Big Brother Is Listening

The NSA has the ability to eavesdrop on your communications—landlines, cell phones, e-mails, BlackBerry messages, Internet searches, and more—with ease. What happens when the technology of espionage outstrips the law's ability to protect ordinary citizens from it?

James Bamford, The Atlantic, April 2006 Issue
https://www.theatlantic.com/magazine/archive/2006/04/big-brother-is-listening/304711/

On the first Saturday in April of 2002, the temperature in Washington, D.C., had taken a dive. Tourists were bundled up against the cold, and the cherry trees along the Tidal Basin were fast losing their blossoms to the biting winds. But a few miles to the south, in the Dowden Terrace neighborhood of Alexandria, Virginia, the chilly weather was not deterring Royce C. Lamberth, a bald and burly Texan, from mowing his lawn. He stopped only when four cars filled with FBI agents suddenly pulled up in front of his house. The agents were there not to arrest him but to request an emergency court hearing to obtain seven top-secret warrants to eavesdrop on Americans.

As the presiding justice of the Foreign Intelligence Surveillance Court, known as the FISA court, Lamberth had become accustomed to holding the secret hearings in his living room. "My wife, Janis … has to go upstairs because she doesn't have a top-secret clearance," he noted in a speech to a group of Texas lawyers. "My beloved cocker spaniel, Taffy, however, remains at my side on the assumption that the surveillance targets cannot make her talk. The FBI knows Taffy well. They frequently play with her while I read some of those voluminous tomes at home." FBI agents will even knock on the judge's door in the middle of the night. "On the night of the bombings of the U.S. embassies in Africa, I started the first emergency hearings in my living room at 3:00 a.m.," recalled Lamberth. "From the outset, the FBI suspected bin Laden, and the surveillances I approved that night and in the ensuing days and weeks all ended up being critical evidence at the trial in New York.

"The FISA court is probably the least-known court in Washington," added Lamberth, who stepped down from it in 2002, at the end of his seven-year term, "but it has become one of the most important." Conceived in the aftermath of Watergate, the FISA court traces its origins to the mid-1970s, when the Senate's Church Committee investigated the intelligence community and the Nixon White House. The panel, chaired by Idaho Democrat Frank Church, exposed a long pattern of abuse, and its work led to bipartisan legislation aimed at preventing a president from unilaterally directing the National Security Agency or the FBI to spy on American citizens. This legislation, the 1978 Foreign Intelligence Surveillance Act, established the FISA court—made up of eleven judges handpicked by the chief justice of the United States—as a secret part of the federal judiciary. The court's job is to decide whether to grant warrants requested by the NSA or the FBI to monitor communications of American citizens and legal residents. The law allows the government up to three days after it starts eavesdropping to ask for a warrant; every violation of FISA carries a penalty of up to five years in prison. Between May 18, 1979, when the court opened for business, until the end of 2004, it granted 18,742 NSA and FBI applications; it turned down only four outright.

Such facts worry Jonathan Turley, a George Washington University law professor who worked for the NSA as an intern while in law school in the 1980s. The FISA "courtroom," hidden away on the top floor of the Justice Department building (because even its location is supposed to be secret), is actually a heavily protected, windowless, bug-proof installation known as a Sensitive Compartmented Information Facility, or SCIF. "When I first went into the FISA court as a lowly intern at the NSA, frankly, it started a lifetime of opposition for me to that court," Turley recently told a group of House Democrats looking into the NSA's domestic spying. "I was shocked with what I saw. I was convinced that the judge in that SCIF would have signed anything that we put in front of him. And I wasn't entirely sure that he had actually *read* what we put in front of him. But I remember going back to my supervisor at NSA and saying, 'That place scares the daylights out of me.'"

Lamberth bristles at any suggestion that his court routinely did the administration's bidding. "Those who know me know the chief justice did not put me on this court because I would be a rubber stamp for whatever the executive branch was wanting to do," he said in his speech. "I ask questions. I get into the nitty-gritty. I know exactly what is going to be done and why. And my questions are answered, in every case, before I approve an application."

It is true that the court has been getting tougher. From 1979 through 2000, it modified only two out of 13,087 warrant requests. But from the start of the Bush administration, in 2001, the number of modifications increased to 179 out of 5,645 requests. Most of those—173—involved what the court terms "substantive modifications."

This friction—and especially the requirement that the government show "probable cause" that the American whose communications they are seeking to target is connected in some way to a terrorist group—induced the administration to begin circumventing the court. Concerned about preventing future 9/11-style attacks, President Bush secretly decided in the fall of 2001 that the NSA would no longer be bound by FISA. Although Judge Lamberth was informed of the president's decision, he was ordered to tell no one about it—not even his clerks or his fellow FISA-court judges.

Why the NSA Might be Listening to *YOU*

Contrary to popular perception, the NSA does not engage in "wiretapping"; it collects signals intelligence, or "sigint." In contrast to the image we have from movies and television of an FBI agent placing a listening device on a target's phone line, the NSA intercepts entire streams of electronic communications containing millions of telephone calls and e-mails. It runs the intercepts through very powerful computers that screen them for particular names, telephone numbers, Internet addresses, and trigger words or phrases. Any communications containing flagged information are forwarded by the computer for further analysis.

The NSA's task is to listen in on the world outside American shores. During the Cold War, the principal targets were the communications lines used by the Soviet government and military—navy captains calling their ports, fighter pilots getting landing instructions, army commanders out on maneuvers, and diplomats relaying messages to the Kremlin. But now the enemy is one that communicates very little and, when it does, uses the same telecommunications network as everyone else: a complex system of wires, radio signals, and light pulses encircling and crisscrossing the globe like yarn. Picking up just the right thread, and tracing it through the maze of strands, is difficult. Sometimes a thread leads back inside the United States. An internal agency report predicted a few years ago that the NSA's worldwide sigint operation would demand a "powerful and permanent presence" on the global telecommunications networks that carry "protected American communications." The prediction has come true, and the NSA now monitors not only purely "foreign" communications but also "international" ones, where one end of the conversation might be in the United States. As a result, the issue at hand since the revelation last December of the NSA's warrantless spying on American citizens is not the agency's access to the country's communications network—it already has access—but whether the NSA must take legal steps in preparing to target the communications of an American citizen.

It used to be that before the NSA could place the name of an American on its watch list, it had to go before a FISA-court judge and show that it had probable cause—that the facts and circumstances were such that a prudent person would think the individual was somehow connected to terrorism—in order to get a warrant. But under the new procedures put into effect by Bush's 2001 order, warrants do not always have to be obtained, and the critical decision about whether to put an American on a watch list is left to the vague and subjective "reasonable belief" of an NSA shift supervisor. In charge of hundreds of people, the supervisor manages a wide range of sigint specialists, including signals-conversion analysts separating HBO television programs from cell-phone calls, traffic analysts sifting through massive telephone data streams looking for suspicious patterns, cryptanalysts attempting to read e-mail obscured by complex encryption algorithms, voice-language analysts translating the gist of a phone call from Dari into English, and cryptolinguists trying to unscramble a call on a secure telephone. Bypassing the FISA court has meant that the number of Americans targeted by the NSA has increased since 2001 from perhaps a dozen per year to as many as 5,000 over the last four years, knowledgeable sources told *The Washington Post* in February. If telephone records indicate that one of the NSA's targets regularly dials a given telephone number, that number and any names associated with it are added to the watch lists and the communications on that line are screened by computer. Names and information on the watch lists are shared with the FBI, the CIA, the Department of Homeland Security, and foreign intelligence services. Once a person's name is in the files, even if nothing incriminating ever turns up, it will likely remain there forever. There is no way to request removal, because there is no way to confirm that a name is on the list.

In December of 1997, in a small factory outside the southern French city of Toulouse, a salesman got caught in the NSA's electronic web. Agents working for the NSA's British partner, the Government Communications Headquarters, learned of a letter of credit, valued at more than $1.1 million, issued by Iran's defense ministry to the French company Microturbo. According to NSA documents, both the NSA and the GCHQ concluded that Iran was attempting to secretly buy from Microturbo an engine for the embargoed C-802 anti-ship missile. Faxes zapping back and forth between Toulouse and

Tehran were intercepted by the GCHQ, which sent them on not just to the NSA but also to the Canadian and Australian sigint agencies, as well as to Britain's MI6. The NSA then sent the reports on the salesman making the Iranian deal to a number of CIA stations around the world, including those in Paris and Bonn, and to the U.S. Commerce Department and the Customs Service. Probably several hundred people in at least four countries were reading the company's communications. The question, however, remained: Was Microturbo shipping a missile engine to Iran? In the end, at the insistence of the U.S. government, the French conducted a surprise inspection just before the ship carrying the mysterious crate was set to sail for Iran. Inside were legal generators, not illegal missile engines.

Such events are central to the current debate involving the potential harm caused by the NSA's warrantless domestic eavesdropping operation. Even though the salesman did nothing wrong, his name made its way into the computers and onto the watch lists of intelligence, customs, and other secret and law-enforcement organizations around the world. Maybe nothing will come of it. Maybe the next time he tries to enter the United States or Britain he will be denied, without explanation. Maybe he will be arrested. As the domestic eavesdropping program continues to grow, such uncertainties may plague innocent Americans whose names are being run through the supercomputers even though the NSA has not met the established legal standard for a search warrant. It is only when such citizens are turned down while applying for a job with the federal government—or refused when seeking a Small Business Administration loan, or turned back by British customs agents when flying to London on vacation, or even placed on a "no-fly" list—that they will realize that something is very wrong. But they will never learn why.

More than seventy-five years ago, Supreme Court Justice Louis Brandeis envisioned a day when technology would overtake the law. He wrote:

> Subtler and more far-reaching means of invading privacy have become available to the government … 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 … Can it be that the Constitution affords no protection against such invasions of individual security?

Brandeis went on to answer his own question, quoting from an earlier Supreme Court decision, *Boyd* v. *U.S.* (1886): "It is not the breaking of his doors, and the rummaging of his drawers that constitutes the essence of the offence; but it is the invasion of his indefeasible right of personal security, personal liberty, and private property."

Eavesdropping in the Digital Age

Today, the NSA's capability to eavesdrop is far beyond anything ever dreamed of by Justice Brandeis. With the digital revolution came an explosion in eavesdropping technology; the NSA today has the ability to scan tens of millions of electronic communications—e-mails, faxes, instant messages, Web searches, and phone calls—every hour. General Michael Hayden, director of the NSA from 1999 to 2005 and now principal deputy director of national intelligence, noted in 2002 that during the 1990s, e-communications "surpassed traditional communications. That is the same decade when mobile cell phones increased from 16 million to 741 million—an increase of nearly 50 times. That is the same decade when Internet users went from about 4 million to 361 million—an increase of over 90 times. Half as many land lines were laid in the last six years of the 1990s as in the whole previous history of the world. In that same decade of the 1990s, international telephone traffic went from 38 billion minutes to over 100 billion. This year, the world's population will spend over 180 billion minutes on the phone in international calls alone."

Intercepting communications carried by satellite is fairly simple for the NSA. The key conduits are the thirty Intelsat satellites that ring the Earth, 22,300 miles above the equator. Many communications from Europe, Africa, and the Middle East to the eastern half of the United States, for example, are first uplinked to an Intelsat satellite and then downlinked to AT&T's ground station in Etam, West Virginia. From there, phone calls, e-mails, and other communications travel on to various parts of the country. To listen in on that rich stream of information, the NSA built a listening post fifty miles away, near Sugar Grove, West Virginia. Consisting of a group of very large parabolic dishes, hidden in a heavily forested valley and surrounded by tall hills, the post can easily intercept the millions of calls and messages flowing every hour into the Etam station. On the West Coast, high on the edge of a bluff overlooking the Okanogan River, near Brewster, Washington, is the major commercial downlink for communications to and from Asia and the Pacific. Consisting of forty

parabolic dishes, it is reportedly the largest satellite antenna farm in the Western Hemisphere. A hundred miles to the south, collecting every whisper, is the NSA's western listening post, hidden away on a 324,000-acre Army base in Yakima, Washington. The NSA posts collect the international traffic beamed down from the Intelsat satellites over the Atlantic and Pacific. But each also has a number of dishes that appear to be directed at domestic telecommunications satellites.

Until recently, most international telecommunications flowing into and out of the United States traveled by satellite. But faster, more reliable undersea fiber-optic cables have taken the lead, and the NSA has adapted. The agency taps into the cables that don't reach our shores by using specially designed submarines, such as the USS *Jimmy Carter,* to attach a complex "bug" to the cable itself. This is difficult, however, and undersea taps are short-lived because the batteries last only a limited time. The fiber-optic transmission cables that enter the United States from Europe and Asia can be tapped more easily at the landing stations where they come ashore. With the acquiescence of the telecommunications companies, it is possible for the NSA to attach monitoring equipment inside the landing station and then run a buried encrypted fiber-optic "backhaul" line to NSA headquarters at Fort Meade, Maryland, where the river of data can be analyzed by supercomputers in near real time.

Tapping into the fiber-optic network that carries the nation's Internet communications is even easier, as much of the information transits through just a few "switches" (similar to the satellite downlinks). Among the busiest are MAE East (Metropolitan Area Ethernet), in Vienna, Virginia, and MAE West, in San Jose, California, both owned by Verizon. By accessing the switch, the NSA can see who's e-mailing with whom over the Internet cables and can copy entire messages. Last September, the Federal Communications Commission further opened the door for the agency. The 1994 Communications Assistance for Law Enforcement Act required telephone companies to rewire their networks to provide the government with secret access. The FCC has now extended the act to cover "any type of broadband Internet access service" and the new Internet phone services—and ordered company officials never to discuss any aspect of the program.

The NSA won't divulge how many people it employs, but it is likely that more than 38,000 worldwide now work for the agency. Most of them are at Fort Meade. Nicknamed Crypto City, hidden from public view, and located halfway between Washington and Baltimore, the NSA's own company town comprises more than fifty buildings—offices, warehouses, factories, laboratories, and a few barracks. Tens of thousands of people work there in absolute secrecy, and most never tell their spouses exactly what they do. Crypto City also houses the nation's largest collection of powerful computers, advanced mathematicians, and skilled language experts.

The NSA maintains a very close and very confidential relationship with key executives in the telecommunications industry through their membership on the NSA's advisory board. Created shortly after the agency's formation, the board was intended to pull together a panel of science wizards from universities, corporate research labs, and think tanks to advise the agency. They keep the agency abreast of the industry's plans and give NSA engineers a critical head start in finding ways to penetrate technologies still in the development phase.

One of the NSA's strategies is to hire people away from the companies that make the critical components for telecommunications systems. Although it's sometimes difficult for the agency to keep up with the tech sector's pay scale, for many people the chance to deal with the ultimate in cutting-edge technology and aid national security makes working for the NSA irresistible. With the help of such workers, the agency reverse-engineers communication system components. For example, among the most crucial pieces of the Internet infrastructure are routers made by Cisco. "Virtually all Internet traffic," says one of the company's television ads, "travels across the systems of one company: Cisco Systems." For the NSA, this is an opportunity. In 1999, Terry Thompson, then the NSA deputy director for services, said, "[Y]ou can see down the road two or three or five years and say, 'Well, I only need this person to do reverse-engineering on Cisco routers (that's a good example) for about three or five years, because I see Cisco going away as a key manufacturer for routers and so I don't need that expertise. But I really need somebody today and for the next couple of years who knows Cisco routers inside and out and can help me understand how they're being used in target networks.'"

The Temptations of Secrecy

The National Security Agency was born in absolute secrecy. Unlike the CIA, which was created publicly by a congressional act, the NSA was brought to life by a top-secret memorandum signed by President Truman in 1952, consolidating the country's various military sigint operations into a single agency. Even its name was secret, and only a

few members of Congress were informed of its existence—and they received no information about some of its most important activities. Such secrecy has lent itself to abuse.

During the Vietnam War, for instance, the agency was heavily involved in spying on the domestic opposition to the government. Many of the Americans on the watch lists of that era were there solely for having protested against the war. Among the names in the NSA's supercomputers were those of the folk singer Joan Baez, the pediatrician Benjamin Spock, the actress Jane Fonda, the civil-rights leader Martin Luther King Jr., and the newspaper editor David Kahn, whose standard history of cryptology, *The Codebreakers*, contained information the NSA viewed as classified. Even so much as writing about the NSA could land a person a place on a watch list. The NSA, on behalf of the FBI, was also targeting religious groups. "When J. Edgar Hoover gives you a requirement for complete surveillance of all Quakers in the United States," recalled Frank Raven, a former senior NSA official, "and when Richard M. Nixon is a Quaker and he's the president of the United States, it gets pretty funny."

Of course, such abuses are hardly the exclusive province of the NSA; history has repeatedly shown that simply having the ability to eavesdrop brings with it the temptation to use that ability—whatever the legal barriers against that use may be. For instance, during World War I, the government read and censored thousands of telegrams—the e-mail of the day—sent hourly by telegraph companies. Though the end of the war brought with it a reversion to the Radio Act of 1912, which guaranteed the secrecy of communications, the State and War Departments nevertheless joined together in May of 1919 to create America's first civilian eavesdropping and code-breaking agency, nicknamed the Black Chamber. By arrangement, messengers visited the telegraph companies each morning and took bundles of hard-copy telegrams to the agency's offices across town. These copies were returned before the close of business that day.

A similar tale followed the end of World War II. In August of 1945, President Truman ordered an end to censorship. That left the Signal Security Agency (the military successor to the Black Chamber, which was shut down in 1929) without its raw intelligence—the telegrams provided by the telegraph companies. The director of the SSA sought access to cable traffic through a secret arrangement with the heads of the three major telegraph companies. The companies agreed to turn all telegrams over to the SSA, under a plan code-named Operation Shamrock. It ran until the government's domestic spying programs were publicly revealed, in the mid-1970s. The discovery of such abuses in the wake of the Watergate scandal led Congress to create select committees to conduct extensive investigations into the government's domestic spying programs: their origin, extent, and effect on the public. The shocking findings turned up by the Church Committee finally led to the formation of permanent Senate and House intelligence committees, whose primary responsibility was to protect the public from future privacy abuses. They were to be the FISA court's partner in providing checks and balances to the ever-expanding U.S. intelligence agencies. But it remains very much an open question whether these checks are up to the task at hand.

Who Watches the Watchmen?

Today, the NSA has access to more information than ever before. People express their most intimate thoughts in e-mails, send their tax returns over the Internet, satisfy their curiosity and desires with Google searches, let their hair down in chat rooms, discuss every event over cell phones, make appointments with their BlackBerrys, and do business by computer in WiFi hot spots.

NSA personnel, the customs inspectors of the information superhighway, have the ultimate goal of intercepting and reviewing every syllable and murmur zapping into, out of, or through the United States. They are close to achieving it. More than a dozen years ago, an NSA director gave an indication of the agency's capability. "Just one intelligence-collection system," said Admiral William O. Studeman, referring to a listening post such as Sugar Grove, "can generate a million inputs per half hour." Today, with the secret cooperation of much of the telecommunications industry, massive dishes vacuuming the airwaves, and electronic "packet sniffers," software that monitors network traffic, diverting e-mail and other data from fiber-optic cables, the NSA's hourly take is in the tens of millions of communications. One transatlantic fiber-optic cable alone has the capacity to handle close to 10 million simultaneous calls. While most communications flow through the NSA's electronic net unheard and unread, those messages associated with persons on the agency's watch lists—whether guilty or innocent—get kicked out for review.

As history has shown, the availability of such vast amounts of information is a temptation for an intelligence agency. The criteria for compiling watch lists and collecting information may be very strict at the beginning of such a program, but the

reality—in a sort of bureaucratic law of expansion—is that it will draw in more and more people whose only offense was knowing the wrong person or protesting the wrong war.

Moreover, as Internet and wireless communications have grown exponentially, users have seen a corresponding decrease in the protections provided by the two institutions set up to shield the public from eavesdroppers. The first, the FISA court, has simply been shunted aside by the executive branch. The second, the congressional intelligence committees, have quite surprisingly abdicated any role. Created to be the watchdogs over the intelligence community, the committees have instead become its most enthusiastic cheerleaders. Rather than fighting for the public's privacy rights, they are constantly battling for more money and more freedom for the spy agencies.

Last November, just a month before *The New York Times* broke the story of the NSA's domestic spying, the American Bar Association publicly expressed concern over Congress's oversight of FISA searches. "The ABA is concerned that there is inadequate congressional oversight of government investigations undertaken pursuant to the Foreign Intelligence Surveillance Act," the group stated, "to assure that such investigations do not violate the First, Fourth, and Fifth Amendments to the Constitution." And while the administration did brief members of Congress on the decision to bypass FISA, the briefings were limited to a "Gang of Eight"—the majority and minority leaders of the House and Senate and the chairmen and ranking members of the two intelligence committees. None of the lawmakers insisted that the decision be debated by the joint committees, even though such hearings are closed.

Frank Church, the Idaho Democrat who led the first probe into the National Security Agency, warned in 1975 that the agency's capabilities

could be turned around on the American people, and no American would have any privacy left, such [is] the capability to monitor everything: telephone conversations, telegrams, it doesn't matter. There would be no place to hide. If this government ever became a tyranny, if a dictator ever took charge in this country, the technological capacity that the intelligence community has given the government could enable it to impose total tyranny, and there would be no way to fight back, because the most careful effort to combine together in resistance to the government, no matter how privately it is done, is within the reach of the government to know. Such is the capacity of this technology.

It was those fears that caused Congress to enact the Foreign Intelligence Surveillance Act three years later. "I don't want to see this country ever go across the bridge," Senator Church said. "I know the capacity that is there to make tyranny total in America, and we must see to it that [the National Security Agency] and all agencies that possess this technology operate within the law and under proper supervision, so that we never cross over that abyss. That is the abyss from which there is no return."

Name: _____
Period: _____ Date: _____

Big Brother is Watching

This essay was published in 2006. A lot has come to light regarding government intrusion into its citizens lives since.
Consider this question: **To what extent (if at all) should it be permissible for the government to invade peoples privacy to protect national harmony and international peace?**
You are expected to do a five minute free-write on this topic…this is where you do not stop writing for five minutes. Just let your thoughts flow. A formal structure is not necessary, but your pencil will not stop for five minutes.
This is preparatory for a discussion/debate on the topic we will have in class.