PRIVACY IN THE DIGITAL AGE

SENATOR D. BRENT WALTZ*

INTRODUCTION

The evolution of the concept of "privacy in the digital age" has been almost as dynamic as the technology itself that has driven humanity's mastery of our planet. The American roots of the "privacy in a digital age" concept began in the troubled birth of a nation. It endured an uncertain adolescence as conflicts arose because inventions and technological advancements allowed drastic increases in a government's ability to intrude on the communication of its citizens. It reached maturity as society continues to attempt to balance the tension between modern technology and historical jurisprudence on what may very well be the most significant constitutional question of the twenty-first century.

A. The History of American Privacy

Even the most casual student of American Constitutional scholarship will note that the notion of "privacy" as a distinct legal construct is lacking in our founding documents.[1] Efforts to piece together a semblance of its preconception is challenging at best in the common law, Magna Carta, and the English parliamentary reforms following the Glorious Revolution of 1688.[2] One piece of what was destined to be known as the privacy "penumbra" emerges in the Third Amendment to the U.S. Constitution[3]—a somewhat surprising conclusion considering that the more frequently invoked Fourth and Fifth Amendments seem to receive much more scrutiny and acceptance as a constitutional basis of privacy in both legal theory and practice.[4]

The prohibition of the quartering and maintenance of soldiers in the private homes of a free citizenry inherent in the Third Amendment would appear to be a quaint and outdated historical need to house an army to ward off attacks from

---

* Senator D. Brent Waltz is a graduate of Wabash College, President of the Indianapolis based investment banking firm Baron Group, and has served in the Indiana General Assembly since 2004.

1. David Luban, *The Warren Court and the Concept of a Right*, 34 HARV. C.R.-C.L. L. REV. 7, 27 (1999).

2. CARL BECKER, NEW LIBERTIES FOR OLD 79 (1941); *see generally* Bill of Rights Institute, *Magna Carta (1215)*, BILL OF RIGHTS INSTITUTE, http://billofrightsinstitute.org/resources/educator-resources/americapedia/americapedia-documents/magna-carta/ (last modified 2010); *see also* U.S. National Archives & Records Administration, *Featured Documents*, NATIONAL ARCHIVES & RECORDS ADMINISTRATION http://www.archives.gov/exhibits/featured_documents/magna_carta/ (last visited Aug. 10, 2014).

3. Luban, *supra* note 1, at 31.

4. *Id.* (explaining that although the Fourth and Fifth Amendments are included in the penumbra of the right to privacy, the Third Amendment protects privacy rights within the home and thus belongs within the penumbra of the right to privacy).

French and Indian encroachment on the frontier in the mid-1700s.[5] Yet this conclusion seems to contradict basic military tactics of that period.[6] British troops were seldom quartered in private homes along the frontier; rather they were stationed in forts along strategic locations such as river convergences and mountain passes.[7] Besides the protections these fortifications provided, there was a practical need for not having troops spread out over large geographic distances.[8] The "Brown Bess" musket, standard issue for the British army at the time, was a highly inaccurate weapon.[9] Lacking a rifled barrel, soldiers carrying these muskets were traditionally ordered to form a line against a similarly equipped and organized opposing force.[10] British soldiers stationed in American cities in the years leading up to, and during, the American Revolution would have had a role more akin to an occupying military garrison.[11] The Third Amendment prohibits this function of government intrusion into the privacy of its citizenry.[12]

Having eyes and ears present inside the homes of citizens would have been an extremely effective method of intelligence gathering in the Age of Enlightenment.[13] A solider would report any suspicious or disloyal comments or activities to their superiors while discouraging dissent.[14] The technology did not exist to record or gather intelligence from great distances.[15] Nor were most communications physically recorded by their content, participants, or duration.[16] What would later be known as "Humint"—human intelligence—was the primary means of acquiring knowledge of potential threats.[17] The Third Amendment played a critical role in protecting privacy in the early days of the Republic.[18]

---

5. James P. Rogers, *Third Amendment Protections in Domestic Disasters*, 17 CORNELL J.L. & PUB. POL'Y 747, 751 n.34 (2008).

6. *Id.* at 751-52.

7. Robert A. Gross, *Public & Private in the Third Amendment*, 26 VAL. U. L. REV. 215, 218 (1991) (discussing that quartering soldiers was a last resort).

8. *Id.* at 217 (explaining that quartering troops in private homes was "hardly a good way to run an army").

9. Don Higginbotham, *The Second Amendment in Historical Context*, 16 CONST. COMMENT. 263, 267 (1999).

10. EDWARD HAGERMAN, THE AMERICAN CIVIL WAR & THE ORIGINS OF MODERN WARFARE: IDEAS, ORGANIZATION, & FIELD COMMAND (1992).

11. *See* Gross, *supra* note 7.

12. Luban, *supra* note 1, at 32.

13. *Id.*

14. Major Felix F. Moran, *Free Speech, the Military, & the National Interest*, AIR U. REV. (1980).

15. *See generally* Office of the Director of National Intelligence, *Data Gathering*, INTELLIGENCE.GOV, www.intelligency.gov/mission/data-gathering.html (last visited Aug. 10, 2014) (explaining human intelligence gathering is the oldest form of collecting information).

16. *See generally id.*

17. *See generally id.* (describing human intelligence data collection).

18. IRVING FANG, A HISTORY OF MASS COMMUNICATION: SIX INFORMATION REVOLUTIONS xvii- xix (1997), *available at* www.ebooksmagz.com/pdf/a-history-of-mass-communications-

B. American Privacy in Today's Society

By the dawn of the twentieth century, technology had dramatically increased a person's ability to communicate across greater distance than previously imagined.[19] The telegraph, followed by the telephone, radio, and eventually television provided the means to disseminate information through new mediums.[20] However, technological advances also increased the ability to track and identify communication on a grand scale.[21] The 1920s saw the first use of wiretaps by the U.S. federal government in criminal investigations.[22] The landmark 1928 U.S. Supreme Court decision in *Olmstead v. United States* defined for a generation the government's ability to wiretap telephone conversations without a warrant.[23] This gathering of evidence would have been impossible without the new technological means to do so.[24] In *Olmstead*, prohibition officers used wiretaps to determine that Roy Olmstead and others were violating the National Prohibition Act.[25] The Court determined that the Fourth Amendment's protection of houses, persons, papers, and effects did not extend to telephone wires.[26] Furthermore, Chief Justice Taft in his opinion drew a clear distinction between the physical search and seizure of evidence secured only by the sense of hearing.[27]

This distinction has a modern corollary that has been in place for nearly thirty years, which is roughly the time it took the U.S. Supreme Court to reverse *Olmstead* in its 1967 *Katz v. United States* ruling.[28] In 1986, Congress passed the Electronic Communications Privacy Act.[29] This legislation bifurcated the protections afforded to private documents and communications.[30] Documents

---

54454.pdf.

19. *Id.*

20. *Id.* at xix-xx.

21. William Lee Adams, *Brief History: Wiretapping*, TIME MAG. (Oct. 11, 2010), http://content.time.com/time/magazine/article/0,9171,2022653,00.html.

22. *E.g.*, Olmstead v. United States, 277 U.S. 438 (1928).

23. *Id.* at 466 (holding that "the wiretapping here disclosed did not amount to a search or seizure within the meaning of the Fourth Amendment").

24. *See, e.g.*, *id.* at 473 (Brandeis, J., dissenting) (stating that "[s]ubtler and more far reaching means of invading privacy have become available to the government. Discovery and invention have made it possible for the government . . . to obtain disclosure in court of what is whispered in the closet.").

25. *Id.* at 456-57.

26. *Id.* at 465.

27. *Id.* at 464.

28. Katz v. United States, 387 U.S. 347, 352 (1967) (overruling *Olmstead* by holding that the Fourth Amendment extends to "the recording oral statements overheard without any 'technical trespass' under local property law").

29. Electronic Communications Privacy Act of 1986, 18 U.S.C. §§ 2511-22 (1986).

30. *Id.*; 18 U.S.C. §§ 3121-3127 (2014); *see generally*, Deidre K. Mulligan, *Reasonable*

that were typed or written physically were granted greater constitutional protection than those that might be stored in an electronic format.[31] Likewise, conversations that were spoken face-to-face were viewed differently than those transmitted over the airwaves or by wire.[32] This statute provides the impetus for much of the confusion and conflict regarding privacy in the digital age.[33] It is a law that is in desperate need of revision, if not repeal.

It may be useful to consider the level of technological sophistication in 1986 to determine which is more antiquated—the method of communication in use at the time, or the laws that govern them.[34] The "facsimile machine" was considered state-of-the-art in sending written documents across great distances through the growing number of fiber optic telephone lines.[35] Fiber optic transmissions began to usher in a new stage of communication—the Internet.[36] The rate of transmission between computers was an impressive—by the standards of the time—several hundred characters *per minute*.[37] The Commodore 64 was eponymous for the nascent personal computer industry, achieving a storage capacity of *64,000 bytes* of information—not enough to store this article on its hard drive.[38] Floppy disks could add a few thousand bytes of additional memory, provided one possessed a disk drive roughly the size of a shoebox to read its data.[39] Cell phones were largely confined to automobiles because of their need for a power source better than the internal battery technology of the time.[40] Email, chat rooms, the World Wide Web, on-line auctions, Microsoft Internet Explorer, iPhones, satellite communications for non-military purposes, digital conference calls, electronic bill paying, and a host of other modern electronic conveniences simply did not exist or were in their infancy.

All of the aforementioned technologies are subject to the uses and abuses of

---

Expectations in Electronic Communications: A Critical Perspective on the Electronic Communications Privacy Act, 72 GEO. WASH. L. REV. 1557, 1565-71 (2004).

31. Electronic Communications Privacy Act of 1986, 18 U.S.C. §§ 2511-22 (1986).

32. *Id*.

33. *See also* Mulligan, *supra* note 30, at 1571 (noting that there is a gap between current privacy laws under the Electronic Communications Privacy Act and society's expectation of privacy).

34. *See also id*. at 1571-76 (noting that the disconnect between privacy laws and society's privacy expectations is the result of legislation written before recent technological innovations).

35. *See* Fang, *supra* note 18, at 226-29.

36. *Id.* at 232-33.

37. Seung-Que Lee et al., *The Wireless Broadband (WiBro) System for Broadband Wireless Internet Services*, IEEE COMM. MAG. 106, 107 (2006), *available at* http://www.jcbroadband.com/Library/jcbwb4.pdf.

38. Mark Ollig, *Commodore 64 Is Tanned, Rested, and Ready for a Comeback*, HERALD JOURNAL (Apr. 11, 2011), www.herald-journal.com/archives/2011/columns/mo041111.html.

39. ENCYCLOPEDIA OF LIBRARY & INFORMATION SCIENCE: VOLUME 52 228 (Allen Kent, ed., 1993).

40. *Cell Phone Battery History*, CHARGEALL.COM (Mar. 31, 2012), chargeall.com/cell-phone-battery-history/.

the Electronic Communications Privacy Act of 1986.[41] It would be as if in the decades before the invention of the printing press, a government guaranteed the freedom to self-expression only in handwritten documents and books, and this law remained in place once printed newspapers, broadsides, and pamphlets were the societal norm. One can imagine Thomas Paine furiously scribbling copies of *Common Sense* as he sought to share his ideas of liberty and freedom with his countrymen.[42] As new technologies are integrated into modern culture it becomes increasingly difficult for those living today to appreciate the difference between the printed word in an electronic format and the hard copy one—just as people a few generations ago would have failed to differentiate a printing press from a quill and ink well.[43] Yet this is a distinction with several practical differences in our legal system.

Nearly a decade ago police departments around the United States began purchasing devices known as "Stingrays."[44] These devices, the size of a laptop computer, would send out a fake transmission to cell phones and Internet enabled computers in order to fool or "spoof" them into communicating with the device.[45] Once connected, the person operating the Stingray could access all information on their phone or computer.[46] Any emails, texts, websites recently visited, calendars, telephone numbers, contact data, photographs, and documents stored in the memory of a cell phone or laptop computer are subject to the search and seizure of any police department possessing this device *without a search warrant* because of the legal differentiation between written and electronic information.[47] Many civil libertarians once aware of the existence of these devices questioned the possibility of governmental abuse.[48] They frequently met resistance in their attempts to ascertain the circumstances and frequency of government's use of

---

41. Electronic Communications Privacy Act of 1986, 18 U.S.C. §§ 2510-22 (1986).

42. *See generally* THOMAS PAINE, COMMON SENSE (Edward Larkin ed., 2004).

43. James A. Dewar, *The Information Age and the Printing Press: Looking Backward to See Ahead*, RAND.ORG www.rand.org/content/dam/rand/pubs/paper/2005/P8014.pdf (last visited Aug. 10, 2014) (describing the similarities between the information age and the time of the printing press).

44. John Kelly et al., *Law Enforcement Using Methods from NSA Playbook*, USA TODAY, Dec. 9, 2013, *available at* http://www.indystar.com/story/news/2013/12/08/indiana-state-police-tracking-cellphones-but-wont-say-how-or-why/3908333/.

45. *Id.*

46. *Id.*

47. *See generally Electronic Communications Privacy Act (ECPA)*, ELECTRONIC PRIVACY INFORMATION CENTER, http://epic.org/privacy/ecpa/#background (last visited Aug. 10, 2014). However, this is called into question by *Riley v. California*, which held that police must get search warrants to search cellular telephones seized incident to an arrest. *See generally* Riley v. California, 134 S. Ct. 999 (2014).

48. Ryan Sabalow, *Indiana State Police Tracking Cell Phones—But Won't Say How or Why*, INDIANAPOLIS STAR, Dec. 9, 2013, http://www.indystar.com/story/news/2013/12/08/indiana-state-police-tracking-cellphones-but-wont-say-how-or-why/3908333/.

Stingrays.[49] The Author of this article, who, in his capacity of Indiana State Senator, is drafting legislation to limit the use of these devices without a warrant by state and local law enforcement, was denied this information when he requested it in 2012. The Indiana State Police even refused to confirm they possessed such a device citing "security concerns."[50] It was only after the National Security Agency (NSA) revelations by Eric Snowden, and a subsequent *Indianapolis Star* and *USA Today* investigation that uncovered a purchase agreement totaling nearly $374 thousand (the approximate cost of a Stingray) from its manufacturer that the Indiana State Police acknowledged they had purchased one.[51] Even then, the Indiana State Police refused to acknowledge what "due process" they used to determine when a Stingray would be utilized.[52] They stated that law enforcement would "consult" with a judge before the device was deployed but refused to share what, if any, restraints they felt obliged to abide by.[53]

Such lack of judicial and legislative oversight simply begs for abuses to occur. Prior to his removal by pro-democracy forces, Ukrainian President Viktor Yanukovych employed such devices to identify protestors against his government in Kiev.[54] The morning following a major rally, those that had been present received a text or telephone message warning them that the government knew where they had been the day before and to stop their illegal gathering.[55]

Unfortunately, there was similar surveillance by local law enforcement in the United States.[56] In Miami, local police used their Stingray to develop a list of phone numbers belonging to protestors during a recent rally against the World Trade Organization in their city.[57] It is regrettable that members of the American law enforcement community would utilize similar intelligence gathering tactics ascribed to former members of the KGB and their affiliates. As the cost of this technology becomes lower and the technology becomes more widespread, it is likely that additional abuses like those documented in the Congressional testimony surrounding the NSA data collection efforts will become more common. It does not seem a serious reach to imagine that a sheriff deputy might deploy such a device in a fit of jealousy to learn about an ex-wife's activities, or for someone to come into private possession of one of these devices for some other nefarious purpose. The prevalence of more invasive technology, if left unchecked, could establish conditions consistent with the worse parts of George

---

49. *Id.*

50. *Id.*

51. *Id.*

52. *Id.*

53. *Id.*

54. *A Lesson from Ukraine on Cell Phone Metadata*, HERE & NOW (Jan. 24, 2014), http://hereandnow.wbur.org/2014/01/24/ukraine-metadata-lesson.

55. *Id*.

56. Sabalow, *supra* note 48.

57. *Id*.

Orwell's novel, *1984*.[58]

But American society need not slip into an Orwellian nightmare. Much can be done on both the federal and state levels to provide robust protections against privacy violations. The most effective would be to adopt an amendment to the U.S. Constitution preventing the distinction between digital and written documents for the purposes of ascertaining privacy protection. Missouri is currently in the process of amending its state constitution to do exactly that.[59] Indiana will begin its amendment process in 2015 to eliminate this distinction as well.[60] The repeal or material alteration of the Electronic Communications Privacy Act of 1986 would also reduce the potential for government overreach. The U.S. Supreme Court recently reviewed cases from California and Massachusetts in which citizens were convicted primarily on information found in a digital format—in both cases the suspect's cell phones—that were searched without the legal protections afforded paper documents.[61]

CONCLUSION

It seems no analysis of privacy in any age, digital or otherwise, would be complete without invoking the wisdom of Justice Louis Brandeis on the subject. In his now legendary *Harvard Law Review* article on privacy, the future Justice based the foundational construct of the right to privacy in that the law had not evolved to the point society had developed to ensure a "fundamental right to be left alone."[62] His prescient words were echoed in his *Olmstead* dissent that reminded one that in prior days the government had only "force and violence" to compel self-incrimination.[63] In the digital age, the capabilities legally permitted by law enforcement agencies throughout the United States would have made the most committed members of the Gestapo, Stasi, Republican Guard, Apparatchik, or KGB extremely jealous. While the future advancement of technology appears to be assured, the success in preserving liberty is not. It is up to free societies that value both liberty and privacy to refuse to yield to the seemingly unrelenting march of governments to restrict these fundamental freedoms.

---

58. GEORGE ORWELL, 1984 (1949).

59. S. J. Res. 27, 97th Gen. Assem., 2d Reg. Sess. (Mo. 2014).

60. H.B. 1009, 180th Gen. Assem., 2d Reg. Sess. (Ind. 2014); H.B. 1384, 180th Gen. Assem., 2d Reg. Sess. (Ind. 2014).

61. Riley v. California, 134 S. Ct. 999 (2014) (holding that the search incident to lawful arrest exception to the Fourth Amendment's general warrant requirement does not apply to a cell phone seized during an arrest).

62. Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890).

63. Olmstead v. United States, 277 U.S. 438, 473 (1928) (Brandeis, J., dissenting).