none of them was enclosed."[7] As a result, the police officer "was in a position where another individual would normally be expected to be," and anyone "in that position was likely to overhear portions of a conversation at any of the other telephones."[8]

The example of a phone booth door illustrates a simple point: One usually needs some resource, like a door, wall, or envelope, in order to produce privacy in the first place. Taking those resources away—eliminating the ability to take precautions—can be a very effective way to destroy privacy because "[w]hat a person knowingly exposes to

---

2. 389 U.S. 347, 352 (1967) (emphasis added).

3. *See, e.g.*, Melissa Arbus, Note, *A Legal U-Turn: The Rehnquist Court Changes Directions and Steers Back to the Privacy Norms of the Warren Era*, 89 VA. L. REV. 1729, 1737 (2003) (stating that *Katz* stands for the principle that Fourth Amendment protection is triggered when people "take everyday, conventional measures to maintain their privacy").

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

5. United States v. Muckenthaler, 584 F.2d 240 (8th Cir. 1978).

6. *Muckenthaler*, 584 F.2d at 243.

7. *Id.* at 245.

8. *Id.*; *see also* State v. Constantino, 603 A.2d 173, 176 (N.J. Super Ct. 1991) (stating that the defendant had no reasonable expectation of privacy because he "was talking on a public pay phone . . . [that] was not enclosed by a glass or metal booth and was located in a public place").

the public . . . is not a subject of Fourth Amendment protection."[9] Even without outright criminalization or resource prohibition, the government could make it harder for us to take precautions—or it could make the precautions we do take less effective. Relatively little attention has been paid to the right to take privacy precautions.[10] Fourth Amendment search law is mostly about government action that violates our personal or informational boundaries or is directed at collecting information. Banning envelopes clearly reduces our privacy, but is not obviously a search in itself. Diluting or discouraging precautions looks even less like a search.[11]

This Article addresses the question: To what extent do we have the right to protect our privacy? At one level, the answer is obvious. There must be some right to take precautions. After all, one often does not even have a reasonable expectation of privacy without precautions, whether preexisting (like the architecture of phone booths and their doors) or created in real time (like whispering). Taking precautions is generally a necessary, if not always sufficient, condition for enjoying Fourth Amendment privacy.[12] It seems intuitively clear that the Fourth Amendment would be violated if the government enacted a law banning phone booth doors the day after *Katz* was decided. If the law says that we have no reasonable expectation of privacy unless we take precautions, then we ought to be able to take those necessary precautions.[13]

This Article attempts to unpack some of the conceptual issues surrounding precautions and the Fourth Amendment. My thesis is that the Fourth Amendment restricts state action that unduly burdens people's ability to take precautions, much as the First Amendment restricts state action that unduly burdens speech. This Article further argues that there is a constitutional cluster of rights surrounding the taking of privacy precautions. We have a privilege to take privacy precautions, a claim against the government that it may not interfere in certain ways with actions under that privilege, and an immunity

9. *Katz*, 389 U.S. at 351.

10. For a useful discussion of precautions and privacy, see Arbus, *supra* note 3. *See also* William Heffernan, *Fourth Amendment Privacy Interests*, 92 J. CRIM. L. & CRIMINOLOGY 1, 32–63 (2002) (contrasting the "vigilance" and "forbearance" approaches to privacy).

11. *See, e.g.*, United States v. Karo, 468 U.S. 705, 712 (1984) (involving installation of an unmonitored beeper in an automobile). The Court stated that this "created a potential for an invasion of privacy, but we have never held that potential, as opposed to actual, invasions of privacy constitute searches for purposes for the Fourth Amendment." *Id.*

12. *See, e.g.*, *Katz*, 389 U.S. at 361 (Harlan, J., concurring) (Fourth Amendment protection requires that "a person have exhibited an actual (subjective) expectation of privacy.").

13. What a person "seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected." *Katz*, 389 U.S. at 351 (footnotes omitted).

against government attempts to reshape that privilege. This combination of privilege, claim, and immunity may be referred to as the "precautions cluster-right."

Legislation that bans or discourages precautions or their use must, therefore, be subject to significant constitutional scrutiny. I do not assume or argue as a normative matter that we must take precautions in order to be protected by the Fourth Amendment.[14] As discussed below, the Fourth Amendment, however, places great importance upon those precautions we do take.

The precautions cluster-right raises one major question. Does it include an immunity against the government? In other words, does the government lack the power to deprive us of the right to take precautions? Some argue that the government has a right to an effective search and therefore the power to restrict precautions that would interfere with that right.[15] I argue that we must have such an immunity because the well recognized right that the government may not search us unreasonably does not make sense unless we also have the precautions cluster-right.[16]

Part II briefly analyzes precautions and introduces the issue in somewhat more detail, including how the Supreme Court has addressed precautions, how precautions relate to privacy, what kinds of precautions there are, and whether they are all the same. It also sets forth a rough analytical framework for thinking about the Fourth Amendment and precautions. Part III attempts to ground the precautions cluster-right doctrinally and normatively. Part IV further details what the right might actually entail, by discussing the ideas of crippled encryption and mandated "tappability" in the context of the Communications Assistance for Law Enforcement Act (CALEA).

II. WHY PRECAUTIONS MATTER AND WHAT THEY ARE

In common privacy practices, privacy is a function of privacy precautions. We put letters into envelopes. We promise to keep others'

14. For instance, the fact that we do not defend against technologies that can "see" through walls should not constitute "knowing exposure" of in-home activities. Christopher Slobogin, *Peeping Techno-Toms and the Fourth Amendment: Seeing Through* Kyllo*'s Rules Governing Technological Surveillance*, 86 MINN. L. REV. 1393, 1411 (2002) ("Members of our society should be constitutionally entitled to expect that government will refrain from *any* spying on the home—technological or otherwise—unless it can demonstrate good cause for doing so.").

15. *See, e.g.*, Lawrence Lessig, *Reading the Constitution in Cyberspace*, 45 EMORY L.J. 869, 880–82 (1996).

16. Given the complexity of the subject, I do not pretend that this analysis is complete. I believe, however, that we will never approach a coherent analysis of Fourth Amendment privacy without a framework for thinking about precautions.

secrets. Even in a crowded room, a couple may produce some conversational privacy by whispering.

Many scholars have written about the relation of precautions to the existence of a Fourth Amendment reasonable expectation of privacy.[17] But a very different question—whether we have any kind of constitutional right to take those precautions in the first place—has hardly been addressed.[18] I will focus on the following four issues here, mostly in a descriptive vein: (1) How the Supreme Court has viewed precautions and the Fourth Amendment; (2) the kinds of precautions that we use to protect our privacy; (3) the ways that government might interfere with precautions and precautions-taking; and (4) an analytical framework for thinking about rights.

A. The Doctrinal Significance of Precautions—Why Precautions Matter

Fourth Amendment search law is mostly about searches, which are "governmental inspections of activities and locations in which an individual has a reasonable expectation of privacy from observation."[19] As a result, to determine whether there has been a search, we usually ask: Does the person have a reasonable expectation of privacy, and if so, is the government's search behavior reasonable?

Whether one has any expectation of privacy (reasonable or not), often depends on whether one takes precautions (consciously or not), which in turn depends on whether one can actually do so.[20] Many

17. *See, e.g.*, Thomas Clancy, *Coping with Technological Change:* Kyllo *and the Proper Analytical Structure to Measure the Scope of Fourth Amendment Rights*, 72 MISS. L.J. 525, 532–35 (2002) (arguing that the Court has "too readily made privacy expectations contingent on technology," as well on "observability"); David Harris, *Superman's New X-Ray Vision and the Fourth Amendment: The New Gun Detection Technology*, 69 TEMP. L. REV. 1, 18 (1996) ("Fourth Amendment protection depends not only on how an individual protects his privacy, but where and in what situation he does so."); Ramsey Ramerman, Comment, *Shut the Blinds and Lock the Doors—Is That Enough?: The Scope of Fourth Amendment Protection Outside Your Own Home*, 75 WASH. L. REV. 281, 292–96 (2000).

18. *See* Heffernan, *supra* note 10, at 90–93 (discussing the role of precautions in social privacy); Arbus, *supra* note 3, at 1743–45. Ironically, a recent discussion of precautions explains how government can reshape the social environment to promote precautions against crime, including ways of negating some privacy precautions. *See generally* Neil Katyal, *Architecture and Crime Control*, 111 YALE L.J. 1039 (2002).

19. Sherry Colb, *The Qualitative Dimension of Fourth Amendment "Reasonableness"*, 98 COLUM. L. REV. 1642, 1643 (1998).

20. Christopher Slobogin, *Technologically-Assisted Physical Surveillance: The American Bar Association's Tentative Draft Standards*, 10 HARV. J.L. & TECH. 383, 392 (1997). Professor Slobogin argues that "[e]ven an area normally associated with an expectation may not be entitled to Fourth Amendment protection if no efforts are made to keep it private." *Id.* (citing United States v. Dunn, 480 U.S. 294, 298 (1987) (holding that a flashlight inspection of a barn was not a "search" because police were able to see through netting material)). *See generally*

Fourth Amendment cases have turned on whether the defendant took "normal precautions to maintain his privacy."[21]

Unfortunately, the Supreme Court has been less than clear about what makes a precaution "normal" or even effective.[22] Some commentators have even argued that the Court's view of precautions is that they are not effective unless total or perfect.[23] Such a belief that it is necessary for an individual to avail oneself of all available privacy precautions developed from a series of landmark Supreme Court cases in which the Court held that defendants who subjectively believed they had taken effective precautions, actually had failed to absolutely guard against prying eyes.

The first classic example in which an individual failed to take necessary privacy precautions is the "abandoned garbage" case, *California v. Greenwood*.[24] In *Greenwood*, a policeman received a tip that Greenwood may have been involved in drug trafficking, so he asked the trash collector to collect Greenwood's garbage bags and give them to him.[25] The officer then searched the garbage without a warrant and found evidence of drug use.[26]

The Supreme Court held that even though Greenwood may have expected that the police would not inspect his garbage, that expecta-

---

Sherry Colb, *What Is a Search? Two Conceptual Flaws in Fourth Amendment Doctrine and Some Hints of a Remedy*, 55 STAN. L. REV. 119 (2002).

21. California v. Ciraolo, 476 U.S. 207, 211 (1986) ("So far as the normal sidewalk traffic was concerned, this fence served that purpose, because respondent took normal precautions to maintain his privacy." (citation and internal quotation marks omitted)); Rawlings v. Kentucky, 448 U.S. 98, 105 (1980) (stating that "the precipitous nature of the transaction hardly supports a reasonable inference that petitioner took normal precautions to maintain his privacy").

22. Arbus, *supra* note 3, at 1739 (arguing that courts "expect[ ] precautions far beyond the bounds of what society would consider reasonable and rel[y] on the absence of such precautions as a justification for finding that the defendant did not have a reasonable expectation of privacy" (footnote omitted)); *see also* Wayne LaFave, *The Forgotten Motto of* Obsta Principiis *in Fourth Amendment Jurisprudence*, 28 ARIZ. L. REV. 291, 301–04 (1986). Professor LaFave criticizes the "knowing exposure" doctrine that "there is a dramatic difference, in privacy terms, between revealing bits and pieces of information sporadically to a small and often select group for a limited purpose and a focused police examination of the totality of that information regarding a particular individual." *Id.* at 304.

23. *See, e.g.*, Daniel Solove, *Digital Dossiers and the Dissipation of Fourth Amendment Privacy*, 75 S. CAL. L. REV. 1083, 1133 (2002) ("The Court's new conception of privacy is one of total secrecy. If any information is exposed to the public or if law enforcement officials can view something from any public vantage point, then the Court has refused to recognize a reasonable expectation of privacy"); Arbus, *supra* note 3, at 1745 ("Katz merely looked to the conventional steps taken by the individual, rather than requiring that individual to take perfect precautions," but post-*Katz* cases require "individual precautions to be nearly perfect in order to afford constitutional protections.").

24. 486 U.S. 35 (1988).

25. *Id.* at 37.

26. *Id.* at 37–38.

tion was not reasonable because the bags are "readily accessible to animals, children, scavengers, snoops, and other members of the public."[27]

Another example is *California v. Ciraolo*,[28] where police received a tip that Ciraolo may have been growing marijuana in his backyard.[29] Unable to inspect Ciraolo's backyard from the ground because of the six-foot outer fence and ten-foot inner fence, the officers secured an airplane and flew over Ciraolo's backyard without a warrant.[30]

The Supreme Court found that while Ciraolo had exhibited a subjective expectation of privacy in the contents of his backyard by enclosing it with two fences, that expectation was not objectively reasonable.[31] The Court explained, "In an age where private and commercial flight in the public airways is routine," Ciraolo could not reasonably expect that the marijuana growing in his backyard was protected from aerial observation.[32]

On the other hand, *Arizona v. Hicks*[33] suggests that the precautions sufficient to create a Fourth Amendment reasonable expectation of privacy can be quite trivial. In *Hicks*, police entered Hicks's apartment after a bullet was fired through Hicks's floor, injuring a man in the apartment below.[34] One of the officers noticed expensive stereo equipment that seemed out of place in the apartment, which led him

---

27. *Id.* at 40. The standard critique of cases like *Greenwood* is that they "ignore[ ] the actual probability of surveillance by the general public" and "fail[ ] to recognize the difference between public observation and police surveillance." Arbus, *supra* note 3, at 1747; *see also* Colb, *supra* note 20, at 127–28. The Supreme Court "treated a person who takes the risk that something might occur as having invited the materialization of that risk." *Id.* Thus, "permitt[ing] the officer to act as though the garbage, which was in fact safely enclosed within an opaque bag, had actually been strewn about by all manner of errant creatures in the neighborhood." *Id.* at 128 (footnotes omitted). Justice Brennan, in his dissent in *Greenwood*, argued:

> The mere *possibility* that unwelcome meddlers *might* open and rummage through the containers does not negate the expectation of privacy in their contents any more than the possibility of a burglary negates an expectation of privacy in the home; or the possibility of a private intrusion negates an expectation of privacy in an unopened package; or the possibility that an operator will listen in on a telephone conversation negates an expectation of privacy in the words spoken on the telephone.

Greenwood, 486 U.S. at 54.

28. 476 U.S. 207 (1986).

29. *Id.* at 209.

30. *Id.*

31. *Id.* at 213–14.

32. *Id.* at 215. Indeed, the Court even cast doubt on whether Ciraolo had exhibited a subjective expectation of privacy. *Id.* at 211 ("Yet a 10-foot fence might not shield these plants from the eyes of a citizen or a policeman perched on the top of a truck or a two-level bus.").

33. 480 U.S. 321 (1987). The Supreme Court has more recently construed *Hicks* as a "home" case, in which "*all* details are intimate details." Kyllo v. United States, 533 U.S. 27, 37 (2001).

34. *Hicks*, 480 U.S. at 323.

to suspect that the equipment was stolen.[35] On his hunch, and without a warrant, he moved some of the equipment so he could see and record the serial numbers.[36]

The Supreme Court found that a search occurred because the officer moved the equipment: "[T]aking action . . . which exposed to view concealed portions of the apartment or its contents, did produce a new invasion of [Hicks's] privacy unjustified by the exigent circumstances that validated the entry."[37] Further, the Court reasoned that the distinction between looking at something and moving it in order to see something hidden is of great consequence in Fourth Amendment analysis.[38] The Court explained, "a truly cursory inspection—one that involves merely looking at what is already exposed to view, without disturbing it—is not a 'search' for Fourth Amendment purposes, and therefore does not even require reasonable suspicion."[39] The Court reasoned that treating even a minor disturbance as less than a full-blown search would undermine the principle that the "plain view" doctrine "may not be used to extend a general exploratory search from one object to another until something incriminating at last emerges."[40]

Bond v. United States[41] points in the same direction, and further suggests that the Supreme Court may be shifting its view of how precautions relate to reasonable expectations of privacy. In *Bond*, the defendant was traveling across the country on a bus, which made a regular stop at a permanent U.S. Border Patrol checkpoint in Texas.[42] The Border Patrol agent squeezed the passengers' luggage stored in the overhead compartments.[43] When he squeezed Bond's soft-sided green canvas bag, he felt a "brick-like object" inside the bag.[44] Bond consented for the agent to open his bag, which revealed a brick of methamphetamine wrapped in duct tape and rolled in a pair of pants.[45]

Because Bond consented to the agent's opening of the bag, the key issue was whether the agent's physical manipulation of the bag was an

35. *Id.*
36. *Id.*
37. *Id.* at 325.
38. *Id.*
39. *Id.* at 328.
40. *Hicks*, 480 U.S. at 328 (quoting Coolidge v. New Hampshire, 403 U.S. 443, 466 (1971) (internal quotation marks omitted)).
41. 529 U.S. 334 (2000).
42. *Id.* at 335.
43. *Id.*
44. *Id.* at 336.
45. *Id.*

unlawful search.[46] The Supreme Court found that Bond had exhibited the requisite subjective expectation of privacy by using an opaque bag and by placing that bag in the luggage compartment directly above his seat.[47] Moreover, the Court held that Bond's privacy expectation was reasonable.[48]

Bond is significant for two reasons. First, the Supreme Court did not require extraordinary privacy precautions. Bond could have protected himself by using hard-sided luggage, much as Ciraolo could have protected himself against aerial observation by covering his entire backyard.[49] Second, the Court did not assess the privacy risk in terms of the techniques of the "snoop," as it did in *Greenwood*.[50] Instead, the Court distinguished ordinary handling of his bag from "exploratory" squeezes: "[A] bus passenger clearly expects that his bag may be handled," but "[h]e does not expect that other passengers or bus employees will, as a matter of course, feel the bag in an exploratory manner."[51] The approach in *Bond* is thus faithful to the Court's point in *Katz* that what a person "seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected."[52]

Hicks and *Bond* are also interesting because the precautions in both cases were in a sense unconscious, or at least not deliberate. Hicks almost certainly did not deliberately conceal the serial numbers of the stereo equipment; rather, it probably just happened to be the case that the serial numbers were in a place that could not be seen. Had Bond anticipated "exploratory" squeezing by law enforcement, he probably would have used hard-sided luggage.

Some readers may think that these are not examples of precautions-taking because the privacy protection was more by chance than purposive protection. At this stage in the analysis, however, it makes sense to think that precautions need not be deliberately taken and can be

---

46. *Id.*

47. *Bond*, 529 U.S. at 338–39.

48. *Id.* at 338.

49. *Id.* at 343 (Breyer, J., dissenting) (stating that "the traveler who wants to place a bag in a shared overhead bin and yet safeguard its contents from public touch should plan to pack those contents in a suitcase with hard sides").

50. Noting that "scavengers and snoops" often rummage through garbage left on the sidewalk, the Supreme Court used the behavior of "snoops" as its privacy baseline and concluded that the defendants had exposed their garbage to the public even though the garbage was in an opaque bag. California v. Greenwood, 486 U.S. 35, 40–41 n.4 (1998); *see also* Heffernan, *supra* note 10.

51. *Bond*, 529 U.S. at 338–39.

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

contextual or architectural.[53] On this view, *Hicks* and *Bond* suggest that one can have a reasonable expectation of privacy by virtue of a simple, preexisting precaution that passively protects privacy.

Another reason that precautions are important is that precautions can provide actual, as opposed to legal, privacy. In our time, the coverage of the Fourth Amendment as well as other privacy laws is unclear, especially when new technologies are at issue.[54] Thus, precautions can protect our privacy even when it is not clear that the law does—or when it is clear that the law does not. Under current law, for instance, there is no reasonable expectation of privacy in one's movements in public.[55] A person might choose to wear a mask in public to avoid public video surveillance, or use a "blocker chip" to guard against surveillance of radio frequency identification tags. Thus, the creation of actual privacy is significant for those activities that are under-protected or unprotected by the law.[56]

---

53. The most obvious reason to include contextual precautions comes from thinking about how the government might interfere with them. The government could require equipment manufacturers to put serial numbers on every exposed surface so that the police would not need to move the equipment. Alternatively, the serial numbers could be stored in radio-frequency identification (RFID) chips that law enforcement could access with a sensing device. As we live in more of a panopticon, these architectural precautions are less likely to be effective.

54. *See, e.g.*, Raymond Shih Ray Ku, *The Founders' Privacy: The Fourth Amendment and the Power of Technological Surveillance*, 86 MINN. L. REV. 1325, 1350–56 (2002) (discussing technologies for searching and protecting electronic communications); Slobogin, *supra* note 20, at 440–50 (discussing video surveillance, telescopic cameras, location-tracking devices, thermal detection devices, and weapons- and contraband-detection technologies).

55. United States v. Knotts, 460 U.S. 276, 281–82 (1983) (involving beeper tracking of an automobile). The Supreme Court stated:

> A person traveling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another. When [codefendant] Petschen traveled over the public streets he voluntarily conveyed to anyone who wanted to look the fact that he was traveling over particular roads in a particular direction, the fact of whatever stops he made, and the fact of his final destination when he exited from public roads onto private property.

Id.; *see also Katz*, 389 U.S. at 351 ("What a person knowingly exposes to the public . . . is not a subject of Fourth Amendment protection" (citations omitted)). Professor LaFave has trenchantly criticized *Knotts*:

> Only an army of bystanders, conveniently strung out on the route and who not only "wanted to look" but also wanted to pass on what they observed to the next in line, would—to use the language in *Knotts*—"have sufficed to reveal all of these facts to the police." Just why the disclosure of these fragments to an imaginary line of bystanders must be treated as a total surrender of one's expectation of privacy concerning his travels is never explained.

LaFave, *supra* note 22, at 303–04 (quoting *Knotts*, 460 U.S. at 282) (footnote omitted).

56. Importantly, these kinds of threats are posed by private parties as well as by the government. *See generally, e.g.*, Patricia Bellia, *Surveillance Law Through Cyberlaw's Lens*, 72 GEO. WASH. L. REV. 1375 (2004); Solove, *supra* note 23. Indeed, as Professor Solove argues in detail, the government routinely takes advantage of information gathered by private actors. *Id.* at

B. What Kinds of Precautions Are There?

Precautions can be classified in several different ways, depending on the purpose of the classification. Precautions can be classified on the basis of legal distinctions, physical versus social mechanisms, or passive versus active precautions.

1. Distinguishing Precautions Based on Their Legal Force

From a legal perspective, there are three kinds of precautions. First, some precautions are needed even to have a reasonable expectation of privacy. Phone booth doors represent this kind of precaution under *Katz*.[57] Second, some precautions enhance existing privacy expectations. For example, I might not only lock the door to my house but also destroy incriminating files. Alternatively, I might encrypt my phone calls so that even if my phone were tapped, the wiretapper would have difficulty understanding what I say. Finally, some precautions do not create a reasonable expectation of privacy, but nonetheless provide practical or actual privacy. One might, for instance, speak in a foreign language as protection against casual over-hearers.[58]

2. Physical Versus Social Precautions

One may also classify precautions based on whether they are primarily physical or social.[59] Many precautions work physically or technologically, by actually blocking sensory access. For example, a person may cover an unsightly scar with one's clothes or may close a door. Or a person may encrypt his or her phone calls and e-mail, making it much harder for unauthorized parties to understand the communication even if they can capture the electronic signals.

1090–92. Solove also argues that "[t]he government is increasingly contracting with private sector entities to acquire databases of personal information." *Id.* at 1095 (footnote omitted).

57. *See supra* notes 2–4 and accompanying text.

58. In *United States v. Longoria*, 177 F.3d 1179 (10th Cir. 1999), members of a narcotics conspiracy took privacy precautions by speaking in Spanish when they were around non-conspirators. *Id.* Unfortunately, they discussed their plans in the presence of a government informant who recorded the conversation and later translated it into English. *Id.* The court rejected the argument that that they had a reasonable expectation of privacy in their conversations, saying that defendant "exposed his statements by speaking in a manner clearly *audible* by the informant. His hope that the informant would not fully understand the contents of the conversation is not an expectation society is prepared to recognize as reasonable." *Id.* at 1183 (internal quotation marks and citation omitted).

59. *See, e.g.*, Heffernan, *supra* note 10, at 44–45 ("The system of privacy hinges on a series of convention-based expectations as to how people will behave: expectations about how they will respond to closed doors, sealed envelopes, markings that something is confidential, and so on."). *See also* ERVING GOFFMAN, RELATIONS IN PUBLIC 41–44 (1971) (discussing everyday use of boundary markers to define or lay claim to personal territories).

Other precautions are more social, appealing to or relying on social conventions or practices. One might share a secret with someone on the condition that he or she executes a nondisclosure agreement. One who closes the door to a bathroom stall expects as a matter of social convention that others will not peer over the top or through any opening.[60]

Some existing case law supports recognizing the legal effectiveness of social precautions. Perhaps the most obvious support comes from third-party consent cases.[61] For instance, in *United States v. Matlock*,[62] the Supreme Court found that the proper question is whether the third party "possessed sufficient common authority over or [possessed] other sufficient relationship to the premises" such that one could validly admit the police to the premises.[63] Co-tenants could therefore agree that certain parts of a house are not common areas and instead belong exclusively to one person.[64] If so, it should also be possible for other private agreements to provide effective precautions.

Most of the time our precautions are mixed—they work both physically and socially. Closing a door normally only makes it harder to eavesdrop. In *Katz*, for instance, the government was able to listen to the conversation by using a powerful microphone to amplify the spo-

---

60. As Heffernan notes,

> [i]n the typical restroom, closing the door to a toilet stall does not wholly limit exposure . . . . Someone standing outside a stall can still peer through the slit that remains between the closed door and the beam to which it can be bolted. Does that mean that privacy conventions do not protect the person inside? Certainly not.

Heffernan, *supra* note 10, at 49. Heffernan more generally argues that our social privacy norms are grounded "in an expectation of forbearance on the part of others—that is, in an expectation that others will restrain their curiosity with respect to those aspects of life that are essential to defining and maintaining individual identity," while cases like *Greenwood* and *Ciraolo* fit a "vigilance model" of privacy "that requires people to be constantly alert to the way in which others can intrude on their lives." Heffernan, *supra* note 10, at 6.

61. *See, e.g.*, Minnesota v. Carter, 525 U.S. 83, 90 (1998) (holding that where visitors were present in a third party's home "for a[n illegal] business transaction and were only in the home a matter of hours[, the visitors] . . . had no legitimate expectation of privacy in the apartment"); Minnesota v. Olsen, 495 U.S. 91 (1990) (protecting the privacy of an overnight guest staying in a host's apartment); Stoner v. California, 376 U.S. 483, 489 (1964) (concluding that searching a hotel room without a warrant violated the Fourth Amendment, despite the fact that one who engages a hotel room gives implied permission to personnel such as maids, janitors, or repairmen to enter to perform their duties); Chapman v. United States, 365 U.S. 610, 616–18 (1961) (concluding that searching a house occupied by a tenant violated the Fourth Amendment, despite the fact that the landlord had authority to enter the house for some purposes).

62. 415 U.S. 164 (1974).

63. *Id.* at 171. *But see* Illinois v. Rodriguez, 497 U.S. 177 (1990); Florida v. Jimeno, 500 U.S. 248 (1991). These cases diminish the role of social precautions by focusing on the third party's "apparent authority."

64. While it is true that this is ultimately a legal, not a factual question, it is hard to imagine that facts about the third party's relationship to the search target could be completely irrelevant.

ken words.[65] But closing a door also invokes a well-known privacy convention that we use to send privacy signals to others, and *Katz* rests largely on this convention's force.

An obvious issue here is the strength of the precaution. Notably, there is a modal problem. A glass phone booth door blocks most sound, but not light. But the fact that anyone could open the phone booth door does not change the fact that the phone booth user has created a socially recognized temporary zone of privacy by closing the door. Additionally, there is a competence problem. Locks prevent the ordinary person from intruding, but not the locksmith or an experienced burglar. Therefore, depending upon one's level of expertise in frustrating the effectiveness of a specific precaution, it might not take much effort to defeat that precaution. The container cases, as well as *Katz*,[66] suggest that the more important issue is the force of the social component of the precaution.[67] For example, "a traveler who carries a toothbrush and a few articles of clothing in a paper bag or knotted scarf [may] claim an equal right to conceal his possessions from official inspection as the sophisticated executive with the locked attaché case."[68]

Furthermore, a precaution might block only one mode of intrusion. Katz remained visible to the public after closing a transparent phone booth door. But the force of the social privacy convention about closed doors made it irrelevant that Katz could be physically seen; he sought to exclude the uninvited ear, not the uninvited eye.[69] Thus, judicial recognition that a precaution generates a reasonable expectation of privacy contemplates that the precaution need not be total, nor block all modes of sensory perception.[70]

---

65. *Katz*, 389 U.S. at 348.

66. In *Katz*, the Court did not merely rest on the fact that the phone booth door had been closed; it also referred to "the vital role that the public telephone has come to play in private communication." *Katz*, 389 U.S. at 352.

67. *See, e.g.*, *Bond*, 529 U.S. at 337–39 (finding that bus passengers have a reasonable expectation that others will not, "as a matter of course, feel the bag in an exploratory manner" and that a government agent's "probing tactile examination" of the passenger's soft-sided luggage "far exceeded the casual contact" that would reasonably have been expected).

68. United States v. Ross, 456 U.S. 798, 822 (1982) (rejecting a constitutional distinction between "worthy" and "unworthy" containers).

69. *See Katz*, 389 U.S. at 352 (rejecting the government's argument that Katz lacked privacy because "the telephone booth . . . was constructed partly of glass, so that he was as visible after he entered it as he would have been if he had remained outside").

70. Indeed, the Supreme Court has held that even when Federal Bureau of Investigation (FBI) agents lawfully possessed boxes of films, and the labels on the boxes gave them probable cause to believe that the films were obscene and that their shipment in interstate commerce violated federal law, warrantless viewing of the films was a "search of the contents of the films" that unreasonably invaded the owner's constitutionally protected privacy interest. Walter v.

3. *Active Versus Passive Precautions*

A third distinction is between active and passive precautions. Often, we rely on "normal" features of the status quo for privacy. A couple picnicking in the woods, believing that they are alone, may decide to have an intimate conversation. Similarly, people may do things in the dark that they would not do in a well-lit setting.[71] Here again, the Supreme Court has not sent consistent signals.

In *Smith v. Maryland*,[72] the defendant argued that he had a reasonable expectation of privacy in the numbers he dialed from his home phone because the phone company tracked long distance phone calls but not local calls.[73] The Supreme Court disagreed, saying that "[t]he fortuity of whether or not the phone company in fact elects to make a quasi-permanent record of a particular number dialed does not . . . make any constitutional difference."[74] Yet in *Katz*, telephone users were accorded Fourth Amendment protection even though such users ordinarily take no precautions against the phone company's ability to record conversations that take place over the phone company's system.[75]

Katz and *Smith* also illustrate how the precautions issue will frequently involve third parties because we often rely on third parties for our privacy.[76] Unfortunately, the Court has not respected such reli-

---

United States, 447 U.S. 649, 654 (1980); *see also id.* at 652 n.2 (noting that the films could not "be examined successfully with the naked eye").

71. In an early Fourth Amendment search case, the Supreme Court found that using artificial light to penetrate darkness was not a search. *See* United States v. Lee, 274 U.S. 559 (1927). In that case, a searchlight revealed contraband on the deck of a boat. *Id.* at 561; *see also* Texas v. Brown, 460 U.S. 730, 739–40 (1983) (holding that looking into the interior of a car with the aid of a flashlight is not a search).

72. 442 U.S. 735 (1979).

73. *Id.* at 745. For purposes of my argument, I assume that Smith knowingly relied on this phone company practice.

74. *Id.* The Court stated:

> Under petitioner's theory, Fourth Amendment protection would exist, or not, depending on how the telephone company chose to define local-dialing zones, and depending on how it chose to bill its customers for local calls. Calls placed across town, or dialed directly, would be protected; calls placed across the river, or dialed with operator assistance, might not be. We are not inclined to make a crazy quilt of the Fourth Amendment, especially in circumstances where (as here) the pattern of protection would be dictated by billing practices of a private corporation.

Id. at 745.

75. *See Smith*, 442 U.S. at 746–48 (Stewart, J., dissenting) (noting that telephone companies have equipment to record or overhear conversations).

76. Such "third-party precautions" should not be viewed as a separate class of precautions, because so much of our lives is now recorded in "extensive digital dossiers." Solove, *supra* note 23, at 1084 ("Detailed records of an individual's reading materials, purchases, diseases, and website activity enable the government to assemble a profile of an individual's finances, health, psychology, beliefs, politics, interests, and lifestyle. This data can unveil a person's anonymous

ance on third parties in the past thirty years.[77] For instance, in *United States v. Miller*, the Court found that bank customers have no expectation of privacy in the papers they fill out when conducting transactions with their banks because they assume the risk that any such information might be disclosed to the government.[78] Yet in older third-party consent cases, the Court refused to leave privacy "secure only in the discretion of their landlords" or in the "unfettered discretion of an employee of the hotel."[79]

In summary, our ordinary social expectations of privacy frequently turn on our use of or reliance on "normal" precautions, which often mix physical, social, active, and passive elements. Fourth Amendment law, however, has been deeply conflicted about how to handle the many types of precautions used in everyday life, and especially reluctant to recognize predominant social conventions.

C. *How the Government Might Interfere with Precautions*

Just as we can categorize precautions, we can categorize government interferences with precautions and with precautions-taking. The two most obvious ways are: To make the act of precautions-taking illegal[80] and to ban a resource essential to precautions-taking, like phone booth doors. In both cases, the problem is that if we cannot take pre-

---

speech and personal associations." (footnotes omitted)). Perhaps more fundamentally, rejecting third-party precautions as precautions ignores the importance of relationships in our social privacy norms. *See* Mary Coombs, *Shared Privacy and the Fourth Amendment, or the Rights of Relationships*, 75 CAL. L. REV. 1593, 1593 (1987) ("Much of what is important in human life takes place in a situation of shared privacy. The important events in our lives are shared with a chosen group of others; they do not occur in isolation, nor are they open to the entire world.").

77. *See* Colb, *supra* note 20, at 153 (tracing Supreme Court doctrine since *Katz* and criticizing the "equation of small and large intrusions upon a particular expectation of privacy" for "allow[ing] government officials to treat as knowingly exposed to the world (and thus to the police as well) . . . those things that have been knowingly exposed to *any* third party").

78. 425 U.S. 435, 443 (1976). As Heffernan notes, customer privacy is an integral part of banking:

> Banks are physically arranged so as to make it possible for customers to avoid broadcasting to the public-at-large the nature of their transactions. Tellers' cages are constructed so that a customer can turn her back to the queue and carry out her business. Automatic teller machines envelop a customer, creating barriers to snoops in the rear who might want to find out about the customer's transactions. And, most important, banks do not provide members of the public-at-large with information about their customers; indeed, no bank could stay in business if it did so. Customers thus *rely* on their banks to keep financial information private.
>
> On the *Miller* Court's account, this consistent pattern of confidentiality vis-à-vis that public-at-large counts for nothing in the calculation of privacy interests given the government's subpoena power over banks.

Heffernan, *supra* note 10, at 87.

79. Stoner v. California, 376 U.S. 483, 490 (1964).

80. Because this technique of interference is so obvious, I do not discuss it further.

cautions, we often will have no reasonable expectation of privacy and the Fourth Amendment simply will not apply.

The government's interference with precautions-taking is not limited exclusively to physical resources like doors, luggage, and envelopes. The government can also interfere with resources that are not physical at all. For example, knowledge or information is also a resource with which the government can interfere. Knowledge of a privacy threat is a resource for precautions-taking; we are unlikely to take precautions if we are not aware that our privacy is threatened. If the government installs highly conspicuous video surveillance cameras in some public places, people who do not like to be photographed might avoid those places. They would have no reason to avoid those places if the cameras were hidden.

Also, knowledge or information can be a resource for actually taking precautions. Even if people know that their Internet activities may be monitored, they cannot protect themselves against such monitoring unless they know how to use privacy enhancing technologies like anonymous remailers, anonymizing proxies, or encryption.

Less obviously, the government could make it harder or less attractive to take precautions. Instead of making it unlawful to use envelopes, it could tax them or otherwise raise the price of using envelopes. Instead of installing conspicuous video surveillance cameras,[81] it could conceal them.[82]

The government could also cripple precautions.[83] The government might impose mandatory data retention requirements on banks or communications providers, which would defeat private arrangements

81. The example of public video surveillance provides an additional insight into precautions. Some precautions are "normal," while others are abnormal. Arguably, public video surveillance exploits the fact that precautions like wearing a ski mask on the streets of San Francisco are abnormal.

82. Notice requirements for public surveillance have been urged in the literature. *See, e.g.*, Slobogin, *supra* note 20, at 442–43 (arguing that "government searches that affect large groups of people should be mediated through the public process"); Christopher Slobogin, *Public Privacy: Camera Surveillance of Public Places and the Right to Anonymity*, 72 Miss. L.J. 213, 297–98 (2002) (arguing that public notice of public video surveillance should be required).

83. Defeating or overcoming precautions is not the same as crippling or interfering with them. Part of what is interesting about precautions is that defeating precautions often does not seem as bad as interfering with them. When I was a child, my mother and I would often converse in public about private family matters—but in Chinese. We created privacy, but we were vulnerable to others who understood Chinese. The government could defeat or overcome this precaution by employing Chinese speakers. Or the government could interfere with the precaution by banning Chinese.

to purge records.[84] It might require or create incentives for "recoverable encryption," which would build a backdoor into otherwise "unbreakable" encryption.[85] Alternatively, it might require that communications providers design and use equipment that permits ready government access to communications content and identifying information, like phone numbers and internet protocol (IP) addresses.[86]

This last mode of interference overlaps with the knowledge issue mentioned earlier. It is obvious that covert surveillance relies on the target's ignorance of the surveillance. The general point is that people are much less likely to take precautions when they do not know about a privacy threat. Crippling precautions that are internal to complex technological systems, like the phone system or the Internet, may well weaken privacy with little publicity or understanding. Unfortunately, because the Supreme Court has failed to analyze precautions in any depth, these sorts of government interferences with precautions are invisible to modern Fourth Amendment law. In the remainder of this Article, I attempt to construct a framework for thinking about a Fourth Amendment right to take precautions.

D. An Analytical Framework for Thinking about Rights

This section analyzes the Fourth Amendment's search jurisprudence using Professor Judith Jarvis Thomson's analytical framework for thinking about rights.[87] Thomson's framework, which I review briefly here, helps analyze the various components of complex rights.

Thomson argues that people have four kinds of rights: claims, privileges, powers, and immunities.[88] A claim is a familiar kind of right; it is always correlated with another entity's duty.[89] If I have a claim that someone gives me $100, then that individual has a correlative duty to

84. *See generally* Catherine Crump, Note, *Data Retention: Privacy, Anonymity, and Accountability Online*, 56 STAN. L. REV. 191 (2003) (discussing the constitutionality of mandatory data retention).

85. *See generally* A. Michael Froomkin, *The Metaphor Is the Key: Cryptography, the Clipper Chip, and the Constitution*, 143 U. PA. L. REV. 709 (1995).

86. *See generally* Susan Freiwald, *Uncertain Privacy: Communication Attributes After the Digital Telephony Act*, 69 S. CAL. L. REV. 949 (1996).

87. *See generally* JUDITH JARVIS THOMSON, THE REALM OF RIGHTS (1990). I do not defend Thomson's approach to rights, I merely adopt it. My analysis will be subject to the same criticisms as hers, but I assume that her analysis has sufficient theoretical currency to make my own analysis plausible. Thomson's analysis is an attractive candidate for this task because, although it is a moral theory of rights, it is partly inspired by a seminal work in legal literature: WESLEY HOHFELD, FUNDAMENTAL LEGAL CONCEPTIONS (1919).

88. THOMSON, *supra* note 87, at 40.

89. *Id.* at 41 ("X's having a claim is equivalent to Y's being under a duty").

give me $100. A privilege is also familiar; it is defined by the lack or absence of a duty. Thus, if I have a privilege to close my door, then I have no duty to anyone not to close my door.

Privileges, however, are weak in a way that is probably unfamiliar because they do not by themselves entail any claims.[90] Thomson uses a simple example of a person, *C*, who owns a salad but gives another person *D* permission to eat it.[91] *D* now has a privilege to eat the salad—but does that mean that *C* cannot also eat the salad? Or that *C* cannot decide to put the salad away before *D* has actually eaten it?[92]

Thomson's answer is no: A privilege is only the lack of a duty.[93] Because *D* has a privilege to eat *C*'s salad, *D* does not wrong anyone in doing so. But *D*'s privilege is not a claim, which means that no one has a corresponding duty of any kind. Thus, *D*'s privilege does not mean that *C* has a duty to allow *D* to eat it; it only means that *C* has no ground for complaint if *D* does eat the salad. In short, the mere privilege to do something does not mean one has a claim to be able to do it.

Powers and immunities are relatively unfamiliar species of rights.[94] The easiest way to understand them is through the familiar idea that constitutional rights may not be altered by legislative or executive action.[95] In Thomson's terms, this aspect of rights is analyzed in terms of powers and immunities. One who owns a typewriter has power over the typewriter by virtue of ownership: He or she can unilaterally give the typewriter to someone else. More generally, "a power is an ability to cause, by an act of one's own, an alteration in a person's rights, either one's own rights or those of another person or persons, or both."[96]

---

90. *Id.* at 47 ("No privilege entails any claim.").

91. Thomson views property ownership as including a range of rights, including powers to alter others' rights. *Id.* at 57–58. As owner of the salad, *C* has the power to allow others to eat it.

92. *Id.* at 51.

93. *Id.* at 44, 51 (explaining that the salad hypothetical can be understood as *C*'s having said: "Eat the salad, *if you can*," or "[y]ou have my license to do so, but *I don't agree not to interfere with you.*").

94. As Thomson notes, "[p]eople do say such things as that a person who owns a piece of property has a right to give it away or sell it," but they are "likely to mean to be ascribing a power." THOMSON, *supra* note 87, at 59.

95. The judiciary's role in altering the meaning of constitutional rights is beyond the scope of this Article.

96. THOMSON, *supra* note 87, at 57. Thomson further distinguishes "large-scale" and "small-scale" powers: Large-scale powers, like those associated with outright property ownership, are abilities to make large-scale alterations in people's claims and privileges. *Id.* at 58. A "small-scale" power is a situation in which *X* makes a promise to *Y* to do something, so that *Y* has a

Immunities correlate to powers as duties correlate to claims.[97] That is, "for X to have an immunity against Y just is for Y to lack a power as regards X."[98] For example, the federal Freedom of Information Act (FOIA) generally provides that any person may obtain disclosure of agency records, subject to several statutory exceptions.[99] Congress, however, has the power to amend the FOIA and add new exceptions or to enact statutes that satisfy FOIA's criteria and thereby permit agencies to refuse to disclose additional agency records. Therefore, unlike constitutional rights, statutory rights are not immune against the power of the legislature.[100]

III. THE FOURTH AMENDMENT IMPLICATIONS OF PRECAUTIONS

The Fourth Amendment restricts state action that unduly burdens people's ability to take precautions, much as the First Amendment restricts state action that unduly burdens speech. We have a right to lock our doors, go into a secure area to talk, or encrypt our e-mail in order to prevent the government, or anyone else, from gaining access to our things, our space, or our communications. We have a related right to challenge the government if it elects to unduly interfere with our precautions-taking. More precisely, I argue that we have a cluster of "rights" against the government with regard to privacy precautions. This cluster of rights has three aspects: (1) The privilege to take precautions; (2) a claim that the government may not interfere with our acts of taking precautions; and (3) an immunity for both the privilege and the claim.

A. Privileges, Claims, and Immunities: The Cluster of Rights Upon Which the Government May Not Trample

First, we have a privilege of action. In other words, we have a privilege to take precautions to protect our privacy. We have no duty to refrain from whispering to prevent overhearing; conditioning disclosure of information to others on their promise to keep the information confidential; going from the sidewalk into one's home to converse pri-

claim against *X* that *X* has to do something. *Id.* If I release one from one's promise to me, I relinquish that claim. *Id.*

97. *Id.* at 59.

98. *Id.*

99. Freedom of Information Act, 5 U.S.C. § 552(b)(3) (2000).

100. *See, e.g.*, THOMSON, *supra* note 87, at 282 (discussing the importance of immunities associated with "our rights to a voice" in government action and "immunity to state action in the absence of a voice in it"). Thomson's analysis of rights is intended as a general framework, and does not address the distinction between strongly protected constitutional rights, like First and Fourth Amendment rights, and statutory rights.

vately; enclosing letters within envelopes to make it harder for letters to be read.

Second, we have a claim that the government may not interfere with this privilege, all other things being equal; the government has a duty toward us that it not interfere with our taking the kinds of precautions mentioned above. This duty is not "absolute." Having this claim does not necessarily cause such government interference to be automatically wrong.[101] But it does mean that absent special circumstances, government interference with precautions-taking would infringe our claim, and even when such infringement is permissible or would be right, there are things the government may nevertheless have a duty to do, such as seek a release in advance or compensate us later for harms caused by the infringement.[102]

Third, we have an immunity with respect to this privilege and claim. The government does not have indiscriminate power to take away the privilege or the non-interference claim. In other words, because there is no search without a reasonable expectation of privacy, the government should not be able to evade the Fourth Amendment's prohibition of unreasonable searches by preventing one from being able to create the needed reasonable expectation of privacy.[103] Although the government can take away the privilege and claim, it can only do so by enacting legislation that withstands "exacting" scrutiny or by amending the Constitution.[104]

At the heart of this argument is the concept of precautions-taking. My key point is that our constitutional privacy, secured mainly by the Fourth Amendment's protection against unreasonable searches and

---

101. Much of Thomson's book argues that claims are not absolute. *See id.* at 79–122. Instead, our having a claim means that the person who holds the correlative duty (in this case, the government) is significantly constrained in his or her actions. *Id.* at 123 (stating that "it is only in special circumstances that Y may permissibly fail to accord the claim; other things being equal, Y ought to accord it").

102. *Id.* at 96.

103. Interference with precautions should be subject to strict scrutiny given that "[t]he security of one's privacy against arbitrary intrusions by the police—which is at the core of the Fourth Amendment—is basic to a free society." Wolf v. Colorado, 338 U.S. 25, 27 (1949). The Court, however, has not used the rubric of strict scrutiny in evaluating the Fourth Amendment challenges to statutes or regulations. In some cases, the Court uses the concept of "reasonableness." California Bankers Ass'n v. Schultz, 416 U.S. 21, 67 (1973) (deciding a challenge to regulations imposing reporting requirements on banks in terms of "reasonableness"). In other cases, the Court has evaluated the statute in light of the Fourth Amendment's underlying historical purpose of repudiating the British practice of general warrants. Berger v. New York, 388 U.S. 41, 58 (1967) (explaining that the Fourth Amendment's requirement that a warrant be particular in its description of places to be searched and things to be seized repudiated general warrants and findings that the state's eavesdropping statute was too "indiscriminate").

104. *See infra* notes 174–178 and accompanying text.

seizures, cannot be disassociated from precautions-taking.[105] Privacy depends on context, and if we do not have the right to create that context for ourselves, there ultimately will be no "breathing space" for privacy.[106] Put slightly differently, unless the Constitution is interpreted as securing the precautions cluster-right on at least a constitutional par with the right against unreasonable searches and seizures, then the latter right is illusory.

B. The No-Search Claim and the Government's Duty

The Fourth Amendment secures an individual right against the government. Specifically, this right is:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and 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.[107]

Textually, the Fourth Amendment secures two basic rights: A general right against "unreasonable" searches and a more precise right that any search pursuant to a warrant be based on an affirmation of probable cause[108] and further that the warrant itself particularly describe the place to be searched and the persons or things to be seized.[109] Warrants are often unnecessary, but many warrantless searches still require probable cause.[110]

---

105. *See generally* Colb, *supra* note 19; Heffernan, *supra* note 10; Arbus, *supra* note 3.

106. *See* NAACP v. Button, 371 U.S. 415, 433 (1963) ("Because First Amendment freedoms need breathing space to survive, government may regulate in the area only with narrow specificity." (citation omitted)).

107. U.S. CONST. amend. IV.

108. *See, e.g.*, Maryland v. Garrison, 480 U.S. 79, 84 (1987). In *Garrison*, the Court stated that "[b]y limiting the authorization to search to the specific areas and things for which there is probable cause to search, the requirement ensures that the search will be carefully tailored to its justifications." *Id.* Consequently, "the scope of a lawful search is defined by the object of the search and the places in which there is probable cause to believe that it may be found." *Id.* (internal quotation marks and citation omitted). In *Katz*, the Court held that "searches conducted outside the judicial process, without prior approval by judge or magistrate, are per se unreasonable under the Fourth Amendment subject only to a few specifically established and well-delineated exceptions." *Katz*, 389 U.S. at 357 (footnotes omitted).

109. Groh v. Ramirez, 540 U.S. 551, 560 (2004). The Court stated that

> unless the particular items described in the affidavit are also set forth in the warrant itself (or at least incorporated by reference, and the affidavit present at the search), there can be no written assurance that the Magistrate actually found probable cause to search for, and to seize, every item mentioned in the affidavit.

Id.

110. For instance, the so-called "automobile exception" to the Fourth Amendment permits warrantless searches of almost any vehicle for which probable cause to search exists. David Moran, *The New Fourth Amendment Vehicle Doctrine: Stop and Search Any Car at Any Time*, 47

In Thomson's terms, we have a right against the government that it cannot search us unreasonably.[111] Thomson calls this kind of right a "claim," and we can say that the Fourth Amendment secures the no-search claim.

Claims are always accompanied by correlative duties.[112] In this analysis, because we have a claim that the government cannot unreasonably search us, the government has a corresponding duty not to engage in unreasonable searches.[113] Of course, the government may search us if it complies with the warrant requirement and its many exceptions. The best way to think about the ways that searches are permissible flows from Thomson's point that claims are not absolute, using the familiar notion that one may infringe a right without violating it.[114] A violation of a claim, then, is a wrongful infringement of a claim. In the case of the Fourth Amendment right against government searches, government searches generally infringe the no-search claim, but properly executed, warranted searches based on probable cause (and other justified searches) do not violate that claim.[115]

C. *Powers, Immunities, and the No-Search Claim*

Fourth Amendment rights are constitutional rights. Thus, just as the government cannot decide that we lack the First Amendment right to free exercise of religion, the government cannot unilaterally decide that we lack the right against government searches. In my view of Thomson's framework, our Fourth Amendment rights include some immunity against governmental alteration of the no-search claim.[116]

In summary, the Fourth Amendment apparently secures to individuals a right (claim) against the government that it cannot search us, and the government has a correlative duty not to search us. When the government searches, it infringes that right. But the Warrant Clause and various other rules and exceptions[117] provide that not all infringe-

---

VILL. L. REV. 815, 817 (2002) (chronicling the expansion of the automobile exception since *Carroll v. United States*, 267 U.S. 132 (1925)).

111. *See* THOMSON, *supra* note 87, at 37–60.

112. "[E]very claim is a right that an entity *has against an entity*. One cannot have a claim that is a claim against nothing. . . . This issues from the fact that . . . X's having a claim is equivalent to Y's being under a duty." *Id.* at 41.

113. *Id.*

114. *Id.* at 122.

115. It is not clear whether defining the right this way—as opposed to a right against unjustified searches—makes a difference to the analysis.

116. *See supra* note 100 and accompanying text.

117. Thus, in *Carroll v. United States*, 267 U.S. 132 (1925), the Court found that a warrantless search of an automobile was reasonable under the Fourth Amendment so long as it was based on probable cause "where it is not practicable to secure a warrant, because the vehicle can be

ments are violations.[118] Searches, for example, justified by properly issued particular warrants based on probable cause, do not violate our Fourth Amendment right against government searches.[119] Our Fourth Amendment rights, moreover, include a strong immunity against the government; the government lacks the power to alter the claim (except by constitutional amendment).

D. The Precautions Privilege

Under the Fourth Amendment, we have a no-search claim and an immunity against the government in regard to the no-search claim, subject to the government's warrant power, the exercise of which negates our no-search claim and the government's no-search duty in a particular fact situation.

But government restrictions on precautions and precautionary behavior raise problems for this level of analysis because it is hard to think of these restrictions as "searches." Providing back doors into encryption or banning phone booth doors facilitates searches or can transform what would otherwise be a search into a non-search, but neither seems like a search. If the Fourth Amendment is to protect precautionary behavior, we need a different approach. So I further suggest that we also have the following rights: A privilege to take precautions to protect our privacy, a claim against the government that it not interfere in certain ways with that privilege, and immunities against the government for both the privilege and the claim.

As we have seen, taking privacy precautions can be as simple as whispering or putting a letter inside an envelope. In Thomson's framework, these kinds of actions are generally comprehended as privileges.[120] Katz had a privilege to close the phone booth door behind him, precisely because he had no duty not to close the door.[121]

I think there is no serious dispute that the precautions privilege exists, at least as an aspect of our basic liberty of action. We may lock

---

quickly moved out of the locality or jurisdiction in which the warrant must be sought." *Id.* at 153. The Court has since expanded the automobile exception greatly. *See, e.g.*, Moran, *supra* note 110.

118. For instance, restraining a person's freedom to move away is a Fourth Amendment seizure, but whether such a seizure actually violates the Fourth Amendment turns on whether the seizure is "reasonable." *See, e.g.*, Brown v. Texas, 443 U.S. 47, 50–51 (1979) (explaining that detentions are less intrusive than arrests, and that the reasonableness analysis requires weighing "the gravity of the public concerns served by the seizure, the degree to which the seizure advances the public interest, and the severity of the interference with individual liberty").

119. *See supra* notes 107–108 and accompanying text.

120. *See* THOMSON, *supra* note 87, at 43–45.

121. *Id.* at 46 (stating that "a privilege is merely the lack of a duty"). In other words, Katz had no legal obligation to leave the phone booth door open.

our doors, hide our papers, or even destroy our things. We have no general duty to preserve things or communications so that a lawful government search will be fruitful. As Thomson puts it, "you have a claim against me that I not enter your house? You need only lock your doors and windows, and that is on any view something it is permissible for you to do."[122] Thus, taking precautions is part of our general set of privileges.

E. The Claim to Non-Interference and Its Immunity

Privileges by themselves are weak because they do not entail any claim, and thus entail no correlated duty. As previously described, the mere privilege to take precautions does not include any kind of claim against the government. The real question is whether we have more than a mere privilege to take precautions.

In Thomson's salad example, *C* gave *D* the privilege to eat *C*'s salad, which meant that *D* could eat the salad without doing anything wrong to *C*.[123] But *C* did not promise not to interfere with *D*'s attempt to eat the salad. For instance, *C* could have locked the salad in a box without authorizing *D* to open the box. In other words, privileges in themselves do not entail a claim of non-interference. But *C* could also give *D* the claim that *C* not interfere with *D*'s eating the salad. As Thomson puts it, "in the typical case in which you give Bloggs permission to eat your salad, you give him more than merely a privilege, as regards you, of eating your salad: you surely also give him a claim against you to your noninterference with his eating of it."[124]

In short, what we colloquially think of as a freedom or "liberty" to act is actually a privilege to do something combined with some claim of non-interference.[125] Thus, I argue we have a *claim* against the government that it should not interfere with our privilege to take precautions. We have a *privilege* to close phone booth doors, and the government has a duty not to interfere, whether by ordering us not to or by causing doors to be removed.

Furthermore, because the claim to non-interference is rooted in the Fourth Amendment, and is thus of constitutional dimension, one more

122. *Id.* at 111.

123. *Id.* at 51.

124. *Id.* at 50. Thomson further explains that this claim to non-interference is not the same as a claim "to his actually eating the salad, or even to your assistance in eating it." *Id.* You do not, on this account, do anything wrong if you do not provide a plate or fork. THOMSON, *supra* note 87, at 150.

125. *Id.* at 54 (stating that "the liberty to do such and such contains all of those privileges . . . and claims to noninterference . . . whose possession is necessary and sufficient for being at liberty to do the such and such").

component is added—an immunity against ordinary government action. The mere privilege to take precautions could be taken away; the added components of a non-interference claim and an immunity against the government are what give our standard constitutional liberties their force.[126] As Thomson puts it, "At the heart of the right to liberty . . . is not privileges and claims, but *immunities*."[127]

F. Grounding the Non-Interference Claim and Its Immunity

I have asserted that we have a claim to non-interference with our privilege to take precautions, and that both the privilege and the claim are immune from government alteration. The remaining question pertains to our immunity with respect to this privilege and claim, which corresponds to the government's lack of a power to alter the non-interference claim.[128] Why should we recognize a strong right to take precautions?

There are at least two normative arguments for this immunity. The clearest argument is the simple "argument from equivalence"—that the privilege to take precautions and its associated claim to non-interference is functionally equivalent to the no-search claim.[129] Our constitutional rights are in theory immune unless the courts exercise their power of judicial review or the Constitution is amended. Because all Fourth Amendment rights are constitutional rights, ordinary legislative or executive action cannot alter them.[130]

But whether we have Fourth Amendment rights in any given situation depends on whether the government engaged in a "search;" that is, whether the government infringed a reasonable expectation of privacy.[131] Under current Fourth Amendment jurisprudence, reducing precautions can mean diminished or even extinguished privacy expectations, and thus weak or no Fourth Amendment rights.[132] Thus, to the extent that government action interferes with precautions needed

126. *See supra* note 100 and accompanying text.

127. *Id.* at 282.

128. *Id.* at 59 (explaining that the meaning of *X*'s having an immunity against *Y* is simply that *Y* lacks a power as regards *X*).

129. *See supra* Part II.A (explaining how Fourth Amendment protection often depends on taking precautions).

130. Given that "the Fourth Amendment, at its most fundamental level, is designed to protect people from the government," the legislature should not be able to change our Fourth Amendment rights. Clancy, *supra* note 17, at 549.

131. *See, e.g.*, *Greenwood*, 486 U.S. at 39 ("The warrantless search and seizure of the garbage bags . . . would violate the Fourth Amendment only if respondents manifested a subjective expectation of privacy in their garbage that society accepts as objectively reasonable.").

132. *See supra* notes 107–127 and accompanying text.

to have Fourth Amendment rights at all, there should be constitutional limits on such action.[133]

Once the relationship between precautions and searching is recognized, then all the reasons to limit government searches support the right to take precautions and to limit encroachment on those precautions.[134] Privacy is, of course, the main reason.[135] But the Fourth Amendment is also animated by the general goal of the Constitution—"to define and limit governmental power."[136] This separation of powers goal is at special risk from executive or legislative interference with precautions because of the agency problem, that is "protecting the people generally from self-interested government."[137] We should expect that absent external restraint, law enforcement agencies would seek to interfere with privacy precautions.[138]

The weakness of this argument is that it may under-protect us against future threats. The example of banning phone booth doors works because it is clear that the government is depriving us of something we already have. It does not work as well if we do not yet have

---

133. Arguably, the Fourth Amendment's textual reference to "persons, houses, papers, and effects" provides minor support for some precautions privilege because it assumes at least two kind of precautions: keeping or doing things within the boundaries of one's body or home. *See* United States v. Ross, 456 U.S. 798, 822 (1982). For example, Justice Stevens stated:

> For just as the most frail cottage in the kingdom is absolutely entitled to the same guarantees of privacy as the most majestic mansion, so also may a traveler who carries a toothbrush and a few articles of clothing in a paper bag or knotted scarf claim an equal right to conceal his possessions from official inspection as the sophisticated executive with the locked attaché case.

Id. (footnote omitted).

134. In many cases, of course, objections can be based on other constitutional rights. For instance, an obvious obstacle to criminal investigation is the fact that many of our conversations are never recorded. Imagine a law requiring total data retention of every conversation, phone call, and e-mail. Moreover, all such communications would be turned over to the government for secure safekeeping. While such a scheme would obviously violate the First Amendment, it should also be found to violate the Fourth Amendment.

135. Cardwell v. Lewis, 417 U.S. 583, 584 (1974) (stating that "the primary object of the Fourth Amendment is the protection of privacy").

136. Shih Ray Ku, *supra* note 54, at 1337. *See* Maryland v. Garrison, 480 U.S. 79, 84 (1987) (noting that the prohibition of general warrants was one of the central purposes of the Fourth Amendment).

137. Akhil Reed Amar, *The Bill of Rights as a Constitution*, 100 YALE L.J. 1131, 1177 (1991). Professor Amar argues generally that the Bill of Rights is concerned more about protecting "the society against the oppression of its rulers" than protecting individuals and minorities against majorities. *Id.* at 1132–33 (quoting THE FEDERALIST No. 51, at 323 (J. Madison) (C. Rossiter ed., 1961)).

138. *See* United States v. U.S. District Court, 407 U.S. 297, 317 (1972) ("The Fourth Amendment does not contemplate the executive officers of Government as neutral and disinterested magistrates . . . The historical judgment, which the Fourth Amendment accepts, is that unreviewed executive discretion may yield too readily to pressures to obtain incriminating evidence and overlook potential invasions of privacy and protected speech." (footnote omitted)).

that reasonable expectation of privacy because we cannot as strongly argue that the action deprives us of anything. Unfortunately, the question of a reasonable expectation of privacy often arises where new technologies are concerned.[139]

The second, more forward-looking argument is that the government should not be free to manipulate our expectations. A familiar notion in constitutional law is that preferred constitutional liberties, like freedom of speech, function to preserve "spheres of autonomy" based on private ordering.[140] The danger of government action aimed at precautions and precautions-taking is that it distorts the "natural" evolution of social privacy practices, which are supposedly the source of reasonable expectations of privacy.[141] Government interference with precautions reorders the private realm, and in the case of Fourth Amendment privacy, may well be strategic action intended to thwart precautions that might, like doors and envelopes, become perceived as necessary for the meaningful exercise of our Fourth Amendment rights.[142]

Oddly, *Smith v. Maryland* lends support to this argument. In *Smith*, the Supreme Court admitted that *Katz*'s reasonable expectation test would fail in cases where the government had "conditioned" individu-

---

139. *See generally, e.g.*, Freiwald, *supra* note 86 (discussing how the uncertainty surrounding new communication technologies like e-mail led to weak protection for non-content attributes of communications).

140. *See, e.g.*, Steven J. Heyman, *Spheres of Autonomy: Reforming the Content Neutrality Doctrine in First Amendment Jurisprudence*, 10 WM. & MARY BILL RTS. J. 647, 656–64 (2002) (discussing notions of autonomy in First Amendment law); Kathleen Sullivan, *Unconstitutional Conditions*, 102 HARV. L. REV. 1413, 1490 (1989) ("Preferred constitutional liberties generally declare desirable some realm of autonomy that should remain free from government encroachment.").

141. United States v. White, 401 U.S. 745, 786 (1971) (Harlan, J., dissenting). Justice Harlan argued in dissent:

> Our expectations, and the risks we assume, are in large part reflections of laws that translate into rules the customs and values of the present. Since it is the task of the law to form and project, as well as mirror and reflect, we should not, as judges, merely recite the expectations and risks without examining the desirability of saddling them upon society.

Id.; *see generally* Lee Tien, *Cheap Surveillance, Essential Facilities, and Privacy Norms*, 1999 STAN. TECH. L. REV. 10 (arguing that widespread public surveillance can distort social evolution of privacy norms); Lee Tien, *Architectural Regulation and the Evolution of Social Norms*, 9 INT'L J. COMM. L. & POL'Y 1 (Autumn 2004), *at* http://www.ijclp.org/Cy_2004/pdf/Lee_Tien_ijclp-paper.pdf.

142. A closely related point is that the government should not be able to ban or inhibit precautions, because we have a right to protect ourselves from other people. This argument may not seem to be based on the Fourth Amendment, since other people are not the government. But the social system of privacy norms that grounds "reasonable" privacy expectations depends on precautions and precautions taking, and government interference with precautions will unduly affect this social system. I am indebted to Professor Christopher Slobogin for this point.

als' subjective expectations of privacy in a way "alien to well-recognized Fourth Amendment freedoms," and that in such situations "a normative inquiry" would be appropriate.[143] If this is so, a normative inquiry should be appropriate when the government attempts to shape or "condition" individuals' objective expectations of privacy by shaping the resources needed to assert them.[144]

Kyllo v. United States also supports, although obliquely, some right to take precautions.[145] In *Kyllo*, the Court found that the use of a thermal imaging device to interpret heat emanations from the home is a search requiring a warrant based on probable cause.[146] In so holding, the Court expressly noted that thermal imaging technology is "not in general public use,"[147] suggesting that current social conditions should play a significant role in determining Fourth Amendment rights.[148] If so, then the government should be limited in its ability to manipulate those conditions.

To some extent, this approach departs from the standard individualistic view of Fourth Amendment rights[149] by recognizing that society itself—not just atomistic individuals—has an interest in Fourth Amendment rights.[150] But if privacy expectations are grounded in social practices,[151] then there ought to be some legally cognizable interest in protecting those practices against deliberate government

143. Smith v. Maryland, 442 U.S. 735, 741 n.5 (1979).

144. Government interference with precautions obviously implicates many non-Fourth Amendment issues. For instance, restrictions on encryption technology that apply to the publication of scientific information raise First Amendment issues. *See, e.g.*, Junger v. Daley, 209 F.3d 481, 485 (6th Cir. 2000) (holding that a law professor's intended Internet publication of encryption source code in a law school course website was protected by the First Amendment).

145. Kyllo v. United States, 533 U.S. 27 (2001).

146. *Id.* at 40.

147. *Id.* at 34. In *Dow Chemical Co. v. United States*, aerial surveillance infringed no objective privacy expectation because it used "a conventional, albeit precise, . . . camera commonly used in mapmaking." 476 U.S. 227, 238 (1986). The Court, however, also stated that, "highly sophisticated surveillance equipment not generally available to the public . . . might be constitutionally proscribed absent a warrant." *Id.* For extensive analysis of the "not in general public use" concept, see Slobogin, *supra* note 14.

148. Indeed, the notion of "general public use" could be viewed as Fourth Amendment prophylaxis about precautions. If a surveillance technology is not in general public use, few people will know about the threat, and they will not take relevant precautions or precautions may not be commercially available.

149. Alderman v. United States, 394 U.S. 165, 174 (1969) (stating that "Fourth Amendment rights are personal rights").

150. *See* Coombs, *supra* note 76; Donald L. Doernberg, *"We the People": John Locke, Collective Constitutional Rights, and Standing to Challenge Government Action*, 73 CAL. L. REV. 52, 105–06 (1985).

151. Rakas v. Illinois, 439 U.S. 128, 143 n.12 (1978) (one source of "legitimate" Fourth Amendment privacy expectations is "understandings that are recognized and permitted by society"); *see generally* Christopher Slobogin & Joseph Schumacher, *Reasonable Expectations of Pri-*

interference. After all, "[p]art of the definition of personal privacy is what might be called social or communal privacy, the interest people have in the security of their arrangements for sharing what they have with others."[152]

IV. CONCRETE EXAMPLES EMBODIED IN THE COMMUNICATIONS ASSISTANCE FOR LAW ENFORCEMENT ACT

Suppose there is a right to precautions in the manner that I have suggested. In practical legal terms, what would it look like? This Part focuses on the idea of crippled encryption and the idea of mandated "tappability" embodied in CALEA.

Since the advent of the telephone, law enforcement has exploited two features of electronic communications. First, electronic communications are carried by wires or in over-the-air signals, channels that are easy to "tap" or intercept because they are covertly and remotely accessible.[153] Second, for many years there was no electronic equivalent of an envelope; the signals, once accessed, were open to view.[154] Unsurprisingly, wiretapping became a useful tool for law enforcement.[155]

In the early 1990s, the federal government concluded that technological changes could make wiretapping less useful to law enforcement.[156] On the one hand, the technology of encryption was

---

vacy and Autonomy in Fourth Amendment Cases: An Empirical Look at "Understandings Recognized and Permitted by Society", 42 DUKE L.J. 727 (1993).

152. James Boyd White, *The Fourth Amendment as a Way of Talking About People: A Study of* Robinson *and* Matlock, 1974 SUP. CT. REV. 165, 217.

153. *See, e.g.*, COMPUTER SCI. AND TELECOMMUNICATIONS BD., NAT'L RESEARCH COUNCIL, CRYPTOGRAPHY'S ROLE IN SECURING THE INFORMATION SOCIETY 2 (Kenneth W. Dam & Herbert S. Lin eds., 1996) [hereinafter CRISIS Report] (referring to "the ease with which personal telephone calls can be tapped, especially those carried on cellular or cordless telephone calls"). *See* Olmstead v. United States, 277 U.S. 438, 456–57 (1928) ("Small wires were inserted along the ordinary telephone wires from the residences . . . and those leading from the chief office. The insertions . . . were made in the basement of the large office building. The taps from house lines were made in the streets near the houses.").

154. CRISIS Report, *supra* note 153, at 67 (noting the demand for encryption in the wake of publicity about intercepted cellular telephone calls).

155. For discussion of the general importance of electronic surveillance in the 1950s and 1960s, see Berger v. New York, 388 U.S. 41, 60–62 (1967); *id.* at 124 ("[E]lectronic surveillance is: *the single most valuable weapon in law enforcement's fight against organized crime.*" (Appendix to White, J., dissenting) (citation omitted)).

156. *See* CRISIS Report, *supra* note 153, at 113–215 (reviewing federal attempts to control encryption technology); Freiwald, *supra* note 86, at 975–82 (discussing federal attempts to control telephone technology in 1994 and 1995).

becoming more available.[157] On the other hand, electronic communications were becoming less "tappable."[158]

A. *Crippled Encryption*

The ability to tap electronic communications is distinct from having the ability to understand them. Encryption obviously could frustrate wiretaps because even after the police intercept the electronic signals, the meaning of the message would be inaccessible.[159] Indeed, modern encryption is strong enough that it is possible that properly designed encryption is unbreakable.[160]

Suppose the government banned ordinary encryption and required that all encryption contain a law enforcement "back door" that would allow the government to obtain the unencrypted plain text of communications without the cooperation or knowledge of the user.[161] That is, even though the encryption would provide confidentiality against most people, the government would be able to bypass that protection and read or understand the message. The main feature of proposals

---

157. In 1995, FBI Director Louis Freeh told Congress that, "unless the issue of encryption is resolved soon, criminal conversations over the telephone and other communications devices will become indecipherable." CRISIS Report, *supra* note 153, at 91.

158. Freiwald, *supra* note 86, at 975 (noting that in 1994, the FBI was "[c]oncerned that the use of call forwarding, cellular telephones and new digital communications technologies generally presented technological impediments to law enforcement agents' ability to wiretap" (footnotes omitted)).

159. To some extent, the ease with which over-the-air electronic communications like cordless and cellular telephone calls can be intercepted may have stimulated demand for encryption. CRISIS Report, *supra* note 153, at 67. The Board stated:

> The impetus for thinking seriously about security is usually an event that is widely publicized and significant in impact. An example . . . is the recent demand for encryption of cellular telephone communications. In the past several years, the public has been made aware of a number of instances in which traffic carried over cellular telephones was monitored by unauthorized parties. (footnotes omitted).

Id.

160. Even if any particular message is practical to decrypt, encryption as a general practice might still sharply decrease the utility of wiretapping. On the other hand, encryption only operates over the transmission channel. Whether the message is oral, as over telephones, or written, as with e-mail or faxes, the message necessarily begins and ends as plain text (i.e., in unencrypted form).

161. In 1993, the government actually introduced government-designed encryption aimed at ensuring law enforcement access to the contents of encrypted communications, but on a voluntary rather than mandatory basis. *See* CRISIS Report, *supra* note 153, at 167–215. The basic idea was that the encryption would provide "very strong cryptographic confidentiality . . . for users against *unauthorized* third parties, but no confidentiality at all against third parties who have *authorized* exceptional access." *Id.* at 169; *see id.* at 170–75 (explaining "Clipper Chip" proposal for telephone communications); *id.* at 176–77 (describing "Capstone/Fortezza" initiative for data storage and communications).

for crippled encryption was that the government would have access to special keys that could unlock the encrypted communication.[162]

Because such regulation does not look like a search or seizure, the standard Fourth Amendment analysis of government-crippled encryption begins by asking "whether forcing individuals to disclose their private keys to the government constitutes a search or seizure."[163] This approach has focused on the keys that "unlock" the encrypted data. Is the obtaining of keys a search or seizure? Is the storing of the keys a search or seizure? Would a key recovery system constitute a search or seizure?

My precautions approach avoids these questions. Encryption is a precaution that increases electronic communications privacy, just as envelopes are a precaution that increases paper communications privacy. The question is not whether recoverable encryption is a search or seizure, but whether government action to restrict encryption violates our right to take precautions. As one court stated,

> Whether we are surveilled by our government, by criminals, or by our neighbors, it is fair to say that never has our ability to shield our affairs from prying eyes been at such a low ebb. The availability and use of secure encryption may offer an opportunity to reclaim some portion of the privacy we have lost. Government efforts to control encryption thus may well implicate . . . the constitutional rights of each of us as potential recipients of encryption's bounty.[164]

Government attempts to cripple encryption clearly infringe our precautions rights for the same reasons that we have a right to be protected against unlawful searches of our communications.

B. Mandated Tappability

In response to the Federal Bureau of Investigation's complaint that advanced telephone technologies would hinder law enforcement attempts to intercept communications,[165] Congress enacted CALEA.[166]

---

162. In this early proposal, each device has a unique serial number and unique encryption key. The government would keep a copy of these serial numbers and keys, enabling it to identify and decipher every message sent using them. The keys, however, would be split into two halves held by different government entities or "escrow agents." *Id.* at 171 (Box 5-1, "Key Technical Attributes of the Clipper Initiative").

163. Wyman Berryessa, *Escrowed Encryption Systems: Current Public Policy May Destroy Valued Constitutional Protections*, 23 U. DAYTON L. REV. 59, 80 (1997). Froomkin, *supra* note 85, at 827 ("Is mandatory key escrow, which takes place without a warrant, a search and seizure? If so, is it a reasonable warrantless search or seizure, or should a warrant be required?" (footnote omitted)).

164. Bernstein v. U.S. Dep't of Justice, 176 F.3d 1132, 1146 (9th Cir. 1999), *withdrawn by* 192 F.3d 1308, 1309 (9th Cir. 1999).

165. The problems asserted by the FBI included the following: The growth of wireless systems that could not always "accommodate multiple surveillances;" "increased competition in the tele-

CALEA requires telecommunications service providers to be able to provide law enforcement with the entire contents of a wiretapping target's communications, no matter what technology or service was involved in the transmission. It also provides "call setup information," such as information about who is calling, who is being called, and other information not directly related to the content of the conversation.[167]

Since CALEA's enactment, the Federal Bureau of Investigation (FBI), the Federal Communications Commission, and the telecommunications industry have been in continual struggles to establish compliance standards for CALEA's tappability requirements.[168] Currently, the FBI is seeking to extend CALEA to a variety of other services, including Internet telephony.[169]

---

communications industry" that permitted people to use more than one service provider, "making one-stop surveillance impossible;" "problems intercepting calls rerouted through call forwarding services and the inability to identify the destination of [speed-dialed calls];" "trouble in covertly isolating the communication stream associated with a particular target as multiplexed transmission technologies and fiber cables replaced the paired copper wires that traditionally had been associated uniquely with each customer." James X. Dempsey, *Communications Privacy in the Digital Age: Revitalizing the Federal Wiretap Laws to Enhance Privacy*, 8 ALB. L.J. SCI. & TECH. 65, 89–90 (1997) (footnote omitted).

166. Communications Assistance for Law Enforcement Act (CALEA), Pub. L. No. 103-414, 108 Stat. 4279 (1994) (codified at 47 U.S.C. §§ 1001–1010 (2000) and in scattered sections of 18 U.S.C.).

167. 47 U.S.C. § 1002 (2000). This information is needed to identify the calls that law enforcement wishes to intercept.

168. *See* Michael O'Neil & James X. Dempsey, *Critical Infrastructure Protection: Threats to Privacy and Civil Liberties and Concerns with Government Mandates on Industry*, 12 DEPAUL BUS. L.J. 97, 108 (1999/2000). Two commentators explained:

> An industry technical standards body spent years developing standards for digital switching equipment to accommodate law enforcement's need for continued ability to perform court ordered wiretaps only to have the FBI reject the effort because it did not contain additional capabilities the FBI had either disavowed or never mentioned at the time the statute was drafted.

Id.; *see also* Lillian BeVier, *The Communications Assistance for Law Enforcement Act of 1994: A Surprising Sequel to the Break Up of AT&T*, 51 STAN. L. REV. 1049, 1114–15 (1999) ("Claiming always to be acting according to CALEA's letter and spirit, the FBI has often overreached and more often than not adopted an intransigent bargaining position.").

169. In early 2004, the Justice Department, the FBI, and the Drug Enforcement Administration jointly petitioned the Federal Communications Commission (FCC) to impose the CALEA requirements on Internet voice and broadband access providers. *See* Joint Petition for Rulemaking to Resolve Various Outstanding Issues Concerning the Implementation of the Communications Assistance for Law Enforcement Act, RM-10865 (filed Mar. 10, 2004), *available at* http://www.askcalea.com/docs/20040310.calea.jper.pdf. The FCC then issued a Notice of Proposed Rulemaking to solicit public comment on the DOJ/FBI petition, and issued a proposed rule. Communication Assistance for Law Enforcement Act, 69 Fed. Reg. 56,976 (Sept. 23, 2004) (to be codified at 47 C.F.R. pts 22, 24, 26). In the Notice of Proposed Rulemaking, the FCC tentatively concluded that CALEA should be applied to all facilities-based providers of broadband Internet access service, "including wireline, cable modem, satellite, wireless, broadband access

CALEA in effect mandates that telecommunications be designed to facilitate government surveillance. This initiative illustrates my second normative argument against government interference with precautions—the concern that government will distort the normal development of technological privacy precautions. Under CALEA, "carriers must take steps to ensure that the broad technological trends in the industry do not eliminate law enforcement access to communications of targeted individuals."[170] CALEA therefore affects all of the privacy precautions associated with new and future telephony technologies. For instance, carriers subject to CALEA cannot provide carrier-based encryption services without assuring that law enforcement can decrypt the communications.[171] Users can still encrypt their own communications, but one of the most natural points for embedding privacy precautions—the phone companies themselves—was made less attractive from a privacy standpoint because of CALEA's "tappability" requirement.

CALEA also illustrates a longer-term practical danger with serious privacy implications: "[U]se of the law's coercive powers to order telecommunications providers to devise technological solutions to law enforcement's emerging technology-generated problems and in its insertion of the government into the *design* of the nation's telecommunications infrastructure."[172] A company that develops a CALEA-compliant protocol or product may do so on its own, or at the behest of the government.[173] A pervasive government role in technology development and implementation may make it impossible even to distinguish private from government interferences with precautions.

The privacy precautions associated with "digital telephony" were unintentional in the sense that the telephone companies did not intend to frustrate government surveillance. They were, however, privacy precautions nonetheless, and like the phone booth doors in *Katz*, might have become part of our societal privacy expectations. If the government wishes to infringe our right to use these precautions, it should face significant constitutional scrutiny.

---

via powerline companies," and also to "managed" or "mediated" voice over Internet protocol (VoIP services). *Id.* at 59,678.

170. *See* Dempsey, *supra* note 165, at 90.

171. 47 U.S.C. § 1002(b)(3) (2000) ("A telecommunications carrier shall not be responsible for decrypting, or ensuring the government's ability to decrypt, any communication encrypted by a subscriber or customer, unless the encryption was provided by the carrier and the carrier possesses the information necessary to decrypt the communication.").

172. BeVier, *supra* note 168, at 1072.

173. For instance, Cisco Systems, Inc. published a proposal for CALEA-friendly routers. *See* Declan McCullagh, *New Spy Tools—for Good or Evil?*, CNET News.com (Apr. 21, 2003), *available at* http://zdnet.com.com/2100-1107-997590.html.

C. How to Decide Whether the Precautions Right Has Been Violated

For two reasons, the precautions cluster-right should be protected by a version of strict scrutiny. These reasons are that government actions must be open and that laws and regulations must be able to withstand challenges due to the vulnerability of the Fourth Amendment's protections. Mandated tappability illustrates how the analysis might work.

First, any such government action must be open and public, otherwise, there is too great a risk that the public will be unaware that the government has manipulated the social environment, or even if they are aware, how it had been manipulated.[174] That is, even if the government publicly announced that it would randomly conduct surveillance, the public would not necessarily know what kinds of surveillance were being used. It should be unconstitutional for the government to make, or attempt to make, secret arrangements with telephone companies, Internet Service Providers, or equipment vendors that interfere with precautions.[175] Moreover, absent a clear public statement, judicial review of such interferences would be difficult.[176] Government may only interfere with precautions via con-

174. The obvious analogy is to covert surveillance. In the early 1950s, Americans held contradictory views about electronic surveillance:

> On the one hand, they feared that eavesdroppers were using increasingly sophisticated electronic tools to violate their privacy and record their every move and conversation. On the other hand, they considered tales of such surveillance to be the overblown product of paranoia. The public did not know whether to believe law enforcement's claim that if it was using electronic surveillance at all it was for a good cause and strictly limited.

Susan Freiwald, *Online Surveillance: Remembering the Lessons of the Wiretap Act*, 56 ALA. L. REV. 9, 10 (2004) (citing SAMUEL DASH ET AL., THE EAVESDROPPERS 3–4 (photo. reprint 1979) (1959)).

175. As Freiwald explains, government agents often conducted illegal electronic surveillance "with the cooperation of local phone companies, who conspired with agents to keep surveillance secret in order to maintain public confidence in the telephone networks." *Id.* at 12 (footnote omitted).

176. One might draw an analogy to First Amendment doctrines shaped by concerns about self-censorship. Licensing schemes for speech or tools of speech like news racks may be tested on their face; they must articulate "narrow, objective, and definite" licensing standards for officials to follow; and they must contain procedural safeguards to limit officials' strategic use of discretion. City of Lakewood v. Plain Dealer Publ'g Co., 486 U.S. 750, 756–59 (1988). Without clear standards, "*post hoc* rationalizations by the licensing official and the use of shifting or illegitimate criteria are far too easy." *Id.* at 758.

gressional enactments or publicly noticed administrative proceedings with significant accountability provisions.[177]

Second, it should be possible to challenge such laws or regulations, subject to the familiar strict scrutiny test, which demands a "compelling" government interest and that the restriction must be the least restrictive alternative. The stringency of this test is justified based on the need for "Fourth Amendment prophylaxis"[178] to secure the fundamental right conferred by the Fourth Amendment.

Mandated tappability provides an example of how the analysis might work. CALEA might fail the requirement that government interference with precautions must be open and public. Although CALEA is a public law and contains some public accountability mechanisms, its "safe harbor" standards are developed by industry with considerable FBI input.[179] The overall accountability of CALEA implementation is opaque to outsiders.

Notably, CALEA independently might fail the strict scrutiny test. While a law enforcement or national security interest would certainly be asserted in favor of restricting precautions, it is impossible to say whether the government could empirically establish the interest. The government first would have to establish the value of electronic surveillance as a law enforcement tool,[180]

---

177. *See, e.g.*, Dempsey, *supra* note 165, at 102–04 (discussing the need for accountability in CALEA implementation); Slobogin, *supra* note 82, at 297 (discussing notice for public video surveillance).

178. Prophylaxis, in this context, means overprotecting a constitutional right or value because of its expected vulnerability. *See, e.g.*, NAACP v. Button, 371 U.S. 415, 432–33 (1963) (explaining that First Amendment doctrines of vagueness and overbreadth apply even if the complainant did not engage in conduct protected by the First Amendment, because "[t]hese freedoms are delicate and vulnerable, as well as supremely precious in our society"); Brian Landsberg, *Safeguarding Constitutional Rights: The Uses and Limits of Prophylactic Rules*, 66 TENN. L. REV. 925, 926–27 (1999) (defining "prophylactic rules" as "those risk-avoidance rules that are not directly sanctioned or required by the Constitution, but that are adopted to ensure that the government follows constitutionally sanctioned or required rules" and "directed against the risk of noncompliance with a constitutional norm" (footnote omitted)); David Strauss, *The Ubiquity of Prophylactic Rules*, 55 U. CHI. L. REV. 190, 190 (1988) (discussing First Amendment prophylaxis and suggesting that prophylactic rules "are a central and necessary feature of constitutional law").

179. Dempsey, *supra* note 165, at 96 (arguing that "the FBI's participation went beyond the consultation intended by Congress and instead amounted to an effort to dominate the standards process and dictate specific surveillance features").

180. As Professor BeVier has argued,

> [o]ne would need more factual support than . . . repeated assertions that it is theoretically useful in thwarting terrorists, kidnappers, and organized criminals. One would need to know such things as the cost of each tap in terms of law enforcement resources, the opportunity costs of using wiretapping instead of devoting the same resources to other crime fighting techniques, how many (and what kinds) of crimes were actually prevented, detected, or proven by wiretaps, and how many of those would (probably) have gone unprevented, undetected, or unproven without wiretaps.

and then establish the value of CALEA in maintaining tappability.[181]

V. CONCLUSION

This Article has argued that we have a constitutional right to take privacy precautions. Privacy precautions are important for two reasons. First, for better or worse, the Supreme Court has made precautions significant to the judicial determination of whether our privacy expectations are reasonable, or even exist. Our Fourth Amendment privacy rights therefore depend on the variety of precautionary techniques—both physical and social—that we use to produce privacy in everyday life. Second, Fourth Amendment privacy turns on social "understandings" that "must have a source outside of the Fourth Amendment"[182] and "are in large part reflections of laws that translate into rules the customs and values of the past and present."[183]

Precautions are a central part of the social system of privacy. One might say that precautions are essential to the language of privacy: We use precautions to express our desire for privacy and we expect others to respect those precautions. Accordingly, our precautionary behavior is an integral part of our social "understandings," and as such they should be protected against undue government interference.

BeVier, *supra* note 168, at 1113.

181. *Id.* at 1112–13 (noting that "CALEA practically guarantees that either too few or too many resources will be devoted to actually maintaining wiretap capability"); *id.* at 1113–14 ("CALEA is an invitation to allocational inefficiency" because "a substantial portion of the costs of maintaining its technological capability are externalized by the FBI to the telecommunications industry . . . . in disregard of one of economics' most basic insights" (footnote omitted)). Professor BeVier further argued that

> the FBI, which is the agency that ought to have the most incentive to measure costs and benefits accurately—to minimize the costs, maximize the benefits, and stop expending resources when costs exceed benefits—instead will have no real way even to *know* the costs. It will be motivated to externalize (and thus hide) as many of the costs as possible and to exaggerate the benefits.

Id. at 1114 (footnote omitted). Whether CALEA is the least restrictive alternative for furthering the government's law enforcement interest is far beyond the scope of this Article.

182. Rakas v. Illinois, 439 U.S. 128, 143 n.12 (1978).

183. United States v. White, 401 U.S. 745, 786 (1971) (Harlan, J., dissenting); *cf. Rakas*, 439 U.S. at 143–44 n.12 (finding that it is "merely tautological" to base legitimate expectations "primarily on cases deciding exclusionary-rule issues in criminal cases").