The NSA, the National Security Agency

or Nothing's Secret Anymore?

Who among us has not read a book or seen a movie in recent years with a central plot device that involves some clandestine intelligence agency using fantastic, whiz-bang technology to track down the bad guys by tracing and monitoring their cell phones, smartphones and computers? Really cool guy stuff! But in fact, much of the technology and methods portrayed are in use every single day by our government and have been for a very long time. Evidence the capture or killing of any number of high ranking al-Qaeda terrorists, including Osama bin Laden.

This technology and the methods used by our intelligence gathering agencies has fascinated me since I was a young boy reading my first James Bond novel…and then the Edward Snowden disclosures happened and the agency largely responsible for the electronic monitoring and tracking of any number of our country's enemies was thrust into a very much unwanted spotlight. Thus began my research into the National Security Agency. Based on my reading and research, I put it to you that the fictional accounts are likely just the tip of the iceberg of what information is available to our intelligence agencies. Gentlemen, the title of my paper is "The NSA, the National Security Agency or Nothing's Secret Anymore?"

The National Security Agency (NSA) is the US intelligence agency responsible for global monitoring, collection, decoding, translation and analysis of information and data for foreign intelligence and counterintelligence purposes, a discipline known as signals intelligence (SIGINT). The NSA is also charged with protection of US government communications and information systems against penetration and network warfare. The agency is authorized to accomplish its mission

through clandestine means, among which are bugging and monitoring electronic systems. However, unlike the Defense Intelligence Agency and the Central Intelligence Agency, both of which specialize primarily in foreign human espionage, the NSA has no authority to conduct human source intelligence gathering, although it is often portrayed doing so in popular culture.

The NSA was formally established by Harry Truman in a memorandum of October 24, 1952, that revised National Security Council Intelligence Directive9. Since President Truman's memo was a classified document and the existence of the NSA was not known to the public at that time, due to its ultra- secrecy, the US intelligence community referred to the NSA as "No Such Agency".

The number of NSA employees is officially classified but there are several sources providing estimates. In 1961, the NSA had 59,000 military and civilian employees which grew to 93,000 in 1969, of which 19,300 worked at the agency's headquarters, at Fort Meade, Maryland, just outside of Baltimore. By 1989 this number had shrunk to around 75,000, of which 25,000 worked at the NSA headquarters. Between 1990 and 1995 the NSA's budget and workforce were cut by one third, which led to a substantial loss of its experienced workforce. In 2012, the NSA said more than 30,000 employees work at Fort Meade and other facilities. John C. Inglis, the deputy director at that time, said the total number of NSA employees is "somewhere between 37,000 and 1 billion" as a joke, and stated that the agency is "probably the biggest employer of introverts." More widely, it has been described as the world's largest single employer of mathematicians. While its headquarters is located at Fort Meade, it is separate from other compounds and agencies that are based within the same military installation. The NSA is recognized as the largest employer in the state

of Maryland and two thirds of its personnel work at Fort Meade. In 2011 the NSA was Maryland's largest consumer of power purchasing more electricity than the city of Annapolis, the capital city of Maryland. I don't think it was because someone kept forgetting to turn the lights off! The Baltimore Sun reported in 1995 that the NSA is the owner of the single largest group of supercomputers. Recently the NSA held a groundbreaking ceremony at Ft. Meade for its High Performance Computing Center expected to open in 2016. Called Site M (don't you just love the names they come up with??) the center has a 150 megawatt power substation, 14 administration buildings and at a cost of $3.2 billion covers 227 acres. There are two additional phases planned that would quadruple the space. The NSA also has a number of other facilities across the country.

In the 1960s, the NSA played a key role in expanding America's commitment to the Vietnam War by providing evidence of the North Vietnamese attack on the US destroyer USS Maddox during the Gulf of Tonkin incident. It also provided voluminous information to the US military. However, during the war, a secret operation code-named "Minaret" was set up by the NSA to monitor the phone communications of Senators Frank Church and Howard Baker, as well as major civil rights leaders, including Dr. Martin Luther King, and prominent US journalists and athletes that had criticized the war. But the project turned out to be highly controversial, and an internal review by the NSA concluded that its Minaret program was "disreputable, if not outright illegal." In the aftermath of the Watergate scandal, a congressional hearing in 1975 led by Sen. Frank Church revealed that the NSA, in collaboration with other intelligence agencies had routinely intercepted the international communications of prominent anti-Vietnam War leaders Jane Fonda and Dr. Benjamin Spock. The investigation also uncovered NSA wiretaps on targeted American citizens. After the

Church committee hearings, the Foreign Intelligence Surveillance Act of 1978 was passed into law. This law was designed to limit the practice of mass surveillance in the United States but was enacted before the explosion of the internet and the mass use of cellphone technology.

NSA surveillance has been a matter of political controversy on several occasions, including its spying on prominent anti-Vietnam War leaders and efforts involving economic espionage. In 2013, the extent of the NSA's secret surveillance programs was revealed to the public by Edward Snowden, a contractor for the NSA. According to the leaked documents, the NSA intercepts the communications of over 1 billion people worldwide and tracks the movement of hundreds of millions of people using cell phones. It has also created or maintained security vulnerabilities in most software and encryption, leaving the majority of the Internet susceptible to cyber-attacks from the NSA and other governmental agencies. Domestically, it contributes to mass surveillance in the United States by collecting and storing all phone records of most American citizens.

In the aftermath of September 11, 2001 attacks, the NSA created new IT systems to deal with the flood of information from new technologies like the Internet and cell phones. Programs names such as ThinThread, Trailblazer and Turbulence were developed with advanced data mining capabilities. The massive extent of the NSA's spying, both foreign and domestic, was revealed to the public in a series of detailed disclosures of internal NSA documents beginning in June 2013, most of which were leaked by Snowden. It was revealed that, in addition to intercepting telephone and internet communications of over 1 billion people worldwide seeking information on terrorism, the NSA was also gathering information on foreign politics, economics and "commercial secrets". It was also revealed that the NSA spied extensively on the

European Union, United Nations and numerous governments including allies and trading partners Europe, South America and Asia.

The NSA also tracks the locations of hundreds of millions of cell phones, allowing them to map people's movements and relationships in detail. It reportedly has access to all communications made via Google, Microsoft, Facebook, Yahoo, YouTube, AOL, Skype, Apple and Pal talk and collects hundreds of millions contact lists from personal email and instant messaging accounts each year. It has also managed to weaken or evade much of the encryption used on the internet by collaborating with, (read coercing or otherwise infiltrating) numerous technology companies so that the majority of internet privacy is now vulnerable to the NSA and other attackers. Domestically, the NSA collects and stores metadata records of phone calls, including over 120 million US Verizon subscribers as well as Internet communications, relying on a secret interpretation of the Patriot Act whereby the entirety of US communications may be considered "relevant" to a terrorism investigation if it is expected that even a tiny minority may relate to terrorism.

President Obama has claimed on several occasions that these programs have congressional oversight. Despite these claims, members of Congress stated they were unaware of the existence of a number of the NSA programs or the secret interpretation of the Patriot Act, and have reportedly been denied access to basic information about the programs. President Obama also claims that there are legal checks in place to prevent inappropriate access of data and that there had been no examples of abuse, however, the secret Foreign Intelligence Surveillance Court (FISC) charged with regulating the NSA's activities is, according to its Chief Judge, incapable of investigating or verifying how often NSA breaks even its own secret rules. A March 2009 opinion of the FISC,

released by court order, states that protocols restricting data queries have been "so frequently and systematically violated that it can be fairly said that this critical element of the overall regime has never functioned effectively."

Legal opinions on the NSA's bulk collection program have differed. In mid-December, 2013, US District Court Judge Richard Leon ruled that the "almost Orwellian" program likely violates the Constitution, and wrote, "I cannot imagine a more 'indiscriminate' and 'arbitrary invasion' then this systematic and high-tech collection and retention of personal data on virtually every single citizen for purposes of querying and analyzing it without prior judicial approval. Surely, such a program infringes on 'that degree of privacy' that the Founders enshrined in the Fourth Amendment. Indeed I have little doubt that the author of our Constitution, James Madison, who cautioned us to beware 'the abridgment of freedom of the people by gradual and silent encroachments by those in power,' would be aghast."

However, conversely, later that same month US District Judge William Pauley ruled that the NSA's collection of telephone records is legal and valuable in the fight against terrorism. In his opinion, he wrote, "a bulk telephone metadata collection program is a wide net that could find isolated gossamer contacts among suspected terrorists in an ocean of seemingly disconnected data," and noted that a similar collection of data prior to 911 might have prevented the attack.

The NSA has responded to some of the public controversy. On March 20, 2013, the director of national intelligence, Lieut. Gen. James Clapper, testified before Congress that the NSA does not wittingly collect any kind of data on millions or hundreds of millions of Americans. However he retracted his statement in June of that year after details of the NSA Prism program were published, and stated instead

that metadata of phone and Internet traffic are collected, but no actual message contents. This was corroborated by the NSA director, Gen. Keith Alexander, before it was revealed that the XKeyscore program collects the contents of millions of emails from US citizens without warrants, as well as "nearly everything a user does on the Internet." Alexander later admitted that "content" is collected, but stated that it is simply stored and never analyzed or searched unless there is a "nexus to Al Qaeda or other terrorist groups". In any event the US government has aggressively sought to dismiss and challenge any Fourth Amendment cases raised against it, and has granted retroactive immunity to internet service providers and telecoms participating in domestic surveillance.

The NSA defends its practices as legal and respectful of Americans privacy. According to an NSA spokesperson, if American communications are "incidentally collected during NSA's lawful signals intelligence activities," the agency follows "minimization procedures that are approved by the US attorney general and designed to protect the privacy of United States persons." As another US official puts it, the NSA is not "wallowing willy-nilly" through Americans idle online chat. "We want high grade ore." To achieve that, the programs used by the NSA use complex algorithms that, in effect, operate like filters placed over a stream with holes designed to let certain pieces of information flow through. After the 2001 terrorist attacks, the NSA widened the holes to capture more information when the government broadened its definition of what constitutes "reasonable" collection.

The NSA's US programs have been described in narrower terms in some of the documents released by Edward Snowden. One, for instance, acquires Americans phone records; another, called Prism, makes requests for stored data to internet companies. By contrast, this set of programs shows the NSA has the capability to track almost anything that

happens online, so long as it is covered by a broad court order. The NSA programs are approved and overseen by the secret Foreign Intelligence Surveillance Court (FISC). The NSA is required to destroy information on Americans that doesn't fall under exceptions to the rule, including information that is relevant to foreign intelligence, encrypted, or evidence of a crime.

While the NSA is focused primarily on collecting foreign intelligence, the streams of data monitors inevitably include both foreign and domestic communications. Therefore, officials say, some US Internet communications are scanned and intercepted, including both metadata about communications such as the "to and from" lines in an email, and the contents of the communications themselves. Much, but not all, of the data is discarded. Just how much data is not discarded is one of the issues currently in controversy. Some lawmakers and civil libertarians say that, given the volumes of data the NSA is examining, privacy protections are insufficient.

Documents obtained by the Washington Post indicate the NSA is collecting billions of records a day to track the location of mobile phone users around the world. The bulk collection, performed under the NSA's international surveillance authority, taps into telephone links of major telecommunications providers including providers in the United States.

So how does the NSA track mobile phone users? Just by virtue of being on, a mobile device reveals its location in multiple ways on the basic signaling pathways of the global telephone network. Much of that data crosses US territory, even for foreign registered phones. When mobile devices connect to a cellular network they announce their presence on one or more "registers" maintained by telephone providers in order to connect and bill their counterparts for telephone calls. Registration messages often include a device's "coarse" location, at the level of a city

or country, or a "finer" position based on distance from a particular cellular tower. Many mobile devices and smart phones use Wi-Fi signals as well to fix their location, relying on databases that map millions of hotspots around the world. These signals can locate a device down to a city block. GPS receivers, built into many cellular and satellite telephones can locate a device within a 100 meter radius or less. Most mobile operators also track phones precisely by triangulating their distance from multiple towers in order to provide location-based emergency services.

Three appeals courts are hearing lawsuits against the bulk phone records program used by the NSA, creating the potential for an eventual Supreme Court review. Judges in lower courts, meanwhile, are grappling with the admissibility in terror prosecutions of evidence gained by the NSA's warrantless surveillance. Prior to the Snowden disclosures, courts were generally relegated to the sidelines of the discussion. Now, judges are poised to make major decisions on at least some of these matters in the coming months. Though it is unclear whether the Supreme Court will weigh in, the cases are proceeding at a time when the justices appear increasingly comfortable taking on the digital privacy matters, including GPS tracking of cars and police searches of cell phones.

The New York based 2nd Circuit Court of Appeals recently heard arguments relating to a judge's opinion that upheld NSA's programs legality. Appeals are also being heard by the DC Appeals Court and by the 9th Circuit Court of Appeals. Any court opinion before Congress takes action could influence the lawmakers debate. But even if Congress passes legislation concerning the government's statutory authority to collect bulk records, courts might still be left with confronting constitutional privacy questions. At issue is a provision of the Foreign Intelligence Surveillance Act known as Section 702, which allows the

government to collect communications of non-Americans located outside the US for counterterrorism purposes. However, the program also sweeps up communications of US citizens who have contact with foreign nationals. A critical deadline is June 1, 2015 when the section of law authorizing the bulk records collection is set to expire. If no action is taken before then, that could lessen the chances of a Supreme Court review. Congress may also act first, which could resolve some of the outstanding statutory issues. How NSA data collection would be affected by the expiration of the law is unclear, but some say that the NSA's legal authority to collect many types of data it currently collects would end.

Signaling a "post-Snowden era", smartphone and computer manufacturers are revising their encryption programs and methods. While devoted customers of Apple products these days worry about whether their new iPhone6 will bend in their jeans pockets, the NSA and the nation's law enforcement agencies have a different concern: that the smart phone is the first of a post-Snowden generation of equipment that will disrupt their investigative abilities. The iPhone6 encrypts emails, photos and contacts based on a complex mathematical algorithm that uses a code created by, and unique to, the phone's user, and that Apple says it will not possess. The result, the company is essentially saying, is that if Apple is sent a court order demanding the contents of the iPhone6 be provided to intelligence agencies or law enforcement, it will turn over gibberish, along with a note saying that to decode the phone's emails, contacts and photos, investigators will have to break the code or get the code from the phone's user.

Already the new phone has led to an eruption from the director of the FBI, James B. Comey. At a news conference in September of this year devoted largely to combating terror threats from the Islamic state, Mr.

Comey said "what concerns me about this is a company is marketing something expressly to allow people to hold themselves beyond the law." Apple declined to comment but officials inside the intelligence agencies, while letting the FBI make the public protests, say they fear the company's move is the first of several new technologies that are clearly designed to defeat not only the NSA, but also any court orders to turn over information to intelligence and law enforcement agencies. They liken Apple's move to the early days of Swiss banking, when secret accounts were set up precisely to allow national laws to be evaded.

The move raises a critical issue, the intelligence officials say: who decides what kind of data the government can access? Until now, those decisions have largely been a matter for Congress, which passed the Communications Assistance for Law Enforcement Act in 1994, requiring telecommunications companies to build into their systems an ability to carry out a wiretap order if presented with one. But despite intense debate about whether the law should be expanded to cover email and other content, it has not been updated, and it does not cover content contained in a smartphone.

At Apple and Google, company executives say the United States government brought these changes on itself. The revelations by the former NSA contractor Edward Snowden not only killed recent efforts to expand the law on data collection, but also made nations around the world suspicious that every piece of American hardware and software, from phones to servers made by Cisco Systems, has "backdoors" for American intelligence and law enforcement to access information on those systems. This month, just before releasing the iPhone6 and IOS8, Apple took steps to underscore its commitment to customer privacy, publishing a revised privacy policy on his website. The policy described

the encryption method used in IOS8 as so deep that Apple could no longer comply with government warrants asking for customer information to be extracted from devices. "Unlike our competitors, Apple cannot bypass your passcode, and therefore cannot access data," the company said. By the way, the new security and IOS8 only protects information stored on the device itself, not data stored on Apple's cloud service. On Google's Android operating system users may go into their settings and establish their own encryption for information on that smartphone. The next version of Android will have encryption as the default so the user won't even have to think about turning it on.

So gentlemen, at the risk of wobbling close to a "political discussion", our nation has some very tough issues to tackle in the coming months and years with regard to privacy matters. Concerning the Edward Snowden disclosures, how much of the government and public vitriol is based on the fact that they consider him a traitor or is it that he pulled back the curtain revealing the "all-powerful Oz"? Many law-abiding citizens, me included, believe that "reasonable" intrusions into our everyday privacy are a price of freedom. I certainly want our intelligence agencies to be able to locate and prosecute terrorists and foreign enemies. But we must be ever vigilant about our freedoms. Small erosions in our freedoms can, over time, become dangerous chasms. The NSA's technology is an incredibly powerful weapon…but, like all weapons, in the hands of an ethical and moral person, it can be a tool for good. In the hands of an unethical, immoral person, it can be a tool for evil. Here's hoping that we can find a vigilant watchdog to oversee and control the immense power held in the hands of the NSA. Thank you, gentlemen. This paper will self-destruct in 15 seconds……