Texas A&M Law Review

Volume 2 | Issue 4 Article 4

2015

Security, Privacy, and Technology Development: The Impact on National Security

Abraham R. Wagner

Paul Finkelman

ARTICLES

SECURITY, PRIVACY, AND TECHNOLOGY DEVELOPMENT: THE IMPACT ON NATIONAL SECURITY+

By: Abraham R. Wagner & Paul Finkelman***

TABLE OF CONTENTS

+ Paper prepared for presentation at the Symposium *New Technology and Old Law: Rethinking National Security*, Texas A&M University School of Law, October 17, 2014. An earlier version of portions of this piece was presented previously in a White House Report tendered in response to a Request for Input. *See* Abraham R. Wagner, *Cybersecurity and Privacy: The Challenge of Big Data*, *in* WHITE HOUSE: BIG DATA REQUEST FOR INPUT art. 11, 1–12 (2014).

* Columbia Law School; Visiting Professor New York University.

** Ariel F. Sallows Visiting Professor of Human Rights Law, University of Saskatchewan College of Law and Senior Fellow, Program on Democracy, Citizenship, and Constitutionalism, University of Pennsylvania.

I. INTRODUCTION

The evolution of modern communications and information technology sparked a revolution of unprecedented proportions, bringing about an explosion in terms of users and capabilities, as well as increasing demands for both security and privacy. To meet these security demands, new technologies are evolving that can in fact provide a secure and protected environment. At the same time, however, the technology-development path is being increasingly impacted by two other major dynamics: the legal environment and user expectations with respect to privacy. Within the past four years in particular, several major court decisions as well as the official release of documents and illicit "leaks" have drawn enormous attention to what privacy protections must be afforded to various types of data and communications. Users, increasingly aware of intrusions into their data and communications—ranging from intelligence services to hackers and criminals—are demanding greater levels of protection. While technological approaches to greater privacy are possible, they are not cost-free—particularly in terms of the computational overhead and other constraints imposed on new systems.

The understanding of how the current concept of privacy fits into the notion of a free and democratic society in the United States has been an evolutionary process that is still ongoing. The rights that define the United States as a "free" society are a fairly well-defined package beginning with the Bill of Rights, the first ten Amendments to the Constitution, in which privacy is largely covered by the Fourth Amendment's[1] protection against warrantless or unreasonable searches and seizures.[2] This right is not absolute and has been interpreted and modified by statute as well as various court decisions over time that recognize changing individual and societal expectations, new technologies, and the needs of society for public goods such as law enforcement and national security. The net result has been a dynamic tension between evolving concepts of what people expect in terms of privacy as well as the compelling needs of society to provide law enforcement and national security.

Recent history has seen both the rapid evolution of cyberspace, accompanied by an enormous expansion in terms of users and capabilities, as well as unprecedented technological, economic, and social

1. U.S. CONST. amend. IV ("The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.").

2. There are also privacy implications in the right of association found in the First Amendment, the Fifth Amendment, and the Ninth Amendment. *See* U.S. CONST. amends. I, IX; *see also* Griswold v. Connecticut, 381 U.S. 479 (1965) (finding a right of privacy in the penumbras of the Bill of Rights).

revolutions. These new technologies have also led to a virtual explosion in the amounts of data resident on servers and in systems across the globe—often referred to as Big Data. Along with a host of benefits, the era of Big Data has also brought with it a new set of challenges in terms of security and privacy that increasingly affect the lives of Americans.[3]

Cyberspace has created a new venue for crime, warfare, and espionage, as well as for private acts of aggressive commercial marketing, violating personal privacy, insulting neighbors and strangers, and embarrassing celebrities, pubic officials, governments, and unlucky private individuals. At the same time, the availability of Big Data has also provided an opportunity for the commercial sector to analyze and utilize the data for non-criminal purposes that may still pose serious security and privacy questions. Increasingly, the links between those that store Big Data, commercial users, and the government have come under great public scrutiny while the courts are dealing with new cases where constitutional issues of privacy are at issue.[4]

Overall, this paradigm shift is not simply one of technology. It embraces radical changes in the economics of information as well as the culture of modern society. This is one of the most significant changes in media since the invention of moveable type in the 15th Century and ranks with other sea changes in communications, such as the inventions of the telegraph, the telephone, movies, radio, and television. While Americans have been quick to embrace the new cyber technologies and the capabilities they offer—just as they embraced the telephone and radio in an earlier era—public policy and the legal regime have not changed nor developed alongside the new technology and are in need of serious updating and modernization.[5] Here, the existing laws are decades behind the current technologies and the problems that Big Data poses.[6]

---

3. *See* Abraham Wagner, *Cybersecurity; From Experiment to Infrastructure*, DEF. DOSSIER, Aug. 2012, at 16, 16–18, *available at* http://www.afpc.org/files/august 2012.pdf; Abraham R. Wagner, AM. FOREIGN POLICY COUNCIL, *Cybersecurity: New Threats and Challenges*, 1 DEF. TECH. PROGRAM BRIEF (Sept. 2013), *available at* http://www.afpc.org/files/getContentPostAttachment/224.

4. *See, e.g.*, *In re* Search of Info. Associated with [Redacted]@mac.com that is Stored at Premises Controlled by Apple, Inc., 13 F. Supp. 3d 145, 149–50 (D.D.C. 2014); *see also* Orin Kerr, *Searches and Seizures in a Digital World*, 119 HARV. L. REV. 531, 532–33 (2005).

5. Policy studies undertaken since the late 1990s have identified serious problems in the infrastructure, but the response by both the government and the commercial sector has proved to be grossly inadequate. *See* Presidential Decision Directive on Critical Infrastructure Protection, PDD/NSC-63 (May 22, 1998); Presidential Directive on Critical Infrastructure Security and Resilience PPD-21, 2013 DAILY COMP. PRES. DOC. 92 (Feb. 12, 2013). It is striking that these two Presidential directives, coming well over a decade apart, come to the same conclusions with almost nothing having been done in between.

6. As discussed at greater length below, one good example is the Electronic Communications and Privacy Act (ECPA) enacted in 1986 and codified at 18 U.S.C.

It is also the case that Americans themselves see Big Data as well as the security and privacy concerns raised differently than in years past. Greater use of the technologies and increased awareness of potential problems have changed privacy expectations significantly. For their part, both state and federal courts have responded to a myriad of cases with a far more encompassing view of the privacy protections afforded under the Fourth Amendment.[7] Today's challenge is therefore multifaceted. As both the government and the private sector continue to collect, analyze, and utilize data, norms, policies, and statutes are needed to address the privacy and security needs of Americans while promoting the free flow of information and the huge economic value from the technology in ways that are consistent with these needs.

This Article considers how the important dynamics of the evolving legal environment and user expectations with respect to privacy and security potentially impact the development of new security technologies and legal arrangements to support them. Further, the Article explores new security technologies and how related environmental concerns will impact national security missions and operations.

II. Privacy in a Free Society: Constitutional Origins

The Founding Fathers spent a great deal of time working on the nature of the free society but included very few specific rights in the Constitution. The Constitution created a stronger national government to replace the weak system under the Articles of Confederation but did not set out what "rights" the people had. Citizens were unhappy with the state of affairs as a British colony as well as under the Article of Confederation, which was adopted during the Revolution and remained in force following independence,[8] but they differed on how strong the new government should be. Opponents of the Constitution complained that the new document lacked a bill of rights, but

§§ 2510–2522. *See* discussion *infra* Part X concerning Electronic Communications and Privacy Act ("ECPA") and the Stored Communications Act. The ECPA also added new provisions prohibiting access to stored electronic communications, i.e., the Stored Communications Act, 18 U.S.C. §§ 2701-12.

7. *See* Abraham Wagner, *Cybersecurity and Privacy: The Challenge of Big Data*, Ctr. for Advanced Studies on Terrorism (CAST) (Apr. 2014), http://media.wix.com/ugd/9e0486_fa3763e7579a456f8da03b707cbadead.pdf; *see also* Michael Warner, *Privacy and Security, Yesterday and Today*, *in* Cybersecurity and Privacy: Report of the Expert Workshop Held for the Defense Advanced Research Projects Agency (DARPA) (Inst. for Def. Analyses 2014).

8. The concept of a constitutional democracy was new and unique, and it was very much a work in progress. Unfortunately, the minutes of the Constitutional Convention are very spotty, and all that exists are formal records and votes on proposals and private notes from some of the delegates, most importantly James Madison. We do have rather voluminous debates over the ratification of the Constitution and the debates in 1787–1788 over whether to have a bill of rights. We have less helpful debates over the actual adoption of the Bill of Rights.

supporters of the Constitution—the Federalists—dismissed these as meaningless fears of small-minded men.[9] The Constitution itself does not contain any serious definition of a free society. After the ratification of the Constitution, Congress proposed twelve amendments, ten of which were ratified at the time and became the Bill of Rights.[10]

Most of the leading Federalists opposed a written bill of rights as being unnecessary, useless, or even dangerous.[11] While campaigning for ratification and rejecting the idea that a bill of rights or a protection of freedom of the press was necessary, James Madison, Alexander Hamilton, and John Jay launched a media campaign in New York newspapers, publishing a huge series of essays in support of the Constitution that were later collected as *The Federalist Papers*. Throughout the Federalist essays the authors denied the need for a Bill of Rights.[12] However, after the ratification of the Constitution, James Madison, while running for a seat in the new Congress, agreed to introduce a bill of rights in order to appease some of his constituents who feared the federal government would undermine their religious liberty.[13] But, even when he introduced the Amendments in Congress, Madison showed little enthusiasm for changing the Constitution. He did not argue with passion or even much conviction for his proposal, admitting that he had "never considered this provision so essential to the federal constitution" that the lack of a bill of rights should have been allowed to impede ratification.[14] But, with the Constitution ratified, Madison was willing to concede "that in a certain form and to a certain extent, such a provision was neither improper nor altogether useless."[15]

Despite Madison's reservations about the need for a bill of rights, he nevertheless worked hard to create a series of protections for personal liberties. While he did not include a specific right to privacy, Madison's amendments went to the heart of the natural rights of liberty and the right to be protected from an overly intrusive government. Over the years, Courts have correctly found in these Amendments a comprehensive right to privacy and to protection from unwarranted—and warrantless[16]—government observation and snooping. Madison's amendments, as understood today, created a

9. Cecilia Kenyon, *Men of Little Faith: The Anti-Federalists on the Nature of Representative Government*, 12 WILLIAM & MARY Q. 3, 18–19, 43 (1955).

10. The first two proposed amendments were not ratified at the time, but the original second amendment, which prevented members of Congress from raising their own salary during the term they were elected, was finally ratified in 1992 as the Twenty-Seventh Amendment.

11. Paul Finkelman, *James Madison and the Bill of Rights: A Reluctant Paternity*, 1990 SUP. CT. REV. 301, 309.

12. *See id.*

13. *Id.* at 344.

14. *Id.* at 341 (citing 1 ANNALS OF CONG. 453 (1789) (1834)).

15. *Id.* (citing 1 ANNALS OF CONG. 453 (1789) (1834)).

16. U.S. CONST. amend. IV.

fundamental right to privacy. As the Supreme Court long ago observed in *Griswold v. Connecticut*,[17] the right to privacy is embedded in many of the amendments and easily emanates from their penumbras. Thus, "the First Amendment has a penumbra where privacy is protected from governmental intrusion."[18] The Court similarly found protections of privacy in the Third, Fourth, Fifth, and Ninth Amendments.[19] Justice William O. Douglas noted that "[t]he Fifth Amendment in its Self-Incrimination Clause enables the citizen to create a zone of privacy which government may not force him to surrender to his detriment."[20] The Court in *Griswold* found a "zone of privacy created by several fundamental constitutional guarantees."[21]

Thus, included in the original "package" of rights are many provisions that protect privacy. Freedom of religious practice, speech, press, and association—all embedded in the First Amendment—are all both public and private rights. The right to publish one's thoughts is a public right. But the right to have a diary or send thoughts, ideas, or letters (or in the modern age e-mails or text messages) to only one person or a select group, is a private right. Religious observance is protected in the privacy of one's home, as well as in the cathedral, church, synagogue, temple, mosque, ashram, or in the streets.[22] The right to speak in public is a right of free speech, but so too would be a telephone conversation or a Skype conversation.[23] We may associate with like-minded individuals in a public meeting or demonstration, but we may also secretly meet with our political cohorts and not divulge to the government who was at the meeting.[24]

In addition to First Amendment free speech rights and the rights of privacy and personal autonomy, there are largely Fourth Amendment rights, which prevent unreasonable searches and require warrants and probable cause for such searches. The Fourth Amendment was immediately connected to the patriot opposition to the British writs of assistance before the American Revolution. Freedom from unreasonable searches came as a reaction to the invasion of homes by British redcoats and tax collectors. In the new nation, such searches were to be barred, except under a warrant issued after the presentation of probable cause to a judge or magistrate. Individual privacy could be vio-

17. Griswold v. Connecticut, 381 U.S. 479, 485 (1965).
18. *Id.* at 483.
19. *Id.* at 484.
20. *Id.*
21. *Id.* at 485.
22. Cantwell v. Connecticut, 310 U.S. 296, 303–04 (1940).
23. *See* Olmsted v. United States, 277 U.S. 438, 475–76 (1928) (Brandeis, J., dissenting); Katz v. United States, 389 U.S. 347, 353 (1967). The right to speak either in public or in private, on a telephone, Skype or any other device are of course covered by the First Amendment. Issues raised with respect to private communications, such as those raised in *Olmstead* and later in *Katz*, are largely Fourth Amendment privacy issues.
24. *See* N.A.A.C.P. v. Alabama *ex rel.* Patterson, 357 U.S. 449, 462–63 (1958).

lated for a public good (e.g., law enforcement), but a judge had to decide this was the case upon sufficient evidence of probable cause.

In terms of applying the concept to communications, the Constitution preceded the development of any electronic communications by half a century, so certainly it was not an issue at the time.[25] Interestingly, however, mail service had existed for centuries, and there is no mention in the Constitution of this medium in the context of privacy,[26] other than the oblique reference to the idea that the concept of privacy attaches to personal "papers," presumably within the home, and no reference to letters that might be in transit outside.[27] Compared to free speech and other freedom and rights issues, there were few concerns—and virtually no cases—over privacy in the press or the courts for about a century after ratification of the Constitution.

III. LOUIS BRANDEIS IN THE *OLMSTEAD* AND *KATZ* CASES

In 1890, Louis D. Brandies and his law partner Samuel Warren published "The Right to Privacy" in the *Harvard Law Review*.[28] This innovative and path-breaking exploration of the right to be let alone by the press—and presumably by the government—is one of the most celebrated articles in American legal history. The article largely reflected Warren's concerns about an integrated theory or concept of privacy that went well beyond the concerns of the framers in protecting the sanctity of the home embodied in the Fourth Amendment.[29]

25. Samuel F. B. Morse, who perfected the telegraph, sent his first message from the U.S. Capitol building to his associate in Baltimore on May 24, 1844. Bernard S. Finn, *Morse, Samuel Finley Breese*, AM. NAT'L BIOGRAPHY ONLINE (2000), http://www.anb.org/articles/13/13-01183.html?a=1&n=Morse%2C%20Samuel&d=10&ss=0&q=1.

26. The Constitution does empower the national government to create a postal system and build roads to support that system. U.S. CONST., art I § 8, cl. 7.

27. During the Cold War, the CIA engaged in a mail-opening program within the U.S. at various post offices, which became subject to a scandal later on, reported in the *Family Jewels* study, but most of the objections related to CIA operations within the U.S., barred by statute, rather than to privacy issues. Some later cases make reference to mail and its "oblique packaging" where the user has an expectation the contents will not be seen. None of the cases appear to cover post cards with writing on the outside.

28. Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890) [hereinafter Warren & Brandeis, *The Right to Privacy*]. For a nice edition of this article with an introduction, see SAMUEL D. WARREN & LOUIS D. BRANDEIS, THE RIGHT TO PRIVACY (Alan Childress eds., Quid Pro Books ed. 2010) (1890).

29. *See id.* Written primarily by Brandeis, it was the first publication in the United States to advocate a right to privacy, articulating that right primarily as a "right to be let alone." *See* Dorothy J. Glancy, *The Invention of the Right to Privacy*, 21 ARIZ. L. REV. 1, 1–5 (1979). It began at the suggestion of Warren, based on his "deep-seated abhorrence of the invasions of social privacy," *id.* at 6 (citing Letter from Brandeis to Warren (Apr. 8, 1905), and introduces the fundamental principle that "the individual shall have full protection in person and in property." *See* Warren & Brandeis, *The Right to Privacy*, *supra* note 28, at 193. They acknowledge that this is a fluid principle that has been reconfigured over the centuries as a result of political, social, and eco-

The article focused on the right of individuals to hold a property interest in unpublished materials, in their own image, and, in effect, material about their private lives.

The authors noted the alarming fact that "[i]nstantaneous photographs and newspaper enterprise have invaded the sacred precincts of private and domestic life; and numerous mechanical devices threaten to make good the prediction that 'what is whispered in the closet shall be proclaimed from the house-tops.'"[30] They argued that "[f]or years there has been a feeling that the law must afford some remedy for the unauthorized circulation of portraits of private persons"[31] and that something had to be done to remedy "the evil of the invasion of privacy by the newspapers,"[32] which had been "long keenly felt."[33] They also argued that this right was essentially rooted in property, since there was no constitutional claim they could make. At the same time, they argued for a new tort—the invasion of privacy.

The article was instantly important. One contemporary scholar called it "one of the most brilliant excursions in the field of theoretical jurisprudence which the recent literature of the law discloses."[34] Roscoe Pound argued that it did "nothing less than add a chapter to our law."[35] It "remained the most cited article in American legal scholarship until 1947"[36] and led to a whole field of litigation based on invasion of privacy.[37]

While the Warren and Brandeis article created a new field for private individuals, it also helped Americans think about government intrusion in a new way. This was necessary because the early 20th century saw significant technological advances and rapid growth in telecommunications. Both law enforcement agencies and intelligence services found that intercept operations could yield useful data and that a greater public good was achieved in doing so. However, for years they encountered little opposition to such activities.[38]

---

nomic change. *See* Glancy, *supra*, at 7–8. The essay begins by describing the development of the law with regard to life and property. *See* Warren & Brandeis, *The Right to Privacy*, *supra* note 28, at 193. Originally, the common law "right to life" only provided a remedy for physical interference with life and property. *Id.* Later, the scope of the "right to life" expanded to recognize the "legal value of sensations," and the concept of property expanded from protecting only tangible property to intangible property. *Id.*

30. Warren & Brandeis, *The Right to Privacy*, *supra* note 28, at 195.

31. *Id.*

32. *Id.*

33. *Id.*

34. MELVIN I. UROFSKY, LOUIS D. BRANDEIS: A LIFE 101 (2009) (quoting Elbridge L. Adams, *The Right of Privacy and Its Relation to the Law of Libel*, 39 AM. L. REV. 37, 37 (1905)).

35. *Id.* (quoting Roscoe Pound, Dean of the Harvard Law School).

36. *Id.*

37. *Id.*

38. *See, e.g.*, JEFFREY T. RICHELSON, A CENTURY OF SPIES: INTELLIGENCE IN THE TWENTIETH CENTURY (1997).

The question of whether communications interception without a warrant violated the Fourth Amendment privacy guarantee did not even reach the Supreme Court until the *Olmstead* case in 1928.[39] Chief Justice Taft's majority opinion held that the privacy guarantee in the Fourth Amendment applied to the "place" and did not cover electronic communications traveling outside the home.[40] A dissenting opinion in *Olmstead* by Louis Brandeis, now a Supreme Court justice, argued otherwise. Updating his 1890 argument, Brandeis asserted that the Fourth Amendment privacy guarantee should in fact attach to the person, and to personal communications, and not be limited to a place such as the home. Most legal scholars see the Brandeis dissent in *Olmstead* as one his great pieces of legal authorship, but the fact remained that it was only a dissenting opinion, and Chief Justice Taft's opinion remained the law of the land until *United States v. Katz* in 1967.[41]

Brandeis was ultimately vindicated in 1967 in *Katz*, which remains the leading case on government searches involving electronic communications and involving more generally the notion that individuals have an expectation of privacy in their homes and also in some public places, such as telephone booths.[42] Concurring, the second Justice John Marshall Harlan succinctly noted:

> I join the opinion of the Court, which I read to hold only (a) that an enclosed telephone booth is an area where, like a home, *Weeks v. United States*, 232 U.S. 383, and unlike a field, *Hester v. United States*, 265 U.S. 57, a person has a constitutionally protected reasonable expectation of privacy; (b) that electronic as well as physical intrusion into a place that is in this sense private may constitute a violation of the Fourth Amendment; and (c) that the invasion of a constitutionally protected area by federal authorities is, as the Court has long held, presumptively unreasonable in the absence of a search warrant.[43]

Here, the Court not only reversed *Olmstead*, it also set forth two major principles. As Brandeis argued earlier, it changed the Fourth

39. Olmstead v. United States, 277 U.S. 438, 455 (1928).

40. *Id.* at 455–65. Most legal scholars see Chief Justice Taft's decision in *Olmstead* as one of the worst Supreme Court decisions ever. However, Taft and the majority of the Court were largely reflecting a concept of privacy that was reasonably well-settled at the time, although they seemed to be totally disconnected from the reality of technological change.

41. Katz v. United States, 389 U.S. 347 (1967). The modern doctrine of a "right to privacy" developed out of cases denying women—even married women—the right to obtain birth control. *See* Griswold v. Connecticut, 381 U.S. 479 (1965); Eisenstadt v. Baird, 405 U.S. 438 (1972).

42. *Katz,* 389 U.S. at 359. Unfortunately Brandeis, who retired from the Court in 1939 and died in 1941, did not live to see this change. In *Katz* there was a 7–1 majority of the Court with Justice Stewart writing for the majority, as well as a concurring opinion by Justice Harlan. *Id.* at 348. In the case, Katz was calling his bookie from a phone booth where his call was intercepted by the police. *Id.* at 351.

43. *Id.* at 360–61 (Harlan, J., concurring).

Amendment concept of privacy as attaching to the "person" rather than the "place" (i.e., a home). It also established a two-fold test for applicability of the Fourth Amendment protection, with the first being whether the person has a "reasonable expectation of privacy" and the second being whether this particular expectation is one that society sees as reasonable.

Even in *Katz*, however, the entire Court did not accept the Brandeis concept. In a dissenting opinion, Justice Hugo Black, a justice honored for his strong defenses of civil liberties and civil rights, argued that the Fourth Amendment, as a whole, was only meant to protect "things" from physical search and seizure; it was not meant to protect personal privacy. Black further argued that wiretapping was analogous to the act of eavesdropping, which was around even when the Bill of Rights was drafted, and concluded that if the drafters of the Fourth Amendment had meant for it to protect against eavesdropping they would have included the proper language.[44]

Under *Katz* there was no recognized expectation of privacy in data about communications, which the Intelligence Community calls "externals" and has been referred to over the years as "pen register data, trap and trace data," and most recently "metadata." Metadata is literally "data about data," so in the context of telecommunications, it would include records of the day, time, length of a phone call, and what phone numbers were involved. In the pre-Internet days this would have been the basis of a phone bill that listed all calls made to and from a number. But metadata does not include the content of the call and in the case of a phone call would have involved some sort of wiretap or other mechanical listening device. Actual content could only be obtained with a court order and warrant. In the context of e-mail conversations, metadata also includes information about the source of an e-mail, the IP address from which it was sent, the size of the e-mail communication, whether it had attachments or not, and the e-mail address (the Internet equivalent of a phone number), but not the actual content of the e-mail.

As early as 1979, in *Smith v. Maryland*, the Supreme Court recognized the important difference between actual conversations and the content of electronic communications, and metadata.[45] In *Smith*, the Court viewed metadata (such as records of phone calls) as business records rather than personal communications. Thus, the collection of metadata (i.e. phone records) did not require a warrant, while actually listening to the conversations did. The Court's analysis here was based on the idea that phone users cannot really have any actual expectation of privacy regarding the numbers they dial, since they typically know that these are held by the telephone company for various

44. *Id.* at 364 (Black, J., dissenting).
45. Smith v. Maryland, 442 U.S. 735, 741 (1979).

legitimate business purposes. Indeed, in 1979 all long distance calls were considered "toll calls" and were logged by the phone company for billing purposes because these calls were billed separately, at a per minute rate. In the past this had been done with local calls as well. Under the well-established "third party" doctrine, users gave this information to the phone company when they initiated the calls and assumed the risk it might be revealed to the police and others.[46] Some debate remains as to whether this "metadata" created on phone company computers is the phone company's or became "personal data" when mailed to the subscriber. One complication to this issue is that the records—all the metadata—are actually produced by the phone company, not by the customer using the phone.

Most recently, the entire concept of privacy expectations with respect to metadata has become a subject of debate in various court cases, as have other types of data that did not even exist at the time of *Smith*, and in Congressional debate over the reauthorization of Section 215 of the USA PATRIOT Act.[47] The argument of civil libertarians is that aggregating large amounts of metadata by the government poses a threat to privacy and is leading to a constitutional crisis.[48] The government asserts that this bulk data collection is necessary for national security and law enforcement but does not threaten individual privacy and that it has been securely storing this data otherwise maintained by the telephone companies, which is not searched without a specific warrant from a federal court.[49]

---

46. *Id.* at 744. Under some phone plans long distance calls (especially calls made to non-U.S. numbers are still logged by the phone company and billed as "toll calls." In addition, cell phone companies keep a record of all calls made to and from cell phones and sometimes include them in the cell phone bill. While cell phone plans are increasingly moving toward unlimited calls (as land lines are in most places in the U.S.), there are still cell phone plans with limited numbers of calls, which of course means the company must keep a record of all calls for billing purposes.

47. There is extensive literature on the debate over Section 215. See, for example, Abraham Wagner, *Does NSA Need Section 215?* (Center for Advanced Studies on Terrorism, May 14, 2015) and Dia Kayyali, *Section 215 of the Patriot Act Expires in June, Is Congress Ready?*, ELECTRONIC FRONTIER FOUND. (Jan. 29, 2015), *available at* www.eff.org/deeplinks/2015/01/section-215-patriot-act-expires-june-congress-ready.

48. Laura K. Donohue, *Bulk Metadata Collection: Statutory and Constitutional Considerations*, 37 HARV. J.L. & PUB. POL'Y 757 (2014); David Gray & Danielle Citro, *The Right to Quantitative Privacy*, 98 MINN. L. REV. 62 (2013).

49. In June 2015, Congress failed to reauthorize Section 215 of the USA PATRIOT Act but rather enacted a compromise law, the USA Freedom Act, which largely ended bulk collection of metadata by NSA and left the various telephone companies to maintain this data on their computers. This solution makes little legal or logical sense. Civil liberties advocates seem to think that holding the metadata on private servers, subject to hacking and maintained by personnel with no background checks or security clearances, is preferable to the NSA maintaining it on highly secure servers. In either case it can only be accessed with a court order. The new solution also has serious flaws in that multiple telephone companies are involved; they are not required to maintain the data for an extended period; and timely access may be impossible for terrorism investigations.

IV. PRIVACY IN THE AFTERMATH OF *KATZ*

The landmark *Katz* case had an immediate impact on the public good, largely in the area of law enforcement where police had routinely engaged in unrestricted wiretapping. Congress responded to the decision with the Omnibus Safe Streets and Crime Act of 1968,[50] which established criteria for the police to obtain judicial warrants for wiretaps supporting their lawful investigations.[51] This imposed a level of order on the domestic side of wiretaps and surveillance for the next decade or so. But the *Katz* regime began to break down in the 1980s (or before) in the wake of new communications technologies, new surveillance technologies, and the emergence of new threats (or the perception of new threats) to domestic peace and national security.[52]

The declaration of a "War on Drugs" by President Richard M. Nixon in June 1971[53] soon led to a plethora of demands for relaxation of strict warrant requirements and abandonment of the idea of an expectation of privacy, even in one's own home.[54] This trend was exacerbated in the 1980s when President Reagan "pledg[ed] an 'unshakable' commitment 'to do what is necessary to end the drug menace'" in the United States.[55] This soon led to what scholars and even jurists called the "drug exception" to Fourth Amendment law and other areas of law.[56] In *Skinner v. Railway Labor Executives' Ass'n*, Justice Thurgood Marshall protested in dissent that "[t]here is no drug exception to the Constitution, any more than there is a com-

50. Omnibus Crime Control and Safe Streets Act of 1968, 18 U.S.C. §§ 2510–2520 (2012).

51. *Id.* §§ 2011, 2013, 2015.

52. An excellent review of the legal regime in this area can be found in GINA STEVENS & CHARLES DOYLE, CONG. RESEARCH SERV., 98-326, PRIVACY: AN OVERVIEW OF FEDERAL STATUTES GOVERNING WIRETAPPING AND ELECTRONIC SURVEILLANCE (2012) (providing an excellent review of the legal regime in this area).

53. *A Brief History of the War on Drugs*, DRUG POLICY ALLIANCE, http://www.drugpolicy.org/new-solutions-drug-policy/brief-history-drug-war (last visited Apr. 2, 2015).

54. Paul Finkelman, *The Second Casualty of War: Civil Liberties and the War on Drugs*, 66 S. CAL. L. REV. 1389, 1410–11 (1993) [hereinafter Finkelman, *Second Casualty of War*].

55. Steven Wisotsky, *Crackdown: The Emerging "Drug Exception" to the Bill of Rights*, 38 HASTINGS L.J. 889, 890 (1987) (quoting President's Reagan Message Announcing Federal Initiatives Against Drug Trafficking and Organized Crime, 18 WEEKLY COMP. PRES. DOC. 1311, 1312–14 (Oct. 14, 1982)).

56. For a full discussion of how the War on Drugs impacted the entire Bill of Rights, including freedom religion, speech, press, and the right to an attorney, see Finkelman, *Second Casualty of* War, *supra* note 54, at 390; Paul Finkelman, *The War on Defense Lawyers*, *in* NEW FRONTIERS IN DRUG POLICY 113 (Arnold S. Trebach & Zevin B. Zeese eds., 1991); Paul Finkelman, *The Latest Front on the War on Drugs: The First Amendment*, 2 DRUG L. REP. 229 (1991); and Paul Finkelman & Michael W. Gadomski, *Overdose: The Failure of the U.S. Drug War and Attempts at Legalization: Introduction*, 6 ALB. GOV'T. L. REV. vii (2013).

munism exception or an exception for other real or imagined sources of domestic unrest."[57]

While legal academics, lawyers, and courts focused on privacy issues in the context of the War on Drugs, in the national security area, *Katz* had little impact for about a decade. At the time the very existence of the National Security Agency ("NSA") itself had been classified, and there was limited public discussion of foreign intercepts supporting intelligence and military missions.[58] A vast majority of the legal and political community (and the nation as a whole) assumed the government had a perfect right to spy overseas to protect the nation. Furthermore, most of the electronic intercepts targeted foreign nationals outside the United States, and thus there were no clear constitutional issues involved. The Bill of Rights, especially in the case of the Fourth Amendment, limits what the government may do and would therefore apply to foreign nationals in the United States, but courts at that time had never extended the general protections of the Bill of Rights to activities taking place outside the United States, especially when they involve noncitizens.[59] This well-ordered universe was upset by several events during the 1970s. Leaks in the *New York Times* of the CIA Family Jewels study disclosed major abuses by NSA, which had been engaging in warrantless domestic collection operations ordered by the Nixon White House.[60]

---

57. The Skinner v. Ry. Labor Execs.' Ass'n, 489 U.S. 602, 641 (Marshall, J., dissenting).

58. The NSA was officially established in October 1952 by a secret directive from President Truman as the successor to the Armed Forces Security Agency. Its actual existence was classified for several years, and the term NSA was jokingly referred to as "No Such Agency" and "Never Say Anything." In the current wake of disclosures, leaks, and lawsuits, the NSA has been engaged in a publicity campaign to garner public support for its important national security and cyber security missions.

59. Illustrative of this were the "Insular Cases," heard by the Supreme Court in the wake of the Spanish-American War. In these cases the Court refused to apply the Constitution to new territories under U.S. control. Thus, in *Dorr v. United States*, 195 U.S. 138 (1904), the Court held that even though the United States occupied and governed the Philippines, there was no right to jury trial there under the Constitution. In this, and other cases, the Court held that the Constitution did not follow the flag. *See* 2 MELVIN I. UROFSKY & PAUL FINKELMAN, A MARCH OF LIBERTY: A CONSTITUTIONAL HISTORY OF THE UNITED STATES 592–95 (3rd. ed. 2011). Clearly, if the Constitution did not protect the due process rights of an American citizen, residing in a United States territory, then the Constitution did not protect the rights of non-U.S. citizens living in places not under the jurisdiction or control of the United States.

60. *See* Seymour Hersh, *Huge C.I.A. Operation Reported in U.S. Against Antiwar Forces, Other Dissidents in Nixon Years*, N.Y. TIMES, Dec. 22, 1974, at 1. "Widely known as the 'Family Jewels,' this document consists of almost 700 pages of responses from CIA employees to a 1973 directive from Director of Central Intelligence James Schlesinger asking them to report activities they thought might be inconsistent with the Agency's charter." CIA, *The Family Jewels* (May 16, 1973), *available at* http://www.foia.cia.gov/collection/family-jewels. Most relevant here are operations such as NSA's *Project SHAMROCK* and *Project MINARET* which illegally collected against anti-war activists inside the United States. Such activities violated the charter of the CIA, which was only authorized to operate outside of the United States. These

These leaks led to congressional investigations of abuses by national security agencies through the Church and Pike Committee investigations in the Senate and House.[61] After these investigations, Congress passed legislation that provided for both increased oversight of intelligence activities as well as specific limitations on foreign surveillance activities in the Foreign Intelligence Surveillance Act of 1978 ("FISA").[62] FISA accomplished several important things in terms of privacy. For what it termed "U.S. persons," the law established a warrant requirement for intercept, even where one party might be outside the country.[63] It also established a special federal court, the Foreign Intelligence Surveillance Court ("FISC"), to review applications for warrants to be issued under FISA.

V. Privacy Post-9/11

The terrorist attacks on the United States on September 11, 2001, opened up a new era in national security in several dimensions. Threats to the homeland from non-state actors were of central concern, but the use of cell phones and Internet services to facilitate terrorist operations suddenly became a major concern. Responding to this threat, the Intelligence Community rapidly scaled up new collection programs with some legal cover from the Justice Department.[64] The Intelligence Community began this undertaking to meet serious national security challenges involving not only new technologies but

projects actually date from 1945 and were initiated by the Armed Forces Security Agency (AFSA), a predecessor to NSA.

61. Senator Frank Church of Idaho was chairman of the United States Senate Select Committee to Study Governmental Operations with Respect to Intelligence Activities in 1975; Representative Otis Pike of New York was chair of the House Select Committee on Intelligence in 1975.

62. Foreign Intelligence Surveillance Act of 1978, 50 U.S.C. § 1801 (2012).

63. *See* 50 U.S.C. § 1801. It remains somewhat unclear precisely who are included as U.S. persons now. *Id.* § 1801(i). Clearly it includes citizens and legal immigrants. *Id.* Most likely it will be interpreted to cover illegal immigrants and possibly tourists and others who might be in the U.S. for any number of reasons. The "Law Enforcement Access to Data Stored Abroad Act" currently before Congress does define a "U.S. person" as one who is "a citizen or lawful permanent resident alien of the United States, or an entity or organization organized under the laws of the United States or a State or political subdivision thereof." Law Enforcement Access to Data Stored Abroad Act, S. 2871, 113th Cong. § 3 (2014); *see also* Jack M. Balkin, *The Constitution in the National Surveillance State*, 93 Minn. L. Rev. 1 (2008).

64. An initial analysis dated September 25, 2001, from the Office of Legal Counsel at Justice, authored by John Yoo, argues that the recently enacted Authorization for the Use of Military Force ("AUMF"), passed after the terrorist attack on 9/11, provided adequate legal authority for these programs. Memorandum from John C. Yoo, Deputy Assistant Attorney Gen., U.S. Dep't of Justice, to the Deputy Counsel to the President, On the President's Constitutional Authority to Conduct Military Operations Against Terrorists and Nations Supporting Them (Sept. 25, 2001), *available at* http://www.lawfareblog.com/wp-content/uploads/2013/10/Memorandum-from-John-C-Yoo-Sept-25-2001.pdf. The key program was highly classified (heavily compartmentalized), and government lawyers from other offices were not cleared or consulted. These actions continue to be at the core of an ongoing debate.

users outside and inside the United States moved well beyond the constraints of FISA as initially enacted. At the time, the government elected to rely more on secrecy than statute.

Initial leaks to the *New York Times* in 2005 created a firestorm within the Intelligence Community and in the courts. That firestorm has yet to abate. For a decade now the government has been fighting one court battle after another with respect to privacy issues raised by these ongoing collection operations. Congress attempted to ameliorate the problem with the passage of the FISA Amendments Act of 2008 ("FAA"),[65] which provides additional authorities to the Intelligence Community in Sections 215 and 702 of the FAA, as well as retroactive immunity to service providers for assisting in these collection operations. At present, major challenges to the FAA as being an unconstitutional violation of the Fourth Amendment right to privacy are pending in the federal courts, and a Supreme Court ruling in the matter is probably a year away.[66]

VI. Privacy as a Dynamic Concept

For most of history people have had very little to keep private. Literacy was limited, communications were costly and even more limited, and there was no Big Data. Basic concerns in this area related to the sanctity of the home and family relations within the home, and, in most cultures, to the coverage of parts of the body aptly termed "private parts." Widespread literacy, new technologies, and related economics changed the world—largely within the past few decades. While the landmark *Katz* case moved the nation to the Brandeis concept of legally protected privacy, new technologies radically increased the amounts of personal data needing protection. At the same time, a host of factors—including media disclosures, greater public awareness, and others—have changed individual expectations with respect to privacy.

65. FISA Amendments Act of 2008, Pub. L. No. 110-261, 122 Stat. 2436 (codified as amended in scattered sections of 50 U.S.C.).

66. The first major challenge was rejected by the Supreme Court in *Clapper v. Amnesty Int'l USA*, 133 S. Ct. 1138 (2013), on the basis of standing and did not reach the constitutional issue. Most recently, the *Klayman* case (D.C. Circuit) again raises the constitutional issue, and the district court found no issue with repect to standing, although the D.C. Court of Appeals held differently and has recently remanded the case. Klayman v. Obama, 957 F. Supp. 2d 1 (D.D.C. 2013), *vacated and remanded*, 800 F.3d 559 (D.C. Cir. 2015). The same issue was also raised in the Second Circuit in *ACLU v. Clapper*, 959 F. Supp. 2d 724 (S.D.N.Y. 2013), *aff'd in part, vacated in part, remanded*, 785 F.3d 787 (2d Cir. 2015), where that court held that there was no reasonable expectation of privacy in conformity with the Supreme Court's holding in *Smith v. Maryland*. On appeal, the Second Circuit did not reach the constitutional issues because it concluded that the challenged program was not authorized by the statute on which the government based its claim of legal authority. ACLU v. Clapper, 785 F.3d 787, 824 (2d Cir. 2015).

Privacy has become a dynamic concept, and in many respects the legal regime is several generations behind current technology and how it is being utilized. For most of the 20th century "privacy" usually concerned letters mailed from one person to another, telegraph communications, photographs privately made, conversations among a few people in person or on the telephone, or between two parties. New technologies and the way they are utilized have radically changed people's expectations with respect to both privacy and the security of their personal data.[67] At the outset it is important to recognize that both the type and amount of personal data has grown by astronomic proportions, in what is now being referred to as the era of "Big Data."[68] What is generated and stored has grown by many orders of magnitude. Apart from anything else, people have a great deal more to be concerned about.[69] To what extent they are actually concerned—aside from what is indicated by the amount of interest shown by civil rights organizations such as the American Civil Liberties Union ("ACLU"), Electronic Frontier Foundation ("EFF"), and others—is an open question, but clearly there are major concerns.[70]

One aspect of the modern technical world is that physical media of all kinds are rapidly vanishing. Not only are communications electronic, but photographs, movies, music, books, newspapers, health records, and virtually anything else that once existed as paper or plastic are now digital files that are stored and downloaded. Servers, clouds, and personal devices to access them have become central to modern life. As users entrust increasing amounts of personal data to these systems, their concerns and expectations about privacy and security understandably grow far more significant. In the pre-electronic age, a private or intimate letter could not be easily shared with large numbers of people, and, once destroyed, the letter was gone. Today, e-mail and photographs sent electronically, or even just stored electronically, can be shared with untold numbers of people through a few keystrokes. The recent hacking of servers holding personal images of

67. The media are filled on a daily basis with stories of hacks and invasions of various servers and stores of personal data of all kinds, including communications, financial data, health records, personal images, and a host of other things.

68. *See* Big Data: Seizing Opportunities, Preserving Values (Executive Office of the President, May 2014).

69. For one important exploration of the magnitude and implications of the lack of privacy in data, see LORI ANDREWS, I KNOW WHO YOU ARE AND I SAW WHAT YOU DID: SOCIAL NETWORKS AND THE DEATH OF PRIVACY (2012).

70. As a practical matter, the vast majority of Americans simply don't care that NSA may be storing old phone billing data, now called "metadata," which the phone carriers themselves store, and generally appreciate that NSA's mission is to protect the nation from terrorist attacks and other significant threats. At the same time, civil libertarians at the ACLU and Electronic Frontier Foundation ("EFF"), for example, think otherwise, and their view appears to have prevailed.

entertainment personalities, including Jennifer Lawrence, Kate Upton, and others, received considerable media attention.[71]

It is also the case now that the nature of the data and individual expectations of privacy are getting somewhat confused, particularly in the area of social media. Old distinctions between truly personal communications, for example, and business records are difficult to apply to many things like Facebook and Instagram postings. While it is clear that specific personal communications and even data such as private photographs intended to be shared only with designated recipients still retain their private character, postings to social media sites to a massive group of "friends" and the public alike take on a different character and possibly a different set of expectations.[72] Here a new concept of "quasi-private" data may be an approach to consider.

A second new area of concern involves questions of privacy from whom. Virtually all of the prior statutes, case law, and doctrines relate to government surveillance, generally for law enforcement and national security purposes. Currently, commercial vendors and hackers are madly using and abusing data in their possession as service providers or thieves. The third-party doctrine that has been applied is seriously outdated, and it is likely that many new cases and statutes will evolve in the near future. It is also the case that protection of commercial infrastructure has become a national security concern, and currently the NSA has been assigned to protect the infrastructure for some sixteen specific commercial sector activities.[73]

Certainly the legal regime with respect to privacy and security itself is seriously outdated. The Electronic Communications Privacy Act ("ECPA") (1986) is decades old, even with some minor amendments. Similarly, the Computer Fraud and Abuse Act ("CFAA") for felony computer hacking and sharing of addresses and other information needs revision. New legislation has stalled in Congress for years now. At the same time, case law in federal and state courts over various privacy and security issues continues to grow.[74]

---

71. Alana Horowitz & Stephanie Marcus, *Jennifer Lawrence's Nude Photos Leak Online, Other Celebs Targeted*, HUFFINGTON POST (Aug. 31, 2014, 6:34 PM), http://www.huffingtonpost.com/2014/08/31/jennifer-lawrence-nude-photos_n_5745260.html.

72. Understanding the so-called "privacy settings" and operations of Facebook, for example, is a legal and technical challenge to say the least. How broadly any posted image on Facebook will be shared or seen regardless of the users intended settings is difficult for any user to determine.

73. Interview with Mike Rogers, Admiral, USN, Dir., NSA, and Commander, CYBERCOM (Feb. 4, 2015).

74. *See, e.g.*, United States v. Auernheimer, 748 F.3d 525 (3d Cir. 2014); *In re* Google Inc. Cookie Placement Consumer Privacy Litig., 988 F. Supp. 2d 434 (D. Del. 2013); *In re* iPhone Application Litig., 844 F. Supp. 2d 1040 (N.D. Cal. 2013); Pirozzi v. Apple Inc., 913 F. Supp. 2d 840, 847 (N.D. Cal. 2012); United States v. Warshak, 631 F.3d 266, 288 (6th Cir. 2010); Joffe v. Google Inc., 746 F.3d 920 (9th Cir. 2013); *In re* Google Inc. St. View Elec. Commc'ns Litig., 733 F. Supp. 2d 1381 (J.P.M.L. 2010).

VII. Evolution of Cyberspace and Big Data

At the outset of what may be called the Internet Era, few anticipated the extent to which rapidly evolving information and communications technologies would come to dominate all aspects of modern life, including governmental and commercial operations. For well over a decade little was done to provide adequate privacy and security protections for government and commercial systems. This mirrors other technological developments. Movable type printing revolutionized European society starting in the mid-15th century. But it took more than a century for England to begin to regulate printing,[75] and English courts did not begin to regulate seditious libel in any significant way until the 1606 case *De Libellis Famosis*.[76] Similarly, the first commercial radio station (KDKA in Pittsburgh) began operating in November 1920, but Congress did not attempt to regulate commercial broadcasting until the passage of the Radio Act of 1927,[77] and significant modern regulation of commercial broadcasting did not come about until the Communications Act of 1934,[78] which created the Federal Communications Commission ("FCC").

Following this pattern of only slowly responding to new communications technology, the United States has been incredibly tardy in passing legislation responding to new Internet technology. This has been true both for the protection of users from government surveillance, as well as to protect users from hackers, commercial exploitation, or criminal banditry. But it has also been true for the failure to provide guidelines for Internet surveillance for legitimate law enforcement and national security purposes. At the same time, most users were initially slow in demanding security and privacy features. Within the past few years, however, radical changes in the number and nature of attacks on systems of all types have greatly increased the demand for new privacy technologies.

The rapid evolution of cyberspace and the accompanying rise of Big Data has clearly been one of the greatest technological revolutions in recorded history. What began as a Defense Department experiment at the Advanced Research Projects Agency ("ARPA," later "DARPA") in the late 1960s has transformed almost all aspects of life

75. Fredrick S. Siebert, Freedom of the Press in England, 1476–1776: The Rise and Decline of Government Control 27 (1952).

76. De Libellis Famosis, (1606) 5 Co. Rep. 125a (Court of the Star Chamber); 77 Eng. Rep. 250 (Star Chamber).

77. The Radio Act of 1927, Pub. L. No. 69-632, 44 Stat. 1162 (repealed 1934). An Act to Regulate Radio Communication, Pub. L. No. 62-264, 37 Stat. 302 (1912) (repealed 1927), provided for licensing of private radio operators but did not contemplate commercial radio stations and had no provisions for regulating them. Passed in the wake of the sinking of the RMS Titanic in April 1912, the act was mostly aimed at insuring that ships at sea have radios on board at all times.

78. Communications Act of 1934, 7 U.S.C. § 151 (repealed 2000).

with new technologies and an explosive growth in e-mail, the world wide web, and net-based applications never anticipated.

Security and privacy were not essential elements of the original ARPAnet design. At the outset the ARPAnet was an experiment in optimizing network resources with "switched packet" technology as an alternative to traditional "line switching."[79] E-mail was not even a part of the concept, the web did not yet exist, there were no browsers or net-based content, and there were no early commercial or national security applications. Quite simply, in these early days there was nothing on the net to steal or hack, and access to the net was limited to a few scientists and other users who had hardwired connections to mainframe computers.

Apart from DARPA's developmental work, a wide range of users—including the government, commercial firms, and educational institutions—acquired computers connected to various networks, adding data at an exponential rate. With the transition to the Internet, networks were given low-cost global connectivity. For the first time in history, the marginal cost of worldwide communications fell to almost zero, as the web made it easier for users with new applications and web-based content to grow exponentially.

Few entrants into cyberspace were aware of or cared about the myriad security vulnerabilities that existed in operating systems, server software, middleware, application layers, router software, and elsewhere in the Internet world. For well over a decade, the prevailing notion was that if there were problems, it must be somebody else's job to fix them.

A. *Early Vulnerabilities and Security Efforts*

The commercial world was quick to adopt the net, offer a vast range of applications, and generate Big Data, but it was largely unwilling and uninterested in paying to either secure it or provide privacy. Even banks failed to address the problem until they had been robbed of large sums. Government users were not much better as they quickly embraced cost-effective networked systems but failed to address critical vulnerabilities.[80]

Internet programmers recognized vulnerabilities in operating systems as well as server design. Early attacks generally involved malware, which disabled vulnerable computers and exploited unprotected data, stealing large amounts of it from servers connected to the net. Microsoft distributed "fixes" and "patches" to deal with some vulnerabilities while third party vendors like Norton sold security software that attempted to deal with a wider range of malware, in-

79. *See* STEPHEN SEGALLER, NERDS 2.0.1: A BRIEF HISTORY OF THE INTERNET 68, 373 (1998).

80. *See* Wagner, *supra* note 3.

stalled firewalls, and gave users regular updates as new threats were identified.

These early entrants into the field saw the threat from malicious net activity and tried to protect users from malware by removing suspicious code—such as viruses, worms, and Trojans—from infected computers. Other firms offered encryption software, such as Pretty Good Privacy ("PGP") that enabled their users to protect sensitive files, while a secure version of net protocol, :/https, enabled secure transactions over the web. In some ways cyberspace was becoming safer and more secure, but the adversarial threat was advancing at an even greater pace.[81]

B. *Growing Threats from Home and Abroad*

Growth of e-commerce and Big Data brought new demands for privacy and security, while the proliferation of networked national security systems also required secure networks and applications of higher standards. Vulnerabilities continued to be identified while new threats were seen on a daily basis. As the financial sector entered cyberspace, lucrative targets for cybercrime emerged, and net-based theft from banks and credit card fraud became a booming business. Big Data became both a target and a commodity.

While the early threats came largely from youthful hackers and disgruntled system administrators, this past decade witnessed the evolution of far more serious cyber threats from expert criminals as well as well-trained military units and national security agencies assigned to cyber-warfare and cyber-espionage missions. Debate continues over the range of potential threats, ranging from denial of service to a type of apocalyptic attack often referred to as a "digital Pearl Harbor," which could involve massive denial of net services, widespread theft of data, possibly the corruption of data being sent over the net, or even a total shutdown of the Internet. Any of these events would not only affect business, banking, airline and train service, and national security, but would totally disrupt the services of a modern society, such as the delivery of electricity, water, or natural gas, the use of telephones and the operation of hospitals, grocery stores, fire departments, emergency (911) services, and police departments. Modern life in industrial nations is now almost entirely dependent on functioning computers and a smoothly operating Internet.

VIII. The Evolving Legal Regime

As in other areas, the legal regime for privacy and security is a composite of constitutional law, federal statutes, case law, executive orders, and regulations that have the effect of statutes. Looking first to

81. *Id.*

the Constitution and the framers' intent, the Constitution itself says very little about national security and nothing about intelligence whatsoever. The technologies of the time did not include electricity or any type of communications other than the postal service, which at the time was costly and highly limited. Inferring what the framers might have said and done if they had been in the Internet Era remains a subject of ongoing discussion among legal scholars.[82]

As discussed above, the issue of privacy in electronic communications did not reach the U.S. Supreme Court until 1928 in *Olmstead*, even though the telegraph had been around for close to a century and the telephone for about a half-century. Wiretapping, which came into use shortly after the Civil War, has generally been attributed to criminals seeking information about which trains to rob by tapping telegraph lines adjacent to railroad tracks.[83] While the historical literature in this area is limited, it can be assumed that law enforcement authorities followed suit in an effort to catch criminals soon thereafter.

In the national security area, intelligence services began watching international cable traffic almost as soon as these cables were installed in the early 20th century. One limiting factor was that the intelligence services in both the United States and Great Britain had only a handful of staff, and of these only a few engaged in so-called "signals intelligence."[84] In both nations these activities were shielded in secrecy and largely unknown to the general public. In Great Britain, the Official Secrets Act of 1911 shielded these activities,[85] while in the United States, these limited activities conducted by the Black Chamber were hidden in New York City and were generally unknown to most people.[86]

---

82. Several current Supreme Court justices have remarked that they do not entirely understand all new technologies but nevertheless need to deal with cases involving them.

83. *See, e.g.*, Michael Warner, *Privacy and Security, Yesterday and Today*, IDA REPORT, *supra* note 7.

84. *The Black Chamber: The Man Who Made Edward Snowden Inevitable,* THE ECONOMIST, Dec. 19, 2015, at 39. The numbers are quite amazing. In 1900, for example, Great Britain's intelligence service (The War Office Intelligence Branch) had a total staff of twenty-seven, which was then the largest in the world. In the U.S., the Office of Naval Intelligence (ONI), which was the nation's intelligence service at the time, had a total staff of seven, which was reduced to five during a budget crisis in 1903. In those days, intelligence was simply not a serious business, and of this, the fraction of the staff devoted to intercept or signals intelligence was even smaller. These limited activities were conducted in secret and attracted little or no attention at all, which helps to explain why there were no court challenges.

85. Official Secrets Act, 1911, 1 & 2 Geo 5 c 28 (U.K.).

86. This was done for both technical as well as security reasons, as it gave this early SIGINT service access to the AT&T cables, which terminated in New York. The service operated under the belief that they were probably in violation of the Communications Act of 1934 but never sought to test this proposition. Communications Act of 1934, 7 U.S.C. § 151 (repealed 2000).

During the first half of the 20th century, radio systems came into use for communications, in addition to existing wire and cable systems, particularly for "long-haul" uses. The complicating assumption here was that, by broadcasting a radio wave where anyone with a receiver could listen, there could be no expectation of privacy. Radio-based systems were certainly a godsend for intelligence services who found that in many cases proliferating receivers was easier than cable tapping. In domestic law enforcement applications, there were few radio-based systems until the advent of cellular telephone, and the legal regime dealt almost exclusively with landline technologies.[87]

Keeping things in perspective, *Olmstead*, which was the law from 1928 until *Katz* in 1967, held that all warrantless domestic wiretapping was lawful, and it did not even touch the concept of intercept for intelligence purposes, presumably done outside the U.S. but in many cases actually involving domestic technical operations.[88] As already discussed at some length above, *Katz* radically changed the game for domestic law enforcement and the conception of privacy under the Fourth Amendment. At the time, neither the CIA nor NSA saw it as having any impact on their intelligence operations. It was simply assumed that foreign nationals had no rights under the Constitution and that any domestic privacy rights did not apply to Americans abroad.

This relatively well-settled legal universe did not last long, falling victim to disclosures of illegal or at least questionable activities in the 1970s and new technologies in the 1980s and 1990s. As already mentioned, the disclosure of the CIA Family Jewels report called NSA and CIA operations into severe question with resulting increases in Congressional oversight. Other complaints related to the Vietnam conflict and surveillance operations led to the Foreign Intelligence Surveillance Act of 1978[89] and Executive Order 12333 (1981), which further defined the roles and missions of the Intelligence Community. At this point, however, the legal evolution largely halted for roughly two decades. Cases were largely limited to the classified proceedings before the FISA Court ("FISC"), and House and Senate intelligence committees conducted their deliberations largely in secret as well.

---

87. The landmark *Katz* case (1967) was well before the development and proliferation of cellular systems in the 1980s, and only recently have cases begun to deal with issues related to cell phones. Katz v. United States, 389 U.S. 347 (1967).

88. Olmstead v. United States, 277 U.S. 438, 467 (1928). The operative statute here being the National Security Act of 1947. National Security Act of 1947, 50 U.S.C. §§ 401–442 (2012). Among other things, this major overhaul of the U.S. national security structure established the Department of Defense and the Central Intelligence Agency, proscribing CIA activities within the U.S. Intercept and signals intelligence were left with the military intelligence services until the establishment of the National Security Agency ("NSA") by a classified Presidential directive in 1952. *See* STEPHEN A. CAMBONE, A NEW STRUCTURE FOR NATIONAL SECURITY POLICY PLANNING (1998).

89. Foreign Intelligence Surveillance Act of 1978, 50 U.S.C. § 1801 (2012).

Major changes on the technology front seriously unsettled this universe, particularly the rapid proliferation of cellular phone systems worldwide and the Internet's explosive growth after 1990. The only significant piece of federal legislation during this period came in the Electronic Communications Privacy Act of 1986 ("ECPA"), which preceded the transition to the public Internet by some four years and by all accounts stands in serious need of revision. Apart from the ECPA and a few other less significant statutes discussed above already, law in this area has been dominated by an increasing number of federal and state cases, which are often in conflict or technologically behind the times.

On the national security and intelligence side, the 9/11 terrorist attacks radically changed the legal regime. Use of new technologies such as cell phones and the Internet by al Qaeda operatives to support their operations quickly drove the Intelligence Community to the realization that thwarting future terrorist attacks required far more extensive access to these communications abroad, as well as within the United States. A creative interpretation of the 2001 Authorization for the Use of Military Force ("AUMF") by the Justice Department Office of Legal Counsel substantially expanded the scope of NSA activities and provided the basis for greatly enhanced surveillance of suspected terrorists based on the claim that proposed NSA activity did not violate the Fourth Amendment.[90] Subsequent disclosures about the highly classified program undertaken in 2005 led to both federal court challenge as well as the FISA Amendments Act of 2008 ("FAA"), which sought to codify what the Justice Department had previously seen as legal and provide retroactive immunity for firms assisting the government in these efforts. As noted, court challenges to the FAA are still ongoing.[91]

Apart from the court challenges to NSA operations against suspected terrorists by civil liberties groups such as the ACLU and the EFF, most Americans probably see such intelligence activities as essential to protecting the nation and simply do not have an issue with

90. *See* Memorandum from John C. Yoo, Deputy Assistant Attorney Gen., U.S. Dep't of Justice, to David Kris, Associate Deputy Attorney Gen., on Constitutionality of Amending Foreign Intelligence Surveillance Act to Change the "Purpose" Standard for Searches (Sept. 25, 2001), *available at* https://ccrjustice.org/files/memoforeignsurveillanceact09252001.pdf.

91. *See, e.g.*, Pl.'s Compl., Wikimedia Found v. Nat'l Sec. Agency, 2015 WL 1033734 (D. Md. Mar. 10, 2015). The initial challenge to the 2008 FISA Amendment Act ("FAA") was ultimately dismissed by the Supreme Court in *Clapper v. Amnesty*, 133 S. Ct. 1138 (2013), on the basis of standing without addressing the constitutional issue. Subsequently two major cases have been brought where standing does not appear to be an issue. In *ACLU v. Clapper*, 133 S. Ct. 1138 (2d Cir. 2013), the Second Circuit reversed the trial court ruling and held that the FAA violated Section 215 of the USA PATRIOT Act. In *Klayman v. Obama* (D.C. Cir. 2013) also held that the bulk data collection program was a violation. In light of recent Congressional action the matter is likely moot.

NSA storing their phone-record data or even their e-mails if it serves to make the nation safe.[92] However, this attitude is also based on the fact that most Americans do not believe *their* Internet communication will be subject to government surveillance. As these systems have come to dominate almost all aspects of modern life, users have, however, become far more sensitive to privacy issues. Here too both Congress and the courts have come to view the constitutional privacy protections far differently and appear to be on a legislative and judicial path that will further constrain future technology development and government operations.[93] This calls for a new balance between rights and responsibilities as both the technologies and the law evolve, including user expectations as well as legal interpretations of how constitutional guarantees apply to new technologies and government efforts to meet critical national security concerns.

In some significant areas, major issues are still before the courts, and in others, the new and evolving technologies are simply not well understood. Rapid and seemingly unstoppable technological development continues to greatly outpace existing law. At the same time user expectations and demands for enhanced security and privacy promise to place even greater strains on the system as new technologies, media, and uses develop.

IX. Demands for Internet Privacy and Anonymity Impact of National Security

Complicating demands for Internet privacy is the emergence of Internet anonymity. Just as users demand personal "privacy," they now encounter additional problems raised by anonymous postings that can be libelous, fraudulent, or the Internet equivalent of intentional infliction of emotional distress. Clearly some Internet web sites and traffic can pose significant threats to national security. Increasingly, there are sites used to recruit terrorists, support their operations, and provide a communication medium. It is also the case that in the current technology environment geography is no longer relevant as it was in prior days. Distinguishing U.S. operations and even "U.S. persons" from

92. It remains to be seen whether the Supreme Court will ultimately overturn *Smith v. Maryland,* 442 U.S. 735 (1979), and extend the privacy concept to what is now being referred to as "metadata" and was previously seen as business records rather than personal information protected under *Katz*.

93. This has not always been the case. Until the landmark case *Katz v. United States*, 389 U.S. 347 (1967), the Supreme Court held that the constitutional protections of the Fourth Amendment did not apply to electronic communications at all. Subsequent decisions, and particularly the recent case *United States v. Jones*, 132 S. Ct. 945 (2012), have greatly broadened the scope of privacy protection. Statutes such as the Electronic Communications Privacy Act (1986) and others also add to this domain. *See* Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848 (codified as amended in scattered sections of 18 U.S.C.).

"non-U.S." persons and operations has become an exceedingly difficult and often impossible task.

Additional complications are raised by the nature of the new media. Some Internet traffic is purely private—between two people or a select small number of people—and presumably is protected, and more importantly users have come to expect such protection of their personal communications since *Katz*. Indeed, to preserve the essence of American liberty and the letter and the goal of the Fourth Amendment, it must be protected from warrantless scrutiny in keeping with the Court's criteria in *Katz*. Other data, which is now termed "metadata" (such as phone numbers called or the IP address of Internet communications) has not traditionally been protected in the same manner but is the subject of an ongoing legal debate. The Court in *Smith* saw such data more as business records than personal communications and did not accord it the type of Fourth Amendment protection that it afforded personal communications in *Katz*.[94]

There is, however, a third category, which could be called "quasi-private data"—where users post information to social media sites, list servers, and other public websites (or to large segments of the public). The extent to which this category is in fact actually private or warrants the same types of protection is an area that is just beginning to be explored by legal scholars and the courts. Finally, there is a huge area of basically unregulated data, and the collection of that data, by e-commerce entities. These companies mine data, e-mails, and Internet searches for commercial purposes. The data is then used in-house or sold to third parties for advertising purposes and other commercial activities, including determining who might receive credit card offers, who might be eligible for a housing loan, or who might be offered a job.[95]

X. SECURITY, PRIVACY, AND THE LAW IN THE *JONES* ERA

The first part of the 21st century brought a world of new devices, applications, and accompanying Big Data. At the same time, there have been dramatic changes in user expectations of both privacy and security. In addition, various disclosures as well as major studies about government surveillance programs adopted since the 9/11 attacks have fueled a broader debate over essential security requirements and competing privacy demands.[96]

94. Smith v. Maryland, 442 U.S. 735, 749 (1979). Congress, however, began to impose similar warrant requirements on such data, known then as "pen register" or "trap and trace" data under the Electronic Communications Privacy Act of 1986 (ECPA). *See* 18 U.S.C. ch. 206 (2012). To date, the ECPA has not been challenged as being unconstitutional, and the Court has yet to overturn *Smith v. Maryland*.

95. This issue is set out in great detail in ANDREWS, *supra* note 69.

96. *See* PRIVACY & CIVIL LIBERTIES OVERSIGHT BD., REPORT ON THE TELEPHONE RECORDS PROGRAM CONDUCTED UNDER SECTION 215 OF THE USA PA-

It is generally agreed that the legal regime for cyberspace is seriously outdated and generations behind current technologies. Several key cases are currently before the courts, and proposed legislation awaits action before Congress. Major concerns exist as to how new presidential directives, laws, privacy and national security interests, and court decisions will impact technology development. Certainly the technology path will not stop or be reversed. Increasing Big Data gathering will continue to accumulate it on systems worldwide, presenting an ever greater challenge to public policy.

Increasingly many Americans believe that the Fourth Amendment protects privacy from government surveillance as a right and that freedom and independence may not be possible without some semblance of this privacy.[97] As early as 1963, three decades before the Internet was commonly used, Supreme Court Chief Justice Earl Warren noted that technological innovation was diminishing privacy expectations and predicted this problem would get worse.[98] Justices Douglas, Brandeis, and others have also interpreted the Fourth Amendment as providing a fundamental right to privacy that needs to be upheld in order for justice and freedom to prevail.[99] At the same time, national security requirements have required practices and intelligence operations that, in the wake of the 9/11 attacks, have been viewed as critical for the nation's safety. However, increasingly these practices and operations have recently come under attack.[100]

Data privacy suits have increased in number and notoriety in recent years, and the issue of "injury in fact" has become an early challenge for privacy plaintiffs to prove.[101] Normally this type of injury is rarely

---

TRIOT ACT AND ON THE OPERATIONS OF THE FOREIGN INTELLIGENCE SURVEILLANCE COURT (Jan. 23, 2014); *see also* RICHARD A. CLARKE ET. AL., LIBERTY AND SECURITY IN A CHANGING WORLD: REPORT AND RECOMMENDATIONS OF THE PRESIDENT'S REVIEW GROUP ON INTELLIGENCE AND COMMUNICATIONS TECHNOLOGIES (Dec. 12, 2013). At the same time as these outstanding studies, unlawful disclosures by Edward Snowden first published on June 5, 2013, in the British newspaper *The Guardian* have received widespread media attention and have served to focus additional attention in this critical area.

97. Olmstead v. United States, 277 U.S. 438, 472–73 (Brandeis, J., dissenting). Significantly, as Andrews notes, most Americans seem oblivious to the massive collection of private (often very personal) data by Internet providers, web sites, and commercial data miners. The collection of this data is almost entirely unregulated, even though it can be deeply personal, can affect the financial, employment, and even health care status of people, and has been used (or abused) by corporations with pernicious results. ANDREWS, *supra* note 69.

98. Lopez v. United States, 373 U.S. 427, 441 (1963) (Warren, J., concurring).

99. Osborn v. United States, 385 U.S. 323, 343 (1966) (Douglas, J., dissenting); *Olmstead*, 277 U.S. at 472–73 (Brandeis, J., dissenting).

100. See the opinion of Judge Claire Egan for explanation of the FISA court's rationale for approving the Section 215 telephone records program. *In Re* FBI for an Order Requiring the Prod. of Tangible Things from Redacted, No. BR 13-109, 2013 WL 5741573 (FISA Ct. Aug. 29, 2013).

101. *In re* Google, Inc. Privacy Policy Litig., No. C-12-01382-PSG, 2013 WL 6248499, at *4 (N.D. Cal. Dec. 3, 2013) (citing *In re* iPhone Application Litig., No.

an issue in lawsuits but is as big an obstacle for data privacy plaintiffs as Mount Kilimanjaro is for hikers.[102] Here, the Wiretap Act of 1968[103] (which was actually Title III of the Omnibus Crime Control and Safe Streets Act of 1968)[104] comes into play. This statute provides a private right of action against any person who "intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication."[105] Furthermore, the Stored Communications Act[106] (actually Title III of the Electronic Communications Privacy Act of 1986) prohibits providers of electronic communication from "knowingly divulging to any person or entity the contents of a communication."[107] Congress is now seeking to extend this protection to the data of Americans that is stored abroad on servers and cloud services in the Law Enforcement Access to Data Stored Abroad Act ("LEADS Act").

When Congress passed the Electronic Communications Privacy Act ("ECPA"),[108] including the Stored Communications Act, in 1986 it was landmark legislation.[109] Passed close to three decades ago, it preceded the Internet by several years. Clearly technology has evolved dramatically in these decades in ways never imagined.[110] Still, by 1986 the use of computers and network-related technology had grown sig-

5:11–md–02250–LHK, 2013 WL 6212591, at *1012 (N.D. Cal. Nov. 25, 2013)); Pirozzi v. Apple Inc., 913 F. Supp. 2d 840, 847 (N.D. Cal. 2012).

102. *Id.*

103. 18 U.S.C. §§ 2510-2522.

104. *Privacy Wiretap Act*, INTERNET LAW TREATISE, https://ilt.eff.org/index.php/Privacy:_Wiretap_Act (last modified Jan. 28, 2007, 7:14 PM).

105. 18 U.S.C. § 2511(1)(a); *see id.* § 2520.

106. Stored Wire and Electronic Communications Act, 18 U.S.C. §§ 2701–2712 (2012). According to the Department of Justice, "The Electronic Communications Privacy Act and the Stored Wire Electronic Communications Act are commonly referred together as the Electronic Communications Privacy Act (ECPA) of 1986." U.S. Dep't of Justice, Office of Justice Programs, *Electronic Communications Privacy Act of 1986 (ECPA), 18 U.S.C. §§ 2510–2522*, JUST. INFO. SHARING, https://it.ojp.gov/default.aspx?area=privacy&page=1285 (last modified July 30, 2013). The ECPA updated the Federal Wiretap Act of 1968, which addressed interception of conversations using "hard" telephone lines but did not apply to interception of computer and other digital and electronic communications. *Id.* Several subsequent pieces of legislation, including The USA PATRIOT Act, clarify and update the ECPA to keep pace with the evolution of new communications technologies and methods, including easing restrictions on law enforcement access to stored communications in some cases." 18 U.S.C. § 2702(a).

107. 18 U.S.C. § 2702(a).

108. 18 U.S.C. §§ 2510–2522.

109. *Id.*

110. Christina Bonnington, *Apple Mac at 30: See the Evolution of an Icon*, WIRED (Jan. 25, 2014, 6:30 AM), http://www.wired.com/2014/01/30th-apple-anniversary/; Matt Honan, *New Tools Show How Deep Glass will Embed in Our Live*, WIRED (Nov. 19, 2013, 3:00 PM), http://www.wired.com/2013/11/google-glass-sdk/; Amanda Scherker, *Family Banned All Technology Made After* 1986, HUFFINGTON POST (Sept. 3, 2013, 5:44 PM), http://www.huffingtonpost.com/2013/09/03/family-living-1986_n_3860365.html.

nificantly and individuals had begun using personal computers to access remote networks and data.[111] When Congress passed the ECPA, one goal was to reassure industry that its growth would not be constrained by individuals' fears regarding the privacy of their communications and data maintained on computer servers.[112] Under then-existing Supreme Court precedent, it was far from clear that the Supreme Court would extend Fourth Amendment protection to these new technologies.[113]

Legal scholars have criticized the current law at length. Professor Orin Kerr argues that the lack of a suppression remedy has confused courts on how to respond (or even provide a remedy) to an unauthorized interception.[114] Others argue that all private communication and stored data should be protected equally.[115] Still others have shown that under the current language the same e-mail is subject to different protection depending on whether it is in transit, stored on a home computer, opened and stored in remote storage, unopened and stored in remote storage for 180 days or less, or unopened and stored in remote storage for more than 180 days. Judges have also expressed concerns about the inconsistent protections within the act. One circuit court has struck down, on constitutional grounds, the provision that does not provide protection for electronic communication after 180 days in temporary storage. The Court found this provision unconstitutional because it authorizes less than a probable-cause standard for government agents seeking a warrant to search private communications.[116]

For decades now, scholars have debated ways to improve the existing legal regime and its intersection with the Fourth Amendment.[117] One side of this debate proposes a universal search warrant require-

111. Melissa Medina, *The Stored Communications Act: An Old Statute for Modern Times*, 63 AM. U. L. REV. 267, 272 (2013).

112. *Id.* at 291 n.166.

113. United States v. Karo, 468 U.S. 705, 721 (1984); United States v. White, 401 U.S. 745, 754 (1971).

114. Orin S. Kerr, *A User's Guide to the Stored Communications Act, and A Legislator's Guide to Amending It*, 72 GEO. WASH. L. REV. 1208, 1243 (2004).

115. *See, e.g.*, Robert A. Pikowsky, *The Need for Revisions to the Law of Wiretapping and Interception of Email*, 10 MICH. TELECOMM. & TECH. L. REV. 1, 49–50 (2003).

116. *See* United States v. Warshak, 631 F.3d 266, 288 (6th Cir. 2010); Marc Zwillinger & Jacob Sommer, *Sixth Circuit's En Banc Reversal in Warshak Sidesteps Constitutionality of Stored Communication Act's Delayed Notification Provision*, 7 PRIVACY & SEC. L. REP. (BNA) No. 32, Aug. 11, 2008, at 49–51.

117. *See* Daniel J. Solove, *Reconstructing Electronic Surveillance Law*, 72 GEO. WASH. L. REV. 1264, 1299–300 (2004); Orin S. Kerr, *The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution*, 102 MICH. L. REV. 801, 808–10 (2004); Orin S. Kerr, *The Mosaic Theory of the Fourth Amendment*, 111 MICH. L. REV. 311, 315 (2012); Daniel J. Solove, *Fourth Amendment Codification and Professor Kerr's Misguided Call for Judicial Deference*, 74 FORDHAM L. REV. 747, 749 (2005); Kerr, *supra* note 114, at 1208–09.

ment. Advocates on the other side of the debate argue that Congress is best suited to enact laws to protect privacy because the Courts are faced with the disadvantage of trying to hit a "moving target" (i.e., the continuing development of technology) while interpreting at a distinct moment in time the case and controversy before them.[118] Most experts, however, agree that the existing legal regime needs to be modified to improve its application to modern technology and the demands of Big Data.[119]

A. *Fourth Amendment Interpretation*

Traditionally, the Fourth Amendment right to privacy has been viewed as a property right,[120] and searches involved physical property—the amendment protected "the right of the people to be secure in their persons, house, papers, and effects."[121] Searches of property required a warrant issued by a magistrate supported by probable cause.[122] While the Fourth Amendment right to privacy and right to be exempt from unreasonable (and usually warrantless) searches still maintains its foundation in property rights, the Supreme Court has also supplemented property-based privacy rights with a reasonable expectation of privacy outside of any physical property.[123]

Current conceptions of privacy are based on *Katz*, where the Court held that, even in a public place, a person could have a reasonable expectation of privacy in his person.[124] Justice Harlan's concurrence in *Katz* has served as the guiding principle for the analysis of whether a search violates a reasonable expectation of privacy, establishing two requirements for a reasonable expectation of privacy: (1) a person has exhibited an actual (subjective) expectation of privacy; and (2) the expectation be one that society is prepared to recognize as "reasonable" (objective).[125] Writing for the majority, Justice Potter Stewart reasoned, "[W]hat a person knowingly exposes to the public, even in his own home or office is not a subject of the Fourth Amendment protec-

118. Orin S. Kerr, *Congress, the Courts, and New Technologies: A Response to Professor Solove*, 74 FORDHAM L. REV. 779, 782–83 (2005).

119. Robert A. Pikowsky, *The Need for Revisions to the Law of Wiretapping and Interception of Email*, 10 MICH. TELECOMM. & TECH. L. REV. 1, 65–66 (2003).

120. *See* United States v. Jones, 132 S. Ct. 945, 949 (2012); Florida v. Jardines, 133 S. Ct. 1409, 1417–18 (2013). Indeed, the famous Warren and Brandeis article, *supra* note 28, grounded the claim for privacy in property rights, with a tort remedy similar to common law trespass. *See also,* Wagner, *supra* note 7, at 7 (Comments in response to the Office of Science and Technology Policy, Government "Big Data" Request for Information, March 4, 2014).

121. U.S. CONST. amend. IV.

122. Shadwick v. City of Tampa, 407 U.S. 345, 354 (1972).

123. *See Jones*, 132 S. Ct. at 954; *Jardines*, 133 S. Ct. at 1417–18; Katz v. United States, 389 U.S. 347, 360 (1967) (Harlan, J., concurring).

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

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

tion."[126] He continued, however, to say, "But what he seeks to preserve as private, even in an area accessible to public, may be constitutionally protected."[127]

For close to a half-century now, *Katz* has served as a foundation for determining whether behavior constitutes a violation of the Fourth Amendment right to privacy. Moving beyond communications, the Court has applied these principles in considering whether there is a reasonable expectation of privacy in "open fields" outside of the curtilage of a home.[128] The reasonable-expectation test remains as to whether there is a reasonable expectation of privacy where there is no property right at issue, such as in electronic communications or data storage.

B. *Exposure to the Public*

Cases following *Katz* stand for the principle that what one knowingly exposes to the public is not subject to Fourth Amendment protection.[129] Furthermore, as the Court articulated in *California v. Greenwood*, "[a]n expectation of privacy does not give rise to Fourth Amendment constitutional protection unless society is prepared to accept that expectation as objectively reasonable."[130] However, it must also be noted that there are numerous drug related cases after *Katz* and both before and after *Greenwood* where the Court seems to have ignored what would seem like common-sense understandings of privacy and security from unreasonable searches, such as the police photographing fenced-in yards or roof tops from planes and helicopters.[131]

---

126. *Id.* at 351.

127. *Id.*

128. Oliver v. United States, 466 U.S. 170, 184 (1984); United States v. Dunn, 480 U.S. 294, 305 (1987).

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

130. California v. Greenwood, 486 U.S. 35, 39–40 (1988). In *Greenwood*, the Court held that garbage left at the side of the road is readily accessible to animals, children, scavengers, and other members of the public. *Id.*

131. In *California v. Ciraolo*, the Court upheld the right of the police to fly over a house in a small airplane, at an altitude of 1,000 feet. California v. Ciraolo, 476 U.S. 207, 209 (1986). From the airplane, the police officers identified marijuana growing in the yard and photographed it. The yard was surrounded by two fences, a six-foot high outer fence and a ten-foot high inner fence. *Id.* After this flyover, the police obtained a search warrant for a physical inspection of the property. *Id.* at 209–10. The Supreme Court held that the overflight did not constitute a search, despite the facts that the yard was within "the curtilage of [defendant's] house," that a fence shielded the yard from observation from the street, and that the occupant had a "subjective expectation of privacy. *Id.* at 211–12. The Court, however, found this expectation "unreasonable and . . . not an expectation that society is prepared to honor." *Id.* at 209, 214. After *Ciraolo*, the Court in *Florida v. Riley* upheld the legality of an observation of an enclosed greenhouse with a helicopter. Using "a camera with a telephoto lens, and while circling over the property at an altitude of 400 feet," a Sheriff's deputy "observed marijuana growing within the greenhouse. The deputy was able to see through the roof because two of the panels in the roof were missing." W.F. "Casey" Ebsary,

Most recently, the Court has issued another landmark privacy decision in *United States v. Jones*, a case involving a GPS tracker which police attached to a drug dealer's vehicle without judicial approval and then used the information from the tracker as evidence to convict him.[132] The Court held that the reasonable expectation of privacy test supplements the property-based expectation of privacy and, therefore, the placing of a GPS tracker on the vehicle in effect constituted an unlawful search.[133] Here, the Court fundamentally overturned prior law established in 1983's *United States v. Knotts,* where the Court under similar circumstances declined to find a violation of the expectation of privacy.[134] The *Knotts* Court held that a person traveling on public roads has no expectation of privacy in his movements because the vehicle's starting point, direction, stops, or final destination could be seen by anyone else on the road, in what has been referred to as the open fields doctrine.

Concurring in the *Jones* decision, Justice Sonia Sotomayor reasoned that unrestrained power to assemble data that reveals private aspects of identity is susceptible to abuse and warned that that it may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties because it is ill-suited to the digital age.[135] Foretelling the issues of Big Data, Justice Sotomayor went on to raise concerns over the comprehensiveness of a record of personal movements and a "wealth of detail about her familial, political, professional, religious, and sexual associations."[136] To protect the information, however, requires that "Fourth Amendment jurisprudence ceases to treat secrecy as a prerequisite for privacy."[137] As Justice Thurgood Marshall stated, "privacy is not a discrete commodity, possessed absolutely or not at all."[138]

A number of courts have subsequently cited *Jones* on a range of privacy issues, including numerous federal appellate courts, FISC, and the Supreme Court itself.[139]

Jr., Note, *Fourth Amendment Aerial Privacy: Expect the Unexpected*, 19 STETSON L. REV. 273, 273 (1989). The Court, characterizing the greenhouse as having a partially open roof, noted that "the helicopter in this case was *not* violating the law" and had not "interfered with respondent's normal use of the greenhouse or of other parts of the curtilage." Florida v. Riley, 488 U.S. 445, 451–52 (1989). These cases are discussed in greater detail in Finkelman, *Second Casualty of War*, *supra* note 54, at 1413–15.

132. United States v. Jones, 132 S. Ct. 945, 948–49 (2012).

133. *Id.* at 949, 952.

134. United States v. Knotts, 460 U.S. 276, 285 (1983).

135. *Jones,* 132 S. Ct. at 956–57 (Sotomayor, J., concurring).

136. *Id.* at 955.

137. *Id.* at 957.

138. Smith v. Maryland, 442 U.S. 735, 749 (1979).

139. *See* Amended Memorandum Opinion, *In Re* Application of the Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things, op. cit., and *Opinion and Order*, No. PR/TT [redacted] (FISA Ct.).

XI. Meeting the Challenge—Toward a National Policy

It is the unfortunate reality that in the 1990s—the Internet's first critical decade—there was virtually no national policy on cybersecurity. Cybersecurity during this important formative stage of the Internet was in large part either nonexistent, badly managed, poorly funded, and in some cases simply absurd. As the Internet exploded in terms of users and applications and as evolving threats emerged, there was little national consensus as to whose responsibility it was to secure cyberspace and respond to these threats. It is true that at the outset cybersecurity was scarcely an issue since there was essentially nothing on the Internet to steal or hack, and access was largely limited to a very few users who were hardwired to a few mainframe computers.[140]

From the beginning, the government, and especially the military, became a large-scale Internet user, and truly the "pig at the trough," while the government did little to protect this vital resource. As a whole, government saw this as a responsibility of the commercial service providers while government programs to deal with it were minimal and inadequate. This is particularly remarkable because, unlike earlier technological breakthroughs in communication—such as Johannes Gutenberg's moveable-type press, Alexander Graham Bell's telephone, and Guglielmo Marconi's radio—the government was in fact the major player in developing the Internet. Moreover, the entire national security community, including the military, were key players in this development. Given the military's penchant for secrecy and security—and the strong military needs for both—it is astounding that the federal government did not take a far greater role in creating and developing effective cybersecurity. The government was, however, clearly aware of the evolving problem. A major study directed by President Bill Clinton in 1998 explored the issue at length and directed the development of a national plan for dealing with the problems.[141] Unfortunately the funding and program direction to implement this plan was never provided.

In the 1990s the nation failed to see the real potential of the cyberthreats, especially from overseas. As government (especially the military and national security agencies) and the financial sector became large Internet users, they added Big Data to the networked world and became lucrative targets for major criminal enterprises and foreign intelligence services and foreign military forces who foresaw cyberwarfare.[142] At the time, America focused largely on defense against hackers and lower-level threats and was not looking to the larger evolving threat environment.

---

140. *See* Wagner, *supra* note 7.

141. *See* Presidential Decision Directive on Critical Infrastructure Protection, NSC 63 (May 22, 1998).

142. *See, e.g.*, *APT1 Exposing One of China's Cyber Espionage Units*, Mandiant (2013), http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf.

While the 9/11 attacks themselves had little to do with cyberwarfare or Big Data,[143] they did provide a catalytic shock to the government in terms of looking far more seriously at new threats, particularly in the technology space. Terrorists' use of cell phones, the Internet, and ATMs now became a serious subject of interest. Programs focusing on these technologies, which languished in the 1990s, received renewed attention and support. At the same time a number of early cyber-attacks such as Moonlight Maze (from Russia in 1999), Titan Rain (from China in 2004), and others attacking critical systems drove home the reality of growing threats.

A. *A Strategy for Cyberwarfare*

Increasing cyberattacks from foreign groups have raised the specter of cyberwarfare as a realistic arena for future conflict. Analysts continue to debate as to how conduct "combat" in this new type of warfare, which has no geography and differs from the traditional model of kinetic warfare. At the moment, no one in the military, the intelligence community, or the legal community knows what "rules" of warfare apply, and the extent to which the elements of loss of life and destruction of property—the two cornerstones of the kinetic model of warfare—might apply in the cyber-war context.

B. *Cyberspace Is Part of a Highly Dynamic World*

Cybersecurity has become an essential element of life in the wired world. This is a highly dynamic universe where both the technology base and the threats continue to evolve. For some time now this world has moved into an era of "digital everything" with an almost seamless merger of communications, computing, and media of all kinds, including largely digital Big Data. Coupled with hardware and communications bandwidth that has become increasingly cheap, the marginal costs of communications are free or, in many cases, nearly so. All these factors—especially the rapidly developing and increasingly inexpensive technology and access to the Internet—have caused use of cyberspace to grow by orders of magnitude in a few short years.

The enabling technologies and economics have also brought about some major changes in culture. Use of the net, devices, and advent of Big Data have brought about modern cultural artifacts from Internet

143. The 9/11 terrorists did use cell phones, e-mail, and ATM machines to facilitate their crime. The United States, on the other hand, generally failed to use readily available electronic tools that might have thwarted some of the attackers. At least three 9/11 terrorists were stopped by police shortly before the attack, but watch-lists, outstanding warrants, and immigration violations were not available to local police at the time, although the technology existed to provide them with this information. Susan Candiott, *Another Hijacker Was Stopped for Traffic Violation*, CNN.COM/U.S. (Jan. 8, 2002, 2:27 AM), *available at* http://edition.cnn.com/2002/US/01/09/inv.hijacker.traffic.stops/.

dating to social awareness streams. Internet-based commerce is fast surpassing all other forms, while businesses as well as the government agencies have become almost totally dependent on Internet-based systems.

System architects are increasingly moving to a cloud concept, while more serious threats from cyber criminals, cyber warriors, and cyber terrorists across the globe continue to grow. Thus, it is increasingly important that any policy or strategy employ effective defensive and offensive elements that aid in meeting overall strategic objectives as well as user demands for privacy, security, and resilience. Meeting these sometimes-competing demands presents an increasingly complex policy challenge.

C. *Building the Technology Base*

Implementing a successful national strategy must necessarily start with building the technology base. This largely involves educating people with the skills necessary to meet the emerging challenges. It is also an area that simply requires the "best and the brightest" to create the type of software and other technologies required. Educating people to meet this challenge requires a new level of commitment to the nation's universities, possibly using the model of the Eisenhower Administration in responding to the Cold War challenges of the Space Race[144] and the need to modernize the national highway system. This might require a concerted effort—and Congressional appropriations to match it—similar to the National Defense Education Act,[145] National Defense Highway Act, and the expansion of support for universities, including the push to provide higher education for more Americans.

This model for cyberspace and Big Data makes good sense, and it is reasonably certain that the universities are not able to meet this challenge utilizing internal resources alone. In the current economic climate even the major private universities are constrained, while most

144. At that critical point in history, the nation undertook a series of coordinated initiatives starting with substantial government investment in higher education, especially in science and math education, under the National Defense Education Act (NDEA). National Defense Education Act of 1958, Pub. L. No. 85-864, 72 Stat. 1580 (codified as amended in scattered sections of 20 U.S.C.). The government initiated new technology agencies, such as the Advanced Research Projects Agency (ARPA), the National Science Foundation (NSF), and others.

145. The National Defense Education Act (NDEA) was signed into law on September 2, 1958, providing funding to U.S. educational institutions at all levels, and was one of several science initiatives inaugurated by President to advance technology in the U.S. National Defense Education Act of 1958, Pub. L. No. 85-864, 72 Stat. 1580 (codified as amended in scattered sections of 20 U.S.C.). Other initiatives included the formation of ARPA (new DARPA) and NASA. At the time there was a growing national sense that U.S. scientists were falling behind scientists in the Soviet Union, catalyzed, arguably, by early Soviet success in the Space Race, notably the launch of the first-ever satellite, Sputnik, the previous year.

public universities are under enormous economic pressure. While there is sound logic that shows there are increasing numbers of jobs in cyberspace, the fact does not seem compelling enough to overcome the level of inertia in education and government funding today.

D. *Acceleration of Government Programs*

Notwithstanding budgetary pressures, it is increasingly clear that the government cannot continue to be the pig at the trough in terms of massive net use. The government cannot be the single largest user of the Internet but fail to adequately fund effective security programs. It can no longer afford to maintain the false expectation that the private sector will recognize the full scope of the problems and remedy them.

Efforts to protect the Internet and Big Data need continued and increasing support. Not all of these tasks can be left to the Defense Department and intelligence agencies. Without exception, all other governmental agencies have become major users of cyberspace and need to become partners in its ongoing protection. The nation may even need an entirely new cabinet-level agency to deal with communications and the Internet.

E. *Partnership with Industry*

Aside from limited government funding, one reason national policy on cyberspace failed in the 1990s was a basic misunderstanding of the role industry could and would play in securing the net and protecting Big Data. There were unreasonable expectations that industry would recognize the vulnerabilities and fix them. It was believed that it was not essential for the government to support this in a meaningful way and that user demands, from both the public and private spheres, would drive industry to meet the challenge—a belief that was only partially correct. What was done was largely inadequate and insufficient to meet the threats that evolved. The reasons for this are obvious. No one was in charge, and no entity had any responsibility to act, so it was in the best interest of each large player to let "the other guy" fix the problem. In addition, average users—who faced embarrassment, identity theft, exposure of the most private aspects of their lives, and asset theft—lacked the requisite knowledge to even understand the problems, much less have any idea how to fix them.

Policy now requires a more realistic approach to industry involvement on several levels. It is essential to recognize that industry built cyberspace and created Big Data—and that industry will fix it, irrespective of who pays. By and large, the government can only write checks, not computer code.[146] Even in the most sensitive areas the

146. Alternatively, the national government could develop some sort of Manhattan Project style enterprise to fix the Internet or create semi-autonomous institutes, along

actual work is outsourced to commercial firms with few programmers being government employees.

Here, the nation needs to move to a model where the technology companies that dominate cyberspace are made a more integral part of the process. The model that was highly effective in dealing with the communications firms for decades is a useful one that has not been effectively employed where cyberspace is concerned. Certainly some of the traditional telecoms are within the tent, but many of the most important and critical firms are not. In the final analysis, the nation needs to look ahead at what the solution is going to be, and work back from that, making sure that the technology base and the supporting industrial base can meet the very real threats and challenges ahead.

Policy has also now evolved to the point that intelligence services such as the NSA, whose mission has been strictly limited to national security requirements, are now being directed by the White House to support some sixteen commercial areas and under a far more modern concept of what national security actually means. Thus, as NSA Director Admiral Mike Rogers noted last year:

> Cyber threats are different from physical threats since they travel beyond geographical boundaries. Cyber threats are also blurring the line between the public and private sectors, sometimes prompting new and unexpected partnerships. If you had told me (in the past) that I was going to be spending time working on an offensive act against a motion picture company, I would have thought: "What? What does that have to do with me?" And yet that's the world we find ourselves in.[147]

Another key element of this partnership needs to be with the holders of Big Data, including the financial sector, the health services industry, and the telecoms and Internet service providers who hold increasingly large amounts of this information. One aspect of this partnership needs to be the timely and accurate provision of threat data coming from government sources and vice versa.[148] Another is a far broader national policy and legal regime that recognizes the role that industry servers and clouds have in maintaining Big Data and protecting both the privacy of users and the security of their data.

These are by no means simple issues. They continue to involve a number of complex technical, legal, and financial considerations, all of

---

the lines of the Rand Corporation, the Jet Propulsion Laboratory, or NASA, to fix this problem. But in the currently political climate this seems unlikely.

147. Mike De Souza, *NSA Chief Says Sony Attack Traced to North Korea After Software Analysis*, REUTERS (Feb. 19, 2015, 9:22 PM), http://uk.reuters.com/article/2015/02/19/uk-nsa-northkorea-sony-idUKKBN0LN27U20150219 (quoting Admiral Rogers interview). Admiral Rogers was referring here to a recent "hack" of Sony Pictures Corporation e-mail attributed to North Korean hackers that was highly publicized. *Id.*

148. The current Defense Industrial Base ("DIB") effort is one useful approach, but a far more extensive set of program is needed.

which are in a constant state of change. Here, it is essential to engage a wide range of Americans in the process of developing an effective national policy in this most critical area. It is also the case that both the executive branch and Congress are aware of the fact that laws in this area are antiquated and new legislation is required. For several years now, a number of well-drafted bills have enjoyed bipartisan support within Congress but have yet to be enacted. While this situation will hopefully change, the courts will continue to bear an increasing burden of balancing security and privacy.