A History of Dragnet Wiretapping

thelastbastille.wordpress.com /2015/03/02/a-history-of-dragnet-wiretapping/

Politicians insist that the government has a “right to know” about the intimate details of an entire citizenry. What they fail to realize is that governments do *not* have rights, which also means that the government has no inherent right to know *anything* about *anybody*. Despite this fundamental truth, these self-imagined rulers arrogantly demand that Americans acquiesce to these invasions of privacy on the grounds of whatever their latest crusade happens to be, yet they insist on maintaining their state secrets privilege. Their desire for the government to become nearly omniscient is so self-evidently dangerous to liberty that their attempts to implement a panopticon ought be commonly resisted.

Wiretapping is but just one method of surveillance whose technological and historical antecedent would most likely be the interception of mail. During the American colonial period, the King’s mandate sanctioned the government’s ability to intercept all mail within the British Empire. In post-revolutionary France, Joseph Fouché intercepted the mails for Napoleon Bonaparte, and José Rodriguez de Francia intercepted Paraguayan mail throughout the early 19th century. Once the telephone was invented in 1876, it provided yet another way for governments to commit espionage against their own citizens, just like how Nicolae Ceaușescu’s Securitate combined the techniques of intercepting both mail and telephone communications in Romania.

The Science of Wiretapping

Unlike a sealed envelope, however, the science of the telephone itself does not value individual privacy. Telephones were originally designed to overcome a human limitation, namely, the need to be in the same physical space before talking to someone else during the same moment of time. Once this had been achieved, it was not too long before it was being exploited for a variety of purposes, not only due to its simplistic design, but also because there was little interest in preventing eavesdropping. Wiretapping differs from eavesdropping insofar as wiretapping is one technique of eavesdropping, but not all eavesdropping is wiretapping, as evidenced by putting your ear against a wall or door in order to better listen to the voices on the other side.

Simply put, wiretapping is the act of intercepting telephonic communications; this could be done by installing either hardwire taps or a transmitting bug within a wall socket, the telephone’s handset, on a nearby telephone pole’s utility junction box, a telephone switching station, or the interception of transmissions by other means, such as snatching radio waves out of the air. Whether it be by landline, cordless, cellular, satellite, ham radio, or VoIP, modern telephony is considered private only to the extent that there is a cultural expectation that it should be so, but not so with regards to the inherent nature of the technology itself. What the science of wiretapping appears to tell us is that it is foolish to project one’s false sense of security by crying “foul” after the fact; however, this is not to imply that technological countermeasures shouldn’t be implemented, for anyone who is serious about his own privacy should move heaven and earth to do so.

The Origins of the National Security Agency

President Harry Truman unilaterally created the National Security Agency (NSA) in 1952, specifically for the reason of preventing another Pearl Harbor surprise attack by way of using signals intelligence (SIGINT). In 1976, the Church Committee hearings revealed that the NSA had exceeded its foreign intelligence surveillance mandate by monitoring the communications of American citizens whom it deemed were engaging in activities that threatened national security. The committee's summary of problems included the finding that:

> *"**Governmental officials** – including those whose principal duty is to enforce the law – have violated or ignored the law over long periods of time and **have advocated and defended their right to break the law**." [emphasis added]*

Ironically, these illegal abuses by NSA occurred alongside Ceaușescu's Securitate similarly tapping Romanian telephones during the Cold War. Despite another 25 years to get its act together, NSA not only failed to prevent the 9/11 attacks, but its own internal security was discovered to have been breached a week after the attacks. Without missing a beat, the NSA and rest of the United States intelligence community lobbied Congress to grant them more power as a reward for their infamous failures, and all in the name of national security for this brand new "War on Terror," whom Brigadier General (now Lieutenant General) Mark Schissler said will go on for another 50 – 100 years.

Government propagandists will convince people there are dangers that only they can protect us from, but in order to do so, they must first infringe upon our freedoms. From early 20th century organized crime and Cold War communism to modern "terrorism," civil servants have regularly sought any excuse to increase their power, regardless of who gets hurt in the process, as mere collateral damage. These convenient bogeymen serve their roles well in the quest for inculcating a climate of unjustified fear, which is used by policy makers as a false pretext to make laws hostile to the U.S. Constitution and the American way of life.

The Legality of Wiretapping

Constitutionally, the Fourth Amendment's Search & Seizure Clause says:

> *"The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated…"*

For the sake of political expediency in the wake of 9/11, former President George W. Bush's White House asserted that pursuant to the Art. II § 2 cl. 1 *delegated* power as the Commander-in-Chief of the Army and

the Navy of the United States (and of the Militia of the several States), the Executive Office of the President enjoyed the *implied* power to wiretap anyone merely suspected of threatening national security. Despite the fact that the Congress has not declared war since World War II (pursuant to Art. I § 8), the executive branch unilaterally assumed a wartime authority to run roughshod over the Fourth Amendment.

Statutorily, the Foreign Intelligence Surveillance Act (FISA) of 1978 was passed by the Congress into law as the intended political reform in the aftermath of the Church Committee's discovery about the NSA's Project MINARET. FISA created the Foreign Intelligence Surveillance Court (FISC), whose duty it was to determine whether secretive warrants should be issued against suspected foreign spies. The Communications Assistance for Law Enforcement Act (CALEA) of 1994 mandated that telecommunications providers give law enforcement agencies backdoors for the purpose of easier wiretapping (eventually for VoIP calls in 2005), and the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001 expanded the FISC's **secret** warrants to permit "roving wiretaps," which lack the specificity required by the Fourth Amendment, and therefore increase the likelihood of incidental intercepts. Ironically, the FISA Amendments Act of 2008 was passed by the Congress into law as the political reform intended to address the abuses caused by the NSA's Stellar Wind surveillance program, thereby repeating what had been done exactly three decades previously.

Judicially, the 1928 *Olmstead v. United States* case ruled that the Fourth Amendment's Search and Seizure Clause did not apply to the use of wiretaps by federal agents, even if in violation of state law, yet almost 40 years later, *Katz v. United States* ruled that the Search & Seizure Clause does protect individuals using a telephone booth from warrantless **eavesdropping**. In his dissenting opinion in *Olmstead*, Judge Louie Brandeis wrote:

> *"**Decency, security, and liberty alike demand that government officials shall be subjected to the same rules of conduct that are commands to the citizen.** In a government of laws, existence of the government will be imperiled if it fails to observe the law scrupulously. Our government is the potent, the omnipresent teacher. For good or for ill, it teaches the whole people by its example. Crime is contagious. If the government becomes a lawbreaker, it breeds contempt for law; it invites every man to become a law unto himself; it invites anarchy. To declare that in the administration of the criminal law the end justifies the means – **to declare that the government may commit crimes in order to secure the conviction of a private criminal – would bring terrible retribution**. Against that pernicious doctrine this court should resolutely set its face." [emphasis added]*

Similarly, Judge William Douglas' concurring opinion in the 1972 *United States v. U.S. District Court* (aka, the Keith case) said:

> *"That 'domestic security' is said to be involved here does not draw this case outside the mainstream of Fourth Amendment law. Rather, the recurring desire of reigning officials to employ **dragnet techniques** to intimidate their critics lies at the core of that prohibition. For it was such excesses as the use of general warrants and the writs of assistance that led to the ratification of the Fourth Amendment." [emphasis added]*

As you could probably tell, the federal judiciary's attitude towards wiretapping (at least before 9/11) wasn't so much about the "reasonableness" of the search and/or seizure in question as it was about the Fourth Amendment's Warrant Clause, which says:

> *"…and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized."*

In other words, the very lack of specificity *is* unreasonable, exceptions to the Warrant Clause notwithstanding. Supreme Court judges did not want to be perceived as hypocrites, so they devised an interpretative scheme whereby as long as warrants did not emulate a writ of assistance, then it would be appropriate for the courts to try and rationalize the demands of the executive branch against the individual privacy of the average American citizen.

Although this was the United States Supreme Court's rather moderate position before 9/11, the federal district and appellate judiciary's attitude after 9/11 seems quite authoritarian. Judge Lewis Kaplan's 2006 memorandum opinion in *United States v. Tomero, et. al.* for the United States District Court for the Southern District of New York ruled that the FBI's installation of roving wiretap bugs in the defendants' cell phones were not unconstitutional. A year later, Judge Alice Batchelder wrote the United States Court of Appeals for the Sixth Circuit's 2007 decision in *ACLU v. NSA*, where the plaintiffs lacked standing to challenge the NSA's Stellar Wind surveillance program because they couldn't prove they were directly targeted by it.

The 2011 *Hepting v. AT&T Corp.* ruling, written by Judge M. Margaret McKeown on the United States Court of Appeals for the Ninth Circuit, found that legal immunity (against being sued) for the telecommunications companies under § 802 of FISA (which is cross-listed under Title 50 USC § 1885a) was constitutional. Several months later in 2012, Judge Raymond Fisher conveyed the appellate Ninth Circuit's ruling in *United States v. Olivia* that the electronic surveillance orders only authorized "standard interception techniques," and therefore did not convert the defendant's cellular telephone into a roving wiretap bug, despite the fact that the police turned the phone into a roving wiretap. Finally, the *Jewel v. NSA* lawsuit (which claimed that Room 641A inside the SBC Communications building was involved in a an NSA dragnet surveillance operation) was dismissed in February of 2015 by Judge Jeffrey White in the United States District Court for the Northern District of California on the grounds that not only could former AT&T technician Mark Klein not determine "the content, function, or purpose" of Room 641A, but also that the plaintiffs failed to established "a sufficient factual basis…[that] they have standing to sue under the Fourth Amendment regarding the possible interception of their Internet communications."

Despite the fact that there was no foreign intelligence exception to the Warrant Clause in either the *Tomero* or *Olivia* cases, the federal judiciary frequently use the excuse of statutory construction in order to perform an end run around the Fourth Amendment. This not only contradicts the Keith case, but it also proves both the Church Committee's findings and Judge Brandeis' dissent in *Olmstead* in the ensuing years. Constitutional avoidance, much?

Contemporary Wiretapping

ECHELON is the code name for some of the SIGINT stations that operate under the auspices of the Five Eyes intelligence alliance, which functions according to the terms of the then secret treaty known as the UKUSA Agreement. Right off the bat, there is a question of constitutionality here, for the Advice & Consent Clause (Art. II § 2 cl. 2) says, in part:

> *"He [the President] shall have Power, by and with the Advice and Consent of the Senate, to make Treaties, provided two-thirds of the Senators present concur…"*

There is no public record available testifying to the fact that the U.S. Senate ever ratified any treaty with either England, Canada, Australia, or New Zealand, since the end of the Second World War, to openly share signals intelligence. Not only that, but it wasn't until July of 2001 when the European Union Parliament issued a report confirming the existence of ECHELON, the UKUSA Agreement, and the Five Eyes SIGINT network.

What is truly disconcerting, though, is that as the foundational basis for the UKUSA Agreement, the NSA works around statutory limitations, like FISA, by having either the Communications Security Establishment, the Government Communications Headquarters, the Australian Signals Directorate, or the Government Communications Security Bureau collect SIGINT from Americans, who then turn around and hand it to the NSA for whatever "national security" purposes they see fit to exercise, such as building the Utah Data Center in order to store massive amounts of information.

For all intents and purposes, the UKUSA Agreement has permitted these four other governments to commit espionage against Americans, and then share that information with the NSA, thereby circumventing the Constitution.

Relying on a combination of transatlantic underwater cables and orbital geostationary satellite uplinks and downlinks, ECHELON provided the framework necessary to implement a plethora of wiretapping tools. For instance, both PRISM and MUSCULAR collect not only metadata, but also the content of VoIP calls. Whether or not black rooms like Room 641A or the roving wiretap bugs have anything to do with the NSA is anyone's guess, but what all of them demonstrate is that the federal government does not care about your individual privacy, and even less so about the rule of law.

Take, for instance, how the federal government treats NSA whistleblowers. Perry Fellwock, Russell Tice, Thomas Tamm, William Binney, Thomas Drake, and Ed Snowden have all been persecuted by the United States government. Costly litigation, pension revocations, and seeking political asylum as a fugitive are but just some of the consequences experienced by these whistleblowers, who under pain of individual conscience, chose to reveal the abuses perpetrated by the NSA. Accusations that these whistleblowers are so-called "limited hangouts" ought to placed under scrutiny for ulterior motives.

Let us now review this history of dragnet wiretapping. The sequence of events are as follows:

- 1760s – 1770s: colonial mail intercepted by Redcoats
- 1799 – 1814: Joseph Fouché intercepted French mail for Napoleon Bonaparte
- 1814 – 1840: José Rodriguez de Francia intercepted Paraguayan mail

- 1876: the invention of the telephone
- 1928: *Olmstead v. United States*, 277 US 438
- 1952: President Truman's memo creating NSA
- 1955: updated UKUSA Agreement
- 1965: Nicolae Ceaușescu began interception of Romanian mail & wiretapping
- 1967: *Katz v. United States*, 389 US 347
- 1968: Omnibus Crime Control and Safe Streets Act (aka, the "Wiretap Statute")
- 1972: *United States v. U.S. District Court*, 407 US 297
- 1976: Church Committee hearings
- 1978: Foreign Intelligence Surveillance Act (FISA)
- 1988: Electronic Communications Privacy Act (ECPA)
- 1989: Ceaușescu executed by firing squad; mail interception & wiretapping ended
- 1994: Communications Assistance for Law Enforcement Act (CALEA)
- 1998: Hollywood film ***Enemy of the State*** released into theaters
- 2001, July: EU Parliament report on ECHELON
- 2001, October: USA PATRIOT Act
- 2004: **A False Sense of Insecurity?** article
    - A libertarian analyst evaluated the true risk of "terrorism"
- 2005: Stellar Wind publicly revealed
- 2006: *United States v. Tomero*, S2 06 Crim. 0008
- 2007: *ACLU v. NSA*, Nos. 06-2095/2140
- 2008: FISA Amendments Act
- 2011: *Hepting v. AT&T Corp.*, No. 09-16676
- 2012: *United States v. Olivia*, No. 10-30126
- 2013: **Liberty & Security in a Changing World** report
    - The Obama White House's official story after Ed Snowden's leaks
- 2015: *Jewel v. NSA*, No. 08-04373

This chronology demonstrates that the interception of communications, and wiretapping specifically, is nothing new. Whether it is by way of legislation or court precedent, the American federal government absolutely refuses to be bound within the chains imposed upon it by the U.S. Constitution. No amount of reformism will reign in the persistent abuses by the NSA. What it can't take by a large bite, they will take by smaller bites. Nothing less than total abolishment of this nefarious administrative agency would even begin to satisfy the demands of natural justice.

Counter-Wiretapping Remedies

Fortunately, the cypherpunks and crypto-anarchists are here to help Americans fend off the NSA in the

ongoing crypto wars. An eclectic mixture of free and open-source software, public-key cryptography, and end-to-end encryption can be used to supply the market demand for inexpensively available secure telephones, whose development should not be as elusive as that of cold fusion. Since encryption is like a sealed envelope, nearly all popular voice communications might as well be verbal postcards. If the OpenPGP standard is already used to encrypt email, and OTR is similarly being used to encrypt instant messages, then there is no good reason that I can fathom as to why ZRTP (Zimmerman Real-time Transport Protocol), or similar software, cannot be built to encrypt at least VoIP, if not also cellular, calls. We need to use secure communications, if we're going to have a reasonable expectation of privacy. This becomes particularly critical for security teams, local Committees of Safety, and any other communications that you feel that the government should not have access to.

With every failure, government is rewarded with more power. From Pearl Harbor to the Boston Marathon bombing, the NSA is not only a catastrophic lead balloon, but also the ears of, what some might call, the slowly emerging New World Order. Because of dragnet wiretapping's inherent threat to individual privacy is why the adage, "Don't say anything on the phone you wouldn't also be comfortable repeating in front of a cop, a judge, or a jury," carries so much sway. As Eric Hughes wrote back in 1993:

> *"Privacy is the power to selectively reveal oneself to the world…[t]o encrypt is to indicate the desire for privacy, and to encrypt with weak cryptography is to indicate not too much desire for privacy…[w]e must defend our own privacy if we expect to have any. We must come together and create systems which allow anonymous transactions to take place. People have been defending their own privacy for centuries with whispers, darkness, envelopes, closed doors, secret handshakes, and couriers. The technologies of the past did not allow for strong privacy, but electronic technologies do."*

Free market technology, not government law, is the solution. Do we want to resort to "whispers, darkness, envelopes, closed doors, secret handshakes, and couriers," or do we want to pursue modern techniques for the maintenance of our right to privacy, as enumerated by the Fourth Amendment, as the Framers intended? About 87 years have passed since the *Olmstead* ruling, and I'll be damned if another decade goes by without me pulling my weight for the cause of liberty. And now that you have read this history of wiretapping, you must ask yourself, are you interested?