Indiana Law Journal

Volume 90 | Issue 1 Article 3

Winter 2015

Furtive Encryption: Power, Trusts, and the Constitutional Cost of Collective Surveillance

Jeffrey L. Vagle
University of Pennsylvania Law School, jvagle@law.upenn.edu

Furtive Encryption: Power, Trust, and the Constitutional Cost of Collective Surveillance

JEFFREY L. VAGLE*

Recent revelations of heretofore secret U.S. government surveillance programs have sparked national conversations about their constitutionality and the delicate balance between security and civil liberties in a constitutional democracy. Among the revealed policies asserted by the National Security Agency (NSA) is a provision found in the "minimization procedures" required under section 702 of the Foreign Intelligence Surveillance Act of 1978. This provision allows the NSA to collect and keep indefinitely any encrypted information collected from domestic communications—including the communications of U.S. citizens. That is, according to the U.S. government, the mere fact that a U.S. citizen has encrypted her electronic communications is enough to give the NSA the right to store that data until it is able to decrypt or decode it.

Through this provision, the NSA is automatically treating all electronic communications from U.S. citizens that are hidden or obscured through encryption—for whatever reason—as suspicious, a direct descendant of the "nothing-to-hide" family of privacy minimization arguments. The ubiquity of electronic communication in the United States and elsewhere has led to the widespread use of encryption, the vast majority of it for innocuous purposes. This Article argues that the mere encryption by individuals of their electronic communications is not alone a basis for individualized suspicion. Moreover, this Article asserts that the NSA's policy amounts to a suspicionless search and seizure. This program is therefore in direct conflict with the fundamental principles underlying the Fourth Amendment, specifically the protection of individuals from unwarranted government power and the establishment of the reciprocal trust between citizen and government that is necessary for a healthy democracy.

---

* Lecturer in Law and Executive Director, Center for Technology, Innovation and Competition, University of Pennsylvania Law School. Special thanks to Jennifer Granick, Duncan Hollis, and Christopher Sprigman for their comments on earlier drafts of this Article.

INTRODUCTION

In June 2013, a twenty-nine-year-old former Central Intelligence Agency (CIA) systems administrator and NSA private contractor named Edward Snowden publicly disclosed that he was the source of top-secret documents disclosed to journalists regarding multiple secret surveillance programs within the NSA and other agencies.[1] The subsequent publication of some of these leaked government documents has triggered a firestorm of discussion—often overheated—on topics ranging from the nature of (and need for) government secrecy;[2] the adequacy of background checks for government employees and contractors;[3] Mr. Snowden's girlfriend;[4] Mr. Snowden's status as hero or traitor;[5] the plight of whistleblowers;[6]

---

1. *See* Barton Gellman, Aaron Blake & Greg Miller, *Man Who Leaked NSA Secrets Steps Forward*, WASH. POST, Jun. 10, 2013, at A01; Glenn Greenwald, Ewan MacAskill & Laura Poitras, *Edward Snowden: The Man Responsible for the Leaks of Secret Documents Detailing the NSA's Widespread Phone and Internet Surveillance*, GUARDIAN, June 10, 2013, at 2; Mark Mazzetti & Michael S. Schmidt, *Ex-C.I.A. Worker Says He Disclosed U.S. Surveillance*, N.Y. TIMES, June 10, 2013, at A1; M.G., *Surveillance in America: Over to the Dark Side*, ECONOMIST (June 10, 2013), http://www.economist.com/blogs/democracyinamerica/2013/06/surveillance-america-0.

2. *See, e.g.*, Mark Bowden, *What Snowden and Manning Don't Understand About Secrecy*, ATLANTIC (Aug. 23, 2013, 7:00 AM), http://www.theatlantic.com/politics/archive/2013/08/bowden-manning-snowden/278973/.

3. *See, e.g.*, Brent Kendall & Dion Nissenbaum, *Leaker's Security Check Faulted*, WALL ST. J., Aug. 28, 2013, at A1.

4. *See, e.g.*, Joe Coscarelli, *Edward Snowden's Girlfriend Is a Pole-Dancing Acrobat with a Dramatic Blog*, N.Y. MAG. (June 11, 2013, 9:14 AM), http://nymag.com/daily/intelligencer/2013/06/edward-snowden-girlfriend-lindsay-mills-blog.html.

5. *See, e.g.*, Dana Milbank, Editorial, *Exposing the Zealous National Security State*, WASH. POST, Aug. 22, 2013, at A02.; Jeffrey Toobin, *Edward Snowden's Real Impact*, NEW YORKER (Aug. 19, 2013), http://www.newyorker.com/news/daily-comment/edward-snowdens-real-impact.

6. *See, e.g.*, Colman McCarthy, *Whistleblowers Shine Necessary Light on US Shadows*, NAT'L CATH. REP., Aug. 30, 2013, at 24; Dana Milbank, Editorial, *The Price of Whistleblowing*, WASH. POST, Aug. 21, 2013, at A17; Adam Waytz, James Dungan & Liane Young, *The Whistle-Blower's Quandry*, N.Y. TIMES, Aug. 4, 2013, at 12 SR; Eyal Press, *Whistleblower, Leaker, Traitor, Spy*, N.Y. REV. BOOKS (Aug. 5, 2013, 2:17 PM), http://www.nybooks.com/blogs/nyrblog/2013/aug/05/whistleblower-leaker-traitor-spy/.

and, finally, the legality, necessity, and wisdom of the secret surveillance of U.S. citizens.[7]

Hidden among the more dramatic revelations like PRISM[8] and XKeyscore[9] was a document approved by U.S. Attorney General Eric Holder that articulated "minimization procedures" required of the NSA under section 702 of the Foreign Intelligence Surveillance Act of 1978 (FISA).[10] One of the provisions listed in this

---

7. The debate over government surveillance of its citizens has created some odd bedfellows, with libertarian conservatives and (liberal) civil libertarians joining to oppose neoconservatives, neoliberals, and supporters of the Obama administration. *See, e.g.*, Philip Giraldi, *Edward Snowden Is No Traitor*, AM. CONSERVATIVE (July 16, 2013), http://www.theamericanconservative.com/articles/edward-snowden-is-no-traitor/; Michael Hayden, *Ex-CIA Chief: What Edward Snowden Did*, CNN (July 19, 2013, 11:31 AM), http://www.cnn.com/2013/07/19/opinion/hayden-snowden-impact; Seth Mandel, *Of Course America Spies on the UN*, COMMENT. MAG. (Aug. 27, 2013, 1:30 PM), http://www.commentarymagazine.com/2013/08/27/of-course-america-spies-on-the-un/; Karen McVeigh, *NSA Surveillance Program Violates the Constitution, ACLU Says*, GUARDIAN (Aug. 27, 2013, 3:31 PM), http://www.theguardian.com/world/2013/aug/27/nsa-surveillance-program-illegal-aclu-lawsuit; Susan Milligan, *Snowden: Both a Hero and a Traitor?*, U.S. NEWS & WORLD REP. (Aug. 1, 2013, 9:35 AM), http://www.usnews.com/opinion/blogs/susan-milligan/2013/08/01/edward-snowden-leaves-russias-moscow-airport-both-a-hero-and-a-traitor; Pierre Thomas, Mike Levine, Jack Date, Luis Martinez & Jack Cloherty, *Officials: How Edward Snowden Could Hurt the U.S.*, ABC NEWS (June 24, 2013, 6:38 PM), http://abcnews.go.com/blogs/headlines/2013/06/officials-how-edward-snowden-could-hurt-the-u-s/.

8. PRISM is the name of a formerly secret NSA mass-surveillance program that gathers data by "tapping directly into the central servers of nine leading U.S. Internet companies, extracting audio and video chats, photographs, e-mails, documents, and connection logs that enable analysts to track foreign targets." Barton Gellman & Laura Poitras, *U.S. Mines Internet Firms' Data, Documents Show*, WASH. POST, June 7, 2013, at A01.

9. XKeyscore is the name of a formerly clandestine NSA system used for searching and analyzing the vast quantities of data collected from individuals across the globe. *See, e.g.*, Sean Gallagher, *NSA's Internet Taps Can Find Systems To Hack, Track VPNs and Word Docs*, ARS TECHNICA (Aug. 1, 2013, 5:30 PM), http://arstechnica.com/tech-policy/2013/08/nsas-internet-taps-can-find-systems-to-hack-track-vpns-and-word-docs/.

10. NSA, EXHIBIT B: MINIMIZATION PROCEDURES USED BY THE NATIONAL SECURITY AGENCY IN CONNECTION WITH ACQUISITIONS OF FOREIGN INTELLIGENCE INFORMATION (2007), *available at* http://www.theguardian.com/world/interactive/2013/jun/20/exhibit-b-nsa-procedures-document [hereinafter MINIMIZATION PROCEDURES EXHIBIT B]. Section 702 of FISA articulates certain procedures and limitations that the Attorney General and the Director of National Intelligence may jointly authorize on "the targeting of persons reasonably believed to be located outside the United States to acquire foreign intelligence information." 50 U.S.C. § 1881a(a) (2012). Among these limitations, which require that any surveillance "shall be conducted in a manner consistent with the fourth amendment to the Constitution of the United States," is the provision that the targeting of surveillance subjects be subject to "minimization procedures" designed to "ensure that an acquisition authorized under subsection (a) is limited to targeting persons reasonably believed to be located outside the United States," and to "prevent the intentional acquisition of any communication as to which the sender and all intended recipients are known at the time of the acquisition to be located in the United States." § 1881a(b)–(e). Compliance with these FISA requirements is subject to review by the Foreign Intelligence Surveillance Court. § 1881a(i)(1)(A).

document applied specifically to encrypted information and allowed the NSA to collect and keep indefinitely any information obtained from "domestic communications"—which includes the communications of U.S. citizens—for "cryptanalytic, traffic analytic or signal exploitation purposes."[11] In other words, under these minimization procedures, the mere fact that data is encrypted is alone enough to give the NSA the right to store that data (regardless of its U.S. or foreign origin) and hold it for as long as it takes to decrypt it.[12]

The implications that flow from this policy are stunning. The NSA is automatically treating all electronic communications from U.S. citizens that are hidden or obscured through encryption—for whatever reason—as suspicious, a direct descendant of the "nothing-to-hide" family of privacy minimization arguments. Common arguments made in the defense of government surveillance typically follow one of two closely related themes: "If you have nothing to hide, you have nothing to fear" (the government's perspective), or "I have nothing to hide, so I have no objection to government surveillance." These "nothing-to-hide" arguments and their ilk can be superficially compelling and have been made for some time.[13] But don't we all have *something* to hide? After all, as Lavrenti Beria, head of Joseph Stalin's secret police, supposedly said, "Show me the man, and I'll find you the crime."[14] This is a rather weak response, however, especially against a "nothing-to-hide" argument based on minimal, nonpublic intrusions of privacy interests. Scholars and commentators have addressed the "nothing-to-hide" argument in more depth.[15]

Putting aside the fact that the NSA had been less than truthful—both to the public as well as to other branches of government—about the existence and nature of such broad and legally questionable surveillance programs,[16] this sort of blanket

---

11. MINIMIZATION PROCEDURES EXHIBIT B, *supra* note 10, at 2.

12. "In the context of cryptanalytic effort, maintenance of technical data bases requires retention of all communications that are enciphered or reasonably believed to contain secret meaning, and sufficient duration may consist of any period of time during which encrypted material is subject to, or of use in, cryptanalysis." *Id*. at 5.

13. *See, e.g.*, HENRY JAMES, THE REVERBERATOR 183 (Grove Press, Inc. 1979) (1888) ("[I]f these people had done bad things they ought to be ashamed of themselves and he couldn't pity them, and if they hadn't done them there was no need of making such a rumpus about other people knowing.").

14. Roger Cohen, *The Real Threat to America*, N.Y. TIMES (Nov. 25, 2010), http://www.nytimes.com/2010/11/26/opinion/26iht-edcohen.html.

15. *See, e.g.*, DANIEL J. SOLOVE, NOTHING TO HIDE: THE FALSE TRADEOFF BETWEEN PRIVACY AND SECURITY (2011); Jennifer Granick, *Surveillance Myth #1: I Have Nothing To Hide*, STAN. L. SCH. CENTER FOR INTERNET & SOC'Y (June 24, 2013, 12:58 PM), http://cyberlaw.stanford.edu/blog/2013/06/surveillance-myth-1-i-have-nothing-hide; Bruce Schneier, *The Eternal Value of Privacy*, WIRED (May 18, 2006), http://www.wired.com /politics/security/commentary/securitymatters/2006/05/70886. I will explore this issue in more detail in Part II, *infra*.

16. In March 2013, Director of National Intelligence James Clapper testified before Congress and was asked whether the NSA collected any type of data on U.S. citizens. He responded, "No sir." Once the documents revealed by Edward Snowden in June 2013 made it clear that this denial was simply not true, Mr. Clapper told NBC that his answer had been the "least untruthful" answer possible. Tabassum Zakaria, *U.S. Spy Agency Edges into the*

suspicion by a government of its citizens goes far beyond the "individualized suspicion of wrongdoing" generally required by the Fourth Amendment for a reasonable search.[17] Exceptions to the Fourth Amendment warrant requirement have been established in the past few decades to permit searches under specified conditions: the government may have "special needs" beyond the scope of normal law enforcement,[18] or the government may have a foreign intelligence surveillance exemption.[19] In this Article, I argue that neither limited exception applies here. Furthermore, generalized domestic government surveillance programs have been anathema to Americans from the earliest days of the nation,[20] and the use of technological methods to achieve what the Framers would have found abhorrent[21] is feeding an accelerating erosion of trust between the U.S. government and its people.

This Article is an effort to demonstrate how collective surveillance without a basis of suspicion not only violates the Fourth Amendment but does so in a way that corrupts two principal constitutional tenets—protection of individuals from undue governmental power and the mutual trust between government and citizen that must exist in a healthy democratic society.[22] Current Fourth Amendment

---

Light After Snowden Revelations, REUTERS, Aug. 25, 2013, *available at* http://www.reuters.com/article/2013/08/25/us-usa-security-nsa-idUSBRE97O08120130825; *see also* Ruth Marcus, Editorial, *More NSA Deceptions*, WASH. POST, Aug. 23, 2013, at A19; John Fund, *Time for Answers from the NSA*, NAT'L REV. ONLINE (Aug. 19, 2013, 4:00 AM), http://www.nationalreview.com/article/356098/time-answers-nsa-john-fund.

17. City of Indianapolis v. Edmond, 531 U.S. 32, 37 (2000) (citing Chandler v. Miller, 520 U.S. 305, 308 (1997)).

18. The "special needs" doctrine has been applied in certain limited circumstances to uphold suspicionless searches where the government program was designed to serve "special needs, beyond the normal need for law enforcement." Vernonia Sch. Dist. 47J v. Acton, 515 U.S. 646, 653 (1995) (quoting Griffin v. Wisconsin, 483 U.S. 868, 873 (1987)) (applying doctrine to random drug testing of student athletes); *see also* Nat'l Treasury Emps. Union v. Von Raab, 489 U.S. 656, 665–66 (1989) (applying doctrine to drug tests for United States Customs Service employees seeking transfer or promotion to certain positions); Skinner v. Ry. Labor Execs.' Ass'n, 489 U.S. 602, 619–20 (1989) (applying doctrine to drug and alcohol tests for railway employees involved in train accidents or found to be in violation of particular safety regulations). I will examine the applicability of this doctrine to the NSA's policy of suspicionless collection and indefinite storage of all domestic encrypted data in Part II, *infra*.

19. I will more fully discuss FISA, 50 U.S.C. §§ 1801–1871 (2012), and related Fourth Amendment exceptions under "national security" conditions, in Part II.E, *infra*. I will note here that the Supreme Court has held that a domestic surveillance exception to the Fourth Amendment does not exist, even when the surveillance is under the umbrella of national security. *See* United States v. U.S. Dist. Court for the E. Dist. of Mich., 407 U.S. 297 (1972).

20. "The makers of our Constitution . . . conferred, as against the Government, the right to be let alone—the most comprehensive of rights and the right most valued by civilized men. To protect that right, every unjustifiable intrusion by the Government upon the privacy of the individual, whatever the means employed, must be deemed a violation of the Fourth Amendment." Olmstead v. United States, 277 U.S. 438, 478 (1928) (Brandeis, J., dissenting), *overruled in part by* Katz v. United States, 389 U.S. 347 (1967).

21. *See Ry. Labor Execs. Ass'n*, 489 U.S. at 655 (Marshall, J., dissenting) (expressing opinion that "the Framers would be appalled by the vision of mass governmental intrusions").

22. In this Article, I distinguish *collective* or *pervasive* surveillance of the kind revealed in the Snowden documents, which show implementation and execution of such surveillance without benefit of law, from *targeted* surveillance of individuals, which requires court

doctrine has, unfortunately, largely ignored these principles in favor of a balancing test between the needs of the government and an individual's reasonable expectation of privacy.[23] While privacy indeed emerges from these principles, advances in surveillance-enabling technologies are rapidly making privacy a poor proxy for protection from government power and the enhancement of mutual societal trust. The Supreme Court's shift to a factual analysis and quantification of privacy has drawn attention away from the consideration of fundamental constitutional values and has led to some rather bizarre, fact-specific arguments.

I argue that our current Fourth Amendment theories of privacy have become a sort of Maginot Line: a once-powerful deterrent made gradually irrelevant by technological advances, one that has therefore become unable to protect individuals from a government with the technological capability and desire to collect and store for future reading that which we have clearly designated as private—our encrypted data. Faced with this reality, we must adjust Fourth Amendment doctrine to protect the underlying constitutional principles at stake.

I begin in Part I with a necessary, but brief, introduction to encryption, its uses, and why it provides an important bulwark against unreasonable government intrusions. Part II examines the amorphous concepts of security, secrecy, and privacy, as well as the mistaken presumption by courts of privacy's factual and quantifiable nature. This Part additionally provides a historical analysis of Fourth Amendment doctrine and its tense relationship with technology. I also examine the historical underpinnings of current Fourth Amendment "balancing" doctrine in light of what Foucault referred to as *panopticism*.[24] In Part III, I argue that the generalized, arbitrary, and warrantless collection by government of its citizens' private communications, merely because those citizens wish to keep those communications private, is in direct conflict with the constitutional intent to protect individuals from undue state power. In Part IV, I return to an analysis of current Fourth Amendment doctrine to argue that this doctrine, based on a reasonable-expectation-of-privacy test, neglects the important constitutional value of trust. I make the case that one of the core principles that gave life to the Constitution is the philosophy that reciprocal trust between government and its citizens is necessary for a healthy democratic society.

I. A GENTLE INTRODUCTION TO CRYPTOGRAPHY

A. Why Encrypt?

The practice of encrypting communications to ensure (or attempt to ensure) their privacy has existed in one form or another for thousands of years.[25] While not all of the examples over the past 4000 years would appear on their surface to be

---

approval on a case-by-case basis.

23. *See infra* Part II.A–B.

24. *Panopticism* is defined as the type of power applied by the State to individual citizens in the form of continuous individual supervision. *See* Michel Foucault, *Truth and Juridical Forms*, *in* POWER: ESSENTIAL WORKS OF FOUCAULT 1954–1984, at 1, 70 (James D. Faubion ed., Robert Hurley et al. trans., The New Press 1994).

25. The earliest known evidence of secret writing—or encryption—dates back to about 1900 BC. *See* DAVID KAHN, THE CODEBREAKERS: THE STORY OF SECRET WRITING 71 (1967).

encryption as we now know it, different forms of cryptography[26] have been used by priests,[27] emperors,[28] diplomats,[29] generals,[30] spies,[31] merchants,[32] insurgents,[33] dissidents,[34] criminals,[35] prisoners, and lovers.[36] Clearly, the specific reasons behind an individual's desire to obscure or otherwise hide her communications or

---

26. *Cryptography* is the science of creating and using methods of obscuring or disguising messages with ciphers, codes, and other techniques so that only certain people can read the original (unencrypted) message. A *cipher* is a method of encrypting any text regardless of its content. A *code* is a system of communication that relies on a prearranged mapping of meanings, for example, a codebook. *Cryptology* is the study of cryptography and cryptanalysis. *See id.* at xiii–xvi.

27. Examples of religious uses of cryptography range from ancient Egyptian hieroglyphics on tomb walls, to the use of substitutions in Hebrew Holy Scriptures, to fourteenth-century Koranic writings, to Viking Age cipher runes. It is not always clear what the reasoning was behind encrypting religious texts, but scholars generally believe that the secrecy added to the mystery and arcane magical powers of religious writings. *See id.* at 71–98.

28. It is believed that Julius Caesar used a cipher to encrypt his messages to Cicero and others, which substituted the letters of the original text with letters three places further down the alphabet. To this day, such substitution ciphers are called Caesar ciphers. *See id.* at 83–84.

29. Blaise de Vigenère, the inventor of the archetype of polyalphabetic substitution cipher systems, was first exposed to cryptology in 1549 while he was a diplomat in service to the Duke of Nevers. *Id.* at 145–46.

30. In eleventh century China, the military document *Wu-ching tsung-yao* ("Essentials from Military Classics") prescribed a code of forty items ranging from requests for arrows to reports from front lines. *Id.* at 73.

31. *Artha-śāstra*, the classic Indian work on statecraft, describes the espionage service of India and recommends that spies be given assignments via secret writings. *Id.* at 74.

32. An early example of encryption to protect valuable intellectual property was found in a 3500-year-old remnant of a Mesopotamian potter's cipher to protect his new glazing formula. BRUCE SCHNEIER, SECRETS AND LIES: DIGITAL SECURITY IN A NETWORKED WORLD 86 (2000).

33. During the French wars of religion, Huguenots encrypted their internal correspondence. The decryption of one of these messages by the French royal army in 1628 led to the surrender of Huguenot forces at Realmont. KAHN, *supra* note 25, at 157.

34. For their official correspondence, Tibetans use a cipher called "rin-spuns," named for its inventor Rin-c'(hhen-)spuns(-pa), who lived in the fourteenth century. *Id.* at 84.

35. During the era of Prohibition in the United States, bootleggers used encoded radio messages to coordinate the movement between ships smuggling liquor from overseas and the small speedboats that would bring the cargo ashore. *Id.* at 802–03.

36. Ovid, in the *Art of Love*, counseled secret lovers on how to keep their correspondence secret:

> If the guard sees through these tricks, she can go one better: / Offer her back to write on, *be* your letter. / Safe and undetectable by the eye / Is writing in milk— later, just apply / A sprinkling of coal-dust and presto! you can read. / Or write in oil of linseed / Oozing from a stalk of flax— / And your words are invisible on what seems blank wax.

OVID, THE ART OF LOVE bk. 3, at 157 (James Michie trans., Modern Library 2002) (c. 2 C.E.) (emphasis in original).

In the nineteenth century, lovers would secretly contact one another through encrypted messages in so-called agony columns of newspapers. Unfortunately for the communicants, most of these messages were encrypted using elementary encryption methods, such that almost anyone could decipher these messages with a bit of effort. KAHN, *supra* note 25, at 775.

papers from unwanted gazes can vary widely. But there is a common thread throughout history of a strong—perhaps innate—need for people to have the ability to keep certain things secret.[37]

One of the more dramatic historical uses of cryptography—and a cautionary tale for those tempted to use weak encryption methods—can be found in the tragic tale of Mary, Queen of Scots.[38] While imprisoned in England by Queen Elizabeth I, Mary used a cipher to encrypt her correspondence with her supporters.[39] Queen Elizabeth, correctly sensing threats to her government (and person) at home and abroad, tasked Sir Francis Walsingham with establishing an espionage network throughout England and Europe.[40] Walsingham's agents intercepted Mary's encrypted messages and discovered a plot to assassinate Elizabeth and install Mary in her place.[41] Mary's coconspirators were quickly arrested and subsequently executed. Mary was tried in October of that year; in February 1587, Queen Elizabeth signed Mary's death warrant, and she was beheaded.[42]

At its core, the ability to keep things secret is a form of power.[43] Similarly, the ability to learn someone's secrets—either surreptitiously or overtly—and use the information learned is also a form of power. The conflict between the individual's power to keep her secrets from the government and the government's power to learn those secrets creates tensions that tend to manifest themselves in arguments over privacy. In this context, "the right to privacy has everything to do with delineating the legitimate limits of governmental power."[44]

Until relatively recently, however, those who wished to keep their communications secret could be much more confident in their privacy than they can today. Simply finding a secluded area well out of earshot of potential eavesdroppers could defeat all adversaries until the invention of the parabolic microphone and similar technologies. If the parties weren't able to have such a face-to-face private conversation, they could encrypt their letters using

---

37.

> Without the ability to keep secrets, individuals lose the capacity to distinguish themselves from others, to maintain independent lives, to be complete and autonomous persons . . . . This does not mean that a person actually has to keep secrets to be autonomous, just that she must possess the *ability* to do so. The ability to keep secrets implies the ability to disclose secrets selectively, and so the capacity for selective disclosure at one's own discretion is important to individual autonomy as well.

KIM LANE SCHEPPELE, LEGAL SECRETS: EQUALITY AND EFFICIENCY IN THE COMMON LAW 302 (1988) (emphasis in original) (footnote omitted).

38. SIMON SINGH, THE CODE BOOK: THE EVOLUTION OF SECRECY FROM MARY QUEEN OF SCOTS TO QUANTUM CRYPTOGRAPHY 32–44 (1999).

39. *Id.* at 37–40.

40. *See id.* at 39.

41. *Id.* at 40–41.

42. *Id.* at 42–44.

43. While "[a] measure of control over secrecy and openness—and thus of one form of power—is needed in personal life for equilibrium, liberty, even survival," when linked, "secrecy and political power are dangerous in the extreme." SISSELA BOK, SECRETS: ON THE ETHICS OF CONCEALMENT AND REVELATION 106 (1982).

44. Jed Rubenfeld, *The Right of Privacy*, 102 HARV. L. REV. 737, 737 (1989).

then-unbreakable ciphers.[45] Even long after the proliferation of the telephone, it was difficult to trace incoming calls due to the slow mechanical equipment used by the carriers, even with a warrant.[46]

Today, networked computing and communication has permeated everyday life.[47] For most of us, significant amounts of information describing our purchases, comings and goings, likes and dislikes, circles of friends, socioeconomic statuses, affiliations, and thoughts now make their way across countless unknown networks to be stored on countless unknown servers and potentially accessible to any number of interested parties. We may choose to willingly share some of this data, or we may concede that certain pieces of information are analogous to our activities while walking down a public street—it may be impossible to control their observation and dissemination. But there are certain segments of our lives that we may only choose to share with a select few. For example, you may see me walk into a bank's local branch and might therefore assume that I have an account there. I am likely aware of this fact, but it does not follow that I want to share my account balances with you as well. In another example, you may send an e-mail rather than a letter to your spouse, but that does not necessarily mean that your expectations of privacy in that e-mail are any different than if you sealed an envelope and entrusted it to the care of the Postal Service. Here, cryptography helps to regain some control over what data we choose to make public.

B. A Political History of Encryption in the United States

The U.S. government's views on the general availability of strong cryptography are complicated. Since World War I, the government has been heavily invested in the research and development of cryptographic systems. It had largely managed to keep a lid on these methods into the 1960s.[48] In 1967, despite the NSA's best

---

45. The Vigenère cipher was considered unbreakable in the seventeenth and eighteenth centuries. *See* SINGH, *supra* note 38, at 62–63. Successfully encrypting letters was, however, no guarantee that the intended recipient would ever receive them.

46. Prior to the invention of the transistor or the microprocessor, the routing of telephone calls took place using the equivalent of "stone knives and bearskins"—giant mechanical switches "jam-packed with wipers and ratchets and pawls and blades and other mechanical clockwork." PHIL LAPSLEY, EXPLODING THE PHONE: THE UNTOLD STORY OF THE TEENAGERS AND OUTLAWS WHO HACKED MA BELL 42–44 (2013).

47. William Gibson has aptly described this phenomenon as the *eversion of cyberspace*. *See* David Wallace-Wells, *William Gibson: The Art of Fiction No. 211*, PARIS REV., Summer 2011, at 107, *available at* http://www.theparisreview.org/interviews/6089/the-art-of-fiction-no-211-william-gibson. That is, the Internet ("cyberspace") we once thought of as *elsewhere*, accessible only through large, bulky boxes that were found only on desktops, and later, smaller (but still bulky) boxes we could optimistically use on our laps, has "colonized" our world—both physically, through networked computers we carry in our pocket and archaically call "phones," and sociologically, through our increased dependence on its availability. *See* William Gibson, Op-Ed., *Google's Earth*, N.Y. TIMES, Sept. 1, 2010, at A23.

48. World War I was the first war to be fought with the general availability of radio technology. Since radio broadcasts were, by definition, available to anyone with a receiver, governments quickly realized that some kind of cryptographic system had to be employed to ensure the secrecy of communications. The rapid advance of technology following the war,

efforts to quash it, David Kahn published *The Codebreakers*, the first nontechnical history of cryptography, which included descriptions of the technologies used in encryption and why they were important.[49] Kahn's book sparked a renewed and widespread interest in cryptography among scientists and engineers working outside the walls of the NSA.[50] By the early 1970s, the NSA conceded that cryptographic technologies should be made available to other agencies within the U.S. government. Together with the National Bureau of Standards, the NSA solicited industry proposals for a new cryptographic standard, which eventually resulted in the publication of the Data Encryption Standard (DES) in 1977.[51]

But the cryptographic genie truly left the government bottle in 1976 with the publication of a paper by two Stanford University researchers, which described a new cryptographic concept called "public key cryptography."[52] By 1977, three young MIT professors—Ron Rivest, Adi Shamir, and Len Adleman—built upon the concepts articulated in this paper to invent the first public-key encryption system, naming it with their initials (RSA).[53] Rivest was invited to present his work at the Institute of Electrical and Electronics Engineers (IEEE) annual meeting in

---

coupled with secret research done under the auspices of what would become the NSA, yielded improved automation and security of these secret government cryptosystems. *See* WHITFIELD DIFFIE & SUSAN LANDAU, PRIVACY ON THE LINE: THE POLITICS OF WIRETAPPING AND ENCRYPTION 49–53 (1998); KAHN, *supra* note 25, at 298–350.

49. Kahn's original manuscript contained information about the NSA, and the agency made attempts to stop its publication, including writing negative reviews of the work to be disseminated through the press to discredit him. JAMES BAMFORD, THE PUZZLE PALACE: A REPORT ON AMERICA'S MOST SECRET AGENCY 168–69 (1982). Kahn and his publisher eventually agreed to remove material concerning the relationship between the NSA and its British counterpart, the Government Communications Headquarters. *Id.* at 171–72.

50. The NSA began losing its monopoly on cryptography research even within the U.S. government. In 1944, a young German immigrant named Horst Feistel was granted U.S. citizenship, a security clearance, and a job at the Air Force Cambridge Research Center (AFCRC), a U.S. Air Force think tank dedicated to improving the cryptographic systems used in the identification of friendly—and unfriendly—aircraft. DIFFIE & LANDAU, *supra* note 48, at 56–57. After the NSA discovered this research, it shut down the AFCRC and appropriated the technology. Feistel then took his research to the Massachusetts Institute of Technology (MIT), Mitre, and eventually IBM. *Id.*

51. *See* SELECT COMM. ON INTELLIGENCE, U.S. SENATE, UNCLASSIFIED SUMMARY: INVOLVEMENT OF NSA IN THE DEVELOPMENT OF THE DATA ENCRYPTION STANDARD (1978), *available at* http://www.intelligence.senate.gov/pdfs/95nsa.pdf.

52. Whitfield Diffie & Martin E. Hellman, *New Directions in Cryptography*, 22 IEEE TRANSACTIONS ON INFO. THEORY 644 (1976), *available at* http://www-ee.stanford.edu/~hellman/publications/24.pdf. The revolutionary concept behind public-key cryptography lies in its ability to "split" the cryptographic key into two parts, a public key and a private key. Applying the mathematical principles I discuss in Part I.C, *infra*, Diffie and Hellman showed that, using their approach—aptly named the Diffie-Hellman key exchange—one could generate public-private key pairs in such a way that it was computationally infeasible to derive the private key solely from the public key. *Id.* Thus, Alice could share her public key with the world, which would allow Bob (and others) to encrypt messages to her using that key that could only be decrypted with Alice's secret key.

53. *See* R. L. Rivest, A. Shamir & L. Adelman, *A Method for Obtaining Digital Signatures and Public-Key Cryptosystems*, COMM. ACM, Feb. 1978, at 120, 126, *available at* http://ocw.bib.upct.es/pluginfile.php/5337/mod_resource/content/1/rsa_base.pdf.

October 1977, but the IEEE received a letter warning that Rivest's talk was a potential violation of the U.S. International Traffic in Arms Regulations (ITAR),[54] since foreign nationals would likely be present at the meeting.[55]

The ITAR regulates the import and export of defense-related goods and services by designating such items to the United States Munitions List (USML), as authorized under the Arms Export Control Act (AECA).[56] Items listed on the USML, unless otherwise exempted, require a license to import or export.[57] In the past, these items included "[c]ryptographic (including key management) systems, equipment, assemblies, modules, integrated circuits, components or software with the capability of maintaining secrecy or confidentiality of information or information systems."[58]

The government's use of ITAR to control the import and export of nonmilitary cryptographic systems and software was curtailed in 1996 when a California federal district court was asked to decide whether the ITAR licensing requirements constituted unlawful prior restraint, thus violating the First Amendment right to free expression.[59] The plaintiff in *Bernstein* was a University of California, Berkeley graduate student in mathematics who developed an encryption algorithm he called "Snuffle."[60] Bernstein had documented his algorithm both as an academic

---

54. 22 U.S.C. § 2778 (2012).

55. *See* Stephen H. Unger, *Privacy, Cryptography and Free Research*, IEEE TECH. & SOC'Y, Dec. 1977, at 8. It was later discovered that the letter's author worked for the NSA. The NSA denied any connection with the letter, and Rivest presented his paper at the IEEE conference in October. DIFFIE & LANDAU, *supra* note 48, at 61–62.

56. 22 U.S.C. § 2778(a)(1).

57. 22 U.S.C. § 2778(b)(2). The USML divides munitions into twenty-one categories. Category XIII of the USML ("Auxiliary Military Equipment") included all cryptographic systems, but has since been revised to include only those "cryptographic devices, software, and components specifically designed, developed, modified, adapted, or configured for military applications." 22 C.F.R § 121.1 (2013). As of January 6, 2014, new Category XIII language applies and includes in part:

> Information security or information assurance systems and equipment, cryptographic devices, software, and components, as follows:
>
> . . . Military or intelligence cryptographic (including key management) systems, equipment, assemblies, modules, integrated circuits, components, and software (including their cryptographic interfaces) capable of maintaining secrecy or confidentiality of information or information systems, including equipment or software for tracking, telemetry, and control (TT&C) encryption and decryption.

22 C.F.R. § 121.1 (2014).

58. 22 C.F.R. § 121.1 (1996).

59. *See* Bernstein v. U.S. Dep't of Justice, 176 F.3d 1132, 1146–47 (9th Cir. 1999) [hereinafter *Bernstein IV*] (affirming district court decision that export regulations on encryption items are unconstitutional), *withdrawn pending en banc reh'g*, 192 F.3d 1308 (9th Cir. 1999).

60. Bernstein v. U.S. Dep't of State, 922 F. Supp. 1426, 1429 (N.D. Cal. 1996) [hereinafter *Bernstein I*]; Bernstein v. U.S. Dep't of State, 945 F. Supp. 1279, 1283 (N.D. Cal. 1996) [hereinafter *Bernstein II*]; Bernstein v. U.S. Dep't of State, 974 F. Supp. 1288, 1293 (N.D. Cal. 1997) [hereinafter *Bernstein III*]. *Bernstein I* and *II* challenged the encryption export control provisions of ITAR. After *Bernstein II*, President Clinton shifted

paper and in computer source code, and he wished to publish and otherwise communicate his findings.[61] When he sought a determination from the State Department as to whether his paper and source code were controlled under ITAR, the State Department replied that Bernstein's source code was a defense article under Category XIII of ITAR and therefore subject to licensing by the State Department prior to export.[62]

Bernstein filed suit in the Northern District of California, seeking a declaratory judgment against the U.S. Department of State to prevent it from enforcing ITAR against him.[63] The court observed that "[Bernstein's] paper, an academic writing explaining [his] scientific work . . . is speech of the most protected kind."[64] As to the source code, the court pointed out that "Bernstein's encryption system is written, albeit in computer language," and the court could "find no meaningful difference between computer language . . . and German or French."[65] In *Bernstein II*, the court held that the licensing requirement for cryptographic software under Category XIII of the USML was an unconstitutional prior restraint on speech, stating that "even if a government may constitutionally impose content-neutral prohibitions on a particular manner of speech, it may not *condition* that speech on obtaining a license or permit from a government official in that official's boundless discretion."[66]

In 1982, the inventors of RSA founded a corporation around their cryptographic algorithm, and they proposed—unsuccessfully—that RSA become a federal cryptographic standard, like DES.[67] But until the prospect of global e-commerce

---

ITAR licensing authority for encryption exports to the Department of Commerce. *See* Exec. Order No. 13,026, 61 Fed. Reg. 58,767 (Nov. 19, 1996); *see also* Encryption Items Transferred from the U.S. Munitions List to the Commerce Control List, 61 Fed. Reg. 68,572 (Dec. 30, 1996). In *Bernstein III*, the district court held that the Commerce Department's encryption export regulations were constitutionally indistinguishable from ITAR with respect to encryption and were therefore unconstitutional. 974 F. Supp. at 1306–08.

61. *Bernstein I*, 922 F. Supp. at 1429–30. Source code is the text of a computer program and is generally written in a high-level language that is two or more steps removed from machine language, which is a low-level language. High-level languages are closer to natural language than low-level languages, which direct the functioning of the computer. Source code must be translated by way of a translating program into machine language before it can be read by a computer. The object code is the output of that translation. It is possible to write a source program in high-level language without knowing about the actual functions of the computer that carry out the program. *See* ENCYCLOPEDIA OF COMPUTER SCIENCE 962, 1263–64 (Anthony Ralston & Edwin D. Reilly eds., 3d ed. 1993).

62. *Bernstein I*, 922 F. Supp. at 1430.

63. *Id.* at 1428.

64. *Id.* at 1434.

65. *Id.* at 1434–35.

66. 945 F. Supp. at 1286 (emphasis in original) (quoting Lakewood v. Plain Dealer Publ'g Co., 486 U.S. 750, 764 (1988)). The Ninth Circuit's decision in *Bernstein IV* was withdrawn when the court voted to rehear the case en banc, and then the case settled before the en banc decision was rendered. *See* Bernstein v. U.S. Dep't of Commerce, No. C 95-0582 MHP, 2004 U.S. Dist. LEXIS 6672, at *2 (Apr. 19, 2004). Therefore, the decision in *Bernstein IV* is no longer valid, even though the underlying decision in *Bernstein III* presumably is.

67. In 1982, the U.S. government solicited proposals for a national public-key cryptography standard. Solicitation for Public Key Cryptographic Algorithms, 47 Fed. Reg. 28,445 (June 30, 1982). RSA Data Security prepared a proposal to make RSA the national standard. The NSA, however, blocked their submission by requesting that the plan to

became feasible through the rapid worldwide adoption of the Internet, commercial interest in cryptographic systems remained a niche business.[68] The reawakened interest in cryptographic systems remained in this semidormant state until someone took steps to put strong cryptography in the hands of the general public.[69]

In 1991, a computer programmer named Phil Zimmermann wrote a program that used the RSA public-key cryptographic algorithm to protect the privacy of e-mail; he called the program "Pretty Good Privacy"—PGP for short—and made it publicly available over the Internet.[70] Zimmermann wrote and published PGP in response to Senate Bill 266, an omnibus anticrime bill, which contained a hidden requirement that would have forced makers of cryptographic equipment to insert secret "back doors" into their products so that the government could decrypt and read anyone's encrypted messages.[71] Zimmermann's goal was to get strong

---

develop a national public-key cryptography standard be dropped. U.S. GEN. ACCOUNTING OFFICE, GAO/OSI-94-2, COMMUNICATIONS PRIVACY: FEDERAL POLICY AND ACTIONS 5 (1993).

68. Cryptographic systems to ensure secured communications remained a tough sell (outside of governments) throughout the 1980s. For much of this time, the selling of cryptography was likened to the selling of insurance, in that the customer was expected to pay to protect against an event that may never happen. *See* DIFFIE & LANDAU, *supra* note 48, at 46.

69. The term *strong cryptography*—as opposed to *weak cryptography*—has no precise definition, since the standard against which we might measure "strong cryptography" today will undoubtedly change over time as computers become more powerful and research reveals new cryptographic techniques. For the purposes of this Article, I will borrow a definition from Bruce Schneier: "There are two kinds of cryptography in this world: cryptography that will stop your kid sister from reading your files, and cryptography that will stop major governments from reading your files. [Strong cryptography is] the latter." BRUCE SCHNEIER, APPLIED CRYPTOGRAPHY, at xix (2d. ed 1996).

Another critical characteristic of successful, strong cryptosystems is their adherence to what is known as *Kerckhoff's Principle*, which states that the security of an encryption scheme must depend only on the secrecy of the key(s) and not on the secrecy of the algorithm or methods. *See* NIELS FERGUSON, BRUCE SCHNEIER & TADAYOSHI KOHNO, CRYPTOGRAPHY ENGINEERING: DESIGN PRINCIPLES AND PRACTICAL APPLICATIONS 24–25 (2010). The reasoning behind this important principle is based in the overall security of the system—the fewer the secrets that one must keep in order to ensure a system's security, the easier it will be to maintain that security. Every secret in a cryptosystem is a potential failure point for that system.

70. *See* Elizabeth Lauzon, *The Philip Zimmermann Investigation: The Start of the Fall of Export Restrictions on Encryption Software Under First Amendment Free Speech Issues*, 48 SYRACUSE L. REV. 1307, 1321–22 (1998).

71. *See* 1 PHILIP ZIMMERMANN, THE OFFICIAL PGP USER'S GUIDE 5–7 (1995) (discussing the reasons for writing, publishing, and using PGP). While these measures ultimately failed, it has since been discovered that the NSA has been conducting a secret program to establish "back doors" into cryptographic systems and other security products by collaborating directly with technology companies. *See, e.g*, Nicole Perlroth, Jeff Larson & Scott Shane, *N.S.A. Able To Foil Basic Safeguards of Privacy on Web*, N.Y. TIMES, Sept. 6, 2013, at A1. These efforts, revealed through the formerly secret documents leaked by Edward Snowden, have been roundly criticized by experts and security companies as bad for security. *See* Ed Felten, *NSA Apparently Undermining Standards, Security, Confidence*, FREEDOM TO TINKER (Sept. 9, 2013), https://freedom-to-tinker.com/blog/felten/nsa-apparently-undermining-standards-security-confidence/; Dan Goodin, *Stop Using NSA-Influenced Code in Our Products, RSA Tells Customers*, ARS TECHNICA (Sept. 19, 2013, 7:43 PM), http://arstechnica.com/security/2013/09/stop-using-nsa

cryptography into the hands of everyone, explaining that, until he published PGP, "ordinary people and grassroots political organizations mostly have not had access to affordable 'military grade' public-key cryptographic technology."[72]

The Internet being a global medium, copies of Zimmermann's PGP quickly found their way outside U.S. borders, a violation of the AECA and ITAR.[73] Additionally, there was some speculation that Zimmermann's use of the RSA algorithm infringed the Rivest-Shamir-Adleman patent, although the claim was probably pretextual.[74] In February 1993, Zimmermann was visited by U.S. Customs Service agents who were investigating a complaint from RSA Data Security alleging the theft and international shipment of their intellectual property.[75] The seed of this initial inquiry quickly bloomed into an investigation of possible ITAR violations by a U.S. Attorney.[76] For years, Zimmermann remained under an investigatory cloud but was never indicted, most likely due to the inexplicable contradictions posed by the export restrictions articulated in ITAR.[77]

-influence-code-in-our-product-rsa-tells-customers/; Matthew Green, *On the NSA*, FEW THOUGHTS ON CRYPTOGRAPHIC ENGINEERING (Sept. 6, 2013, 2:27 AM), http://blog.cryptographyengineering.com/2013/09/on-nsa.html; Matthew Green, *The Many Flaws of Dual_EC_DRBG*, FEW THOUGHTS ON CRYPTOGRAPHIC ENGINEERING (Sept. 18, 2013, 7:28 PM), http://blog.cryptographyengineering.com/2013/09/the-many-flaws-of-dualecdrbg.html? [hereinafter Green, *Many Flaws*]; David Meyer, *Dear NSA, Thanks for Making Us All Insecur*e, BLOOMBERG BUSINESSWEEK (Sept. 6, 2013) http://www.businessweek.com/articles/2013-09-06/dear-nsa-thanks-for-making-us-all-insecure.

72. 1 ZIMMERMANN, *supra* note 71, at 7. To further enable the spread of PGP as far and as fast as possible, Zimmermann released his software as open-source freeware, giving everyone full and free access to the underlying source code used to implement RSA. 2 *id.* at 96–98.

73. *See supra* note 56 and accompanying text. As the court in *Bernstein II* observed, "[i]t seems reasonably clear that uploading an item to an Internet site that can be accessed in a foreign country constitutes 'sending' a defense article out of the country." 945 F. Supp. 1279, 1294 (N.D. Cal. 1996). "Furthermore, exportation as defined by the ITAR would appear to include publication where publication, such as posting software on the Internet or distributing it freely among colleagues, could be said to be tantamount to sending it out of the United States 'in any manner.'" *Id.* at 1288 (quoting 22 C.F.R. § 120.17(a)(1) (1996)); *see also* 22 C.F.R. §§ 120.1–120.9.

74. MIT was granted U.S. Patent 4,405,829 for a "Cryptographic Communications System and Method" that described the RSA algorithm in 1983. Cryptographic Commc'ns Sys. & Method, U.S. Patent No. 4,405,829 (filed Dec. 14, 1977) (issued Sept. 20, 1983). The patent would have expired on September 21, 2000, but the algorithm was released into the public domain by RSA Security on September 6, 2000. Press Release, RSA Security Inc., RSA Security Releases RSA Encryption Algorithm into Public Domain (Sept. 6, 2000), *available at* http://www.linuxtoday.com/infrastructure/2000090600606PRCYSW.

75. *See* STEVEN LEVY, CRYPTO: HOW THE CODE REBELS BEAT THE GOVERNMENT—SAVING PRIVACY IN THE DIGITAL AGE 287–88 (2001). From the start, it was clear that the U.S. Customs agents were ill prepared to understand the technical ramifications of the cryptographic software. They asked Zimmermann questions about the means he used to distribute PGP overseas, but Zimmermann had to explain to them the basic ideas behind cryptography and the distribution of data over the Internet. *Id.* at 287; *see also* DIFFIE & LANDAU, *supra* note 48, at 205–06; Lauzon, *supra* note 70, at 1327.

76. *See* LEVY, *supra* note 75, at 288; Lauzon, *supra* note 70, at 1327.

77. The U.S. Department of Justice investigation of Zimmermann closed without comment from the U.S. Attorney on January 11, 1996. *See Significant Moments in PGP's*

Since the mid-1990s, the civilian and commercial use of cryptographic systems has become widespread, driven initially by concerns for the safety of financial data in electronic commerce and electronic banking but eventually making its way into almost every aspect of our electronic lives.[78] Despite subsequent attempts by the U.S. government to regain exclusive control over the research, implementation, and proliferation of cryptographic technologies, strong crypto has made its way around the globe.[79] This tension between governments and their citizens regarding the use of

---

History: Zimmermann Case Dropped, PHILZIMMERMAN.COM (Jan. 12, 1996, 11:37 PM), https://www.philzimmermann.com/EN/news/PRZ_case_dropped.html. It was clear to many commentators, however, that confusion over ITAR export regulations made enforcement difficult and often absurd. For example, Bruce Schneier's 1994 book, *Applied Cryptography*, *supra* note 69, also attracted the attention of the U.S. government, as it contained detailed mathematical descriptions and explanations of many cryptographic systems. Under the ITAR export regulations, the book itself could be shipped internationally, as the restrictions on the export of cryptographic systems appeared to apply only to strong cryptography in digital form. That is, the book could be exported, but a disk containing the book's contents could not. This interpretation was confirmed when cryptography researcher Phil Karn applied for a "commodities jurisdiction" to export the book along with a floppy disk containing code from the book. The U.S. Department of State replied to Karn that the book could be exported, but the floppy disk could not. *See* Letter from Thomas E. McNamara, Assistant Secretary of State for Political-Military Affairs, U.S. Dep't of State, to Philip R. Karn, Jr. (June 13, 1995), *available at* http://www.toad.com/gnu/export/mcnamara-response.html. As if to thumb its nose at this bizarre export policy, the MIT Press published a book that contained nothing but the source code to the entire PGP program. *See* LEVY, *supra* note 75, at 290. The 933-page book has since become a collector's item, with mint condition copies selling for $200–$300. *See PGP: Source Code and Internals*, AMAZON.COM, http://www.amazon.com/PGP-Internals-Philip-R-Zimmermann/dp/0262240394.

78. Most modern encryption technology operates "behind the curtain" for the average person. For example, every modern web browser contains cryptographic functionality that enables users to establish secure connections to websites using established protocols like Transport Layer Security (TLS), or its predecessor, Secure Sockets Layer (SSL), but these protocols are designed to require little or no technical expertise from web users. *See* William Stallings, *SSL: Foundation for Web Security*, INTERNET PROTOCOL J., June 1998, at 20, *available at* http://www.cisco.com/web/about/ac123/ac147/archived_issues/ipj_1-1/ipj_1-1.pdf. Similarly, the invention and widespread use of computer network access through wireless radio technology (WiFi) led to the establishment of encryption protocols to prevent electronic eavesdropping on open radio channels. *See* WI-FI ALLIANCE, THE STATE OF WI-FI SECURITY: WI-FI CERTIFIED WPA2 DELIVERS ADVANCED SECURITY TO HOMES, ENTERPRISES AND MOBILE DEVICES (2012), *available at* http://davidhoglund.typepad.com/files/20120229_state_of_wi-fi_security_09may2012_updated_cert.pdf.

79. In 1993, the U.S. National Institute of Standards and Technology (NIST) solicited public comment on a proposed Escrowed Encryption Standard. *See* A Proposed Federal Information Processing Standard for an Escrowed Encryption Standard (EES), 58 Fed. Reg. 40,791, 40,791–93 (Jul. 30, 1993). This initiative was born out of the U.S. government's fear of losing the ability to eavesdrop on international communications due to the widespread use of strong cryptography. *See* A. Michael Froomkin, *The Metaphor Is the Key: Cryptography, the Clipper Chip, and the Constitution*, 143 U. Pa. L. Rev. 709, 743 (1995). The EES would solve this problem for the NSA by requiring all users of cryptography to allow the U.S. government to keep a copy of their secret encryption key(s) in escrow, so that encrypted communications could be deciphered by the U.S. government should it become necessary. *Id*. at 743–45. Unsurprisingly, the public reaction to the proposed EES was overwhelmingly

strong cryptography thus remains largely unresolved, and governments have sought alternative—often covert—methods of swinging the pendulum back to their side.

C. The Details of Encryption (From 30,000 Feet)

Before we progress too much further, I believe it is important to understand some of the fundamental mathematical principals behind cryptography. Legislatures and courts often deal with encryption indirectly, through analogy or metaphor, in an effort to show that since encryption is similar in some respects to some other, better known, or easier to understand, technology, it should be treated similarly under the law.[80] As noted above, cryptography can hardly be described as a new technology, and yet, due in large part to the arcane mathematics involved and its relatively late appearance as a commonly available technology, courts and commentators have struggled to find a model of understanding that truly fits.[81] These metaphors are hit-and-miss, sometimes succeeding in capturing one aspect of

---

negative, despite the Clinton administration's full-court marketing press. *See* DIFFIE & LANDAU, *supra* note 48, at 212; Froomkin, *supra*, at 744. Despite these protests, NIST adopted the EES on Feb. 9, 1994. *See* Approval of Federal Information Processing Standards Publication 185, Escrowed Encryption Standard (EES), 59 Fed. Reg. 5997, 5997–98 (Feb. 9, 1994). After a vulnerability in the EES implementation was found, the already tepid acceptance by the industry fell even further, causing EES to fade into obscurity. *See generally* Matt Blaze, *Key Escrow from a Safe Distance: Looking Back at the Clipper Chip*, 27 PROC. ANN. COMPUTER SECURITY APPLICATIONS CONF. 317 (2011), *available at* http://dl.acm.org/citation.cfm?id=2076777; Matt Blaze, *Protocol Failure in the Escrowed Encryption Standard*, 2 PROC. ACM CONF. ON COMPUTER & COMM. SECURITY 59 (1994), *available at* http://dl.acm.org/citation.cfm?id=191193.

80. This analogical approach is not unique to encryption, of course, as reasoning by analogy is one of the most familiar forms of legal reasoning. Cass R. Sunstein, *On Analogical Reasoning*, 106 HARV. L. REV. 741, 741 (1993); *see also* EDWARD H. LEVI, AN INTRODUCTION TO LEGAL REASONING 10–15 (1949). This approach has had some success with certain technologies, such as railroads, that bear enough of a resemblance to their analogical cousins to fit existing models of thought. *See* Vincent M. Brannigan, *Biotechnology: A First Order Technico-Legal Revolution*, 16 HOFSTRA L. REV. 545, 549 (1988) (observing that certain technologies do not require any changes to legal thought, whereas others required fundamental changes). Other, more disruptive, technologies have required more significant changes to existing schools of thought. Air travel, for example, represented an order of magnitude change in technology and required significant changes in the law to address such novel issues as trespass by air. *See* Hinman v. Pac. Air Transp., 84 F.2d 755, 759 (9th Cir. 1936) (allowing airplanes the right to fly over private property).

81. *See, e.g.*, 22 C.F.R. § 121.1 (2013) (cryptography as a "device" and "munition"); A. Michael Froomkin, *The Constitution and Encryption Regulation: Do We Need a "New Privacy"?*, 3 N.Y.U. J. LEGIS. & PUB. POL'Y 25, 26 (2000) (encrypted speech is a language); Froomkin, *supra* note 79, at 871 ("A cipher is armor around a communication much like a safe is armor around a possession."); David Hricik, *Lawyers Worry Too Much About Transmitting Client Confidences by Internet E-Mail*, 11 GEO. J. LEGAL ETHICS 459, 493 (1998) ("Encryption is an electronic 'lock-and-key' technology . . . ."); Ronald L. Rivest, *The Case Against Regulating Encryption Technology*, SCI. AM., Oct. 1998, at 116, 116−17 (encryption technology as gloves to hide fingerprints); Lee Tien, *Publishing Software as a Speech Act*, 15 BERKELEY TECH. L.J. 629, 672 (2000) (encryption as envelope containing the message).

cryptography, but often falling short in others.[82] The problem with attempting to understand the use of cryptography solely through imperfect models of the concept is that these models can quickly outlive their usefulness, transforming from tools that assist our initial understanding into intellectual crutches that oversimplify critical issues.[83] In this Article, I will therefore endeavor to avoid unnecessary metaphors wherever possible. In order to start from a solid foundation, it is necessary to truly understand the basic elements of cryptography and its uses.

The act of transforming a message (*plaintext* or *cleartext*) into an enciphered form (*ciphertext*) in such a way as to hide its substance is called *encryption*.[84] The operations that transform plaintext to ciphertext, and from ciphertext back to plaintext, are forms of mathematical *functions*.[85] More precisely, if a particular function transforms plaintext to ciphertext, then the function that transforms that ciphertext back to plaintext is the original function's *inverse*.[86] Successful

---

82. Courts and commentators are not blind to this issue, of course, but it has been noted that courts are often unprepared when trying to apply existing law to new technologies: "[a]nalogy is the only real road map for courts when technological change leaves them in unknown legal territory," where the technology does "not fit neatly into existing categories." Linda Greenhouse, *What Level of Protection for Internet Speech?*, N.Y. TIMES, Mar. 24, 1997, at D5. Analogy and metaphor are useful tools to begin one's understanding of an abstract concept. As Max Black wrote,

> Why stretch and twist, press and expand, concepts in this way—Why try to see *A* as metaphorically *B*, when it literally is not *B*? . . . [B]ecause we often need to do so, the available literal resources of the language being insufficient to express our sense of the rich correspondences, interrelations, and analogies of domains conventionally separated; and because metaphorical thought and utterance sometimes embody insight expressible in no other fashion.

Max Black, *More About Metaphor*, *in* METAPHOR AND THOUGHT 19, 33 (Andrew Ortony ed., 2d ed. 1993).

83. Linguists, logicians, and philosophers have long been wary of the potential abuses of metaphor. The philosopher Max Black has stated that "[t]o draw attention to a philosopher's metaphors is to belittle him—like praising a logician for his beautiful handwriting. Addiction to metaphor is held to be illicit, on the principle that whereof one can speak only metaphorically, thereof one ought not to speak at all." Max Black, *Metaphor*, 55 PROC. ARISTOTELIAN SOC'Y 273, 273 (1955).

84. SCHNEIER, *supra* note 69, at 1. It should be noted that message privacy or confidentiality is but one of the goals of a cryptographic system. Other objectives include data integrity (the prevention and detection of unwanted data manipulation), authentication (the identification of sender and recipient), and nonrepudiation (the prevention of entities from denying previous commitments or actions). *See* ALFRED J. MENEZES, PAUL C. VAN OORSCHOT & SCOTT A. VANSTONE, HANDBOOK OF APPLIED CRYPTOGRAPHY 4 (1997). A full examination of these fundamental goals of cryptography is beyond the scope of this Article, and for the purposes of this argument I will focus—somewhat superficially—on the goal of message confidentiality. I will strive mightily to keep the mathematics in this Article to a minimum.

85. *See* MENEZES ET AL., *supra* note 84, at 6–8.

86. *See id.* at 7–8. In order to uphold my promise to keep the mathematics to a minimum in this Article, I have glossed over a number of important mathematical principles necessary for these functions to operate as advertised. For example, in order for a plaintext message to be properly recovered, the encryption function and its inverse must both be special kinds of functions known as *bijections*. While this distinction is crucial to the mathematics behind

cryptosystems depend on special kinds of functions known as *one-way functions* and *trapdoor functions*.[87] A one-way function is a function that is easy to compute but whose inverse is "computationally infeasible" to calculate.[88] A trapdoor function is a one-way function with an additional property that contains information (the trapdoor function's "secret") that makes it computationally feasible to find its inverse.[89] For the purposes of this Article, one can consider encryption as a trapdoor function and decryption as that trapdoor function's inverse. That is, if Alice uses a trapdoor function to encrypt a message to Bob, it would be computationally difficult for anyone who is not privy to the "secret" of the trapdoor function—we can call this the *key*—to decrypt the resulting ciphertext via the inverse of Alice's trapdoor function.

The viability of modern computational cryptography therefore depends quite heavily on what is "computationally infeasible." That is, mathematicians have not been able to prove with certainty that any true one-way functions exist.[90] Since the existence of true one-way functions is unknown, the existence of true trapdoor functions is therefore also unknown.[91] One does not have to be a mathematician to realize that this poses something of a problem for cryptography in general and the long-term secrecy of existing encrypted communications in particular. But while there may come a day when a method to easily invert one-way functions is discovered, thus pulling the rug out from under much of modern cryptography, mathematicians and cryptographers currently agree that that day has not yet arrived.[92] For the time being, the continued viability of modern computational cryptographic techniques depends on the "computational infeasibility" of finding the inverses of trapdoor functions through "brute force" methods on current (and foreseeable) technologies.[93]

---

cryptography, it is not as important for the purposes of this Article. For those interested in a more complete description, see generally *id.*

87. *See id.* at 8–9.

88. *Id.* at 8. A common example of a one-way function is one which takes two very large prime numbers, p and q, and multiplies them to get a new number n, which, by definition, is divisible by 1, p, and q only. The number n is known as a *semiprime* number. Finding the number n is relatively easy, but if p and q are sufficiently large prime numbers, finding the factors p and q of n is computationally difficult, even with today's most powerful computers.

89. *Id.* at 9. Building upon the example in note 88, *supra*, a trapdoor function would provide the additional information of either p or q, thus making the factorization of n much easier.

90. *Id.*; *see also* Jacob Ziv, *In Search of a One-Way Function*, *in* OPEN PROBLEMS IN COMMUNICATION AND COMPUTATION 104–05 (Thomas M. Cover & B. Gopinath eds., 1987).

91. MENEZES ET AL., *supra* note 84, at 9.

92. *See* Ziv, *supra* note 90, at 104–05. In fact, the finding of an easy solution to one-way functions is linked to the "*P* vs. *NP*" problem, one of the great unsolved problems in mathematics. Finding a solution to the "*P* vs. *NP*" problem would have a seismic impact on the world of mathematics far beyond the area of cryptography. *See* STEPHEN COOK, THE P VERSUS NP PROBLEM, *available at* http://www.claymath.org/sites/default/files/pvsnp.pdf. I address this lurking problem and its implications more fully in Part II.A, *infra*.

93. By "brute force" methods, I mean cryptanalytic attacks that attempt to decrypt an enciphered message by trying every possible decryption key until either the message is decrypted or all possible keys have been exhausted. *See* CHRISTOF PAAR & JAN PELZL, UNDERSTANDING CRYPTOGRAPHY: A TEXTBOOK FOR STUDENTS AND PRACTITIONERS 7 (2010). Such direct attacks on well-established and vetted encryption techniques are very rarely the

D. Who Uses Encryption?

Even at the high levels of abstraction I've adopted in presenting the basics of cryptography above, it quickly becomes apparent that the mathematical principles behind cryptography are astoundingly complex and are best understood by—and left to—experts in the field. Fortunately for the rest of us, a great deal of progress has been made over the past few decades to make strong cryptography a generally available reality through (somewhat) user-accessible computer software.[94] The explosive growth of Internet use in the 1990s yielded a storm of commercial cryptographic systems, some of it good, but much of it bad.[95] In fact, the commercial appeal of making easy money by building a cryptographic system and selling it to worried customers as a security panacea led many security experts to warn the public to watch out for cryptographic "snake oil."[96]

---

approach of those who make it their business to read the secret messages of others. Rather, it is generally much more fruitful to seek out gaps in the armor to exploit, which can take the form of implementation mistakes, poorly chosen cryptographic keys, and old-fashioned human weakness. *See, e.g.*, Michael Eisen, *What Exactly Are the NSA's 'Groundbreaking Cryptanalytic Capabilities'?*, WIRED (Sept. 4, 2013, 9:29 AM), http://www.wired.com/opinion/2013/09/black-budget-what-exactly-are-the-nsas-cryptanalytic-capabilities/ (examining possible theories behind NSA cryptanalytic capabilities); Dan Goodin, *Private Crypto Key in Mission-Critical Hardware Menaces Electric Grids*, ARS TECHNICA (Aug. 22, 2012, 12:36 PM), http://arstechnica.com/security/2012/08/mission-critical-hardware-flaw/ (reporting on poor cryptographic engineering resulting in a widespread vulnerability); Matthew Green, *Is the Cryptopocalypse Nigh?*, FEW THOUGHTS ON CRYPTOGRAPHIC ENGINEERING (Aug. 19, 2013, 12:43 PM), http://blog.cryptographyengineering.com/2013/08/is-cryptopocalypse-nigh.html (showing that recent demonstrated attacks only apply to a small subset of cryptographic keys); Green, *Many Flaws*, supra note 71 (providing analysis of flaws in a cryptographic random number generator allegedly sabotaged by NSA); Micah F. Lee, *No Really, the NSA Can't Brute Force Your Crypto*, MICAH LEE'S BLOG (Jan. 23, 2013, 7:11 PM), https://micahflee.com/2013/01/no-really-the-nsa-cant-break-your-crypto/ (demonstrating the computational infeasibility of brute force attacks on cryptographic keys using current technologies); *The NSA's Crypto "Breakthrough,"* ECONOMIST (Sept. 2, 2013, 3:00 PM), http://www.economist.com/blogs/babbage/2013/09/breaking-cryptography (observing that the most likely answer to revelations of NSA decryption program question is the exploitation of bugs in cryptographic protocols).

94. Due to the high degree of expertise and sheer computational horsepower required, strong cryptography has long been the sole domain of governments and militaries. *See* LEVY, *supra* note 75, at 13–15; DIFFIE & LANDAU, *supra* note 48, at 49–59. In the early 1970s, however, a number of key research breakthroughs coincided with the rise of relatively cheap and powerful computers, initiating a cryptography renaissance. DIFFIE & LANDAU, *supra* note 48, at 59–63.

95. Most cryptographers will tell you that "cryptography is very difficult" but "[c]ryptography is the easy part" of cryptographic engineering. FERGUSON ET AL., *supra* note 69, at 12–14.

96. The term itself is derived from a type of patent medicine called "snake oil" that was widely available during the nineteenth century. As applied, modern vendors of cryptographic snake oil were those selling a cryptographic product considered by experts to be bogus or flawed. *See* ZIMMERMANN, *supra* note 71, at 39–43; Matt Curtin, *Snake Oil Warning Signs: Encryption Software To Avoid*, INTERHACK RES. (Apr. 10, 1998), http://www.interhack.net/people/cmcurtin/snake-oil-faq.html; Bruce Schneier, *Snake Oil*, SCHNEIER ON SECURITY

The commodification of the computer and the proliferation of near instantaneous electronic global communication has driven governments, businesses, and (to a somewhat lesser extent) individuals to make a special effort to keep their communications private.[97] As noted earlier, this privacy interest is not a new concept. But unlike the historical examples of messages conveyed via stone, papyrus, paper, telegraph, or radio broadcast, the existence of a nearly ubiquitous data communication infrastructure has forced a reexamination and rebirth of communication and data security principles and practices. The complexity of modern communication protocols means that cryptography is only one element of a broader communications-security regime. An encryption mechanism by itself may be interesting for academic reasons, but it is fairly useless apart from a larger security system.[98] The details behind this design philosophy are beyond the scope of this Article. For our purposes, I only note that, while cryptography is a critical part of any communications-security mechanism, it is generally not the piece of the security system that is the first to fail.[99]

Despite the overall complexities and difficulties in engineering strong cryptographic systems, these systems have become essential components of the modern Internet.[100] To date, most uses of encryption technologies remain largely invisible to the average Internet user. At best, this means that encryption is simply ignored; at worst, it gives users a false sense of security in poorly understood technologies.[101] But growing popular awareness of computer security issues generally, and cryptography's role in data protection specifically, has ignited a broad awakening of interest in, and use of, encryption technologies.[102] And while

---

(Feb. 15, 1999), https://www.schneier.com/crypto-gram-9902.html#snakeoil. Some of the more common signs of such snake oil are claims of "security through obscurity," that is, claiming that the system must be kept secret; the use of "technobabble"; and blanket claims that the cryptographic system in question is "unbreakable." Curtin, *supra*.

97. *See* DIFFIE & LANDAU, *supra* note 48, at 59–61.

98. *See* FERGUSON ET AL., *supra* note 69, at 4.

99. Like any complex system, the weaknesses of communication-security protocols are most often found in the joints between their subsystems. *See id.* at 4–5 (discussing the "weakest link" approach to security-system analysis); *see also* DIFFIE & LANDAU, *supra* note 48, at 38–40.

100. Without the availability of strong cryptographic systems, our current systems of global finance, commerce, medicine, and government would likely face dire consequences, and may fail altogether. *See Cracked Credibility*, ECONOMIST, Sept. 14, 2013, at 65.

101. While it is true that both commercial and open source cryptographic applications can be found in some form in nearly every network-enabled technology today, their use is often limited to whatever default settings were installed with the application. This approach is designed with user convenience in mind, adhering to the unfortunately common principle that the more secure you make something, the less secure it becomes. This is cute shorthand for the phenomenon where users will often find (insecure) shortcuts around application security that gets in their way. *See* Donold A. Norman, *When Security Gets in the Way*, INTERACTIONS, Nov.−Dec. 2009, at 60.

102. Interestingly enough, the trend toward increased user education in cryptography and other computer-security basics has been encouraged by the U.S. government. For example, since 2004, the U.S. Department of Homeland Security has sponsored "National Cyber Security Awareness Month" each October, marking the occasion each year by providing security tips, including recommendations to encrypt files. *See, e.g.*, *National Cyber Security*

truly ubiquitous encryption is not yet a reality, a growing number of individuals, businesses, and other organizations have taken steps to keep their messages and data secret by encrypting their contents.[103]

E. Why Does Encryption Matter?

Cryptographers generally agree that strong cryptography, implemented and used properly, poses a significant, and often realistically insurmountable, obstacle to would-be eavesdroppers, even those with access to nearly unlimited resources like the NSA.[104] One problem with this assumption, however, is the fact that it is not very "future proof." That is to say, the known theory, techniques, and computing power of today will most likely be viewed as quaint in the not-too-distant future, if recent progress is any indication, and what is thought of as computationally infeasible today may very well be child's play in several decades (or fewer).[105]

To illustrate how technological and theoretical improvements can affect the future security of messages encrypted using today's standards, we can look to cryptographic key length.[106] As late as 2005, a 1024-bit RSA public key was considered by standards organizations to provide adequate security for the

---

Awareness Month 2014, DEP'T HOMELAND SECURITY (Oct. 2, 2014), http://www.dhs.gov/national-cyber-security-awareness-month; *Security Tip (ST05-017): Cybersecurity for Electronic Devices*, US-CERT (Feb. 6, 2013), https://www.us-cert.gov/ncas/tips/st05-017.

103. Of course, there are perfectly legitimate reasons, both technical and personal, that may influence an individual's or organization's decision to keep some data freely accessible and readable. In fact, some computer-security experts have warned that the ubiquitous encryption of all Internet traffic would hinder the ability to detect viruses and other malware as it is shared over networks. *See, e.g.*, Rob Holquist, *Growing Network-Encryption Use Puts Systems at Risk*, IEEE COMPUTING NOW (Aug. 2011), http://www.computer.org/portal/web/computingnow/news/growing-network-encryption-use-puts-systems-at-risk (discussing how network encryption protocols widely used in the Internet could be used to hide malicious activity). I do not address these issues in this Article but instead focus on the warrantless government search and seizure of all encrypted data and its legal and societal implications.

104. Questions of flawed implementations aside, the strength of a cryptographic scheme is not achieved through the secrecy of the scheme itself (see the discussion of Kerckhoff's Principle in *supra* note 69) but through the mathematical soundness of the underlying algorithm along with other factors such as the chosen lengths of the cryptographic keys. *See* SCHNEIER, *supra* note 69, at 166–67.

105. Following an observed trend in technology that has continued for over fifty years, it is estimated that the efficiency of computing equipment divided by price doubles every eighteen months and increases by a factor of ten every five years. *Id.* at 167. If this conjecture—known as Moore's Law, named for Intel cofounder Gordon Moore who first described this trend—continues to hold true, the fastest computers in fifty years will be 10^{10}, or ten *billion*, times faster than the computers of today.

106. The size of the keys used in cryptographic systems is often used as a shorthand measure of cryptographic strength. While this is not a perfect or complete measurement, key length does provide an indication as to the degree of security a particular key will provide within a given cryptographic system. *See* MATT BLAZE, WHITFIELD DIFFIE, RONALD L. RIVEST, BRUCE SCHNEIER, TSUTOMU SHIMOMURA, ERIC THOMPSON & MICHAEL WIENER, MINIMAL KEY LENGTHS FOR SYMMETRIC CIPHERS TO PROVIDE ADEQUATE COMMERCIAL SECURITY (1996), *available at* http://people.csail.mit.edu/rivest/bsa-final-report.pdf.

protection of sensitive information through 2015.[107] That is, a stored message encrypted using a properly implemented RSA cryptographic algorithm and a 1024-bit key could safely be considered unbreakable—or at least computationally infeasible to break—through 2015. But in May 2007, a group of researchers used a networked array of four hundred computers to factor a 1039-bit number in eleven months.[108] While the number the researchers factored was not a true RSA number,[109] it was close enough that cryptographers warned users of the RSA cryptographic system not to use keys of size 1024-bit and smaller.[110] Thus, even the most pessimistic of cryptographers, armed with years of empirical research, could not accurately predict a combination of improvements in research and computing power (along with the ever-present and completely unpredictable factor of human ingenuity) that would diminish the future viability of a key size by years.[111]

The limited shelf life of cryptographic keys, and by extension the messages encrypted with those keys, becomes highly significant when we consider the implications of a secret NSA program to collect—and store indefinitely—all encrypted messages sent by U.S. citizens. Cryptography and mathematics researchers worldwide spend countless hours creating, analyzing, and attempting to break cryptographic systems, a time-honored and open process that serves as the

---

107. J. SCHAAD, B. KALISKI & R. HOUSLEY, ADDITIONAL ALGORITHMS AND IDENTIFIERS FOR RSA CRYPTOGRAPHY FOR USE IN THE INTERNET X.509 PUBLIC KEY INFRASTRUCTURE CERTIFICATE AND CERTIFICATE REVOCATION LIST (CRL) PROFILE, at 23, (2005), *available at* http://tools.ietf.org/pdf/rfc4055.pdf. Key length is measured in bits, which is the most basic unit of information in computing, having only two possible values, 0 or 1. A 1024-bit RSA key is a very large number which has over three hundred decimal digits and which is the product of two smaller (but still quite large) prime numbers. As noted in Part I.C, *supra*, the security of the RSA cryptographic system, and others like it, depends on the computational infeasibility of factoring a very large number which is the product of two large prime numbers. Advances in techniques and computing power thus effectively erode a key's cryptographic value over time. *See* M.J.B. ROBSHAW, SECURITY ESTIMATES FOR 512-BIT RSA (1995), *available at* http://www.networkdls.com/Articles/security_estimates.pdf.

108. *See* Jacqui Cheng, *Researchers: 307-Digit Key Crack Endangers 1024-bit RSA*, ARS TECHNICA (May 23, 2007, 6:37 PM), http://arstechnica.com/uncategorized/2007/05/researchers-307-digit-key-crack-endangers-1024-bit-rsa/.

109. Beginning in 1991, RSA Laboratories published a series of large semiprime numbers—known as RSA numbers—as a challenge to researchers to find the two prime factors of each RSA number. *See* RSA Labs., *The RSA Factoring Challenge FAQ*, EMC^2, http://www.emc.com/emc-plus/rsa-labs/historical/the-rsa-factoring-challenge-faq.htm; *see also RSA Number*, WOLFRAM MATHWORLD, http://mathworld.wolfram.com/RSANumber.html. Though it is no longer active, the RSA Factoring Challenge was meant to encourage cryptographic research, as well as to provide a "coal mine canary" to warn researchers when certain key sizes were no longer to be considered cryptographically safe. RSA Labs., *supra*.

110. *See* Cheng, *supra* note 108.

111. The list of unimaginably large semiprime numbers which have since been factored continues to grow. For example, a Mersenne Prime (prime numbers which take the form $2^p - 1$, where p is prime) of size $2^{1061} - 1$, a number with 320 decimal digits, was factored between early 2011 and August 2012. *See* GREG CHILDERS, FACTORIZATION OF A 1061-BIT NUMBER BY THE SPECIAL NUMBER FIELD SIEVE (2012), *available at* http://eprint.iacr.org/2012/444.pdf.

only acceptable proving (and disproving) grounds for strong cryptography.[112] It is therefore not entirely surprising when cryptographic systems are broken, even those designed by recognized experts in the field and in use for years.[113] This fact is not lost on the NSA, which employs thousands of mathematicians, many of whom hold PhDs in the field, to research ways to make and break cryptographic systems.[114] By collecting and storing encrypted messages for indefinite periods of time, the NSA has asserted its own authority to eventually decrypt every such message, regardless of its origin or intent.

In fact, the Snowden documents have shown that, over the past decade, the NSA has increased its efforts to find ways to break cryptographic systems.[115] While some have interpreted these NSA documents to mean that the agency has "cracked much of the encryption" available on the web,[116] most cryptography experts are of the opinion that, in most cases, the NSA is not attacking the cryptographic protocols themselves, since these still pose mathematically intractable problems, but is rather attacking weaknesses in their implementations.[117] More disturbing to

---

112. As described in Part I.C, *supra*, cryptography is an arcane and difficult discipline, and there is no known way to design, implement, and vet systems strong enough to withstand known attacks other than through continual research and testing by the cryptography research community. *See* FERGUSON ET AL., *supra* note 69, at 13.

113. *See id*. An example of a widely used and trusted cryptographic system later found to be fatally flawed is the MD5 message digest algorithm. MD5 is an example of a cryptographic hash function, which takes an arbitrary block of data and returns a fixed-size string (a cryptographic hash value) with the following properties: (1) it is easy to compute the hash value from any given message, (2) it is infeasible to generate a message that has a given hash value, (3) it is infeasible to modify a message without changing the resulting hash value, and (4) it is infeasible to find two different messages with the same hash value. *See* SCHNEIER, *supra* note 69, at 429–36. MD5 was designed by Ron Rivest (the "R" in RSA) in 1992 to replace the flawed MD4. *See* R. Rivest, *The MD5 Message-Digest Algorithm*, IETF.ORG (April 1992), http://www.ietf.org/rfc/rfc1321.txt. In 1996, however, a flaw in MD5 was discovered by researchers who demonstrated that MD5 failed property (4) above. *See* XIAOYUN WANG & HONGBU YU, HOW TO BREAK MD5 AND OTHER HASH FUNCTIONS, *available at* http://merlot.usc.edu/csac-f06/papers/Wang05a.pdf. MD5 has since been considered unsuitable for strong cryptographic applications. *See* Marc Stevens, Arjen K. Lenstra & Benne de Weger, *Vulnerability of Software Integrity and Code Signing Applications to Chosen-Prefix Collisions for MD5*, EINDHOVEN U. TECH. (Jan. 1, 2009), http://www.win.tue.nl/hashclash/SoftIntCodeSign/.

114. *See Critical Skills for National Security and the Homeland Security Federal Workforce Act: Hearing on S. 1800 Before the Subcomm. on Int'l Sec., Proliferation & Fed. Servs. of the S. Comm. on Governmental Affairs*, 107th Cong. 11 (2002) (statement of Harvey A. Davis, Associate Director, Human Resources Services, National Security Agency); *see also* Siobhan Gorman, *Intelligence Chiefs: Shutdown Threatening National Security*, WALL ST. J. (Oct. 2, 2013, 12:33 PM), http://blogs.wsj.com/washwire/2013/10/02/intelligence-chiefs-shutdown-threatening-national-security/.

115. *See* Perlroth et al., *supra* note 71.

116. *Id.*

117. *See, e.g.*, Bruce Schneier, *NSA Surveillance: A Guide to Staying Secure*, GUARDIAN, (Sept. 6, 2013, 9:09 AM), http://www.theguardian.com/world/2013/sep/05/nsa-how-to-remain-secure-surveillance. Cryptographers are well aware of the "weakest link property," which can be summarized by the principle that a cryptographic system is only as strong as its weakest

the cryptographic community, however, is the discovery of NSA manipulation of cryptographic standards and commercial cryptographic systems in order to provide "back doors" to easily decrypt messages without the proper key.[118] These manipulations not only weaken defenses against malicious Internet activities but also directly threaten the trust that must exist between a government and its citizens. This trust is a constitutional value even more fundamental to Fourth Amendment principles than is privacy, and it should be a guide to the Fourth Amendment analysis of the NSA's broad collection of encrypted messages.[119]

II. PRIVACY, POWER, AND THE STRUGGLE FOR PERFECT SECURITY

A. The Development of Current Fourth Amendment Doctrine

The lineage of today's Fourth Amendment jurisprudence can be traced directly back to the Supreme Court's decision in *Olmstead v. United States*.[120] In *Olmstead*, the Court considered whether the warrantless wiretapping of a telephone line violated the Fourth Amendment.[121] The majority held that the defendants' Fourth Amendment rights were not violated by this warrantless wiretapping, stating that "[t]he [Fourth] Amendment . . . shows that the search is to be of material things—the person, the house, his papers or his effects."[122] Since government wiretapping

---

link. *See* FERGUSON ET AL., *supra* note 69, at 3–5. Simply put, the strongest cryptographic protocols are worthless if the system implementing the protocols provides opportunities to read secret messages without actually finding a mathematical shortcut to decryption.

118. In addition to "partnerships with major telecommunications carriers to shape the global network to benefit other collection accesses," the NSA has been "'actively engag[ing] the U.S. and foreign IT industries to covertly influence and/or overtly leverage their commercial products' designs' to make them 'exploitable.'" Perlroth, *supra* note 71. In other words, the NSA has been working with technology companies to provide hidden back doors by "insert[ing] vulnerabilities into commercial encryption systems, IT systems, networks, and endpoint communications devices used by targets." *See Secret Documents Reveal N.S.A. Campaign Against Encryption*, N.Y. TIMES (Sept. 5, 2013), http://www.nytimes.com/interactive/2013/09/05/us/documents-reveal-nsa-campaign-against-encryption.html.

Cryptographers, mathematical researchers, and other scientists have been especially alarmed by the NSA's efforts to "[i]nfluence policies, standards and specifications for commercial public key technologies." Perlroth, *supra* note 71. Mathematicians have recently confirmed that an important cryptographic standard published by NIST was artificially weakened through secret NSA manipulation. *See* Green, *Many Flaws*, *supra* note 71. This has been a suspected flaw since mathematicians aired their suspicions in 2007. *See* Bruce Schneier, *Did NSA Put a Secret Backdoor in New Encryption Standard?*, WIRED, (Nov. 15, 2007), http://archive.wired.com/politics/security/commentary/securitymatters/2007/11/securitymatters_1115. Researchers and commercial entities rely on standards bodies to provide unbiased advice as to which cryptographic protocols and algorithms will provide the most robust protection. To subvert or corrupt this process quickly dissolves the trust relationships necessary for a democratic and free market society to thrive, and we have already begun to see its effects. *See* Goodin, *supra* note 71. I will explore this issue in more detail in Part II, *infra*.

119. *See infra* Part IV.

120. 277 U.S. 438 (1928), *overruled in part by* Katz v. United States, 389 U.S. 347 (1967).

121. *Id.* at 455.

122. *Id.* at 464.

required neither "physical invasion" nor the seizure of "tangible material effects," it was not a search under the Fourth Amendment.[123]

It was Justice Brandeis's famous dissent in *Olmstead*, however, that set the stage for the Court's later Fourth Amendment doctrine. Justice Brandeis criticized the majority's narrow, property-based interpretation of the Fourth Amendment, warning of the effects that advances in technology would have under this doctrine.[124] In particular, he stated that "general limitations on the powers of Government . . . do not forbid the United States or the States from meeting modern conditions by regulations which 'a century ago, or even half century ago, probably would have been rejected as arbitrary or oppressive.'"[125]

The criticisms Justice Brandeis laid out in his dissent placed a Fourth Amendment emphasis on protecting citizens' privacy from unwarranted government intrusion, noting that the Founders "knew that only a part of the pain, pleasure and satisfactions of life are to be found in material things" and that "[t]o protect [Fourth Amendment rights], every unjustifiable intrusion by the Government upon the privacy of the individual, whatever the means employed, must be deemed a violation of the Fourth Amendment."[126] His dissent in *Olmstead* continues to influence the Court even today.[127]

By the 1960s, the Court began to move away from the property-based, trespass theory of the Fourth Amendment found in *Olmstead*, leading to its complete rejection in *Katz v. United States*.[128] In *Katz*, government agents installed a microphone in a telephone booth knowing the defendant used it to discuss illegal gambling operations.[129] The Court addressed the question of whether the evidence gathered by the agents in their warrantless eavesdropping had been obtained in violation of the Fourth Amendment.[130] The *Katz* Court rejected the property-based approach of *Olmstead*, stating that property and trespass did not control the government's ability to conduct Fourth Amendment searches.[131]

The rejection of the Fourth Amendment doctrine articulated in *Olmstead* provided the *Katz* Court with the foundation upon which it created what is now known as the "reasonable expectation of privacy test."[132] This test has its origins in Justice Harlan's concurrence, where he stated that his "understanding of the rule that has emerged from prior decisions is that there is a twofold requirement [for a

---

123. *Id.* at 466.

124. *See* Orin S. Kerr, *Applying the Fourth Amendment to the Internet: A General Approach*, 62 STAN. L. REV. 1005, 1024 (2010).

125. *Olmstead*, 277 U.S. at 472 (Brandeis, J., dissenting) (quoting Village of Euclid v. Ambler Realty Co., 272 U.S. 365, 387 (1926)).

126. *Id.* at 478.

127. *See, e.g.*, United States v. Jones, 132 S. Ct. 945, 959 (2012) (Sotomayor, J., concurring) (citing Justice Brandeis's *Olmstead* dissent in her criticism of a property-based Fourth Amendment doctrine); Mapp v. Ohio, 367 U.S. 643, 659 (1961) (citing Justice Brandeis's *Olmstead* dissent to support application of the exclusionary rule to the states).

128. 389 U.S. 347 (1967).

129. *Id.* at 348.

130. *Id.* at 348−50.

131. *Id.* at 353.

132. *See infra* note 134 and accompanying text.

Fourth Amendment search], first that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as 'reasonable.'"[133]

B. The Twin Problems of Reasonableness and Perspective in Fourth Amendment Analysis

Modern Fourth Amendment doctrine is a direct result of the Supreme Court's decision in *Katz* and the Court's first articulation of a "reasonable expectation of privacy" test for Fourth Amendment protection.[134] The majority in *Katz* declared that "the Fourth Amendment protects people, not places,"[135] and along with Justice Harlan's concurring opinion, established a privacy-based analysis for searches within the amendment.[136] By introducing the concept of privacy into its Fourth Amendment analysis, the Court, perhaps inadvertently, opened the door for later courts to redefine Fourth Amendment protections by using the concept to decide whether a government intrusion was *reasonable* under the amendment.

What ultimately became a reasonableness-balancing test arose out of the Court's decisions in *Camara v. Municipal Court*[137] and *Terry v. Ohio*.[138] The jurisprudence that emerged from these cases balanced an individual's reasonable expectation of privacy against the needs or interest of the government.[139] This balancing test created a sort of reasonableness ratio, where warrants were ultimately evaluated based on the weight of the government's need for the intrusion, and opened the door for a smorgasbord of government intrusions that lacked any sort of individualized probable cause under traditional Fourth Amendment analysis but which the Court could find "reasonable" in the balance. The doctrinal deck has been stacked: how can mere privacy compete with the fundamental importance of the fight against global terrorism, the War on Drugs, or our children's safety?

Post-*Katz* opinions are replete with the Court's recognition of the "special needs" of the government, which thus outweigh the individual's argument under

---

133. *Katz*, 389 U.S. at 361 (Harlan, J., concurring).

134. While the phrase "reasonable expectation of privacy" only appeared in Justice Harlan's concurring opinion in *Katz*, *id.* at 360, it has since become the standard description of the *Katz* test. *Id*. (Harlan, J., concurring); *see also* Scott E. Sundby, *"Everyman's" Fourth Amendment: Privacy or Mutual Trust Between Government and Citizen?*, 94 COLUM. L. REV. 1751, 1756 (1994).

135. *Katz*, 389 U.S. at 351 (majority opinion).

136. Smith v. Maryland , 442 U.S. 735, 740 (1979) ("Consistently with *Katz*, this Court uniformly has held that the application of the Fourth Amendment depends on whether the person invoking its protection can claim a justifiable, a reasonable, or a legitimate expectation of privacy that has been invaded by a government action." (internal quotation marks omitted)). For an excellent discussion of Fourth Amendment doctrine post-*Katz*, see Anthony G. Amsterdam, *Perspectives on the Fourth Amendment*, 58 MINN. L. REV. 349 (1974).

137. 387 U.S. 523 (1967) (applying Fourth Amendment doctrine to housing inspections based on balancing the needs of government against the individual's reasonable expectation of privacy).

138. 392 U.S. 1 (1968) (applying Fourth Amendment doctrine to police "stop-and-frisk" procedures based on reasonable suspicion that the individual was armed).

139. *See* Sundby, *supra* note 134, at 1769–70; *cf.* Orin S. Kerr, *An Equilibrium-Adjustment Theory of the Fourth Amendment*, 125 HARV. L. REV. 476, 487–89 (2011).

the balancing test.[140] This special needs doctrine grew out of the Supreme Court's recognition of the unique issues arising from administrative searches and the Court's attempts to carve out exceptions to traditional Fourth Amendment requirements for these civil searches.[141] Prior to the Court's decision in *Camara*, administrative and civil searches were not subject to Fourth Amendment requirements.[142] In *Camara*, however, the Court held that the Fourth Amendment's warrant clause should also apply to administrative searches, albeit in a somewhat more limited context.[143]

The Court more fully articulated what is now known as the "special needs" doctrine in *New Jersey v. T.L.O.*, where a high school administrator searched a purse belonging to a student he suspected of smoking in the school.[144] The school administrator had neither a warrant nor probable cause to conduct the search, but the Court allowed it based on two factors: first, the administrator's search was conducted for the purpose of "maintaining discipline in the classroom and on school grounds" and not for the purpose of law enforcement;[145] second, high school students have a "lesser expectation of privacy" than citizens in general.[146] Justice Blackmun's concurrence in the judgment laid out a test wherein the special needs doctrine was permitted "[o]nly in those exceptional circumstances in which special needs, beyond the normal need for law enforcement, make the warrant and probable-cause requirement impracticable."[147]

The "War on Terror" that followed the catastrophic events of September 11, 2001, increased the frequency of suspicionless searches by law enforcement, including contexts such as searches at entrances to subways, on ferries, near political conventions, near sports arenas, at protest rallies, and around water reservoirs.[148]

In particular, the genuine problem of global terrorism and the government's duty to provide for national security have added even more momentum to the courts' consistent trend toward analyzing Fourth Amendment problems from the

---

140. *See, e.g.*, Nat'l Treasury Emps. Union v. Von Raab, 489 U.S. 656, 668 (1989) ("[Illegal drugs are] one of the greatest problems affecting the health and welfare of our population."); Skinner v. Ry. Labor Execs.' Ass'n., 489 U.S. 602, 607 (1989) (observing fatalities, injuries, and damages from train accidents where alcohol or drugs were the cause); New Jersey v. T.L.O., 469 U.S. 325, 339 (1985) ("Maintaining order in the classroom has never been easy, but in recent years, school disorder has often taken particularly ugly forms: drug use and violent crime in the schools have become major social problems.").

141. *See, e.g.*, *Camara*, 387 U.S. at 530 (administrative searches related to health and public safety, such as enforcement of housing codes, often require suspicionless searches not easily conducted under traditional Fourth Amendment requirements).

142. *See id.*

143. *Id.* at 534. The Court recognized that although the warrant requirement of the Fourth Amendment applied to administrative searches, the requirement was met without having to reach the level of probable cause required for searches relating to criminal matters.

144. 469 U.S. at 328; *see also* Ric Simmons, *Searching for Terrorists: Why Public Safety Is Not a Special Need*, 59 DUKE L.J. 843, 863–65 (2010).

145. *T.L.O.*, 469 U.S. at 339.

146. *Id.* at 348 (Powell, J., concurring).

147. *Id.* at 351 (Blackmun, J., concurring in the judgment).

148. *See* Simmons, *supra* note 144, at 873−84.

government's point of view.[149] This is not to say that courts routinely adopt the government's arguments in Fourth Amendment cases, but rather that over the past three decades, the Supreme Court has been formulating Fourth Amendment doctrine from the perspective of the government or police agency engaged in searches or seizures.[150] This is contrary to the Court's orientation toward the individual in *Katz* and turns Fourth Amendment doctrine on its head; the Fourth Amendment was designed to protect citizens from unjustified and arbitrary government intrusions, not to facilitate the government's needs.[151] This core constitutional tenet is especially important when addressing government collective-surveillance programs in the face of government claims of national security necessity.

Current Fourth Amendment jurisprudence has been steadily moving toward analysis that begins from the government's perspective, a trend made plain in post-*Katz* cases that complain of the burden placed on government by Fourth Amendment requirements.[152] This doctrinal trend has been even more prevalent in cases argued after September 11, 2001, where the government argues that the needs of national security require an even freer hand unencumbered by naïve Fourth Amendment analysis made quaint by the global war on terrorism.[153]

In *Amnesty International USA v. Clapper*, for example, the Second Circuit Court of Appeals denied *en banc* review of an earlier decision by the court granting standing to plaintiffs who brought claims of Fourth Amendment violations by the government. In its decision, the *Clapper* court accepted, without challenge, the

---

149. *See* Sundby, *supra* note 134, at 1796–97.

150. *See id.* at 1788–90.

151. Justice Brandeis stated that when deciding Fourth Amendment questions, it is "immaterial that the [challenged] intrusion was in aid of law enforcement." Olmstead v. United States, 277 U.S. 438, 479 (1928) (Brandeis, J., dissenting*), overruled in part by* Katz v. United States, 389 U.S. 347 (1967); *see also* Potter Stewart, *The Road to* Mapp v. Ohio *and Beyond: The Origins, Development and Future of the Exclusionary Rule in Search-and-Seizure Cases*, 83 COLUM. L. REV. 1365, 1393 (1983).

152. *See, e.g.*, Griffin v. Wisconsin, 483 U.S. 868, 876 (1987) (observing that requiring probation officers to obtain a warrant before conducting an unrestricted search of a probationer's home would "make it more difficult for probation officials to respond quickly to evidence of misconduct" and would "reduce the deterrent effect that the possibility of expeditious searches would otherwise create"); United States v. Leon, 468 U.S. 897, 907 (1984) (protesting "the substantial social costs exacted by the exclusionary rule for the vindication of Fourth Amendment rights"); Tenenbaum v. Williams, 193 F.3d 581, 603 (2d Cir. 1999) ("[T]here are some [government] agencies outside the realm of criminal law enforcement where government officials have special needs beyond the normal need for law enforcement," and forcing these agencies "to follow ordinary law-enforcement requirements under the Fourth Amendment would impose intolerable burdens . . . ." (internal quotation marks omitted)); Willner v. Thornburgh, 928 F.2d 1185, 1188 (D.C. Cir. 1991) ("[W]hen the burden of obtaining a warrant is likely to frustrate the governmental purpose behind the search, the Fourth Amendment does not require a warrant." (citations omitted) (internal quotation marks omitted)).

153. *See, e.g.*, Amnesty Int'l USA v. Clapper, 667 F.3d 163, 172 (2d Cir. 2011) (Lynch, J., concurring in the denial of rehearing en banc). In 2013, the United States Supreme Court reversed the Second Circuit's earlier decision, finding that plaintiffs lacked Article III standing. Clapper v. Amnesty Int'l USA, 133 S. Ct. 1138, 1143 (2013).

government's contention that the surveillance programs in question were "fully consistent with the Fourth Amendment," and stated in its reasoning that "[i]t is important to remember what is at stake here . . . because the paramount necessity of protecting the nation's security against very real and dangerous external threats requires the limited additional burden on a discrete category of international communications imposed by the statute."[154] This general philosophy had been strongly encouraged by the government, as evidenced by the December 2005 revelation of a secret NSA program to intercept electronic communications between the United States and foreign countries without warrants or probable cause.[155] The Bush administration acknowledged and defended this warrantless wiretapping, with the Department of Justice suggesting that there may be other warrantless eavesdropping beyond what had already been disclosed.[156]

But this analytical perspective runs counter to the individualistic, protection-oriented jurisprudence of *Katz*, replacing it with a government-needs-and-interests-based analysis. This has led to an astigmatic view of the Fourth Amendment's purpose. An important inflection point in this post-*Katz* Fourth Amendment jurisprudence can be found in *Terry*, which initiated the Court's police perspective and introduced a new doctrine of *stop and frisk*.[157]

C. Parallels with Stop-and-Frisk Policies

The NSA's asserted right to collect and keep indefinitely all encrypted communications from U.S. citizens without a warrant, court order, or any particularized suspicion, bears some resemblance to the reasoning used to justify suspicionless stop-and-frisk policies. That is, supporters of the proactive police tool of stop and frisk based on *Terry* and its progeny argue that the tool's effectiveness at preventing crime is justification enough.[158] Stop-and-frisk proponents defend the program even when it is shown that these stops result in a very low number of actual arrests or discovery of contraband and often result in abusive police practices that target certain groups irrespective of a lack of individualized suspicion.[159] Through its collective-surveillance program of seizing and storing every encrypted communication from any U.S. citizen, irrespective of a lack of probable cause or

---

154. *Amnesty Int'l USA*, 667 F.3d at 172.

155. *See* James Risen & Eric Lichtblau, *Bush Lets U.S. Spy on Callers Without Courts*, N.Y. TIMES, Dec. 16, 2005, at A1.

156. *See* U.S. DEP'T OF JUSTICE, LEGAL AUTHORITIES SUPPORTING THE ACTIVITIES OF THE NATIONAL SECURITY AGENCY DESCRIBED BY THE PRESIDENT 5 (2006), *available at* http://www2.gwu.edu/~nsarchiv/NSAEBB/NSAEBB178/surv39.pdf.

157. Terry v. Ohio, 392 U.S. 1 (1968).

158. *See, e.g.*, David Rudovsky & Lawrence Rosenthal, Debate, *The Constitutionality of Stop-and-Frisk in New York City*, 162 U. PA. L. REV. ONLINE 117, 125 (2013), *available at* http://www.pennlawreview.com/online/162-U-Pa-L-Rev-Online-117.pdf.

159. *See, e.g.*, Floyd v. City of New York, 959 F. Supp. 2d 540 (S.D.N.Y. 2013). In *Floyd*, the court found that out of 4.4 million *Terry* stops conducted by the NYPD between January 2004 and June 2012, 98.5% of these found no weapon, 86% of these found no contraband, and 88% resulted in no further law-enforcement action. *Id*. at 556, 558–59.

reasonable suspicion, the NSA is similarly arguing that any improvement in national security—no matter how miniscule—justifies these collective warrantless seizures.[160]

The use of stop-and-frisk policies by police departments has been found constitutionally reasonable under the Fourth Amendment.[161] In these searches, police "stop and briefly detain a person for investigative purposes if the officer has a reasonable suspicion supported by articulable facts that criminal activity 'may be afoot,' even if the officer lacks probable cause."[162] That is, a police officer may conduct a stop and frisk "when the officer has reasonable, articulable suspicion that the person has been, is, or is about to be engaged in criminal activity."[163] At a minimum, "[t]he officer [making the stop] . . . must be able to articulate something more than an 'inchoate and unparticularized suspicion or hunch.'"[164] Reasonable suspicion therefore requires an individualized suspicion of wrongdoing.[165] While the Supreme Court has recognized certain narrow exceptions to this Fourth Amendment requirement, the Court has made no such exception for stops and frisks for the general purpose of controlling crime.[166]

In its examination of the stop-and-frisk practices of the NYPD, the *Floyd* court discussed the police officers' vague justifications for these stops, among the most common of which was a person's "furtive movements."[167] The court stated that if police officers truly believed that this broad description justifies a stop and frisk,

---

160. I do not argue that the NSA's collective-surveillance programs and domestic police stop-and-frisk policies are perfectly analogous. For example, as illustrated in *Floyd*, New York City's stop-and-frisk program resulted in racially motivated stops applied in a discriminatory manner. *Id.* at 660–64. I am not arguing that the NSA's policies are discriminatory. In fact, their collective warrantless seizures are quite indiscriminate in nature, which creates its own set of problems.

161. *See, e.g.*, *Terry*, 392 U.S. at 30–31.

162. United States v. Swindle, 407 F.3d 562, 566 (2d Cir. 2005) (quoting United States v. Sokolow, 490 U.S. 1, 7 (1989)).

163. United States v. Place, 462 U.S. 696, 702 (1983) (citing *Terry*, 392 U.S. at 22)).

164. Alabama v. White, 496 U.S. 325, 329 (1990) (quoting *Sokolow*, 490 U.S. at 7)).

165. *See* City of Indianapolis v. Edmond, 531 U.S. 32, 37 (2000) (citing Chandler v. Miller, 520 U.S. 305, 308 (1997)).

166. *See id*. at 34, 40 (distinguishing between suspicionless stops at checkpoints "for the purposes of combating drunk driving and intercepting illegal immigrants," which are constitutional, and suspicionless stops at checkpoints that primarily aim to advance "the general interest in crime control," which are unconstitutional (quoting Delaware v. Prouse, 440 U.S. 648, 659 n.18 (1979))).

167. Floyd v. City of New York, 959 F. Supp. 2d 540, 561 (S.D.N.Y. 2013). One officer explained his understanding of "furtive movement" as "a very broad concept" that could include a person

> "changing direction," "walking in a certain way," "[a]cting a little suspicious," "making a movement that is not regular," being "very fidgety," "going in and out of his pocket," "going in and out of a location," "looking back and forth constantly," "looking over their shoulder," "adjusting their hip or their belt," "moving in and out of a car too quickly," "[t]urning a part of their body away from you," "[g]rabbing at a certain pocket or something at their waist," "getting a little nervous, maybe shaking," and "*stutter[ing]*."

Id. (emphasis in original). Under these broad conditions, it appears as if almost any ordinary activity could be construed as "furtive movement" by the police.

"then it is no surprise that stops so rarely produce evidence of criminal activity."[168] The court held that the NYPD violated the plaintiffs' Fourth Amendment rights under these conditions, stating that "'[t]he idea of universal suspicion without individual evidence is what Americans find abhorrent . . . .'"[169]

A thought experiment is appropriate here. If a program like stop and frisk is effective in fighting crime—as the City of New York claimed in *Floyd*—what if, on this basis alone, the program was not only allowed to continue but expanded to require suspicionless stops of all citizens, regardless of other circumstances?[170] The *Floyd* court addressed this point, stating that "[m]any police practices may be useful for fighting crime—preventive detention or coerced confessions, for example—but because they are unconstitutional they cannot be used, no matter how effective. 'The enshrinement of constitutional rights necessarily takes certain policy choices off the table.'"[171]

But constitutionality only addresses a part (albeit an important one) of the underlying issues. If the City of New York wanted to ensure the complete effectiveness of its program, it would need to stop, frisk, or question every single person walking or driving the streets of New York. This is impossible, of course, since the numbers required to implement such a universal program are beyond even the NYPD's current strength.[172] Moreover, such a program would introduce an unacceptable drag on the ordinary business and functions within the city. Finally, such a universal program would likely have the opposite effect from that intended, as the increasing friction between the police and those being searched would ultimately erode order.[173] The NYPD tacitly conceded these points in *Floyd*, when a police deputy inspector explained that "stopping 'the right people, [at] the right

---

168. *Id*. at 561.

169. *Id*. at 667 (quoting Charles M. Blow, *The Whole System Failed Trayvon Martin*, N.Y. TIMES (July 15, 2013), http://www.nytimes.com/2013/07/16/opinion/the-whole-system-failed.html).

170. In *Floyd*, the City and the NYPD made repeated claims in testimony and evidence that their focus in applying the stop-and-frisk program was "on effectiveness, not constitutionality." *Id*. at 593. Examples of this philosophy abound in the city's arguments and were applied from the lowest to highest levels within the police department, including evaluation of whether police officers' "impact on declared conditions" was "effective." Moreover, the Chief of Police put pressure on subordinates by measuring effectiveness through numbers of stops. *See id*. at 601–02.

171. *Id*. at 556 (quoting Dist. of Columbia v. Heller, 554 U.S. 570, 636 (2008)). The court later notes that "[e]ven if it were an *effective* gang-suppression strategy to stop every person wearing known gang paraphernalia, it would not be a *constitutional* strategy, because neither carrying beads nor flaunting a bandana is a crime." *Id*. at 599 n.249 (emphasis in original).

172. "The NYPD's current uniformed strength is approximately 34,500." Police Dep't, City of N.Y., *Frequently Asked Questions*, NYC.GOV, http://www.nyc.gov/html/nypd/html/faq/faq_police.shtml.

173. The Supreme Court recognized this outcome in *Terry*, stating that "'[i]n many communities, field interrogations are a major source of friction between the police and minority groups,'" and that friction "increases 'as more police departments [encourage] officers . . . routinely to stop and question person on the street.'" Terry v. Ohio, 392 U.S. 1, 14 n.11 (quoting PRESIDENT'S COMM'N ON LAW ENFORCEMENT & ADMIN. OF JUSTICE, TASK FORCE REPORT: THE POLICE 183 (1967)).

time, [in] the right location' meant not stopping 'a 48-year-old lady [who] was walking through St. Mary's Park when it was closed.'"[174]

These real world constraints provide a natural brake on police search-and-seizure abuses that do not necessarily need a court opinion to have an effect. What happens, however, when technology presents methods of conducting a similar form of collective, persistent surveillance that avoids these natural constraints? This is the case that these newly confirmed government surveillance programs have put before us today, and it is in these cases, where the natural safety nets of limited resources and public opinion are missing, that constitutional diligence must be at its strongest.

D. The Double-Edged Sword of Technology

The steady advance of communication technology since the nineteenth century has effectively brought nearly everyone on the planet within earshot of one another.[175] Within a mere two centuries, messages intended for transoceanic recipients, which would have taken many weeks to reach their destination, can reach their recipient within a fraction of a second.[176] Furthermore, modern modes of communication are not just available to governments or large commercial enterprises but to anyone with a cell phone.[177] The result has been a virtual shrinking of our planet and has spurred a flood of global communication and media that existed solely in the realm of speculative fiction only a few decades ago.[178]

---

174. *Floyd,* 959 F. Supp. 2d at 604 (alterations in original).

175. For example, according to the International Telecommunication Union, there were 6.8 billion mobile phone subscriptions worldwide in 2013, which is roughly equivalent to 96% of the global population. INT'L TELECOMM. UNION, THE WORLD IN 2013: ICT FACTS AND FIGURES 1 (2013), *available at* http://www.itu.int/en/ITU-D/Statistics/Documents/facts/ICTFactsFigures2013-e.pdf.

176. In the early 1800s, a message from the British government to its representatives in Delhi would take six weeks. The telegraph cut this time down to days, then hours. DIFFIE AND LANDAU, *supra* note 48, at 1; *see also* Gibson, *supra* note 47 (explaining that "cyberspace has everted" and "colonized" our everyday world).

177. While citizens of developed nations may enjoy relatively easy access to the Internet through multiple means, this is not the case for much of the developing world. Even so, advances in communications technologies—especially wireless technologies—along with the continued advancement of communications infrastructure in developing nations have resulted in an increase of the percentage of developing nation populations using the Internet, from 7.8% in 2005 to 30.7% in 2013. INT'L TELECOMM. UNION, KEY ICT INDICATORS FOR DEVELOPED AND DEVELOPING COUNTRIES AND THE WORLD (TOTALS AND PENETRATION RATES), *available at* http://www.itu.int/en/ITU-D/Statistics/Documents/statistics/2013/ITU_Key_2005-2013_ICT_data.xls.

178. The myriad ways we have integrated computing and the Internet into our daily lives have brought us to a point where many tasks that would have been seen as miraculous just a few years ago—such as high-quality audio and video on mobile devices, international video conferencing via cell phones, and widespread GPS—have become mundane and therefore transparent. In fact, the ability to put fully functional computers in the tiniest devices is creating what scholars have referred to as the *Internet of Things*—the equipping of nearly every device with computing and networking functionality, thus enabling transformative uses of new and existing technologies. *Cf.* Kevin Ashton, *That 'Internet of Things' Thing*,

These advances have brought with them new and unforeseen opportunities for governments to implement broad, persistent surveillance programs.[179] Courts have slowly begun to realize the impact these technologies may have on existing Fourth Amendment doctrine and have started to question the application of existing jurisprudence to "contemporary forms of communication."[180] Commentators have debated the usefulness of existing Fourth Amendment norms when considering new technologies for some time, with mixed results.[181]

Government use of advances in information technologies to collect and analyze ever larger and more detailed citizen databases should come as no surprise. Questions of efficacy aside for the moment, the State's increased use of data collection and analysis is a predictable result of the continued realization of Moore's Law.[182] Furthermore, this growth is not a new phenomenon. Governments used data collection and analysis long before the post-2001 counterterrorism efforts to accomplish such well-established goals as crime prevention, delivery of welfare benefits, and protection of citizens' rights.[183]

RFID J. (June 22, 2009), http://www.rfidjournal.com/articles/view?4986.

179. *See, e.g.*, *In re* Application of the U.S. for an Order Authorizing the Release of Historical Cell-Site Info., 809 F. Supp. 2d 113 (E.D.N.Y. 2011) (denying the government's application for cell-site-location records, observing that the use of GPS data sent by cell phones could allow for total geographical surveillance by the government); State v. Patino, No. P1-10-1155A, 2012 R.I. Super. LEXIS 139 (Sept. 4, 2012) (explaining that contemporary forms of communication, such as text messages, could provide easily obtainable information to government agencies and are protected under the Fourth Amendment), *aff'd in part and vacated in part*, 93 A.3d 40 (R.I. 2014); Courtney M. Bowman, *A Way Forward After* Warshak*: Fourth Amendment Protections for E-mail*, 27 BERKELEY TECH. L.J. 809, 815–18 (2012) (describing e-mail technology and protocols and the information leaked through third-party doctrine); Kerr, *supra* note 124, at 1012 (discussing Internet communications transmitted over wireless networks that are therefore vulnerable to eavesdropping); *see also supra* Introduction (discussing formerly secret NSA surveillance programs).

180. *Patino*, 2012 R.I. Super. LEXIS 139, at *128 ("[T]he third-party doctrine [under Fourth Amendment analysis] is ill-suited for contemporary forms of communication and thus should not wholly defeat an individual's expectation of privacy in the contents of his or her text messages.").

181. *See* Orin S. Kerr, *The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution*, 102 MICH. L. REV. 801 (2004) (debating the role courts should take when considering Fourth Amendment issues arising out of new technologies and their uses).

182. *Cf.* James X. Dempsey & Lara M. Flint, *Commercial Data and National Security*, 72 GEO. WASH. L. REV. 1459, 1459–64 (2004).

183. The two-edged sword of technological advances leading to increased data collection is not solely a means for social control. Rather, information may be used by governments to protect citizens' rights and provide for their welfare:

> [T]he surveillance systems of advanced bureaucratic nation-states are not so much the repressive machines that pessimists imply, but the outcome of aspirations and strivings for citizenship. If government departments are to treat people equally . . . then those people must be individually identified. To exercise the right to vote, one's name must appear on the electoral roll; to claim welfare benefits, personal details must be documented. Thus . . . the individuation that treats people in their own right, rather than merely as members of families or communities, means freedom from specific constraints

The government, therefore, has many compelling reasons to collect and store information about its citizens, and the increasing ease with which we communicate over the Internet has made it a natural tool for information gathering.[184] With the ability to collect and store virtually all information communicated over the Internet, the government could apply analytical tools to reveal a very detailed portrait of who we are based on what we buy, what organizations we belong to, what we read, and what we watch.[185]

The base analytical tools made available under existing Fourth Amendment doctrine are sound but have been gradually (and artificially) limited to a characterization of the underlying constitutional issues that have little basis in the Framers' intent. This characterization, focusing on an ill-defined concept of privacy and taken from the perspective of the government agent engaged in search and seizure, has been redefined from a prohibition against impermissible government intrusions based firmly on the Fourth Amendment's Warrant Clause[186] to a balancing test which weighs an individual's right to privacy against the government interest in effective law enforcement. This balancing test departs from the language of the Warrant Clause and relies instead on the Reasonableness Clause, based on the special needs of government.[187]

> but also greater opportunities for surveillance and control on the part of a centralized state.

DAVID LYON, THE ELECTRONIC EYE: THE RISE OF SURVEILLANCE SOCIETY 32–33 (1994) (internal quotations omitted). A very early example of government use of citizens' data to facilitate governance can be found in the Domesday Book, commissioned in 1086 by William the Conqueror, which included exhaustive compilations of landholders, tenants, properties, and their values. This early administrative record keeping established four characteristics of the surveillance state which survive today: (1) political power was the essential personage; (2) power was exercised first of all by posing questions, by interrogating; (3) in order to determine the truth, power appealed to notables to give this information; and (4) the king consulted the notables without forcing them to tell the truth through the use of violence, pressure, or torture. Foucault, *supra* note 24, at 45.

184. As Lawrence Lessig once observed, "[C]yberspace does not guarantee its own freedom but instead carries an extraordinary potential for control." LAWRENCE LESSIG, CODE AND OTHER LAWS OF CYBERSPACE 58 (1999).

185. *See* Daniel J. Solove, *Access and Aggregation: Public Records, Privacy and the Constitution*, 86 MINN. L. REV. 1137, 1138–39 (2002).

186. The protections laid out by the Fourth Amendment are principally found in two clauses: the Warrant Clause, which requires that "no Warrants shall issue, but upon probable cause," and the Reasonableness Clause, whose somewhat vague language prohibits "unreasonable searches and seizures." U.S. CONST. amend. IV.

187. *See supra* Part II.B. *But see* Florida v. Jardines, 133 S. Ct. 1409, 1415 (2013) (applying trespass analogy when considering whether a drug search by a dog on a home's front porch is a search under the Fourth Amendment); United States v. Jones, 132 S. Ct. 945, 949 (2012) (citing *Boyd v. United States*, 116 U.S. 616 (1886)) (observing the Fourth Amendment's "close connection to property" and raising the common-law trespass theory of Fourth Amendment jurisprudence). It remains to be seen whether *Jones* and its progeny will yield a new paradigm of Fourth Amendment analysis which relies once again on common-law trespass as a partial basis. Courts appear skeptical of any significant change in the doctrine. *See* United States v. McGuire, No. CR 13-40058, 2013 U.S. Dist. LEXIS 145175, at *25–31 (D.S.D. Oct. 1, 2013) (questioning the trespass analyses in *Jones* and *Jardines*), *magistrate report adopted by* 2013 U.S. Dist. LEXIS 174657 (D.S.D. Dec. 10, 2013).

E. Privacy, Secrecy, Security, and Their Measure

One of the more problematic components of the Fourth Amendment "balancing test" is its dependence on the elusive concept of privacy and its assumed inherent quantifiability.[188] The difficulty with this approach lies both in its implied conflation of a multitude of privacy definitions and in its use as a "fact" rather than as a value by the courts.[189] While courts appear to agree wholeheartedly in the abstract concept of privacy as a cherished constitutional value,[190] it is not the

---

188. *See, e.g.*, Maryland v. King, 133 S. Ct. 1958, 1970 (2013) ("'[R]ather than employing a *per se* rule of unreasonableness, we balance the privacy-related and law enforcement-related concerns to determine if the intrusion was reasonable." (emphasis in original) (quoting Illinois v. McArthur, 531 U.S. 326, 331 (2001))); Bd. of Educ. v. Earls, 536 U.S. 822, 829 (2002) ("[W]e generally determine the reasonableness of a search by balancing the nature of the intrusion on the individual's privacy against the promotion of legitimate governmental interests."); United States v. Knights, 534 U.S. 112, 121 (2001) ("Although the Fourth Amendment ordinarily requires the degree of probability embodied in the term 'probable cause,' a lesser degree satisfies the Constitution when the balance of governmental and private interests makes such a standard reasonable."); United States v. Jacobsen, 466 U.S. 109, 125 (1984) ("To assess the reasonableness of this [search], '[w]e must balance the nature and quality of the intrusion on the individual's Fourth Amendment interests against the importance of the governmental interests alleged to justify the intrusion.'" (quoting United States v. Place, 462 U.S. 696, 703 (1983))); Delaware v. Prouse, 440 U.S. 648, 654 (1979) ("[T]he permissibility of a particular law enforcement practice is judged by balancing its intrusion on the individual's Fourth Amendment interests against its promotion of legitimate government interests.").

189. Privacy violations can involve a wide variety of harmful or problematic activities. Daniel Solove lists examples such as newspapers naming rape victims, reporters gaining entry to a person's home under false pretenses to photograph her, the use of backscatter X-ray machines—colloquially known as "virtual strip-search machines" for their ability to see through clothing—by the U.S. Transportation Security Agency, the government use of thermal sensors to detect heat emanating from private homes, a company marketing a list of millions of elderly incontinent women, and a company selling personal information of customers despite promises not to do so. DANIEL J. SOLOVE, UNDERSTANDING PRIVACY 6 (2008). It is plain that all of these patterns are examples of one sort of privacy violation or another, but they exhibit very different actors and situations. To lump all such examples under a single concept of privacy either fails to properly recognize the problem or unfairly conflates these problems to fit a desired rubric.

190. Courts will often speak in reverent tones about the core constitutional importance of an individual's privacy, and then follow this homage to the abstract concept with an explanation why a particular government search was therefore permissible. *See, e.g.*, Skinner v. Ry. Labor Execs.' Ass'n, 489 U.S. 602, 613–16 (1989) (stating that "[t]he [Fourth] Amendment guarantees the privacy, dignity, and security of persons against certain arbitrary and invasive acts by officers of the Government or those acting at their discretion," and the "physical intrusion" of a blood test "penetrating beneath the skin, infringes an expectation of privacy that society is prepared to recognize as reasonable," yet finding that mandatory government blood and urine tests were reasonable); New Jersey v. T.L.O., 469 U.S. 325, 335 (1985) (noting that "'[t]he basic purpose of [the Fourth] Amendment, as recognized in countless decisions of this Court, is to safeguard the privacy and security of individuals against arbitrary invasions by governmental officials,'" and "the individual's interest in privacy and personal security 'suffers whether the government's motivation is to investigate

principle of privacy but its factual nature that has driven recent decisions.[191] Any Fourth Amendment analysis that treats privacy as merely a factual matter to be quantified and weighed against the concerns of the government unnecessarily complicates Fourth Amendment analysis and ignores the much more fundamental principle first articulated by Justice Brandeis—"the right to be let alone."[192] This problem becomes especially acute when courts attempt to reconcile the balancing approach to Fourth Amendment analysis with technological advances that give the government the ability to invade an individual's privacy with relatively little (or no) perceived physical intrusion.[193]

This shift to a factual analysis and quantification of privacy has not only drawn the courts' attention away from the consideration of the fundamental value of privacy but has also led to some rather strange, fact-specific discussions involving such topics as garbage left on the curb for collection,[194] thermal

---

violations of criminal laws or breaches of other statutory or regulatory standards,'" before holding that a public school teacher's warrantless search of a student's purse was reasonable (alteration in original) (quoting Camara v. Municipal Court, 387 U.S. 523, 528 (1967); Marshall v. Barlow's, Inc., 436 U.S. 307, 312–13 (1978))); Terry v. Ohio, 392 U.S. 1, 17 (1968) (observing that a police frisk was a "serious intrusion upon the sanctity of the person, which may inflict great indignity and arouse strong resentment," but holding that such a frisk was permissible under less than probable cause); Schmerber v. California, 384 U.S. 757, 772 (1966) (upholding a mandatory blood test while noting that "[t]he integrity of an individual's person is a cherished value of our society").

191. *See, e.g.*, Smith v. Maryland, 442 U.S. 735 (1979). In *Smith*, the Court considered privacy as a fact and held that no reasonable expectation of privacy exists in telephone numbers dialed, since

> [t]elephone users, in sum, typically know that they must convey numerical information to the phone company; that the phone company has facilities for recording this information; and that the phone company does in fact record this information for a variety of legitimate business purposes. Although subjective expectations cannot be scientifically gauged, it is too much to believe that telephone subscribers, under these circumstances, harbor any general expectation that the numbers they dial will remain secret.

Id. at 743. Justice Marshall dissented, observing that privacy was a value independent of the underlying facts, since "whether privacy expectations are legitimate . . . depends not on the risks an individual can be presumed to accept when imparting information to third parties, but on the risks he should be forced to assume in a free and open society." *Id*. at 750 (Marshall, J., dissenting).

192. "The makers of our Constitution . . . conferred, as against the Government, the right to be let alone—the most comprehensive of rights and the right most valued by civilized men. To protect that right, every unjustifiable intrusion by the Government upon the privacy of the individual, whatever the means employed, must be deemed a violation of the Fourth Amendment." Olmstead v. United States, 277 U.S. 438, 478 (1928) (Brandeis, J., dissenting), *overruled in part by* Katz v. United States, 389 U.S. 347 (1967).

193. When technological advances give government agents the ability to invade an individual's privacy without the need for an actual physical intrusion, courts tend to use a technologically enabled lesser intrusion as part of the justification for a government search that otherwise would not be allowed. *See* Sundby, *supra* note 134, at 1762–63 (discussing the courts' use of a sliding scale of intrusion minimization to compensate for weaker government justifications for a search).

194. California v. Greenwood, 486 U.S. 35 (1988) (whether an individual has a privacy

imaging devices,[195] hovering helicopters,[196] dogs sniffing near homes,[197] dogs sniffing near cars,[198] the legal status of motor homes as actual homes,[199] DNA collection,[200] conversations in private driveways,[201] and cell phone location information.[202] To put it another way, under current Fourth Amendment doctrine, courts are not asking whether items, activities, or places *should* be kept private according to a set of fundamental values, but whether, under the *facts of each case*, we would expect others to be able to observe these items, activities, or places.[203]

This doctrine runs counter to the Framers' Fourth Amendment intent. Justice Brandeis's famous dissent in *Olmstead* was the Court's first pure articulation of the need to rely on the values and principles underlying the Constitution when interpreting Fourth Amendment protections.[204] This is what Justice Brandeis meant:

---

interest in garbage left on the curb for collection).

195. Kyllo v. United States, 533 U.S. 27 (2001) (whether a subjective expectation of privacy exists against police use of a thermal imaging scanner to detect heat patterns emanating from a private home).

196. Florida v. Riley, 488 U.S. 445 (1989) (whether an individual has a reasonable expectation of privacy from a helicopter flying four hundred feet above a home).

197. Florida v. Jardines, 133 S. Ct. 1409 (2013) (whether a reasonable expectation of privacy exists against a drug-sniffing dog being brought onto a porch).

198. Illinois v. Caballes, 543 U.S. 405 (2005) (whether a reasonable expectation of privacy exists against a drug-sniffing dog brought alongside a car stopped for speeding).

199. California v. Carney, 471 U.S. 386 (1985) (whether a motor home is more like a car or a home with respect to privacy expectations).

200. Maryland v. King, 133 S. Ct. 1958 (2013) (whether a postarrest—but preconviction—collection of DNA via a cheek swab was a violation of a reasonable expectation of privacy).

201. United States v. Scott, 731 F.3d 659 (7th Cir. 2013) (whether an individual has a reasonable expectation of privacy in conversations that take place in his driveway), *cert. denied*, 134 S. Ct. 1806 (2014).

202. United States v. Caraballo, 963 F. Supp. 2d 341 (D. Vt. 2013) (whether an individual has a reasonable expectation of privacy in real-time cell phone location information).

203. Furthermore, the government may not avoid Fourth Amendment protections of private papers and communications merely by announcing that citizens should no longer have an expectation of privacy in these items. For example, in *Smith v. Maryland*, the Supreme Court stated that

> if the Government were suddenly to announce on nationwide television that all homes henceforth would be subject to warrantless entry, individuals thereafter might not in fact entertain any actual expectation of privacy regarding their homes, papers, and effects. Similarly, if a refugee from a totalitarian country, unaware of this Nation's traditions, erroneously assumed that police were continuously monitoring his telephone conversations, a subjective expectation of privacy regarding the contents of his calls might be lacking as well. In such circumstances, where an individual's subjective expectations had been "conditioned" by influences alien to well-recognized Fourth Amendment freedoms, those subjective expectations obviously could play no meaningful role in ascertaining what the scope of Fourth Amendment protection was.

442 U.S. 735, 740 n.5 (1979). Note that, in light of revelations of government surveillance of U.S. citizens' telephone, e-mail, and other electronic information, Justice Blackmun's words take on a special—if unintended—meaning.

204. *See supra* note 192.

certain items should be free from government intrusion via the individual's "right to be let alone."[205] This tenet is a far cry from the case-by-case factual privacy analysis currently employed in Fourth Amendment cases. But while broad principles such as this may work well in theory—we think we know a privacy violation when we see it—they are often too abstract to provide courts with predictable rules.

In the years since the attacks of September 11, 2001, the U.S. government has exacerbated these issues by adopting an overall doctrine that has prioritized security above all else, creating what some scholars have called a "constitutional pathological period" with respect to national security.[206] Of course, one of the government's primary constitutional duties to its citizens is the maintenance of national security, and protecting the population from terrorist attacks certainly falls under this umbrella.[207] Some scholars and commentators have argued that the need for national security in the age of terrorism either allows suspicionless searches under current Fourth Amendment doctrine or entirely supersedes any need for "traditional" Fourth Amendment analysis.[208] National security is an important

---

205. *See supra* Part II.A.

206. *See* Vincent Blasi, *The Pathological Perspective and the First Amendment*, 85 COLUM. L. REV. 449, 459 (1985); Howard M. Wasserman, *Constitutional Pathology, the War on Terror, and* United States v. Klein, 5 J. NAT'L SECURITY L. & POL'Y 211, 215–16 (2011). Professors Blasi and Wasserman define pathological periods of our constitutional government as periods marked by a "sense of urgency stemming from societal disorientation if not panic." Blasi, *supra*, at 468. Their defining characteristic is "a shift in basic attitudes, among certain influential actors if not the public at large," about central constitutional tenets. *Id*. at 467. This panic "affects structural features and arrangements, such as formal and informal separation of powers and checks and balances, which may exert much less of a restraining influence on the political branches and the public." Wasserman, *supra*, at 215 (internal quotations omitted).

207.

> We the People of the United States, in Order to form a more perfect Union, establish Justice, insure domestic Tranquility, provide for the common defence, promote the general Welfare, and secure the Blessings of Liberty to ourselves and our Posterity, do ordain and establish this Constitution for the United States of America.

U.S. CONST. pmbl.

208. *See, e.g.*, RICHARD A. POSNER, NOT A SUICIDE PACT: THE CONSTITUTION IN A TIME OF NATIONAL EMERGENCY 4, 31 (2006) (arguing that "[t]he core meaning of 'civil liberties' is freedom from coercive or otherwise intrusive governmental actions designed to secure the nation against real or, sometimes, imagined internal and external enemies," but courts must engage in a pragmatic cost-benefit analysis to determine the proper balance between the interests in liberty against those of national security); Ricardo J. Bascuas, *Fourth Amendment Lessons from the Highway and the Subway: A Principled Approach to Suspicionless Searches*, 38 RUTGERS L.J. 719, 722 (2007) (arguing that the case for suspicionless New York City subway searches is "relatively easy to make," where the "threat of terrorism promises to proliferate suspicionless searches"); Ronald M. Gould & Simon Stern, *Catastrophic Threats and the Fourth Amendment*, 77 S. CAL. L. REV. 777, 777–78 (2004) (arguing that "traditional Fourth Amendment search-and-seizure doctrine was fine for an age of flintlocks" but that "large-scale searches undertaken to prevent horrific potential harms may be constitutionally sound"); Richard C. Worf, *The Case for Rational Basis Review of*

purpose of government, but it is not its sole purpose, and to elevate antiterrorism to a status that overshadows other values risks the corrosion of our constitutional foundations through a number of possible causes.[209]

Furthermore, similar to the concept of privacy, we often have a difficult time defining exactly what "security" means, despite the fact that the rationale for the privacy-security balance appears to be a given in such discussions.[210] Some commentators have suggested that governments, including the United States, leverage and politicize these ontological ambiguities to promote specific foreign-policy objectives, for example, declaring war on terrorism without a particular definition of what that means in real terms.[211] For primarily this reason, commentators have called into question the presumed existence of a measurable privacy-security balance.[212]

General Suspicionless Searches and Seizures, 23 TOURO L. REV. 93, 131–37 (2007) (stating that suspicionless searches should be seen as reasonable, and therefore constitutional, if they have been approved by the legislature).

209. Eric Posner and Adrian Vermeule categorize the various security policies implemented after September 11, 2011, which include military action, the detention of enemy combatants outside the theater of hostilities, heightened search and surveillance powers, ethnicity-based search and surveillance, coercive interrogation, immigration sweeps and surveillance, enactment of terrorism and material-support statutes, military trials, and censorship. ERIC A. POSNER & ADRIAN VERMEULE, TERROR IN THE BALANCE: SECURITY, LIBERTY, AND THE COURTS 7–9 (2007).

210. *See, e.g.*, Hamdi v. Rumsfeld, 542 U.S. 507, 545 (2004) (Souter, J., concurring in part, dissenting in part, and concurring in the judgment) ("For reasons of inescapable human nature, the branch of the Government asked to counter a serious threat is not the branch on which to rest the Nation's entire reliance in striking the balance between the will to win and the cost in liberty on the way to victory; the responsibility for security will naturally amplify the claim that security legitimately raises."); United States v. Warsame, 547 F. Supp. 2d 982, 992 n.10 (D. Minn. 2008) ("[C]ourts upholding the constitutionality of [the Foreign Intelligence Surveillance Act] have done so not because a FISA order is a 'warrant,' but because . . . FISA strikes a reasonable balance between governmental interests in national security and individual liberty interests."); Doe v. Gonzales, 500 F. Supp. 2d 379, 408−09 (S.D.N.Y. 2007) ("'[T]he high stakes here pressing the scales . . . compel the Court to strike the most sensitive judicial balance, calibrating by delicate increments toward a result that adequately protects national security without unduly sacrificing individual freedoms.'" (quoting Doe v. Ashcroft, 33 F. Supp. 2d 471, 478 (2004))), *aff'd in part, rev'd in part sub nom.* John Doe, Inc. v. Mukasey, 549 F.3d 861 (2d Cir. 2008); DAVID COLE & JULES LOBEL, LESS SAFE, LESS FREE: WHY AMERICA IS LOSING THE WAR ON TERROR 101 (2007) ("[T]here are deep-rooted reasons why government officials are unlikely to balance security and the rule of law fairly or accurately in times of crisis . . . .").

211. *See, e.g.*, Alexander J. Marcopoulos, Terrorizing Rhetoric: The Advancement of U.S. Hegemony Through the Lack of a Definition of 'Terror' 2–3 (Jan. 13, 2009) (unpublished manuscript), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1327155 (arguing that the United States has used ambiguous definitions of security and terrorism to its political advantage).

212. *See, e.g.*, David Cole, *No Reason To Believe: Radical Skepticism, Emergency Power, and Constitutional Constraint*, 75 U. CHI. L. REV. 1329, 1334 (2008) (stating that the argument "that there is a necessary and straightforward tradeoff between liberty and security is far too simplistic" (citation omitted) (internal quotation marks omitted)); Stephen Holmes, *In Case of Emergency: Misunderstanding Tradeoffs in the War on Terror*, 97 CALIF. L. REV.

III. PERSISTENT SURVEILLANCE AND CONSTITUTIONAL WARINESS OF STATE POWER

The origins of the Fourth Amendment can be traced to early Americans' antipathy toward general warrants, which gave British agents authority to conduct indiscriminate, suspicionless searches of people and their homes.[213] While these general warrants led, of course, to privacy problems, the true underlying issue in this context was the individual's relationship to the State and the need to keep a check on the balance of power in that relationship. Scholars and commentators have called for greater reinforcement of this constitutional principle, urging courts to think of the Fourth Amendment as "security from unreasonable governmental intrusion," which follows directly from the Framers' distaste for the "arbitrary exercise of [British government] power to invade their property."[214]

The shift of Fourth Amendment doctrine's focus to one of privacy limits the amendment's ability to protect citizens from arbitrary government power. Justice Jackson observed that the Fourth Amendment was meant to protect more than privacy alone; it was meant to ensure that government intrusions of individual privacy are based on rules established and overseen by the citizens.[215] The current use of a Fourth Amendment balancing test between government need and individual privacy has taken this oversight away from individuals and instead established it in courts and law enforcement.

The ease with which government agencies can now conduct persistent, collective surveillance on every citizen heightens the need to reorient Fourth Amendment doctrine back to its roots in the constitutional principle: to protect individuals from overwhelming government power. Some scholars have characterized this reorientation as a need for a balance of power.[216] This approach often places too much emphasis on courts' abilities to effectively judge (and attenuate) a swinging pendulum of Fourth Amendment doctrine and bears too much

---

301, 313 (2009) (observing that "the master metaphor dominating discussions of the war on terror is the idea of a necessary tradeoff between liberty and security" but that the "metaphor is loaded" because "it is seductively easy to illustrate"); Jeremy Waldron, *Safety and Security*, 85 NEB. L. REV. 454, 456 (2006) ("Although we know that 'security' is a vague and ambiguous concept, and though we should suspect that its vagueness is a source of danger when talk of trade-offs is in the air, still there has been little or no attempt in the literature of legal and political theory to bring any sort of clarity to the concept." (footnote omitted)).

213. The Founders' concerns about unabated government power are shown in three seminal search-and-seizure cases that predate the Constitution: Wilkes v. Wood, (1763) 95 Eng. Rep. 766 (K.B.); 2 Vent. 69; Entick v. Carrington, (1765) 95 Eng. Rep. 807 (K.B.); 19 How. St. Tri. 1030; and the Writs of Assistance Case, *see* M.H. SMITH, THE WRITS OF ASSISTANCE CASE (1978); *see also* Olmstead v. United States, 277 U.S. 438, 463 (1928) (observing that the "well known historical purpose of the Fourth Amendment" was "directed against general warrants and writs of assistance"), *overruled in part by* Katz v. United States, 389 U.S. 347 (1967); Thomas Y. Davies, *Recovering the Original Fourth Amendment*, 98 MICH. L. REV. 547, 558 (1999).

214. Thomas K. Clancy, *What Does the Fourth Amendment Protect: Property, Privacy, or Security?*, 33 WAKE FOREST L. REV. 307, 351−52 (1998).

215. Brinegar v. United States, 338 U.S. 160, 180 (1949) (Jackson, J., dissenting).

216. *See, e.g.*, Kerr, *supra* note 139 (arguing that constantly changing technologies and social practices require the Supreme Court to adjust Fourth Amendment protections to achieve a power equilibrium between citizens and government).

uncomfortable resemblance to the current balancing-test jurisprudence. I recommend, rather, that courts evaluate Fourth Amendment problems posed by mass-surveillance programs by recognizing their true social cost and assessing the fundamental constitutional tenet that protects the individual citizen from the overwhelming power of the State.[217]

A. The Cost of Persistent, Collective Surveillance

As illustrated in Part II.D, *supra*, a protocol calling for the suspicionless, systematic, and physical search of every citizen would not long survive, largely due to the impossibility of such a protocol's practical application and the resentment it would generate among citizens. But what happens when technological advances allow government to collect and store the electronic data we generate, completely unbeknownst to the person being searched? The government can avoid the twin checks of limited police resources and community hostility that ordinarily constrain abusive law-enforcement practices. This new model of surveillance threatens a value just as fundamental to Fourth Amendment analysis as privacy—the mutual trust between government and the governed necessary in any democratic society.[218]

In a 1974 law review article, former Chief Justice William Rehnquist posed the following hypothetical to illustrate the tension between the normative concept of

---

217. The Founders were quite clear on the need for this constitutional principle. For example, James Madison had expressed this view in a letter to Thomas Jefferson on the subject of a possible Bill of Rights:

> In our Governments the real power lies in the majority of the Community, and the invasion of private rights is cheifly [sic] to be apprehended, not from acts of Government contrary to the sense of its constituents, but from acts in which the Government is the mere instrument of the major number of the constituents. . . . [But] there may be occasions on which the evil may spring from [government self-interest]; and on such, a bill of rights will be a good ground for an appeal to the sense of the community.

Letter from James Madison to Thomas Jefferson (Oct. 17, 1788), *in* 11 THE PAPERS OF JAMES MADISON 295, 298−99 (Robert A. Rutland & Charles F. Hobson eds., 1977).

218. The inherent threat to constitutional values from persistent, collective surveillance was acknowledged by Justice Sotomayor in *United States. v. Jones*:

> In cases involving even short-term monitoring, some unique attributes of GPS surveillance relevant to the *Katz* analysis will require particular attention. GPS monitoring generates a precise, comprehensive record of a person's public movements that reflects a wealth of detail about her familial, political, professional, religious, and sexual associations. The Government can store such records and efficiently mine them for information years into the future. [United States v.] Pineda-Moreno, 617 F.3d 1120, 1124 (9th Cir. 2010) (opinion of Kozinski, C.J.). And because GPS monitoring is cheap in comparison to conventional surveillance techniques and, by design, proceeds surreptitiously, it evades the ordinary checks that constrain abusive law enforcement practices: "limited police resources and community hostility."

United States v. Jones, 132 S. Ct. 945, 955−56 (2012) (Sotomayor, J., concurring) (citations omitted). While Justice Sotomayor was addressing the specific issue of surreptitious GPS tracking, the principles she articulates apply to all such "invisible" techniques of government surveillance.

privacy and privacy as interpreted by the Fourth Amendment.[219] In the hypothetical, the reader is asked to imagine that a police officer is required to stand in the parking lot of a bar from the hours of 5:30 p.m. to 7:30 p.m. every day.[220] During this time, the police officer records the license plate of every car that parks in the bar's parking lot in order to make a list of the bar's regular customers.[221] For the purposes of the hypothetical, Rehnquist asked the reader to assume that the police officer has no reason to know of any unlawful conduct at the bar or by the bar's customers.[222]

As Rehnquist points out in his article, this type of persistent surveillance, with no knowledge of any unlawful conduct or other special circumstances, would strike most Americans as an improper police function, with a substantial segment reacting with an "affirmative dislike" of this unwarranted surveillance.[223] But these same people would likely agree that driving a car down a public street to an open parking lot adjacent to a bar that is open to the public is not a *private* act in a normative sense of the term. In fact, any private citizen, newspaper reporter, or survey taker would have the right to do exactly what the police officer in the hypothetical was doing. The difference, as many would see it, is that this sort of baseless, persistent surveillance is not a proper government function.[224] Chief Justice Rehnquist attributed this common reaction to his hypothetical's "extreme" set of facts.[225]

But what may have been considered an extreme—and unworkable—program of persistent surveillance in 1974 is no longer just material for boundary-seeking law school hypotheticals. Rather, breathtaking advances in technology have become so commonplace that they have been blended into our everyday lives and have been allowed to take up residence among some of our most private of activities, while these same technologies make possible the persistent, collective-surveillance programs conducted by the NSA. These warrantless surveillance programs have a toxic effect on fundamental constitutional principles and values that go beyond mere privacy and are therefore prohibited by "the traditional protections against unreasonable searches and seizures afforded by the common law at the time of the framing."[226]

---

219. William H. Rehnquist, *Is an Expanded Right of Privacy Consistent with Fair and Effective Law Enforcement? Or: Privacy, You've Come a Long Way, Baby*, 23 U. KAN. L. REV. 1, 9 (1974).

220. *Id*.

221. *Id.*

222. *Id.*

223. *Id*.

224. *Id*.

225. *Id*.

226. Wilson v. Arkansas, 514 U.S. 927, 931 (1995). In *Wilson*, Justice Thomas explained that although "reasonableness" is a key consideration in the modern Court's Fourth Amendment analysis, the reasonableness of a challenged search or seizure "may be guided by the meaning ascribed to it by the Framers of the Amendment." *Id*.

B. Checks on Arbitrariness of State Power

The Constitution was written to provide citizens with substantive protections against arbitrary and oppressive government actions[227] and, as such, is based squarely upon the principle of limited grants of power to governments.[228] Inherent in these protections is the legitimate constitutional need to control the discretion of government agents in order to prevent arbitrary surveillance without any Fourth Amendment oversight or restraint; however, technological advancements and the near-ubiquity of networked computing and communications have hampered our usual means of oversight.[229]

Following *Katz*, the Supreme Court has approached this problem by considering certain factors in order to determine whether the government's use of a new technology fits into the categories of searches precluded by the Founders.[230] But this approach is a formalistic adherence to *Katz*, at best. What is missing from this analysis is an examination of the constitutional values at stake beyond mere physical privacy.[231] Rather than maintaining focus on government needs or

---

227. One can look to the doctrine of substantive due process for ample evidence of the Court's long recognition of this constitutional principle, which is seen as a "bulwark[] . . . against arbitrary" government action. Hurtado v. California, 110 U.S. 516, 532–36 (1884) (concluding that "arbitrary exertions of power," even those that are "legislative in form," violate due process); *see also* Bank of Columbia v. Okely, 17 U.S. (4 Wheat.) 235, 244 (1819) ("As to the words from Magna Charta, incorporated into the constitution of Maryland, after volumes spoken and written with a view to their exposition, the good sense of mankind has at length settled down to this: that they were intended to secure the individual from the arbitrary exercise of the powers of government, unrestrained by the established principles of private rights and distributive justice.").

228.

> We may rely on the conditions which existed when the Constitution was adopted . . . . [T]hat government by the people instituted by the Constitution would not imitate the conduct of arbitrary monarchs. The abuse of power might, indeed, be apprehended, but not that it would be manifested in provisions or practices which would shock the sensibilities of men.

Weems v. United States, 217 U.S. 349, 375 (1910).

229. This is not a new problem, of course. Congress recognized this issue over two decades ago. *See* ROBERT W. KASTENMEIER, H. COMM. ON THE JUDICIARY, ELECTRONIC COMMUNICATIONS PRIVACY ACT OF 1986, H.R. REP. NO. 99-647 (1986).

> When the Framers of the Constitution acted to guard against the arbitrary use of government power to maintain surveillance over citizens, there were limited methods of intrusion into the "houses, papers and effects" protected by the Fourth Amendment. During the intervening 200 years, development of new methods of communication and devices for surveillance has expanded dramatically the opportunity for such intrusions.

Id. at 16.

230. *See* Christopher Slobogin, *Technologically-Assisted Physical Surveillance: The American Bar Association's Tentative Draft Standards*, 10 HARV. J.L. & TECH. 383, 398−404 (1997) (summarizing factors used in case law).

231. As Professor Amsterdam has observed,

> The ultimate question, plainly, is a value judgment. It is whether, if the particular form of surveillance practiced by the police is permitted to go

bemoaning a loss of government efficiency, courts should reorient their point of view to reestablish the Fourth Amendment as a citizens' tool to regulate government power.[232] The focus, therefore, should be shifted away from the reasonable expectation of privacy balancing test, since "[i]n many instances, what is or isn't protected by the Fourth Amendment bears no relation to the problems caused by government information gathering." Instead, consideration should be paid to "whether it is best to have judicial oversight of law-enforcement activity, what that oversight should consist of, how much limitation we want to impose on various government activities, and how we should guard against abuses of power."[233]

Professor Kerr's equilibrium adjustment theory[234] and Professor Ohm's improvements upon that theory[235] seek to provide practical advice to judges on a shift in Fourth Amendment doctrine from privacy to power. Ohm argues that the relationship between private and public surveillance, where commercial technologies such as cell phones and social networks are gradually becoming omniscient, is turning the current privacy-oriented doctrine from a "slow and partial degradation of the Fourth Amendment" into a "full evisceration."[236] Both approaches suggest that courts reorient their Fourth Amendment balancing test to one that (somehow) measures the balance of power between government and citizen. To apply this measurement, Ohm suggests a metric that strives to maintain a "fixed ratio between [government] efficiency and individual liberty," which courts adjust as our technology continues to improve, thus enforcing a constant—and relatively increasing—level of government inefficiency.[237]

Regardless of the approach, any move from privacy to power as a core fixture of Fourth Amendment doctrine will not come without some amount of disruption. This new paradigm would shift the costs back to the government, and the perspective back to the individual, and would force the reevaluation of post-*Katz* jurisprudence. If the constitutional norm that seeks to protect citizens from government power through unwarranted intrusions once again becomes the focus of the Court's Fourth Amendment doctrine, our freedom from arbitrary governmental action will receive the proper attention from the "federal institutional processes established to protect that freedom."[238]

> unregulated by constitutional restraints, the amount of privacy and freedom remaining to citizens would be diminished to a compass inconsistent with the aims of a free and open society.

Amsterdam, *supra* note 136, at 403.

232. As noted by Justice Brandeis, our constitutional system of checks and balances "was adopted by the [Framers], not to promote efficiency but to preclude the exercise of arbitrary power. The purpose was, not to avoid friction, but, by means of the inevitable friction incident to the distribution of the governmental powers . . . to save the people from autocracy." Myers v. United States, 272 U.S. 52, 293 (1926) (Brandeis, J., dissenting).

233. SOLOVE, *supra* note 15, at 115.

234. *See* Kerr, *supra* note 139.

235. Paul Ohm, *The Fourth Amendment in a World Without Privacy*, 81 MISS. L.J. 1309 (2012).

236. *Id.* at 1311.

237. *Id.* at 1346.

238. Note, *The Void-for-Vagueness Doctrine in the Supreme Court*, 109 U. PA. L. REV. 67, 88 (1960).

IV. COLLECTIVE SUSPICION'S CORROSIVE EFFECT ON MUTUAL SOCIETAL TRUST

A. The Importance of Social Trust in a Constitutional Democracy

The Founders' conception of the Constitution was of a "constitution of principle," securing basic liberties and protecting core values, as opposed to a mere "constitution of detail," which simply enumerates a discrete list of rights.[239] Further, scholars such as the philosopher John Rawls have interpreted the Constitution as an agreement specifying certain liberties in terms of our capacity for a sense of justice and our capacity for a conception of the overall good.[240] Thus, our Constitution is meant to embody the values we see as necessary for social cooperation and governance, which must be based on mutual respect and trust.[241]

Societies without trust tend toward the Hobbesian end of the spectrum and lack the sort of peaceful, stable, and productive communities the Framers intended.[242]

---

239. RONALD DWORKIN, LIFE'S DOMINION: AN ARGUMENT ABOUT ABORTION, EUTHANASIA, AND INDIVIDUAL FREEDOM 119 (1993) (emphasis omitted) (coining and contrasting a "constitution of principle"—a coherent set of abstract, normative principles and values—with a "constitution of detail"—a particularized list of rules); *see also* Lawrence v. Texas, 539 U.S. 558, 578–79 (2003) ("Had those who drew and ratified the Due Process Clauses of the Fifth Amendment or the Fourteenth Amendment known the components of liberty in its manifold possibilities, they might have been more specific. They did not presume to have this insight. They knew times can blind us to certain truths and later generations can see that laws once thought necessary and proper in fact serve only to oppress. As the Constitution endures, persons in every generation can invoke its principles in their own search for greater freedom.").

240. *See* JOHN RAWLS, POLITICAL LIBERALISM 36–37 (1996). Rawls's theory of justice as fairness translates to a constitutional conception of a fair system of social cooperation. Rawls asserts that citizens of a constitutional democracy apply their capacity for a sense of justice when evaluating the justice of social institutions and policies. Similarly, Rawls states that this sense is coupled with our pursuit of a conception of the good, or what is valuable in human life. *See id.* at 15–20, 29–35, 302, 332.

241. The absence of mutual trust can poison even the simplest of social or commercial interactions. *See, e.g.*, Kenneth J. Arrow, *Gifts and Exchanges*, *in* ALTRUISM, MORALITY, AND ECONOMIC THEORY 13, 15 (Edmund S. Phelps ed., 1975) (citing the foundational importance of trust in commercial transactions); Partha Dasgupta, *Trust as a Commodity*, *in* TRUST: MAKING AND BREAKING COOPERATIVE RELATIONS 49, 64 (Diego Gambetta ed., 1988) (defining trust as a public good); Carol M. Rose, *Giving, Trading, Thieving, and Trusting: How and Why Gifts Become Exchanges, and (More Importantly) Vice Versa*, 44 FLA. L. REV. 295, 311–313 (1992) (examining how trust is essential to social exchange).

242. Political theorists strenuously emphasized the importance of societal trust at the time of the Framing. *See, e.g.*, JOHN LOCKE, THE SECOND TREATISE OF GOVERNMENT 124 (Thomas P. Peardon ed., The Liberal Arts Press, Inc. 1952) (1690) ("Whensoever, therefore, the legislative shall transgress this fundamental rule of society, and either by ambition, fear, folly, or corruption, endeavor to grasp themselves, or put into the hands of any other, an absolute power over the lives, liberties, and estates of the people; by this breach of trust they forfeit the power the people had put into their hands for quite contrary ends, and it devolves to the people, who have a right to resume their original liberty, and, by the establishment of a new legislative, such as they shall think fit, provide for their own safety and security, which is the end for which they are in society."); *see also* 1 JOHN STUART MILL, PRINCIPLES OF POLITICAL ECONOMY ch.

Societal trust, in this sense, can be defined as "the actor's belief that, at worst, others will not knowingly or willingly do him harm, and at best, that they will act in his interests."[243] The essence of this theme has been distilled into the description "encapsulated interest."[244] Just as people can build reputations of trustworthiness, so can governments. And just as personal betrayals can destroy individual relationships, a society's health is "dependent . . . on the justice of their community's political decisions."[245] History provides ample empirical evidence of the widespread problems that arise in societies with low levels of trust.[246]

B. The Costs Associated with a Collapse of Trust: Trust as a Constitutional Value

The once-revolutionary concept of mutual trust between government and citizen is firmly embedded as a fundamental value underlying this nation's society. Justice Brandeis articulated the basis of the Fourth Amendment as that of the "right to be let alone—the most comprehensive of rights and the right most valued by civilized men."[247] This core principle has been a basis of our constitutional system of government since its inception.[248] Since our government is granted legitimacy only

---

vii, § 5, at 110 (J.M. Robson ed., Univ. of Toronto Press 1965) (1848) ("Conjoint action is possible just in proportion as human beings can rely on each other. There are countries in Europe, of first-rate industrial capabilities, where the most serious impediment to conducting business concerns on a large scale, is the rarity of persons who are supposed fit to be trusted with the receipt and expenditure of large sums of money."); GEORG SIMMEL, THE SOCIOLOGY OF GEORG SIMMEL 318 (Kurt H. Wolff ed. & trans., The Free Press 1950) (trust "is one of the most important synthetic forces within society").

243. Kenneth Newton, *Trust, Social Capital, Civil Society, and Democracy*, 22 INT'L POL. SCI. REV. 201, 202 (2001). The concept of trust can be somewhat slippery to define, and largely depends on context. David Good has offered a functional definition of trust, where "trust is based on an individual's theory as to how another person will perform on some future occasion." David Good, *Individuals, Interpersonal Relations, and Trust*, *in* TRUST: MAKING AND BREAKING COOPERATIVE RELATIONS, *supra* note 241, at 31, 33 (footnote omitted). Another helpful description belies our need to rely on one another in society: "trust is a device for coping with the freedom of other persons." John Dunn, *Trust and Political Agency*, *in* TRUST: MAKING AND BREAKING COOPERATIVE RELATIONS, *supra* note 241, at 73, 80.

244. RUSSELL HARDIN, TRUST AND TRUSTWORTHINESS 25–27 (2002).

245. Ronald Dworkin, *Liberal Community*, 77 CALIF. L. REV. 479, 502 (1989).

246. Levels of trust shown in social surveys are good indicators of the overall trustworthiness of the societies in which the survey respondents live, telling us more about the societies and their structures than about the individual personality types. *See* ROBERT D. PUTNAM, BOWLING ALONE: THE COLLAPSE AND REVIVAL OF AMERICAN COMMUNITY 138 (2000). Further studies have shown that wealthier nations, and those with greater income equality, have higher levels of trust than poorer and more unequal ones. *See* Ronald Inglehart, *Trust, Well-Being and Democracy*, *in* DEMOCRACY AND TRUST 88 (Mark E. Warren ed., 1999). As one scholar puts it, "Social life without trust would be intolerable and, most likely, quite impossible." Newton, *supra* note 243, at 202.

247. Olmstead v. United States, 277 U.S. 438, 478 (1928) (Brandeis, J., dissenting), *overruled in part by* Katz v. United States, 389 U.S. 347 (1967).

248. As Justice Brandeis so eloquently put it:

> The makers of our Constitution undertook to secure conditions favorable to the pursuit of happiness. They recognized the significance of man's spiritual nature, of his feelings and of his intellect. They knew that only a part of the

through the trust citizens confer via regular elections, this principle is interwoven into the very nature of our institutions.

The Fourth Amendment is a direct result of the Founders' constitutional value of reciprocal trust. Specifically, this amendment requires that government trust its citizens to act responsibly, a principle that is violated when government is allowed to step into citizens' lives without first finding that a citizen has given up that trust by failing to act responsibly.[249] This governing constitutional principle is made even plainer in comparison to totalitarian governments, which maintain power and exercise control by sending a strong message to their citizens that the State is superior to the individual, doing so through monitored communications, random searches, and the use of citizen-informants.[250] Where totalitarian governments tend to maintain stability only through force and control, the long-term stability of our constitutional form of government is due in large part to the value of reciprocal trust between the State and its citizens, which grants those citizens the right and ability to participate in this society in a meaningful way.[251]

While it is unlikely that government's use of collective surveillance will produce the sort of widespread unrest and violence that has resulted from racial alienation

---

> pain, pleasure and satisfactions of life are to be found in material things. They sought to protect Americans in their beliefs, their thoughts, their emotions and their sensations. They conferred, as against the Government, the right to be let alone—the most comprehensive of rights and the right most valued by civilized men.

Id.

249. This trust by government of its citizens was a crucial innovation in liberal democracy:

> Liberal, pluralist democracy is primarily procedural. Its consensus about procedure . . . is the foundation for mutual trust at least in the political arena. Although this consensus does not have to be universal, it does have to be widespread.
>
> . . . .
>
> . . . [M]utal trust, . . . politically defined, is the confidence in or reliance on others who are also committed to a way of conducting and resolving disputes about values; it is the expectation that they will generally comply with the outcomes even when they do not endorse them.

JAMES F. CHILDRESS, CIVIL DISOBEDIENCE AND TRUST 7 (1975) (emphases omitted).

250. Maria Los provides excellent examples and analysis of manifestations in former Communist nations and how these legacies affect their current governments in the digital age. Maria Los, *A Trans-Systemic Surveillance: The Legacy of Communist Surveillance in the Digital Age*, *in* SURVEILLANCE AND DEMOCRACY 173 (Kevin D. Haggerty & Minas Samatas eds., 2010) (describing the surveillance methods left behind in formerly Communist states and applied to new technologies since 9/11, along with their corrosive effects on those societies).

251. For examples of what can happen when this reciprocal trust breaks down and individuals feel powerless to meaningfully affect the system, we can look to the rioting and unrest that has taken place when the government has shown contempt for certain subgroups of the population through biased legislation or unjust law enforcement. *See, e.g.*, DENNIS E. GALE, UNDERSTANDING URBAN UNREST: FROM REVEREND KING TO RODNEY KING (1996) (examining government response to unrest and violence over alienation and lack of participation); Sheldon G. Levy, *Dimensions of Attitudes Toward Race Relations and Polarized Subgroups in Detroit Following the 1967 Riot*, 6 PROC. ANN. CONVENTION AM. PSYCHOL. ASS'N. 307 (1971) (analyzing alienation and race relations as causes of rioting).

and societal powerlessness, milder results such as increased individual cynicism leading to decreased participation or outright mistrust of government agencies and agents can be just as destructive to our democratic society, with the possible devolution of our government into the sort of aristocratic enterprise the Founders wanted to avoid.[252] Further, it is not clear that that these corrosive government practices have any real benefit that might provide some argument in support of their use.[253] The continued misrepresentation of these programs only serves to enhance the levels of mistrust citizens have for their government.[254] A widespread failure of trust of government by its citizens can only serve to harm the complex balance our society has put in place.

CONCLUSION

The Framers of the Constitution were quite clear in their intent to protect citizens from unwarranted intrusions by their government, and this principle was embedded into our constitutional form of government through the language of the Fourth Amendment. While it is expected that government should provide for our common defense, a democratic society such as ours cannot long tolerate secret government surveillance programs that collect, store, and analyze our private communications and papers, with no individualized suspicion of wrongdoing and no basis in law. The needs of national security should not blind us to the legal and societal costs of collective surveillance, nor should we be willing to sacrifice our constitutional values in a quixotic pursuit of perfect security.

This is not a question of whether government needs to conduct directed surveillance in its defense capacity—of course it does. But it should do so without violating the reciprocal trust of citizens and without stepping over the constitutional protections from unwarranted governmental intrusions.[255] Justice Robert Jackson

---

252. *See* Akhil Reed Amar*, The Bill of Rights as a Constitution*, 100 YALE L.J. 1131, 1140 (1991).

253. In a hearing held before the Senate Judiciary Committee, NSA Director Keith Alexander admitted that only thirteen of the fifty-four instances the NSA cited as terrorism plots foiled through collective surveillance had any connection to the United States. Further, Director of National Intelligence James Clapper claimed that, even though there were few examples of any real benefits to the NSA's persistent, collective-surveillance programs, the real measure that should be applied to judge the success of these programs is the "peace of mind metric." Yochai Benkler, *Fact: The NSA Gets Negligible Intel from Americans' Metadata. So End Collection*, GUARDIAN (Oct. 8, 2013, 12:02 PM), http://www.theguardian.com /commentisfree/2013/oct/08/nsa-bulk-metadata-surveillance-intelligence.

254. *See* CHILDRESS, *supra* note 249, at 7 ("[M]utual trust . . . politically defined, is the confidence in or reliance on others who are also committed to a way of conducting and resolving disputes about values; it is the expectation that they will generally comply with the outcomes even when they do not endorse them.").

255. It is worth noting that there has been a cooling of support within some corners of government for the broad surveillance programs initiated in the weeks and months following the attacks of September 11, 2001. *See, e.g.*, Siobhan Gorman, *Leahy Bill Seen as Best Chance for a Revamp to Surveillance*, WALL ST. J., July 30, 2014, at A5. This shift in thinking appears to be part of an overall reexamination of post-9/11 government policies. It is too soon to tell, however, exactly what effect these efforts might have on Fourth

warned that this tension between security and liberty should not lead us to a constitutional "suicide pact" by ignoring common sense and seeking purity of doctrine.[256] But at what point does an imminent danger overwhelm our constitutional right to liberty? This nation and its Constitution have survived even greater existential threats than those we face today. It is not as clear that our society would be able to survive the corrosive effects of collective surveillance. The atrophy of civil liberties would be a "suicide pact" of a different kind, where the loss of our constitutional principles of protection from undue government power and of mutual trust between government and citizen makes our current models of society and government unsustainable.[257]

Contrary to what some within the intelligence community might believe or wish to be true, our society has never operated under the supposition that government agents are entitled to every fact about every individual.[258] Technological advancements have eliminated some of the natural physical boundaries that prevented collective, persistent surveillance programs such as the suspicionless decryption program revealed in the Snowden documents—our system of laws must adjust to fill these gaps. As these physical hurdles continue to fall, default Fourth Amendment doctrine should likewise continue to deny government intrusions without individualized, articulable suspicion. To do otherwise is to relinquish our

---

Amendment doctrine, especially when it comes to questions—real or perceived—of national security.

256.

> This Court has gone far toward accepting the doctrine that civil liberty means . . . that all local attempts to maintain order are impairments of the liberty of the citizen. The choice is not between order and liberty. It is between liberty with order and anarchy without either. There is a danger that, if the Court does not temper its doctrinaire logic with a little practical wisdom, it will convert the constitutional Bill of Rights into a suicide pact.

Terminiello v. Chicago, 337 U.S. 1, 37 (1949) (Jackson, J., dissenting).

257. It is notable that Justice Jackson, despite his warnings of a Fourth Amendment "suicide pact," also made clear his awareness of the dangers inherent in failing to protect citizens' civil liberties:

> [Rights under the Fourth Amendment], I protest, are not mere second-class rights but belong in the catalog of indispensable freedoms. Among deprivations of rights, none is so effective in cowing a population, crushing the spirit of the individual and putting terror in every heart. Uncontrolled search and seizure is one of the first and most effective weapons in the arsenal of every arbitrary government. And one need only briefly to have dwelt and worked among a people possessed of many admirable qualities but deprived of these rights to know that the human personality deteriorates and dignity and self-reliance disappear where homes, persons and possessions are subject at any hour to unheralded search and seizure by the police.

Brinegar v. United States, 338 U.S. 160, 180–81 (1949) (Jackson, J., dissenting).

258. Documents leaked by Mr. Snowden have revealed government agencies and programs "intent on maintaining [their] dominance in intelligence collection," with plans to "expand [their] surveillance powers," without any apparent internal boundaries. James Risen & Laura Poitras, *N.S.A. Report Outlined Goals for More Power*, N.Y. TIMES, Nov. 23, 2013, at A1; *see also* Scott Shane, *No Morsel Too Minuscule for All-Consuming N.S.A.*, N.Y. TIMES, Nov. 3, 2013, at A1.

constitutional checks on government power and destroy the mutual trust necessary for our society to function.

Rethinking Fourth Amendment doctrine is not, of course, an easy or straightforward task. My suggested course at this point, however, is a return to the Brandeisian examination of the "privacies of life," which suffer when warrantless, unparticularized government surveillance becomes "the invasion of his indefeasible right of personal security, personal liberty and private property."[259] Work must be done to recenter Fourth Amendment thought around fundamental constitutional values and avoid the fact-specific hair-splitting that the reasonable expectation of privacy test has yielded.

259. Olmstead v. United States, 277 U.S. 438, 474–75 (1928) (Brandeis, J., dissenting), *overruled in part by* Katz v. United States, 389 U.S. 347 (1967).