Technology's Stories

Vol 2. No. 1 April 2014

Reversing The Whispering Gallery of Dionysius: A Short History of Electronic Surveillance in the United States

Thomas C. Jepsen doi: 10.15763/JOU.TS.2014.4.1.01

Abstract

Disclosures about electronic surveillance by the U.S. National Security Agency have revived interest in issues of privacy and Fourth Amendment rights in the U. S. Seizures and surveillance of telegraphic dispatches figured in major events of the nineteenth and twentieth centuries, including the Civil War, the Hayes/Tilden election of 1876, and both world wars. As the U. S. emerged as a world power in the late nineteenth and early twentieth centuries, routine surveillance of foreign diplomatic correspondence was begun. After the invention of the telephone, disclosures of police wiretapping led to court cases testing the constitutionality of such actions. In the twenty-first century, the National Security Agency began collecting telephone and Internet metadata on a growing number of U.S. citizens. The rapid deployment of the Internet in the late twentieth and early twenty-first centuries has left many privacy issues unresolved. Each attempt by the U.S. government to obtain access to private electronic communication revived a debate about the necessity and constitutionality of such actions.

Keywords: Telegraph; telephone; telecommunications; electronic surveillance; nineteenth century; twentieth century; Fourth Amendment; wiretapping; Internet; metadata; National Security Agency

Introduction – The "whispering-gallery of Dionysius"

Recent disclosures about electronic surveillance of U.S. citizens by the National Security Agency have revived American public interest in issues of privacy and Fourth Amendment rights. In her study of the history of surveillance ("The Prism," *The New Yorker*, 24 June 2013), Jill Lepore perceptively points out that renewed concern about privacy always follows the emergence of a new surveillance technology. Such was certainly the case with the telegraph, which first came into widespread use in the U.S. in the late 1840s; in the September 1858 issue of the *Atlantic Monthly*, Christopher Pearse Cranch, a Transcendentalist poet and Unitarian minister, published a curious and fanciful piece titled "An Evening with the Telegraph-Wires," in which he imagined all the potential uses that the new invention could be put to, including electronic surveillance. Part essay and part science fiction, Cranch's article described how the narrator was put into a hypnotic trance by his cousin, "a powerful magnetizer." He takes a stroll in the country, where he is suddenly seized with a desire to climb a nearby tree. Once in the tree, he notices a humming from the telegraph wires passing through the branches. Placing his hands on the wires, he is astonished to discover that he is able to understand the Morse code message passing through the wires, evidently a result of the mesmeric trance. He vividly described a spider's web of telegraph wires running into the Tuileries in Paris, built with the express purpose of spying upon French citizens by the self-proclaimed Emperor, Louis Napoleon. In a sudden flash of insight that anticipated and foreshadowed WikiLeaks and Edward Snowdon by 155 years, Cranch imagines the technology being turned against the very government that deployed it:

> Then I thought, What a thing this discovery of mine would be for political conspirators--to reverse the whispering-gallery of Dionysius, and, instead of the tyrant hearing the secrets of the people, the people hearing the secrets of the tyrant![1]

---

[1] Cranch, C. P. "An Evening with the Telegraph Wires." *Atlantic Monthly* (September 1858): 490-494. A "whispering gallery" is an elliptical enclosure in which whispers uttered in one part of the space can be heard clearly in another location.

For most Americans in the early nineteenth century, privacy had more to do with proper social behavior and the protection of the domestic sphere from the unwanted gaze of strangers than with fears of government intrusion. Prohibitions against "eavesdropping" - literally, lurking about under the eaves to overhear conversations – had been part of Anglo-Saxon law as far back as the Middle Ages, and were incorporated into English common law which in turn was imported into early American legal practice. The villain in most eavesdropping scenarios in early nineteenth century America was not likely to be the federal government, but rather the town busybody or business competitor.[2]

As the telegraph came into wider use in the 1850s for business commerce and personal messages, it was recognized that opportunities for "eavesdropping" on the part of the operators sending the messages existed. A customer would typically write out a message on a paper blank, which was then handed to the operator for transmission. At the receiving end, the message would again be copied out onto a message blank as it was decoded. Thus there existed an opportunity for an operator to obtain information that was only intended for the recipient. New York passed an act in 1850 making it a misdemeanor for a telegraph operator to use or divulge the content of a telegraph message without the consent of the sender or the recipient; Pennsylvania passed a similar law the following year. Recognizing that an exception might exist where a telegraphic message might become evidence in a court of law, Pennsylvania passed another statute in 1855 that required telegraph companies not only to produce copies of messages when properly subpoenaed, but also to preserve copies of all messages sent and received for a period of three years.[3]

Telegraphers in those early years tended to resist legal remedies to the problem of "eavesdropping," regarding the issue as more one of professionalism and ethics than one requiring legal recourse. The noted telegraph engineer George Prescott, writing on

---

[2] For a detailed discussion of the evolution of privacy concerns in nineteenth century America, see Seipp, *The Right to Privacy in American History*.

[3] Crawford, Susan P. "Transporting Communications." *Boston University Law Review* 89 Rev. 871 (June 2009), 5; "The State v. Alden Litchfield," *American Law Register* 10 (1871), 379.

"Secrecy of Telegraphic Communications" in 1860, remarked that the "high sense of honor which every operator feels upon this point" was a sufficient deterrent to any potential abuse of the customer's private information, and no "oath of secrecy" and no "laws for the punishment of its violation" were needed.[4] But Prescott also acknowledged that cipher codes were already being employed by merchants, brokerage houses, and newspaper reporters, who saw a need to protect the privacy of their dispatches from competitors. Cipher codes involved the use of a dictionary of code words and numbers that could be substituted for entire phrases; in addition to hiding the actual content of a message, they increased the efficiency of transmission by substituting short codes for long phrases.

Mr. Lincoln's "Grand Telegraphic Descent"

In the U.S., the first use of electronic surveillance by the government was motivated by the exigencies of the approaching Civil War. April 1861 found Washington in a state of panic after the secession of the southern states and the attack on Fort Sumter. A pro-secession mob in Baltimore cut the telegraph lines linking Washington with the North, and the poorly defended national capital began to hastily prepare for an anticipated Confederate attack. A pro-Union militia took over the offices of the American Telegraph Company in Washington on 19 April, and ordered the operators to ignore messages from their fellow operators in Richmond.[5] The American Telegraph Company, a private company that dominated telegraph service in the eastern United States, with lines running from Maine to New Orleans, found itself in the peculiar position of maintaining telegraph offices in two hostile nations at war with one another.

Well aware that Confederate sympathizers in the North were using the still-functional wires of the American Telegraph Company to send intelligence on troop movements to the newly formed Confederate government, the federal government, with President Abraham Lincoln's approval, seized control of the telegraph lines running out of Washington on 20 April; a Mr. A. Watson of the War Department was appointed

---

[4] Prescott, *History, Theory and Practice of the Electric Telegraph,* 338.
[5] Harlow, *Old Wires and New Waves,* 261.

military censor, and given authority to inspect and approve all messages sent and received at the Washington office.[6] In the words of the *New York Times*,

> …we are reliably informed that the telegraph lines are now under Government *surveillance*—this last movement being rendered necessary in order to prevent the transmission of intelligence to the Southern traitors.[7]

The American Telegraph Company, under the direction of its president, Edwards S. Sanford, undertook a series of actions that affirmed its loyalty to the Union cause. Its telegraph wires were extended directly to the War Department, the Navy Yard, and the federal arsenal, enabling the federal government to not only monitor messages traveling over its lines, but also to send and receive military dispatches. Later a Military Telegraph Corps would be established for the express purpose of communicating between Washington and commanders in the field.[8]

On 20 May, the federal government, again with Lincoln's approval, took a further step and ordered U.S. Marshals to enter telegraph offices in major cities and seize copies of all telegrams sent and received in the previous year. The government did not disclose its reasons for this unprecedented seizure of private messages; according to the *New York Times*,

---

[6] Plum, *The Military Telegraph*, 64.

[7] "News of the Day" (*New York Times*, April 21, 1861).

[8] For good descriptions of the work of the Military Telegraph Corps, see Plum, *The Military Telegraph*, and Bates, *Lincoln in the Telegraph Office*. On 21 May 1861, the American Telegraph Company found a way out of its awkward position, and, not incidentally, put an end to its responsibility for 'leaks' of military intelligence, by having representatives of its northern and southern operations meet in the middle of the Long Bridge across the Potomac River and agree to sever the wires connecting North and South. An agreement was reached in which Edwards S. Sanford would continue to manage the company's northern interests, while Dr. William S. Morris, a major Southern stockholder, would take over management of the southern portion of the network, re-organized as the Southern Telegraph Company. See Thompson, *Wiring a Continent*, 374.

> It is supposed, however, that an examination of the telegrams will throw a flood of light upon the history of the Southern conspiracy, the length of time it has been actively at work, the material aid it has received from the North, and the names of many of those who have been implicated in it…[9]

Some argued that the seizure of telegrams was unconstitutional, a clear violation of the Fourth Amendment prohibition against unreasonable search and seizure, since the order lacked specificity about which telegrams were to be seized. Many feared abuses of the rule of law when telegraphic surveillance was combined with Lincoln's concurrent suspension of *habeas corpus*. In a Senate debate in December 1861, Senator Lyman Trumbull of Illinois exclaimed

> Why, sir, the power—without charge, without examination, without opportunity to reply, at the click of the telegraph—to arrest a man in the peaceable portion of the country and imprison him indefinitely, is the very essence of despotism.[10]

The number of telegrams seized was enormous—in Chicago alone, over 255,000 telegrams were seized.[11] It soon became clear that examining this vast volume of information, in an age when no automated data processing technology existed, would take a great deal of time. As days went by and no details were divulged by the government on the results of the seizure, some newspapers began to publish lurid and speculative accounts of what they imagined would be discovered. On 12 June, nearly a month after the seizures took place, the *Chicago Tribune* claimed that

> The developments that are likely to follow the seizure of the dispatches filed in the telegraph offices will astound the

---

[9] "Highly Important Movement. Seizure of Telegrams" (*New York Times*, May 22, 1861).
[10] *American Annual Cyclopedia*, 284.
[11] "The Telegraphic Seizures" (*Chicago Tribune*, May 29, 1861).

> country. They will show a system of treachery extending through all grades of official business and social circles. Almost everybody appears to have been engaged in giving aid and comfort to the rebels, and to have furnished means and information for securing a triumph of the rebellion.[12]

However, as time went on and no "system of treachery" was revealed, some began to mock the surveillance effort. *Vanity Fair*, a short-lived humor journal published in New York City, published a tongue-in-cheek piece ("The Grand Telegraphic Descent") in which they claimed that President Lincoln himself had requested their help in deciphering coded messages:

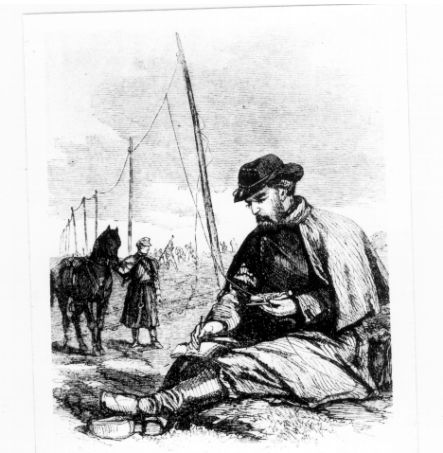
> While the valuable information thus secured has been studiously kept from the daily papers by order of Mr. LINCOLN, that gentleman has nevertheless sent us a few of the most important telegrams obtained in the grand seizure. This act of kindness on the part of Mr. LINCOLN (himself a wag of decided ability) rather overcomes us. It is a scathing refutation of the report that he was jealous of our brilliant and onward career as humorists.

The resident wits at *Vanity Fair* then proceeded to "decipher" a few allegedly seized telegrams. A message from a "J.D." in Memphis to a "Mr. Smithers" in New York, containing an arithmetic sum and the word "punkins," was decoded to reveal the hidden message, "Jeff Davis is sum punkins."[13]

It appears that little useful intelligence was obtained from the seizure of telegrams. James E. Harvey, a newly appointed Minister to Portugal who had been

---

[12] "Developments of the Seized Telegrams" (*Chicago Tribune*, June 12, 1861).
[13] "The Grand Telegraphic Descent: The Most Important of the Seized Dispatches" (*Vanity Fair*, June 1, 1861).



born in South Carolina but had taken up residence in the North, was briefly suspected of having telegraphed information to members of the secessionist government in Charleston, South Carolina, about federal efforts to reinforce Fort Sumter, but was later cleared of the charges.[14] It was discovered that a Southern sympathizer in the Washington office of the American Telegraph Company, a clerk named William Colwell (or Coldwell), had been passing information to the Confederate government; however, Colwell had gotten early warning of the seizure of the Washington telegraph office in April, and as a result had burned incriminating dispatches and absconded to Richmond.[15]

Figure 1. Using a pocket key, a Federal telegrapher taps into a Confederate wire near Egypt, Mississippi. Author's collection. From *Frank Leslie's Illustrated Newspaper*, 1865.

And, ultimately, it appears that the seizure of telegrams did little to stem the flow of useful military intelligence to the Confederacy. In July 1861, Lieutenant General Winfield Scott, commander of the Union army, complained that reports of troop movements telegraphed by reporters and printed in newspapers were sufficiently detailed to enable the enemy to anticipate his strategy; he issued an order on July 8, undersigned by Secretary of War Simon Cameron, forbidding the transmission of reports of troop movements by telegraph.[16]

The Civil War era marked a turning point in the growing public awareness of the significance of the new communications technology in the United States. Samuel Morse's offer to sell the rights to his invention to the government in 1845-6 had been rejected by the Polk administration, which failed to see the value in the new communications medium. However, a growing awareness of the strategic importance of the telegraph in uniting a geographically vast nation led to the passage of the Pacific

---

[14] "James E. Harvey" (*Chicago Tribune*, June 8, 1861); "The Case of James E. Harvey" (*New York Times*, August 6, 1861).
[15] "The Seizure of Telegraphic Dispatches" (*New York Times*, June 9, 1861); "News of the Rebellion" (*New York Times*," June 12, 1861).
[16] "Censorship of the Telegraph" (*Chicago Tribune*, July 10, 1861).

Telegraph Act in 1860, which authorized the building of a transcontinental telegraph line. But it was the ability of the telegraph to provide commanders with real-time information about the situation at the front during the Civil War that gave it great strategic importance, and prompted the federal government to seek more control over the network. Extensive use of the telegraph gave a tremendous advantage to the Union side in the Civil War, which used it far more effectively than the Confederacy. As the *Pittsburgh Evening Chronicle* for 9 May 1861 presciently noted, “This is a war of railroads and telegraphs—they are absolutely of more importance in this age than are cannon and musketry.”

Wiretapping as a means of obtaining military intelligence was widely practiced by both sides during the conflict. Wiretappers often used a portable device called a "pocket telegraph"; it consisted of a key and sounder in a waterproof case, small enough to be held in the hand. All the wiretapper had to do was to climb a telegraph pole, attach a wire to the line, and ground the instrument; he could then listen to all messages passing over the line, or send messages if he desired. To guard against such illicit interception of messages, both sides used elaborate cipher codes. The War Department in Washington not only generated ciphers for use by the Union army, but also undertook to decipher intercepted Confederate messages.[17]

There was little expectation of privacy on the part of either the general public or the telegraph companies for the duration of the conflict. It was assumed that military use of the telegraph network would take precedence over civilian use, and that military censors would monitor the network and prevent the transmission of information that would aid the enemy. There was no legal recourse for individuals who felt that their right to privacy had been compromised by surveillance or seizure of messages sent by telegraph.[18]

Western Union versus the Government

---

[17] Bates, *Lincoln in the Telegraph Office*, 49-85. See also Kahn, *The Codebreakers*, 214-220.

[18] Oliver, Wesley MacNeil. “Western Union, The American Federation of Labor, and the Changing Face of Privacy Advocates.” *Mississippi Law Journal* 81, Nr. 5 (2011): 975. http://www.olemiss.edu/depts/ncjrl/pdf/2011%20Symposium/8-%20Oliver_FINAL.pdf

However, perhaps inevitably, conflicts arose between the federal government and the telegraph companies after the cessation of hostilities in 1865. While Congress and the executive branch had grown accustomed to having the resources of the telegraph companies at their disposal for military purposes, the telegraph companies came to realize that customers expected them to protect the privacy of their messages. One telegraph company in particular, Western Union, having completed the transcontinental telegraph line during the Civil War, had become the dominant player in the telegraph business in the United States after the war. It consolidated its position by acquiring the lines and offices of its two principal rivals, the American Telegraph Company and the United States Telegraph Company, in 1866.

Demands by the federal government to hand over copies of messages sent by telegraph, and attempts by Western Union to resist doing so, figured prominently in a number of high-profile trials and Congressional investigations in the late nineteenth century. One of the first cases to test the limits of privacy in the post-Civil War era was the impeachment trial of President Andrew Johnson in 1868. Seizing upon Johnson's allegedly unconstitutional firing of Secretary of War Edwin M. Stanton, Senate Republicans pressed for a bill of impeachment to be brought forth in the House of Representatives in February 1868. A plot to save Johnson's presidency by bribing Republican senators was organized by New York City politician Thurlow Weed. When several senators changed their votes on Article XI impeachment charges at the last minute and voted for Johnson's acquittal on 16 May 1868, Benjamin F. Butler, the former Civil War general who had campaigned for his House seat on a promise to impeach Johnson, and had been appointed impeachment manager in the House, was furious; he ordered his network of private detectives to seize all evidence of corruption on the part of Weed and his associates.[19]

On 20 May, Butler called managers of the three telegraph companies in Washington before the House committee on impeachment and ordered them to turn over all telegrams sent or received by the alleged conspirators.

---

[19] For a detailed account of the impeachment trial of Andrew Johnson, see Stewart, *Impeached: The Trial of President Andrew Johnson.*

The Western Union Telegraph Company came under fire for cooperating with Butler's investigation. Protecting the privacy of its customers' messages was a fundamental argument used by the company in opposition to those who proposed a government-run telegraph system.[20] However, in the words of the *Nashville Tennessean*:

> If the Western Union Company do not propose to stand on their right to maintain the privacy of all messages, and test, up to the highest courts if necessary, this their duty as the confidential and trusted agents of the public, then one of the strongest practical objections to Governments owning a telegraph line will fall to the ground; for this outrage, by violation of rightful privacy, which a private telegraph company may prevent, or be punished for permitting, a Government could commit with secresy[sic] and impunity.[21]

A case in which telegraphic evidence figured prominently, and Western Union, perhaps chastened by the negative publicity resulting from its cooperation with the Butler investigation, attempted to resist obeying a subpoena, was the government investigation of the "Whisky Ring" in 1875-6, one of the many scandals of the Ulysses Grant administration. The Whisky Ring began in 1871 as an attempt to covertly fund the Republican campaigns of Ulysses Grant and his supporters in Missouri by illegally distilling and selling whisky without reporting the transactions to revenue agents. Once Grant was safely re-elected in 1872, however, the co-conspirators, including Orville

---

[20] Telecommunications services were always provided by private industry in the U.S. in the nineteenth and twentieth centuries, unlike most other countries, where government-run posts, telegraphs, and telephone services existed. For this reason, the history of the U.S. telecommunications industry provides a unique opportunity to study the relationship between government and industry as privacy concerns emerged. For Western Union's position on privacy and government ownership of the telegraph network, see John, *Network Nation,* 140-144.

[21] "Private Telegrams" (*Nashville Tennessean*, May 27, 1868).

Babcock, Grant's private secretary, and John McDonald, revenue agent in St. Louis, abandoned any pretense at political activity and used the proceeds to enrich themselves, confident that Babcock's position as Grant's private secretary would protect them from disclosure.[22]

In the summer of 1875, indictments were brought against most of the conspirators after a grand jury investigation. Only Babcock escaped indictment, due to his close ties to Grant. However, as evidence of his involvement grew, he too was indicted in December 1875.[23] A trial date was set for February 7, 1876, in St. Louis. Critical pieces of evidence were several telegrams which had been exchanged between John McDonald and Orville Babcock, signed by "Sylph." Prosecutors alleged that the telegrams were coded messages sent by Babcock to McDonald in St. Louis, warning him of possible visits by government investigators, and letting McDonald know when Babcock had succeeded in obstructing the investigation. One message was particularly damning; it read, "I succeeded. They will not go. I will write you." ("Sylph" was later alleged to be the nickname of Babcock's former mistress, and was used as a code word in the telegraphic communications.) A handwriting expert, viewing the original written text of the telegram, declared that it had been written by Babcock.[24]


Figure 2 William Orton

In order to obtain the telegrams, government investigators had issued a *subpoena duces tecum* upon William Orton, President of Western Union, ordering him to produce all telegrams exchanged between Babcock and the other conspirators, under a variety of signatures, over a period of eight months. The *subpoena duces tecum* (subpoena for production of evidence) was frequently used by the government in the late nineteenth century as a legal basis for ordering telegraph companies to turn over messages as part of an investigation. Laws existed in many

---

[22] Timothy Rives, "Grant, Babcock, and the Whiskey Ring," *Prologue Magazine*, Vol. 32, No. 3 (Fall 2000), http://www.archives.gov/publications/prologue/2000/fall/whiskey-ring-1.html

[23] Ibid.

[24] Ibid.; "The Whisky Ring Trials," *New York Times*, November 30, 1875.

states that forbade telegraph companies from disclosing the content of telegraphic messages to anyone but the intended recipient; only Missouri, Indiana, and Pennsylvania had laws that specifically allowed the content of telegrams to be disclosed when requested by a court.[25]

Western Union's attorney appeared in United States Circuit Court in St. Louis on February 1, 1876, with a motion to vacate the subpoena, stating that the subpoena lacked specificity, and did not even demonstrate that the telegrams actually existed and were in the possession of Western Union.[26] The presiding judge, however, simply overruled the motion, and ordered the telegrams to be placed in evidence.[27] The fact that Missouri had a statute on the books allowing telegrams to be disclosed as part of a legal proceeding considerably weakened Western Union's position. While Babcock was acquitted, he was forced to resign as Grant's secretary. After being embroiled in another of the Grant administration scandals, he was appointed Superintendent of Public Buildings and Inspector of Lighthouses by Grant, ever loyal to his subordinates. While performing his duties as lighthouse inspector, Babcock drowned near Daytona Beach, Florida, in 1884.

In 1876, events would bring the United States Congress and Western Union to a dramatic confrontation over the issue of the privacy of telegraphic communications that played out on the front pages of the nation's leading newspapers. The presidential election of November 1876 yielded an uncertain outcome, with neither Democrat Samuel J. Tilden nor Republican Rutherford B. Hayes able to claim victory. While Tilden won a clear majority of the popular vote nationwide, the outcome would rest on the electoral results from four states—South Carolina, Florida, Louisiana, and Oregon—where allegations of impropriety in the counting of returns, and highly partisan attempts by both parties to disqualify large numbers of ballots led to a situation where two sets of electors, one claiming victory for Tilden, the other for Hayes, were appointed in each of

---

[25] Oliver, "Western Union," 976.
[26] Oliver, Wesley MacNeil. "America's First Wiretapping Controversy in Context and as Context," *Hamline Law Review* 34 (Spring 2011): 8.
[27] "The Whisky Ring Trials," *New York Times*, February 2, 1876.

the four states. Congress was left with the byzantine task of sorting out which set of electors to recognize from each state.[28]

A special House committee, headed by Democrat William R. Morrison from Illinois, headed to New Orleans in early December 1876 and began to investigate charges that Democratic voters in Louisiana had been threatened and harassed, and that fraudulent vote counts were made by the all-Republican returning board, headed by former Louisiana Governor Madison Wells. (Wells, it was later reported, offered to sell Louisiana's electoral votes to whichever party was the highest bidder.) One of Morrison's first actions was to issue a subpoena ordering Edmund Barnes, the manager of the New Orleans Western Union office, to appear before his committee and produce telegrams exchanged between the Republican Governor, William P. Kellogg, and the national Republican Party leadership.

Barnes, following instructions from Western Union president William Orton, refused to appear, citing his Fourth Amendment rights. The committee responded that while telegraph companies had an interest in protecting the privacy of their messages, this did not outweigh "the superior claim which society has upon the testimony of all its members when essential to the proper administration of justice."[29]

On 15 December, Orton himself responded to the subpoena by refusing to permit Western Union employees to appear before Morrison's committee, protesting that "the officers and agents of the company have been commanded to lay aside the business in which they are engaged, and become spies and detectives upon and inform against the customers who have reposed in us the greatest confidence concerning both their official and private affairs." He pointed out that political damage for both Republicans and Democrats could result from the release of the subpoenaed telegrams: "If the messages of persons connected with one political party are spread before the public, a like course will be taken in respect to those of the other party. Both parties, therefore, have the same interest in publishing to the world the secrets of the telegraph offices, or of preventing such publicity." In closing, however, Orton sounded a more conciliatory note

---

[28] Morris, *Fraud of the Century*, 200-201.

[29] Oliver, "America's First Wiretapping Controversy in Context and as Context," 9.

by conceding that he would be forced to obey the committee's subpoena, if the full House approved it.[30]

On 19 December, Orton received a summons from Samuel J. Randall, Democratic Speaker of the House, ordering him to appear before Morrison's committee in New Orleans with all telegrams requested by the committee relating to the alleged vote counting fraud in Louisiana. On the same day, Orton received a subpoena from Oliver P. Morton, Republican chairman of the Senate Committee on Privileges and Elections, ordering him to appear before that committee and produce telegrams related to the situation in Oregon, where it was alleged that Democrats had paid $8000 to secure an additional electoral vote for Tilden. Orton's response on 23 December to both was similar; he stated that he personally did not possess or have any knowledge of the content of the requested telegrams, and he requested to be excused from appearing before either committee, pleading illness as reason for not appearing in New Orleans.[31] When Orton failed to appear as requested, the committee voted to hold him in contempt, not only for failing to appear, but also for instructing Barnes to refuse to testify.[32] Speaker of the House Randall then issued a subpoena upon the entire Executive Committee of Western Union, ordering them to appear before the House committee and produce the requested telegrams, or face imprisonment.[33]

On 19 January the Executive Committee finally agreed to release the requested telegrams, about three thousand in number, and allow subpoenaed telegraphers to testify, in exchange for being released from the subpoena. There was some debate about how to distribute the requested telegrams. It was decided that that separate packages of telegrams would be prepared and turned over to the House committee and

---

[30] "Refusal of Western Union Orton to Give Up Important Dispatches," (*Nashville Tennessean*, December 16, 1876).
[31] "Orton: He Asks to be Excused from Testifying before the Louisiana Committee" (*Nashville Tennessean*, December 26, 1876.)
[32] "The House Inquiry—Persecution of Democratic Voters" (*Baltimore Sun*, December 27, 1876).
[33] Ibid.; "Mr. Randall on the Telegraph Question," (*Baltimore Sun*, December 27, 1876).

the Senate committee separately, though Western Union officials protested that it would take considerable time to locate and release the requested telegrams.[34]

However, the fraud investigations fell by the wayside as public pressure mounted to end the stalemate and declare a winner. Unable to resolve the political deadlock, the House and Senate committees agreed in early January 1877 to appoint members of a fifteen-member independent Electoral Commission, which would decide which candidate would be inaugurated as President. With eight Republican votes to seven Democratic votes, the selection of Hayes was virtually guaranteed. All the contested electoral votes were awarded to Hayes, and on Friday, 2 March 1877, Rutherford B. Hayes, then on a train outside of Harrisburg, Pennsylvania, was handed a telegram announcing that he had been elected President.[35]

The fraud issue was revived in October 1878, when the *New York Tribune* published a series of coded telegrams sent by operatives of the Democratic Party that proved beyond a shadow of a doubt that the Democrats had conspired to purchase electoral votes, probably with the full knowledge of Tilden; the full text of the "cipher telegrams," as they came to be called, was published in many newspapers, including the *Chicago Tribune* for October 21, 1878.[36] While the *New York Tribune* refused to divulge the source of the cipher telegrams, it was widely assumed that they had been among the telegrams turned over to the Congressional committees by Western Union.

While the controversy over the subpoenaed telegrams ultimately did little to affect the outcome of the 1876 election, it served to re-awaken interest in the issue of telegraphic privacy. In 1880, Western Union scored a small tactical victory in a Criminal Court case in Missouri in which the company had been ordered to turn over a large number of telegrams sent over a fifteen-month period as part of an investigation into a gambling ring.[37] While an appellate court upheld the subpoena request from the lower court, the Missouri Supreme Court reversed the decision, ruling that requests for

---

[34] "Washington" (*Louisville Courier Journal*, January 20, 1877).
[35] Morris, *Fraud of the Century,* 212-239.
[36] "The Cipher Telegrams: Analysis Showing the Depravity of their Authors" (Chicago Tribune, October 21, 1878.) For a detailed description of the technique used to decipher the telegrams, see Kahn, *The Codebreakers*, 221-9.
[37] "Ex Parte Brown, 72 Mo.," *American Law Register* 20, (1881), 423-4.

telegrams had to be more specific. In closing, the state Supreme Court's ruling asserted that

> …To permit an indiscriminate search among all the papers in one's possession for no particular paper, but some paper, which may throw some light on some issue involved in the trial of some cause pending, would lead to consequences that can be contemplated only with horror, and such a process is not to be tolerated among a free people.[38]

The decision of the Missouri Supreme Court in *ex parte Brown* represented a significant victory for Western Union in protecting the privacy of telegraphic communication. The requirement for specificity in subpoena requests established by the *ex parte Brown* case in Missouri became the standard by which such requests were reviewed in other states for the remainder of the nineteenth century, creating a recognized basis for protecting the privacy of telegraphic communications.

The Right to Privacy

In 1890, Samuel Warren and Louis Brandeis published their landmark essay, "The Right to Privacy" in the *Harvard Law Review*. Not only did this essay affirm that a legal right to privacy existed, but also that technological change necessitated changes to the law:

> Political, social, and economic changes entail the recognition of new rights, and the common law, in its eternal youth, grows to meet the new demands of society.[39]

---

[38] Oliver, "America's First Wiretapping Controversy," 10-11.

[39] Brandeis, Louis, and Samuel Warren. "The Right to Privacy," *Harvard Law Review* IV, no. 5 (December 15, 1890): 1. http://groups.csail.mit.edu/mac/classes/6.805/articles/privacy/Privacy_brand_warr2.html One of the motivating factors behind the publication of "The Right to Privacy" was a series of gossipy

Publication of “The Right to Privacy” reflected the impact that modern communications technology had had on the whole idea of privacy. In an earlier age, the town gossip might spread one’s personal information from one end of the town to the other; with the advent of the telegraph, the telephone, and mass-scale printing, details of one’s personal life, whether true or false, could be spread across the entire globe in a matter of minutes.

“The Right to Privacy” also reflected the newly emerging view of personal privacy as a right protected by the Constitution. This new conceptualization of privacy had legal ramifications. While one’s personal information was intangible, it had value; unwanted disclosure of one’s personal information could damage a person’s reputation, social standing, and ability to earn a livelihood. The Fourth Amendment, which had previously been interpreted as protecting only tangible private property, came to be seen as protecting individual privacy as well. The debates over the seizure of telegraphic messages contributed to this changing conceptualization by shifting the focus from the paper on which the message was written to the message itself.

“The Right to Privacy” does not specifically address how the law should be changed as it relates to new technologies, although the telegraph and the telephone were both in widespread use at the time of its writing. Sorting out those issues would take the better part of the twentieth century, and continue into the present, with the development of the Internet.

World War I and the American Black Chamber

By the late nineteenth century, the entire inhabited globe was connected by telegraph cables. Completion of the first successful transatlantic undersea telegraph cable on 27 July 1866 put North America in direct contact with England and Europe, and added an international dimension to the U.S. telegraph network. In November of the same year, U.S. Secretary of State William Seward sent the first diplomatic dispatch

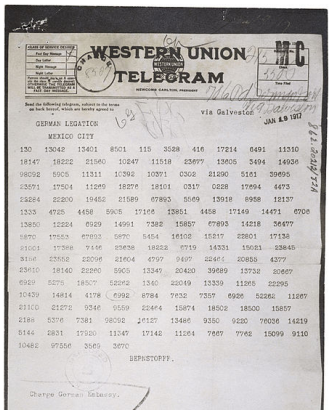
---

newspaper articles about Warren, his wife, and their extended families that Warren felt invaded their personal privacy.

over the new cable. Dispatches that formerly had taken weeks to cross the Atlantic now could be sent, and a reply received, in a matter of minutes.[40]

Western Union controlled access to the transatlantic telegraph cable when it merged with the American Telegraph Company in 1866. A second transatlantic cable was completed in 1883-4 by the Commercial Cable Company, a subsidiary of the Postal Telegraph Company, a Western Union competitor. Twenty years later, in 1903, the Commercial Cable Company's transpacific cable connected the west coast of the U.S. with Asia by means of an island-hopping route via Hawaii, Midway Island, and Guam.[41]

International diplomatic and military dispatches, which formerly had been carried by couriers aboard ships for overseas delivery, now could be sent via telegraph in a matter of minutes. The international telegraph cable network proved particularly useful to the U.S. Navy Department, which was in the process of expanding its fleet as the U.S. emerged as a world power in the late nineteenth and early twentieth centuries. The Navy Department used the cable network to send orders to ships in ports around the world, and receive reports form them quickly. Given the sensitive nature of such correspondence, elaborate cipher codes were developed to prevent unwanted disclosure. Both the U.S. State Department and the Navy Department set up code rooms in Washington to encode messages to be transmitted overseas, and decode incoming messages.[42]


WESTERN UNION TELEGRAM

GERMAN LEGATION
MEXICO CITY

via Galveston JAN 19 1917

BEPSTOFFF.

Figure 3. Zimmermann Telegram, 1917. From U.S. National Archives, 862.20212/82A (1910-1929); General Records of the Department of State; Record Group 59.

U.S. attempts to remain neutral in the first World War ended in the spring of 1917 when it was revealed that German Foreign Minister Arthur Zimmermann had sent a cipher telegram to the German Minister to Mexico, offering financial assistance and portions of U.S. territory to Mexico in exchange for Mexico entering the war on the German side. Ironically, the telegram had been delivered to Mexico City via

---

r the Wire, 169-70.

[41] Prior to the completion of the 1903 transpacific cable, telegrams from North America to Asia had to be sent over the transatlantic cable to England, and from there by landline to Asia, a long and expensive route. See Harlow, *Old Wires and New Waves*, 424-434. Australia had been connected to Asia via undersea cables since the 1870s.

[42] Yardley, *The American Black Chamber*, 1-7; Kahn, *The Codebreakers*, 252-4.

Washington, DC, and Galveston, Texas, using Western Union's cable service, under an agreement the U.S. Government had made with Germany after the British cut the German undersea cables in 1914.[43]

The telegram had been intercepted and deciphered by British intelligence and given to President Woodrow Wilson in February 1917, leading to America's entry into the war in April 1917. The realization that the U.S. did not have the sort of capability possessed by the British and other European nations to intercept and decipher coded messages led to the establishment of a cryptographic bureau by the War Department, called Military Intelligence Department Section 8, or MI-8. For the duration of the conflict, MI-8 would be called upon to decipher messages from suspected spies as well as diplomatic messages sent by nations suspected of aiding the Germans. The sort of privacy issues raised in the late nineteenth century did not apply, since the government had nationalized the telegraph companies during the war, and provisions of the wartime censorship laws gave the State Department access to messages carried by the telegraph and cable companies.[44]

MI-8 also engaged in surveillance of individuals suspected of spying for the Germans. Brigadier General Marlborough Churchill, the head of MI-8 in 1918, recruited Alice Roosevelt Longworth, former President Theodore Roosevelt's daughter, to spy upon an acquaintance of hers, May Ladenburg, who was suspected of providing intelligence to the Germans. Alice, already noted for her unconventional behavior, clearly relished her role as undercover agent; she not only passed information along to General Churchill's staff, but also suggested locations for planting listening devices in Ladenburg's residence. The bugging operation, relatively sophisticated for the age, enabled conversations to be recorded directly using dictograph equipment. On one occasion, Alice Longworth wrote that she

Figure 4. Alice Roosevelt Longworth, c1918. Source: Library of Congress, Prints & Photographs Division, photograph by Harris & Ewing, LC-USZ62-137272

---

[43] Nickles, *Under the Wire*, 137-160.

[44] "The Many Lives of Herbert O. Yardley," *National Security Agency*, no date, 5-6. http://www.nsa.gov/public_info/_files/cryptologic_spectrum/many_lives.pdf.

joined “three or four absolutely charming” military intelligence personnel in listening in on “a most enchanting conversation” between Ladenburg and her lover, Bernard Beruch, chair of Woodrow Wilson’s War Industries Board.[45]

Figure 5. General Marlborough Churchill, Head of MI-8. Source: Library of Congress b/w negative LC-USZ62-100783

The code and cipher section of MI-8 was headed by Herbert O. Yardley, a former telegrapher and cryptologist for the State Department. Yardley brought many of his former co-workers with him from the State Department. MI-8 gained considerable experience and skill from its interactions with the British and French intelligence agencies during wartime.[46]

After the armistice in 1918, MI-8, having accomplished its purpose, was demobilized. However, officials in the War, Navy, and State Departments had come to the conclusion during the war that “in no other manner could the United States obtain an intimate knowledge of the true sentiments and intentions of other nations. They recognized that all the Great Powers maintained Cipher Bureaus, and that if the United States was to be placed on an equal footing it would be necessary to finance a group of skilled cryptographers.” Funding for a covert operation to intercept and decode diplomatic dispatches was obtained from both the State Department and the War Department.[47]

Herbert Yardley was appointed to be head of the clandestine operation in 1919, which he patterned after the “Cabinet Noir” operated by French Intelligence before the war. As State Department regulations forbade funding such activities in the District of Columbia, headquarters of “The American Black Chamber,” as the operation came to be called, were set up in a brownstone front at 3 East 38th Street in Manhattan, just off 5th Avenue. Posing as a private company specializing in cipher codes for

---

[45] Cordery, *Alice*, 269-70; see also Egerton, George, “Diplomacy, scandal, and military intelligence: the Craufurd-Stuart affair and Anglo-American relations 1918-1920.” *Intelligence and National Security*, vol. 2 nr. 4 (1987): 110-114.
[46] Yardley, *The American Black Chamber*, 15-160.
[47] Ibid., 166-7.

commercial businesses, the Black Chamber began its work of routinely intercepting and decoding diplomatic dispatches, on orders from the State and War Departments.[48]

One of the first assignments undertaken by the Black Chamber cryptographers was the decoding of messages sent by the recently formed Soviet government in Russia. During the era of the "Red Scare" and the investigations of Attorney General A. Mitchell Palmer, there was great concern in the U.S. at the time that the Soviets were trying to foment revolution in other countries by recruiting agents. Probably the most significant effort of the Black Chamber, however, was the decoding of the cipher codes used by the Japanese diplomatic corps, which revealed the strategy of the Japanese to increase their military presence in Asia and the Pacific. This effort gave American diplomats advance knowledge of the Japanese position on military strength and armaments in preparation for a disarmament conference to be held in Washington in 1921-2.[49]

The activities of the Black Chamber were ordered terminated in 1929 by President Herbert Hoover's Secretary of State, Henry L. Stimson, who famously said that "gentlemen do not read each other's mail."[50] Suddenly finding himself without employment, Yardley published *The American Black Chamber*, a lurid and melodramatic exposé of the operation, in 1931. Mixing code breaking details with tales of spy-versus-spy derring-do and mysterious *femme fatale* operatives, the book was an instant success. However, like Edward Snowden many years later, Yardley was accused of betraying his country by revealing state secrets. The revelation that the Black Chamber had deciphered the diplomatic codes of nineteen foreign nations created an international furor. While the U.S. government briefly considered prosecuting him, technically he had not committed any crime, since there was no law on the books at the time prohibiting disclosure of foreign diplomatic codes.

The Telephone, Wiretapping, and the Police

---

[48] "The Many Lives of Herbert O. Yardley," 7.
[49] Yardley, *The American Black Chamber,* 166-224.
[50] Kahn, *The Codebreakers*, 360.

In the late nineteenth and early twentieth centuries, issues of communications privacy began to emerge around a new communications technology—the telephone. Unlike a telegram, a telephone conversation left no written record; the only way for a third party to learn the content of a conversation was to tap the wires, and listen to the conversation as it took place.

The New York Police Department began wiretapping the telephone conversations of persons suspected of criminal activity in 1895. A wiretap center was set up in an office building at 50 Church Street in lower Manhattan. With the full cooperation of the New York Telephone Company, capabilities were provided to enable the police to listen in on any telephone call in New York City. As they did not possess recording capability, members of the wiretapping squad took written notes of the conversations they overheard.[51]

An 1881 New York law forbidding tapping telegraph lines had been amended in 1895 to cover telephone wiretaps as well, but it was unclear if the law allowed an exception for law enforcement. Unsure of the legality of their operation, and fearful that the public would react negatively if they knew of its existence, the police kept their wiretaps secret. Evidence obtained through wiretapping was never presented in court, as that would have revealed the existence of the operation. The New York Telephone Company eventually developed qualms about the legality of the wiretaps, and began to require written authorization from the Commissioner of Police for each call to be monitored.[52]

Existence of the wiretapping program was revealed to the general public in 1916 when New York City Mayor John Purroy Mitchel ordered the telephone calls of a Catholic priest monitored after the priest had accused Mitchel of anti-Catholic bias in an investigation of orphanages run by the Catholic church. One of the police wiretappers was a Catholic, and, feeling guilty about wiretapping a priest, told a State Senate committee investigating public utilities about the wiretapping program. The Police Commissioner, Arthur Woods, and the general counsel for the telephone company were

---

[51] Oliver, “America’s First Wiretapping Controversy,” 14-15.
[52] Ibid.

called before the committee to testify about the practice, and the resulting publicity generated great public outrage. Many questioned the constitutionality of the wiretap; the Catholic bishop of New York protested that the wiretapping was "about the most outrageous offense on the constitutional rights of the people that has ever been committed here."[53]

While the mayor lost his bid for re-election due to the scandal, the Police Commissioner emerged largely unscathed, due to the fact that Senate committee members accepted his highly improbable rationale that he believed he had been investigating criminal activity on the part of the priest. As a result, the Police Department continued its program of wiretapping. One revelation that emerged from the investigation was that wiretaps had been ordered not only by local authorities, but also by the federal government on occasion. The telephones of a New York firm, Seymour & Seymour, had been tapped and their calls recorded, evidently on suspicion that the firm's involvement in munitions sales to foreign countries violated the Neutrality Act in place before the U.S. entered the war on the side of the Allies. While no federal official would take responsibility for having ordered the wiretap, the U.S. District Attorney finally admitted knowledge of the shadowy investigation, and confirmed that the New York Police Department had been involved.[54]

As with the cases involving the telegraph, it was observed once again that no federal court had ruled on the constitutionality of communications privacy. The first case to be tried before the Supreme Court regarding communications privacy was Olmsted v. United States, heard in 1928. Ray Olmsted, a Seattle bootlegger, was convicted of illegal importation and sale of alcohol based on evidence obtained by tapping his telephone without a search warrant. When the case was heard before the Supreme Court, his conviction was upheld by a slim five-to-four majority. Chief Justice William Howard Taft, writing the majority opinion, stuck to the traditional nineteenth-century view of the Fourth Amendment as only protecting property, and ruled that since no property was seized, no violation of Fourth Amendment rights took place.

---

[53] Ibid., 17.

[54] "Congressman Loft Calls for House Inquiry into the Seymour Wiretapping Case," *New York Times,* May 20, 1916; "Police Head's Testimony," *New York Times*, May 20, 1916.

The dissenting opinion was written by Louis Brandeis, who had been appointed to the Supreme Court in 1916. Echoing the views he had expressed in the *Harvard Law Review* in 1890, Brandeis argued that there is a constitutionally protected right to be left alone, and that wiretapping was just another form of coerced confession: "Discovery and invention have made it possible for the Government, by means far more effective than stretching upon the rack, to obtain disclosure in court of what is whispered in the closet." Looking toward the future of technology, Brandeis predicted that

> The progress of science in furnishing the government with means of espionage is not likely to stop with wiretapping. Ways may some day be developed by which the Government, without removing papers from secret drawers, can reproduce them in court, and by which it will be enabled to expose to a jury the most intimate occurrences of the home.[55]

Only six years later, the Communications Act of 1934 prohibited wiretapping without a search warrant, validating Brandeis's dissent and effectively reversing the Supreme Court's decision in Olmsted v. United States. Based on a technically dubious provision of the Radio Act of 1927 that forbade the "interception" and "divulgence" of radio broadcasts, the Communications Act of 1934 extended the prohibition to telephone and telegraph communications and thereby created a national standard that applied to all forms of electronic communication.[56]

However, the ban on wiretaps was not destined to last long. President Franklin Roosevelt authorized the Federal Bureau of Investigation to perform domestic telephone wiretaps in the interest of national security as the second World War approached in 1940. The 1934 Communications Act was circumvented through a

---

[55] Lepore, Jill, "The Prism," *New Yorker*, June 24, 2013, 36.
[56] Seipp, *The Right to Privacy in American History*, 104, 110.

language technicality; while the FBI might “intercept” communications, as long as it did not “divulge” what it learned, it was in compliance with the law.[57]

World War II, Enigma, and SHAMROCK

At 1:28 AM on the morning of 7 December 1941, a U.S. Navy receiving station on Bainbridge Island off the coast of Washington state intercepted a coded radio message from Tokyo to the Japanese embassy in Washington DC. The text of the encoded message was sent to the office of the Navy’s cryptologic organization, OP-20-G, in Washington DC. There it was decrypted and sent to the Signal Intelligence Service of the U.S. Army, which translated the decrypted message from Japanese to English. When the translated message was returned, Lieutenant Commander Alwin D. Kramer, the officer in charge of Navy cryptology, realized its import. The Japanese had rejected American offers of negotiation, and war was about to begin. Kramer immediately left the Navy Department building and ran towards the State Department building, to deliver his message to the Secretary of State. In a matter of hours, the Japanese attack on Pearl Harbor in Hawaii would begin.[58]

The termination of the Black Chamber in 1929 had not ended U.S. attempts to intercept and decode military and diplomatic correspondence. Despite Secretary Stimson’s protests, the U.S. Army had continued the work of the Black Chamber in intercepting diplomatic messages as part of its Signal Intelligence Service; the Navy had developed a parallel effort, OP-20-G, in the 1920s, which focused primarily on monitoring naval dispatches. Advances in technology had changed both the way in which messages were sent, and the techniques for encoding and decoding them. Confidential messages were often sent by radio, and elaborate mechanical devices were used to encrypt them. The Japanese were unaware that the American cryptologists had cracked their diplomatic code and were able to read their messages in 1941. For the remainder of the war, Allied and Axis cryptologists battled to decipher each other’s messages, often encrypted using variations of the German Enigma

---

[57] Ibid., 111; “Intelligence Activities and the Rights of Americans,” *Book II, Final Report. Senate Report No. 94-755*, 94th Congress, Second Session, April 26, 1976, 36.
[58] Kahn, *The Codebreakers*, 1-4.

machine, which had proven so popular among cryptologists that both sides employed it.[59]

After World War II, a new secret surveillance program, codenamed Project SHAMROCK, was begun by the Army Security Agency, later part of the U.S. Armed Forces Security Agency. Microfilmed copies and paper tapes of all telegraphic dispatches entering or leaving the U. S. were obtained from the three telegraph companies with international capability—Western Union, the Radio Corporation of America (RCA), and International Telephone and Telegraph (ITT), and delivered to an office located in New York City. If, on initial review, the dispatches were found to contain material of interest to other U.S. intelligence agencies, they were passed on to the FBI, the CIA, the Secret Service, the Bureau of Narcotics and Dangerous Drugs, or the Department of Defense.[60]

In 1952, concerns that the Armed Forces Security Agency had failed to coordinate its activities with other government agencies led to the creation of a new organization, the National Security Agency, or NSA. The new agency was so shrouded in secrecy that few in government knew of its existence. Even the executive order creating the agency, signed by President Harry Truman, was classified. Responsibility for Project SHAMROCK was transferred to the NSA.

After the introduction of computer technology, the microfilmed telegrams were transferred to magnetic tape, and delivered to a processing facility at Fort Meade, Maryland. As many as 150,000 messages per month were intercepted and analyzed by the NSA. Since many of the telegrams intercepted were sent or received by U.S. citizens, the surveillance was clearly in violation of the 1934 Communications Act prohibition of warrantless surveillance. In addition, a Supreme Court ruling in the 1967 case of Katz v. United States had finally stated explicitly what Louis Brandeis had argued in his 1928 dissent—that intangibles such as individual privacy were protected

---

[59] For the story of Enigma and its use during World War II, see Kahn, *The Codebreakers,* 421-613.
[60] Nate Anderson, "How a 30-year-old lawyer exposed NSA mass surveillance of Americans—in 1975," *ArsTechnica*, June 30, 2013. http://arstechnica.com/tech-policy/2013/06/how-a-30-year-old-lawyer-exposed-nsa-mass-surveillance-of-americans-in-1975/.

by the Fourth Amendment, and that warrantless electronic surveillance constituted a violation of individual privacy.[61]

Project SHAMROCK apparently ran for almost 30 years with essentially no oversight. According to a 1975 interview with former NSA Deputy Director Dr. Louis Tordella, President Harry Truman was told of the existence of the project when the NSA was formed in 1952, but in the next 20 years only one Secretary of Defense was briefed on its activities. Due to the secrecy surrounding the project, it was not even clear what the initial purpose of the project was, although it was assumed that it involved surveillance of individuals in Soviet bloc countries as the U.S. entered the Cold War period. The program was finally discontinued in May 1975 on order of Secretary of Defense James Schlesinger.[62]

The activities of Project SHAMROCK came to light as part of the hearings held in 1975-6 by the U.S. Senate Select Committee to Study Governmental Operations with Respect to Intelligence Activities, headed by Idaho Senator Frank Church. The committee's investigation into illegal surveillance activities was initially a response to the revelations surrounding President Richard Nixon's use of government resources to spy on political enemies. In the course of its investigation, however, the committee uncovered a wide range of illegal activities on the part of various government agencies, including both physical and electronic surveillance.[63]

The Church Committee called for sweeping reforms in the laws covering domestic surveillance, and increased oversight of the federal agencies involved. While the Supreme Court decision in Katz v. United States prohibited warrantless surveillance of U.S. citizens, it left unclear what powers the executive branch of government might have regarding gathering of foreign intelligence relating to national security. As a result, the U.S. Congress passed the Foreign Intelligence Surveillance Act (FISA) in 1978, which established the rules for gathering foreign intelligence information communicated between "foreign powers" and the "agents of foreign powers," especially where

---

[61] Ibid.

[62] "Senate Unit Says Cable Companies Aided in Spying," *New York Times*, November 7, 1975.

[63] For the full findings and recommendations of the Church Committee, see "Intelligence Activities and the Rights of Americans."

American citizens were involved. FISA explicitly prohibited the sort of warrantless mass collection of messages sent and received by U.S. citizens that had been done as part of Project SHAMROCK, unless there was probable cause to suspect that U.S. citizens were acting as "agents of foreign powers," in which case a court order permitting the surveillance had to be issued by a secret FISA court.[64]

The NSA and FISA: Finding the terrorist needle in the metadata haystack

The development of the Internet in the late twentieth and early twenty-first centuries raised new issues around privacy and electronic surveillance. In the aftermath of the 9-11 attacks on the World Trade Center in New York City in September 2001, the NSA, with the approval of the administration of President George W. Bush, began a program to collect both content and what was called "metadata" on telephone calls and e-mails in order to gain intelligence on suspected terrorist plots organized by foreign terrorist organizations. Metadata was defined as information about the calls and e-mails, such as phone numbers and Internet addresses, rather than the actual content of phone conversations and e-mails; it was believed that analysis of the metadata would enable investigators to trace a series of messages back to a foreign terrorist source. Since some of the calls and e-mails might be initiated by U.S. citizens, the law required a court order from the FISA court before such data could be collected. However, the Bush administration decided to circumvent the FISA court, arguing firstly that FISA court approval would take too much time; and secondly, that the powers granted to the executive branch by Congress's declaration of war against Al Qaeda on 14 September 2001 gave the President the authority to conduct such searches in the interest of national security. Under what was called the President's Surveillance Program, the NSA began collecting the data with the cooperation of three telecommunications companies, AT&T, Verizon, and BellSouth, during October 2001. On 31 October, the name of the program was officially changed to STELLARWIND.[65]

---

[64] "Foreign Intelligence Surveillance Act of 1978," *Public Law 95-511*, October 25, 1978. http://www.gpo.gov/fdsys/pkg/STATUTE-92/pdf/STATUTE-92-Pg1783.pdf

[65] Ryan Lizza, "State of Deception," *New Yorker*, December 16, 2013, 51-2.

On 16 December 2005, an article in the *New York Times* revealed the existence of the program to the general public. The revelation that the NSA had begun a secret program that included monitoring the calls and e-mails of U.S. citizens initiated a review of the laws covering such surveillance by the Department of Justice and Congressional committees. As a result, beginning in 2006, amendments were added to the FISA act to grant the president additional authority to authorize electronic surveillance, and the "business records" portion of Section 215 of the Patriot Act, passed in 2001, was invoked to justify the mass collection of telephone and Internet metadata.[66]

In a white paper published in August 2013, the Obama administration defended the need for bulk collection of telephone metadata by arguing that "courts have held that the relevance standard permits requests for the production of entire repositories of records, even when any particular record is unlikely to directly bear on the matter being investigated, because searching the entire repository is the only feasible means to locate the critical documents." In support of this argument, the white paper made a technically dubious comparison with a computer hard drive, citing a case in which "seizure and subsequent off-premises search of the computer and all available disks" provided a "sufficient chance of finding some needles in the computer haystack," while blithely ignoring the fact that in the case cited a search warrant had been obtained.[67]

The release of classified NSA documents by former NSA computer specialist Edward Snowden in June 2013 confirmed many details of STELLARWIND, including the fact that many in the government were unsure of the legality of the program. The released NSA documents also revealed the existence of another secret program, called PRISM, begun in 2007, that enabled the NSA to access Internet traffic stored in the servers of Internet service providers. Yet another embarrassing disclosure was the fact that the NSA had monitored the telephone conversations of foreign leaders, including the leaders of Germany and Brazil. Partly in response to these revelations, President Barack Obama announced a series of NSA reforms in a speech on 17 January 2014;

---

[66] "Bush Lets U.S. Spy on Callers Without Courts," *New York Times*, December 16, 2005.
[67] "Bulk Collection of Telephony Metadata Under Section 215 of the USA Patriot Act," *Administration White Paper*, August 9, 2013, 10-11. Ryan Lizza makes use of the "needle in a haystack" metaphor in "State of Deception."

the program of collecting telephone metadata under Section 215 of the Patriot act would be terminated, and ownership of the bulk data records would be taken away from the NSA and given back to the telecommunications companies or a third party.[68]

Conclusions: taking the historical viewpoint

At the end of the day, what lessons can we take away from the ongoing debate about privacy and electronic communications? Taking the historical viewpoint, a pattern emerges in which the U.S. government began electronic surveillance during wartime in the interests of national security, but was reluctant to discontinue the programs in peacetime until confronted with a challenge to the legality of the programs. The U.S. Congress has played an ambiguous role, sometimes initiating surveillance activities, and sometimes investigating them. The private telecom companies have played a similarly ambivalent role, alternating between resisting government surveillance attempts and actively participating in monitoring of their customers' traffic.

It seems surprising to us today that issues of privacy in electronic communications did not come before the U.S. Supreme Court until well into the twentieth century. Privacy, which traditionally had been seen as an issue under common law, first had to be recognized as protected by the Fourth Amendment, and therefore part of constitutional law, before the Supreme Court could rule on it. Each new communications technology has engendered new privacy concerns, and, as Brandeis and Warren observed in 1890, "the common law, in its eternal youth, grows to meet the new demands of society."

However, many privacy issues remain unresolved. The rapid pace of developments in telecommunications technology has created a situation where technological advances have outpaced the law. One such development has been the explosive growth of the Internet. The Electronic Communications Privacy Act of 1986 allows the government to obtain e-mails, mobile phone location information, information

---

[68] "Transcript of President Obama's Jan. 17 speech on NSA reforms," Washington Post, January 17, 2014. http://www.washingtonpost.com/politics/full-text-of-president-obamas-jan-17-speech-on-nsa-reforms/2014/01/17/fa33590a-7f8c-11e3-9556-4a4bf7bcbd84_story.html

from social networking sites, and even data stored in “cloud computing” sites by merely stating that the information is “relevant” to a criminal investigation. To put this in historical perspective, there is an almost exact analogy between the paper copies of telegrams maintained by telegraph offices in the nineteenth century and copies of e-mails stored in servers in the modern Internet. One wonders if the NSA’s contention that it needs “haystacks in order to find the terrorist needle” would have stood up to the scrutiny of the Missouri Supreme Court’s decision in 1880, which prohibited “an indiscriminate search among all the papers in one’s possession for no particular paper, but some paper, which may throw some light on some issue involved in the trial of some cause pending.”

As the legal scholar Wesley Oliver stated in 2011, echoing nineteenth century concerns, “The recent pace of development in communication technology leaves privacy interests in the new media considerably unprotected by comparison with traditional means of communication.”[69] In short, it is *deja-vu* all over again, and there is much we can learn from the past. Above all, what is needed is a vigorous and meaningful national debate in the U.S. about privacy in the Internet age.

---

[69] Oliver, “Western Union,” 986, 972.

Bibliography

The American Annual Cyclopedia and Register of Important Events for the Year 1862. New York: D. Appleton & Company, 1868.

Bates, David Homer. *Lincoln in the Telegraph Office*. New York: The Century Company, 1907.

Cordery, Stacy A. *Alice: Alice Roosevelt Longworth, from White House Princess to Washington Power Broker*. New York: Viking, 2007.

Harlow, Alvin. *Old Wires and New Waves: The History of the Telegraph, Telephone, and Wireless.* New York: Appleton-Century Company, 1936.

John, Richard R. *Network Nation: Inventing American Telecommunications.* Cambridge, Massachusetts: Belknap Press, 2010.

Kahn, David. *The Code Breakers: The Story of Secret Writing*. New York: Scribner, 1996.

Morris Jr., Roy. *Fraud of the Century: Rutherford B. Hayes, Samuel Tilden, and the Stolen Election of 1876.* New York: Simon & Schuster, 2003.

Nickles, David Paull. *Under the Wire: How the Telegraph Changed Diplomacy*. Cambridge, Massachusetts: Harvard University Press, 2003.

Plum, William R. *The Military Telegraph during the Civil War in the United States*, Vol. 1. Chicago: Jansen, McClurg & Company, 1882.

Prescott, George B. *History, Theory, and Practice of the Electric Telegraph*. Boston: Ticknor and Fields, 1860.

Reid, James D. *The Telegraph in America and Morse Memorial*. New York: John Polhemus, 1886.

Seipp, David J. *The Right to Privacy in American History*. Publication P-78-3, Program on Information Resources Policy, July 1978.

Stewart, David O. *Impeached: The Trial of President Andrew Johnson and the Fight for Lincoln's Legacy*. New York: Simon & Schuster, 2009.

Thompson, Robert L. *Wiring a Continent: The History of the Telegraph Industry in the United States, 1832-1866.* Princeton, New Jersey: Princeton University Press, 1947.

Yardley, Herbert O. *The American Black Chamber*. London: Faber & Faber, 1931.