Open Norms and Secret Natures:
Impacts of Intelligence Activities over the Internet[1]

Motohiro TSUCHIYA

Visiting Scholar, Center for International Studies, MIT

Associate Professor, Graduate School of Media and Governance, Keio University

taiyo@sfc.keio.ac.jp

Summary

This paper analyzes the political and technological issues surrounding wiretapping over Internet communications. In late 2005, the New York Times reported that the Bush administration had been wiretapping the Internet without warrants. The government could obtain warrants based on the Foreign Intelligence Surveillance Act (FISA), but President Bush admitted in a speech the next day that he had authorized thirty cases of wiretapping without warrants. In reality, thousands of people, or more, may have been subjected to secret surveillance of their telephone calls and e-mail messages. The “war on terror” has become a central focus of American national security policy, and wiretapping is playing a critical role in that war.

Meanwhile, another war is brewing. While governmental intelligence agencies are increasingly, secretly penetrating cyberspace, members of the Internet community are fighting to protect its integrity as a free, open network. The Internet’s open norms are paraphrased as “Autonomous, Distributed, and Cooperative Systems,” and by the popular slogan, “We reject: kings, presidents and voting. We believe in rough consensus and running code.” This is a battle between open norms and secret natures.

[1] This research is funded by the International Communications Foundation, the Telecommunications Advancement Foundation, and the Keio Gijuku Fukuzawa Memorial Fund for the Advancement of Education and Research. The author thanks each of them for their generous support. He also thanks Professor Richard J. Samuels and other staff at the MIT Center for International Studies for hosting him as a visiting scholar.

1. Introduction

When we follow news reports on the United States' war on terror after the attacks of September 11, 2001, we notice that wiretapping, especially in digital formats, has come to play an increasingly important role in capturing suspects. Many suspects have been caught through cyber-surveillance conducted by the U.S. or other governments. The relationship between intelligence agencies and geeks, who develop such digital technologies, is becoming closer.

The intelligence community has become increasingly influenced by digital network technologies. It is taking advantage of the new technologies, but at the same time, it cannot control the rapid diffusion of such technologies throughout the world. This dilemma is posing one of the biggest problems in the intelligence community today. In this paper, I will focus on the rise of geeks and the tension between two information communities: the Internet community and the U.S. intelligence community. The relationship between these two communities signifies the beginning of a new phase of international politics in the information age.

As Jon Katz describes in *Geeks*, the critical role that geeks play in our information society is changing the image of geeks from negative to positive.[2] Businesses, governments, schools, and other organizations cannot function without computers and networks. Geeks built and maintain network technologies, and they design the network technologies of the future. The technologies they create are actually catching up with – and in some cases even surpassing – the higher technologies of national security. Perhaps the most recognized symbol of this phenomenon is Google Earth, which was launched in 2005. If you download free software from Google, you can view detailed, satellite images of almost any place in the world, and even inside the earth's oceans. Until recent times, technologies such as Google Earth were not accessible to the public; they were restricted to the military and intelligence divisions of national governments. Geeks have made these

[2] Jon Katz, *Geeks: How two Lost Boys Rode the Internet out of Idaho*, New York: Broadway Books, 2001.

technologies available to private citizens, and that situation has more than a few governments deeply worried. Indeed, several governments including India, South Korea, and Netherlands have expressed concerns related to national security about Google Earth.[3]

Geek culture tends to denigrate people who work in large, pyramid-style, organizations. Geeks call such people “wonks” or “suits.”[4] One geek once wrote, “We reject: kings, presidents and voting. We believe in: rough consensus and running code.”[5] The cultural divide between geeks and wonks is deepening, even as our society and its national security systems are becoming increasingly dependent on the technologies that geeks produce.

In the next section, two information communities – the U.S. intelligence community and the Internet community – are outlined. In the third section, legal and technological aspects of U.S. wiretapping frameworks are shown. In the fourth section, the Bush administration’s warrantless wiretapping is discussed. In conclusion, I will argue that a better relationship with geeks is necessary in order to improve the capabilities of intelligence agencies in the digital age.

2. Clash of Two Information Communities

2.1. Intelligence Community and National Security

Jeffrey T. Richelson defines intelligence in national security or foreign policy as the “product resulting from the collection, processing, integration, analysis, evaluation, and interpretation of available information concerning foreign [entities.]”[6] The U.S. intelligence community consists of 16 agencies including the Central Intelligence Agency (CIA), the

[3] Dinesh C. Sharma, “Indian president says Google Earth 'aids terrorists'” CNET <http://news.cnet.co.uk/software/0,39029694,39193293,00.htm> October 18, 2005 (access: January 23, 2009).
[4] Katz, op.cit.
[5] David D. Clark, "A Cloudy Crystal Ball -- Visions of the Future," Presentation given at the 24th Internet Engineering Task Force, July 16, 1992.
[6] Jeffrey T. Richelson, *Intelligence Community, Fifth Edition*, Boulder, Westview Press, 2007, p. 2.

Federal Bureau of Investigation (FBI), and the National Security Agency (NSA). The functions of the intelligence community can be divided into four categories[7]: (1) Information gathering, (2) defense against enemy intelligence and sabotage activities, (3) counter intelligence, and (4) secret or covert operation. Information gathering is the most relevant of these functions to the theme of this paper. While information gathering itself has many categories, the major ones are Human Intelligence (HUMINT), Imagery Intelligence (IMINT), and Signal Intelligence (SIGINT). HUMINT entails collecting information by means of human activities, including spying. IMINT is concerned with photographs or other images taken by satellites or airplanes. SIGINT aims to intercept and analyze electronic communications signals. SIGINT had its origins in the interception of encrypted wireless communications on the battlefields of World Wars I and II. Other categories that overlap with SIGINT include Technical Intelligence (TECHINT), Open Source Intelligence (OSINT), Communication Intelligence (COMINT) and Electronic Intelligence (ELINT).

2.2. Internet Community and Freedom

The Internet itself originated in response to military needs, but it was developed by academic researchers once it was established. It was almost hidden from the public for two decades – from the 1970s to the early 1990s – while researchers were using it for academic purposes with funding from the National Science Foundation. “Internet” literally means “a network of networks.” Today’s Internet does not have any central authority, governing body, or funding source. It is a global network of networks operated and maintained by means of loose, voluntarily cooperation.

The Internet is not however, an utterly wild, electronic wilderness. Several organizations are now working on Internet governance; none of them plays a dominant role, though. Such organizations include, but are not limited to, the Internet Society (ISOC), the Internet Engineering Task Force (IETF), the Internet Corporation for Assigned Names and

[7] In some cases, a state has a single intelligence agency, but in many cases, a state has multiple intelligence agencies and they organize an intelligence community. In this paper, I think mainly of the U.S. intelligence community comprising of 16 agencies. See <http://www.intelligence.gov/>.

Numbers (ICANN), and the World Wide Web Consortium (W3C). In addition to these new organizations, existing telecommunications and other entities have interests in Internet governance. They include the International Telecommunication Union (ITU), the World Intellectual Property Organization (WIPO), the World Trade Organization (WTO), the Institute of Electrical and Electronics Engineers (IEEE), and others.

This group of bodies and organizations are collectively constructing a so-called "Internet community." It does not have a strict membership system, so actually anyone interested in Internet governance can participate. Moreover, there is no king or president of the Internet community. Internet governance is shared in varying degrees among Internet organizations such as IETF and ICANN. Important decisions, therefore, are not made by singular individuals or groups, but through deliberative discussion and the open sharing of information. This type of governance is starkly different from the governing behavior of intelligence agencies which emphasize top-down authority and secrecy.

In principle, intelligence agencies do not make decisions by themselves. They receive directives from policy makers and produce intelligence accordingly. Their organization is hierarchical. Furthermore, becoming a member of an intelligence community is extremely difficult; there are extensive background checks and difficult examinations. In contrast, the organization of the Internet community is flat, allowing anyone to enter and exit. The organizing mechanisms of the two information communities are thus quite different.

What matters most in the Internet community is freedom and openness. Although it originated as a result of military needs, academic researchers developed it into an entity of exceedingly liberal character; one may say that it is the most egalitarian community in the world. Anyone can test almost any new technology on it as long as shared protocols are respected. That is the reason why the Internet developed so rapidly on a global scale in its early stages without major investments from governments and commercial companies. Vinton Cerf, who developed TCP/IP, a core protocol of the Internet, called this phenomenal process "innovation without permission.[8]"

[8] Vinton G. Cerf, "Prepared Statement of Vinton G. Cerf," United States Senate Committee on the Judiciary Hearing on Reconsidering our Communications Laws, Wednesday, June 14, 2006 available at

However, the recent expansion of online intelligence activities is becoming a serious threat to the freedom and openness of the Internet. Censorship, cyber-surveillance, and other such restrictions and clandestine governmental intelligence activities are changing the nature of the Internet; this new model of top-down governance is threatening the simple and naive nature that has characterized the Internet since its creation. The Internet community, and the principles on which it operate, are under siege.

3. Wiretapping in the Digital Age

3.1. Technological Changes of Wiretapping

In the beginning of his memoir published in 1985, Stanfield Turner, the former Director of Central Intelligence (DCI) under the Carter administration, wrote that the U.S. intelligence community was facing "significant changes that have taken place in American intelligence in recent years, especially two that were virtual revolutions." The first was "the imposition of external oversight by the Congress and the White House over all secret intelligence activities." The second was "the growth of technological methods of information-gathering."[9] When he wrote that memoir, the Internet was not available for most of the public, but satellites and computers were becoming available to intelligence agencies. Advancement of these technologies was already changing the CIA and other agencies.

The recent development of "personal" computers and of Internet accessibility have empowered individuals to rapidly develop their information literacy, and as a result the Internet has grown at an explosive pace. With the Internet, people not only exchange personal messages, but also create content, disseminate it, and use it for commercial and political purposes. The mass media are not the sole distributors of information anymore. Potentially everyone can distribute information globally. In addition, the rise of blogs is

<http://judiciary.senate.gov/testimony.cfm?id=1937&wit_id=5416> (access: April 12, 2007).

[9] Stanfield Turner, *Secrecy and Democracy: The CIA in Transition*, New York: Perennial Library, 1985, p. 3.

bringing more power to the people.

Because the way terrorists communicate is network-oriented, it is quite natural that they exploit the Internet to fulfill their objectives. In particular, the anonymity that can be achieved through careful use of the Internet confers advantages to them.

However, anonymity on the Internet is not as complete as most people assume. Some footprints can be traced. Intelligence agencies have had some success at intercepting terrorists' messages; one of the best known examples of this is the capture of Khalid Shaik Mohammed, al Qaida's number 3. He was located by means of a Pakistani HUMINT and U.S.-based wiretapping.

How are illegal wiretaps done? One way involves accessing wireless communications such as cordless telephones and mobile phones. Although these devices use encryption, the technological standards are not confidential. A tech-savvy eavesdropper can break in. Fixed telephone lines are easier to tap. They are usually assembled in a distributing board in a building or an outside facility. If someone can break into such a device or facility, he or she can easily listen in on conversations.

Legal wiretapping is much easier to do. A government agency with a warrant can go to a telecommunications carrier and demand access to its network. Telecommunications carriers keep customer records for billing and other purposes, and so it is quite easy to track customers' activities. Tracking mobile phones is also becoming easier as more mobile phones are incorporating GPS and other location technologies. Customers, meanwhile, usually have no way of knowing whether they are being tracked, monitored, or intercepted.

As for the Internet, there are many methods of tracking and monitoring activity. One involves the use of software robots, or "bots". Bots crawl through networks and record what they read. Computer programs can analyze these records for suspicious information. This is perhaps the most rudimentary method, analogous in many ways to the functioning of search engines such as Google. Using bots in the rapidly expanding World Wide Web is difficult and inefficient. The NSA has the most powerful computer systems in the world, but even with the best computer systems it takes some time to find valuable messages in the massive volume of information by the use of bots.

The second method involves obtaining information about a target in a place near it.

If the target accesses the Internet through a Plain Old Telephone System (POTS), it is easy to access his or her information through a telephone company or ISP. Even if the target is using a direct connection such as optic fiber, with the carrier's cooperation his activities can be tracked. This method is very effective if the tracker knows when and where a target is using communication devices.

Another method involves intercepting a target at a connection point such as the Internet exchange (IX). The Internet is network of networks, and its major connection points are called IXs. At IXs various networks, especially large scale networks, physically connect to each other and provide an intersection for the exchange of traffic. Because the volume of traffic is huge, it is not easy to identify individual items of information. However, it is not impossible. All packets going through the Internet have their own IP addresses – one of the sender, and one of the receiver. Sometimes a sender's address is a fake one, but no message can reach its destination without an accurate receiver's address. Because an IP address does not always identify a real person, that might not be enough to catch a suspect. The 9/11 terrorists knew how the Internet worked and tried to avoid being tracked. They didn't use their own computers, but rather public computers in libraries, hotels, and Internet cafes.

IP addresses and other footprints can be edited, modified, or falsified. A software program called an "anonymizer" enables an Internet user to erase his information. Most spammers use fake sender addresses. However, even in cases where footprints are completely erased, this does not mean that tracking is impossible. Servers in between networks can hold clues.

FBI's Carnivore is a modified MS-Windows computer that functions as an intercepting device. When installed into an ISP's network, it finds registered key words within network traffic and makes copies of them (Chart 1).[10] However, some people are skeptical about its effectiveness. Carnivore devices were installed in ISP networks before the 9/11 attacks, and at that time they stored too much information about citizens who were of no terrorist concern. As a result, the FBI abandoned them. If the devices had worked properly and the FBI had maintained and analyzed the records that they produced, the 9/11

[10] See EPIC's web page for Carnivore <http://www.epic.org/privacy/carnivore/foia_documents.html>.

investigations might have been different. The FBI is said to have stopped using Carnivore by the end of 2001, because devices with similar functions became commercially available. To conclude, when the target is clear, it is easier to intercept his online communications; when the target is not known, he or she is harder to find in the ocean of growing digital information.

Echelon, another type of intercepting program, has received much attention, as it is said to “intercept everything.” It is difficult for people outside the intelligence community to comprehend the full scope of Echelon, but technically speaking, it is almost impossible to “intercept everything” in the world. What seems easier for Echelon to intercept is wireless and satellite communications. Wireless signals broadcast in every direction; even to outer space. In some cases, telecommunications carriers use microwave to connect fixed or mobile phones. Information satellites can receive those signals.

However, it might be more difficult to intercept wired optic fibers without the users realizing the interception. Before optic fiber, coaxial cable was used. It transmits very weak signals. If such signals can be detected, messages or conversations within the cable can be retrieved. During the Cold War, the U.S. Navy’s Operation Ivy Bell did this on the floor of the Sea of Okhotsk to intercept Soviet communication. However, no such signals come out of optic fibers. It could be possible to tap into an amplifying device in the middle of a long optic fiber on the ocean floor, but this would be much more difficult.

Today, more international communications traffic runs through optic fiber than through the slower coaxial cable or insecure wireless frequencies. As a result, Echelon’s capabilities are decreasing. Echelon is a surveillance program of the wireless and analog ages. A new program is becoming increasingly necessary in the digital age.

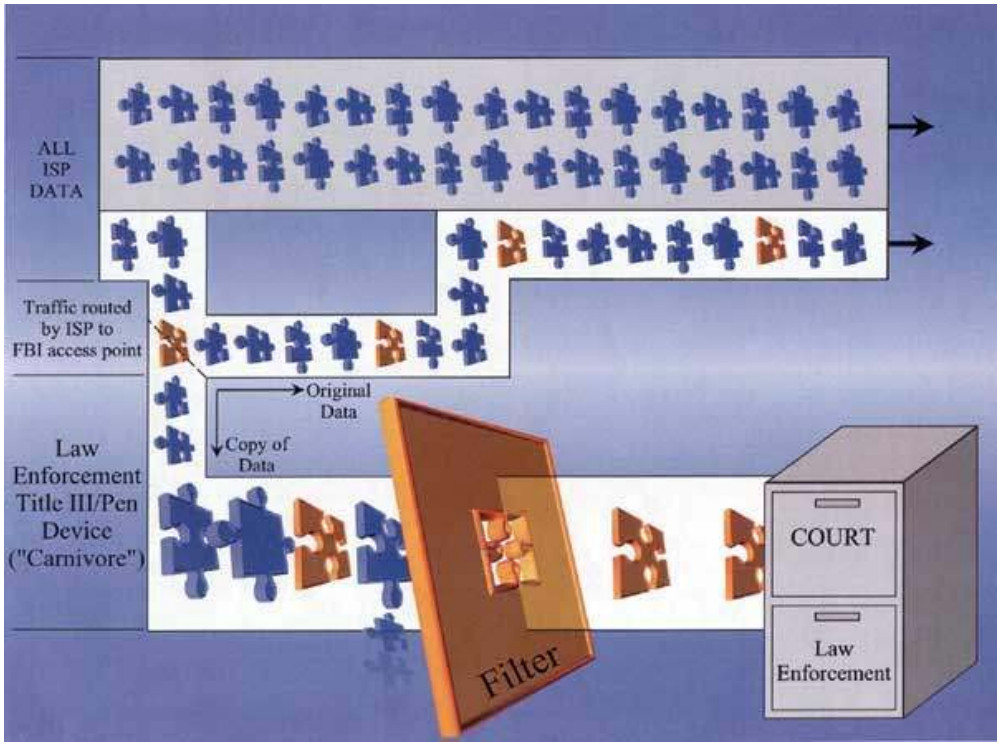

Chart 1: Concept of FBI's Carnivore

Source: FBI website (no longer available as of January, 2009)

3.2. Frameworks of U.S. Wiretapping

Due to today's unceasing, vast flow of information, wiretapping has almost lost its effectiveness. In addition, it is hampered by legal restrictions related to freedoms of privacy and speech. Although the U.S. constitution does not explicitly address secrecy of communications, the first amendment's freedom of speech and the fourth amendment's privacy protection are said to cover secrecy of communications. Freedom of speech requires the protection of secret communication without interception. Also, wiretapping of personal communications without any reason obviously violates people's privacy. Violating secrecy of communication is thus an infringement on constitutional rights.

However, there are two conditions in which such rights do not apply: law enforcement and national security. In order to prove criminality or collect evidence, judicial

wiretapping is used by law enforcement agencies. In rare cases, it is also used to prevent future crimes. Intelligence agencies also engage in executive wiretapping mainly in order to prevent crimes, and particularly organized crimes, including, of course, terrorist attacks. In both cases, “probable cause” is needed to obtain court warrants.[11]

The most important U.S. law related to foreign intelligence is the Foreign Intelligence Surveillance Act (FISA), which was enacted in 1978, as we will see in the next section in more detail. Because the application of FISA warrants is done in secret, there have always been worries that the restrictions on its use are being overlooked.

Many anti-terrorism bills were submitted to Congress after the 9/11 attacks. One of them, which was actually enacted, is the USA Patriot Act (Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism); a combination of the USA and Patriot Acts. This act covers both domestic law enforcement and foreign intelligence, and it modifies and loosens the controls on FISA. One of the most significant elements of this act is the removing of the wall between law enforcement and intelligence. These two groups had not been allowed to share information in the past.

The Patriot Act is a comprehensive law to combat against terrorism, and one of the largest impacts it has had is in the area of wiretapping.[12] Before the Patriot Act, law enforcement and intelligence agencies needed to apply for a separate warrant to intercept each communication device that was used by a suspect. Under the Patriot act, “roving interception” is allowed. Any of a suspect’s communication devices – land line telephone, mobile phone, computer, PDA, etc. – can now be intercepted by a single warrant. Furthermore, agencies can order Internet service providers to submit their records as well as the contents of suspects’ e-mail messages.

The Patriot Act included a number of “sunsets;” sections that were set to expire on December 31, 2005. The Bush administration tried to make the sunset sections permanent,

---

[11] For judicial domestic wiretapping, U.S. Code Title 18 is ruling, especially in Section 119 (Wire and Electronic Communications Interception and Interception of Oral Communications) and Section 121 (Stored Wire and Electronic Communications and Transactional Records Access). For executive foreign wiretapping, U.S. Code Title 50, Chapter 36 (Foreign Intelligence Surveillance) is ruling.

[12] Electronic Frontier Foundation, "EFF Analysis of the Provisions of the USA Patriot Act that Relate to Online Activities," available at <http://www.eff.org/Privacy/Surveillance/Terrorism_militias/20011031_eff_usa_patriot_analysis.html> (access: October 31, 2001).

while some senators and civilian-based groups within the Internet community argued that those sections should expire in two years. The clash of these parties resulted in a compromise: the expiration of sunset sections in four years.

However, there are articles that do not expire after four years. Section 216, for example, gives the attorney general of each state to order the establishment of a "Carnivore" system. This means that orders are not issued by courts, but by attorneys general. Before the Patriot Act, law enforcement and intelligence agencies in the executive branch needed to go to the judicial branch in order to obtain warrants. Under the new law, warrants can be issued from the executive branch. This is a major deregulation.

This change by the Patriot Act was a product of the huge impact of the 9/11 attacks on American society. It also exhibited the U.S. intelligence community's determination to cover up its failure. It was interpreted as a threat to members of the Internet community.

4. Warrantless Wiretapping and the Bush Administration

4.1. New York Times Scoop

On December 16, 2005, the New York Times printed an exclusive story about President George W. Bush's having authorized the NSA to wiretap international communications on a massive scale without court warrants needed required by FISA.[13] The next day, President Bush admitted in his scheduled radio address that he had authorized the wiretapping of telephone calls and e-mails between the U.S. and foreign countries more than 30 times since the 9/11 attacks. According to the Times article, the thirty-time interception actually included hundreds or thousands of calls and messages. However, the President had notified Congressional leaders beforehand. It was not a complete secret within the executive branch.

Wiretapping has a long history of broad application in the United States. There was

[13] James Risen and Eric Lichtblau, "Bush Lets U.S. Spy on Callers without Courts," *New York Times*, available at <http://www.nytimes.com/2005/12/16/politics/16program.html> (publish: December 16, 2005).

no law or regulation over it before World War II. However, under the Nixon administration, wiretapping was abused in the Watergate Scandal. After President Nixon's resignation, Senator Frank Church (D-Idaho) organized a United States Senate Select Committee to Study Governmental Operations with Respect to Intelligence Activities, so-called "Church Committee," in 1975. The committee published a total of 14 reports and recommendations between 1975 and 1976. Those recommendations supported the enactment of FISA and the establishment of the Foreign Intelligence Surveillance Court (FISC) in 1978. When collecting information, FISA "stipulated that we had to use the least intrusive technique that would do the job; that we had to seek only genuine intelligence or counterintelligence, not private information; that the needed information could not reasonably be obtained by normal investigative techniques; and most important of all, that there had to be cause to believe that the United States person being placed under surveillance was an agent of a foreign power."[14] Under FISA, the CIA could not conduct any electronic surveillance inside the United States; it could only initiate requests under FISA and then turn to the FBI to carry them out if the FISC approved.

The FISC oversees all requests for surveillance warrants related to foreign agents in the United States. Under FISA and the FISC, the role of the NSA in domestic wiretapping appeared to end. The NSA itself tried to pull itself out of such activities.[15] However, the 9/11 attacks changed that situation. The FISA, which was enacted in 1978, was no longer functional. President Bush essentially ignored the framework of the FISA.

There were two controversial points in President Bush's wiretapping program. First, why did the Bush administration not obtain warrants from the courts? If warrants had been properly requested and granted, there would have been no controversy. Why did the administration choose to skip the established procedure by issuing its own, secret executive order? Time could not have been the issue, because it was possible to obtain emergency warrants within a few hours even under the 1978 FISA framework.

Second, were some of the subjects of the secret wiretapping United States

[14] Turner op.cit., p. 155.
[15] James Bamford, The Shadow Factory: The Ultra-Secret NSA from 9/11 to the Eavesdropping on America, New York: Doubleday, 2008, p. 27.

persons? According to the law, a "United States person[16]" must not be subjected to wiretapping without probable cause. In the 1970s, civil activists and anti-war groups were subjected to government surveillance. After that, domestic intelligence activities have been more tightly restricted. Secret wiretapping of international calls and e-mail messages could easily include United States persons. Were any privacy protection measures taken during the interception, or were they all ignored?

The case of warrantless wiretapping by the Bush administration reveals that we may no longer assume Internet communications are private; at any time, someone might be listening and/or reading. In fact, though, it has long been possible for anyone in the network to intercept, copy, and/or store people's private calls and messages. Many people know this but are unconcerned because they think have nothing to hide. However, secrecy of communication is a fundamental human right, and a central tenet of democracy that was hard fought and won to protect people from political oppression. The case of the Bush administration underscores that even in democratic societies, the freedom of the Internet community, and with it our fundamental human and civil rights are being threatened. Why did the Bush administration need to do take such a drastic step?

[16] "United States person" is defined as "(A) a natural person who is a citizen of the United States or who owes permanent allegiance to the United States;" and "(B) a corporation or other legal entity which is organized under the laws of the United States, any State or territory thereof, or the District of Columbia, if natural persons described in subparagraph (A) own, directly or indirectly, more than 50 percent of the outstanding capital stock or other beneficial interest in such legal entity."

Internet and Warrantless Wiretapping

Before the 9/11 attacks, President Bush was not deeply involved in intelligence activities. He did not choose his own DCI and kept President Clinton's appointee George Tenet in that position. After 9/11, and probably by November of 2001, he became enticed by NSA's ability to listen to conversations and read messages all over the world. He reasoned that, if the NSA could listen to important conversations among terrorists, the U.S. could prevent future terrorism or at least thwart many attacks. From that point, warrantless wiretapping became a natural extension of his "war on terror."

Chart Two shows the number of FISA applications between 1979 and 2007. The number started increasing when President Clinton was re-elected in 1996, and it increased further under the Bush administration after the 9/11 attacks. This chart does not reflect President Bush's warrantless wiretapping; it shows only the warrants properly authorized by the FISC. In addition, the chart shows that the FISC had denied requests for warrants only nine times in two decades: four in 2003, one in 2006, and four in 2007. The differences among the number of applications and the number of authorizations are due to the government's voluntary withdrawal. At any rate, it is clear from this data that checks by the FISC were not strong.

This trend was influenced by technological changes, and especially by the ever-increasing flood of digital information created by the Internet, mobile phones, PDAs, Voice over IP (VoIP), instant messengers (IM), peer-to-peer (p2p) and other applications. Whereas once communications took place mainly through conventional telephone and facsimile lines, now various kinds of digital bits are sent through a plethora of digital networks, all invented by civilian geeks.

These major, recent technological changes and the 9/11 attacks led President Bush to bypass FISA. He and his administration lay aside the 30-year-old rules and ordered the NSA to eavesdrop on a grand scale. According to James Risen of the New York Times, who first reported about the program, the NSA initially intercepted the calls of five hundreds persons in the U.S. without warrants, and that this trend could lead to the interception of millions of mobile calls and e-mail messages. President Bush ordered this in

secret to locate and uncover hints of terrorism. In order to do this, he signed a secret presidential order in early 2002, and attorneys at the White House, CIA, NSA and the Department of Justice wrote opinion briefs to support his order.

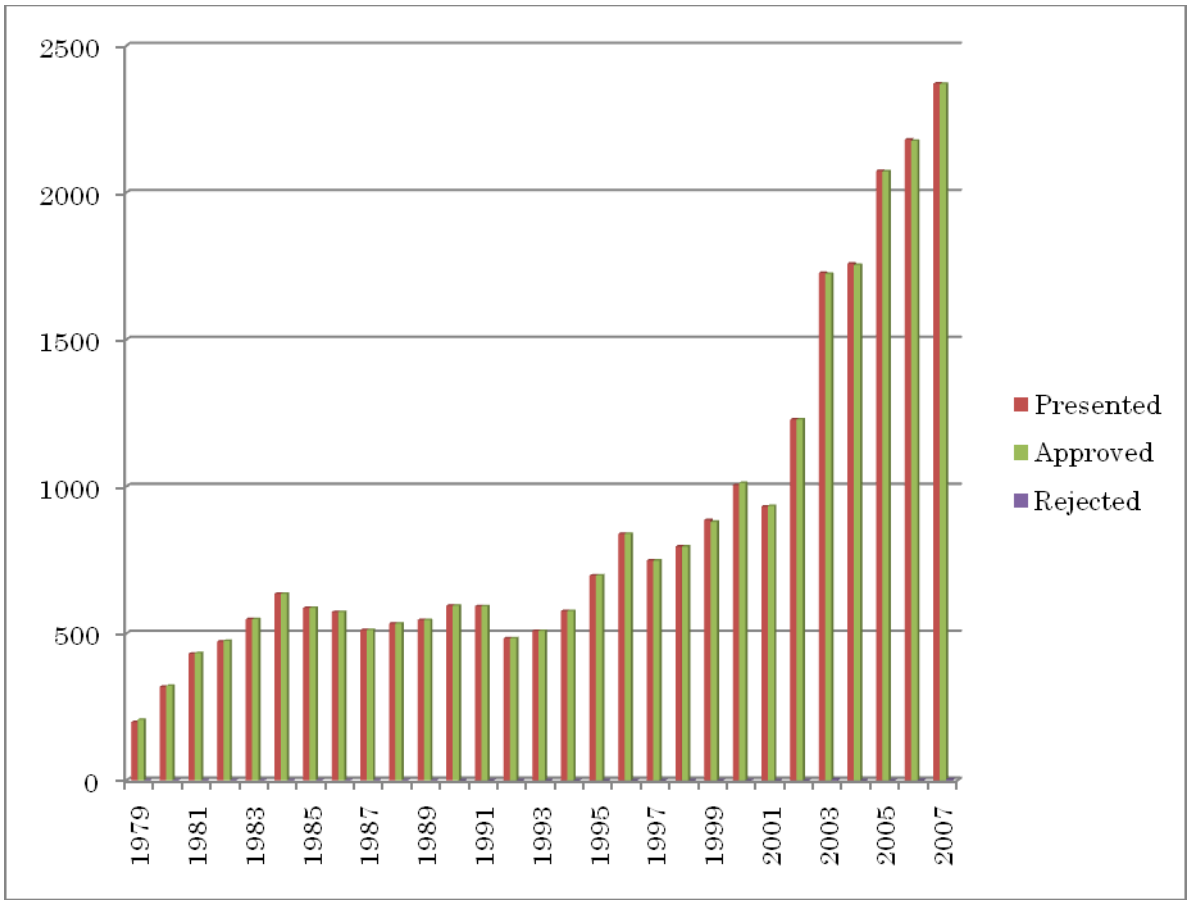

Chart 2: The Number of FISA Applications

Source: <http://www.epic.org/privacy/wiretap/stats/fisa_stats.html> and <http://www.epic.org/privacy/wiretap/>

Why did he do this without courts' warrants? First, the volume of communication traffic was too massive. If the NSA had applied for a warrant to tap each call and record each message, it might have been difficult to catch up with terrorists and to stop terror attacks. In the 1970s, when the FISA was enacted, no one expected such a large volume

of communication. In 2006, nine trillion e-mail messages were sent, and every day one billion mobile phone calls and more than one billion fixed telephone calls were placed. FISA was not written to handle communications in the digital information society. President Bush felt a great urgency to prevent terrorist attacks, and so he reasoned that he could not wait for Congress' actions.

Second, there was actually a great deal of valuable information running through the networks. The United States' long-distance Internet infrastructure is the most advanced in the world, and the U.S. is the world's largest network hub. A lot of global communication traffic goes through U.S. networks, including communications that are neither to nor from the United States. For example, traffic between a Middle Eastern country and a country in Asia might go through the U.S. rather than across India or through the Indian Ocean, because the U.S. route is often faster. If the NSA could access this stream of traffic, it could ostensibly gain various strategic advantages over terrorists.

Chart 3 indicates network bandwidths around the world (domestic routes are not shown). Thicker lines mean more bandwidth. This chart illustrates the Internet's U.S.-centric architecture. The Atlantic lines between the U.S. and Europe are the thickest, and the Pacific lines between the U.S. and Asia also have great capacities.

Chart 4 simplifies the network architecture by bandwidth. Africa is almost completely isolated as it has very little bandwidth. The direct line between Asia and Europe is also quite weak. When someone sends an e-mail from Asia to Europe, it likely goes through the U.S.

Therefore, if the NSA could access traffic between Asia and Europe, invaluable information could be obtained. That is what the Bush administration reasoned.

This decision transformed the world of wiretapping. Even before the Patriot act, American telecommunications operators were required to cooperate with government wiretapping requests, but never had this mandate been so extensively exploited. The Bush administration made requests to carriers on a grand scale and used National Security Letters (NSLs), which obliged those carriers to comply without telling the public what they were doing. Multiple networks of carriers were connected to NSA's network, and the data went to NSA's storage archives to be analyzed. Narus' NarusInsight, a network device that

the NSA was reportedly using, could monitor an entire OC-192 line, which equals 39,000 DSL lines, in a real time. The American Civil Liberties Union (ACLU) released Chart 5 on the Internet to show how carriers' networks were connected to those at the NSA. It was reported that the three major carriers in the U.S. – AT&T, Verizon, and Bell South – were included in the list of companies that cooperated with the NSA. One middle-class carrier, Qwest Communications International, rejected an order to grant access to its network. In a statement on Mat 12, 2005, Qwest CEO Joseph Nacchio asserted that the agency did not have a warrant and that he thought its order was in violation of federal telecommunications laws. Nacchio's stance, however, seems to be a rare case.

After the New York Times article, many people expressed anger and worry about the wiretapping program. The Electronic Frontier Foundation in California has filed a class action against AT&T, which had cooperated with the NSA, and the ACLU has sued the Bush administration. Several other litigations are still underway as of January 2009.

The wiretapping program is changing the way people use the Internet. More people are going online, societies in every part of the world are becoming increasingly dependent on the Internet, but privacy is no longer guaranteed. Although this was true even before the 9/11 attacks, people did not expect the U.S. government was listening and reading their communications on such a grand scale without following established legal procedures. Intelligence activities are required to be undertaken in accordance with the law and under the oversight of both the judicial and legislative branches, but this framework has been broken. As a result, the free and open nature of the Internet is eroding, and the secret nature of intelligence is spreading.

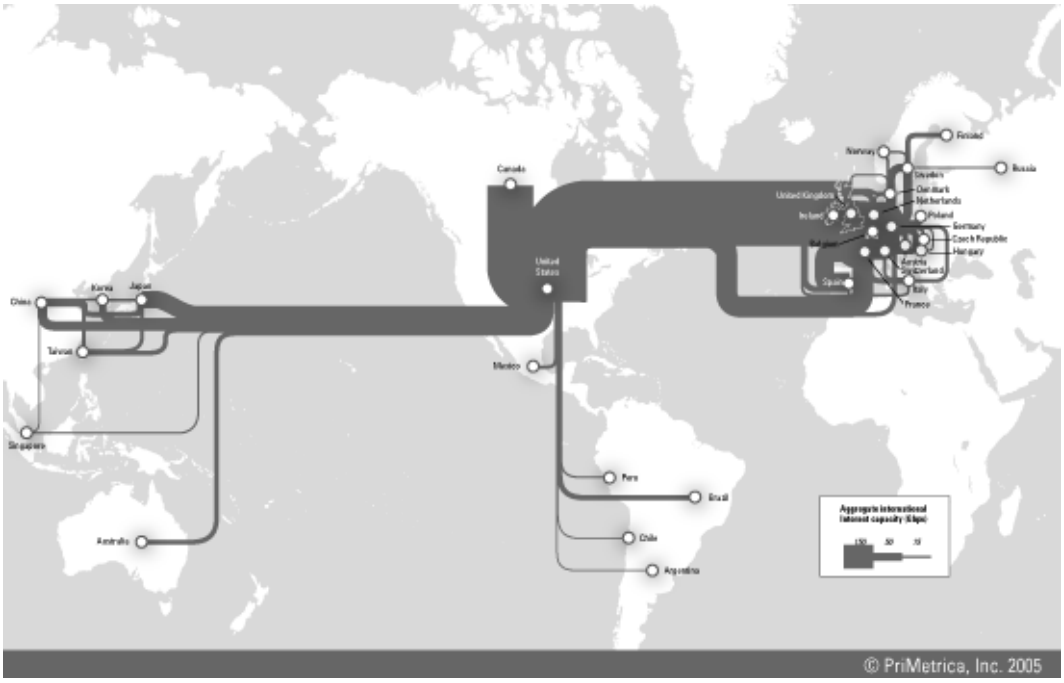

Chart 3: International Internet Architecture

Source: Telegeography.com (c) PriMetrica, Inc. 2005

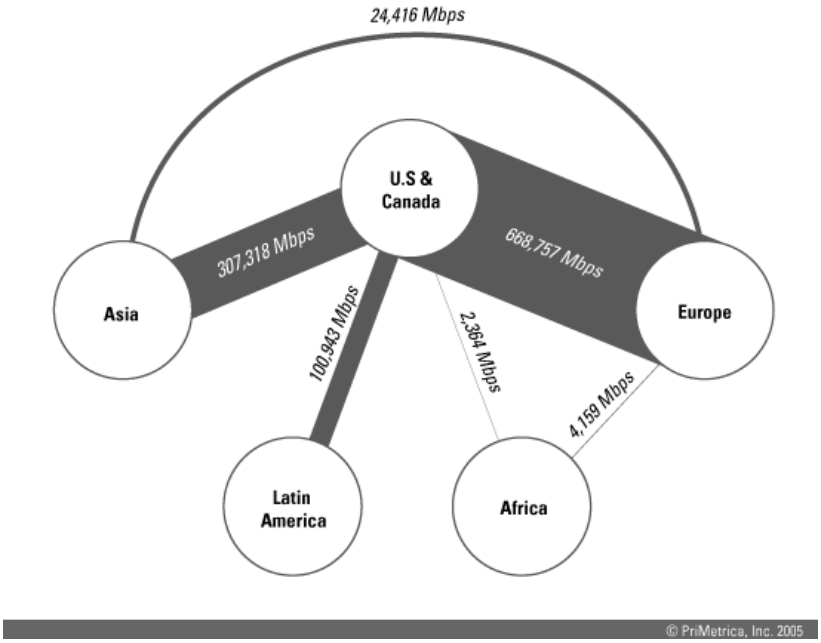

Chart 4: Bandwidth of International Internet Traffic

Source: Telegeography.com (c) PriMetrica, Inc. 2005

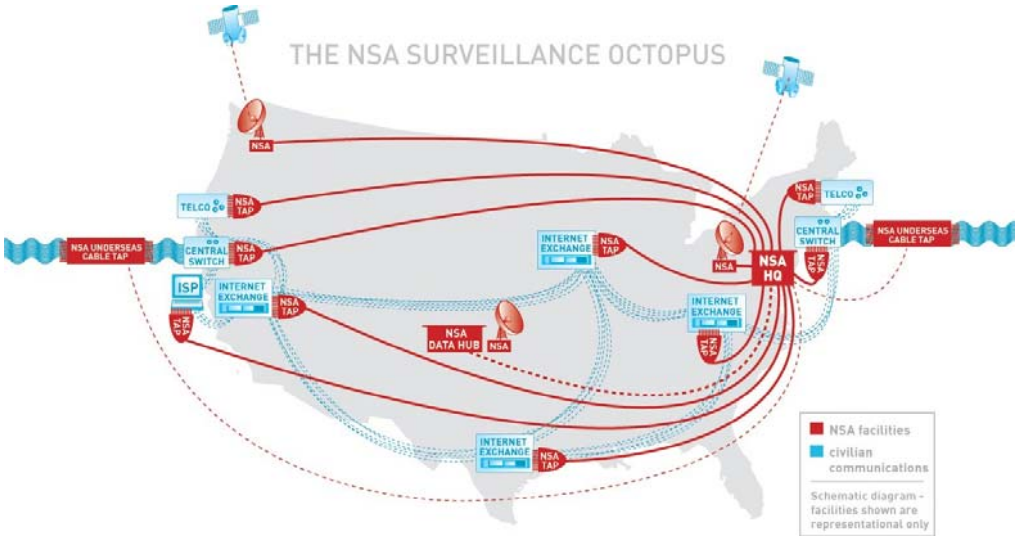

Chart 5: The NSA Surveillance Octopus

Source: http://www.aclu.org/safefree/nsaspying/23989res20060131.html

5. Conclusion

Wiretapping is playing an increasingly important role in today's intelligence activities, as the post-9/11 Bush Administration case bears out. It is a right and responsibility of the judiciary and legislative branches to keep the behavior of the executive branch in check, but this system no longer functions properly. Exacerbating the problem, the U.S. Congress excused the Bush administration's behavior by amending FISA in August, 2008.

What should geeks do then? They have invented and developed systems enabling a massive, global flow of information that governments cannot easily control. In the age of the land-line telephone, intelligence agencies only had to be concerned with snail mail, domestic and international telephone calls, and facsimile. Today, however, digital technologies such as the Internet are easily crossing international borders on a heretofore unimagined scale. Governments are scrambling to devise new ways of dealing with this

unprecedented situation, and in the case of the Bush Administration's warrantless wiretapping, one of the world's most powerful and democratic governments ignored its own system of checks and balances as well as laws that have been on the books for decades in order to streamline its information-gathering, counter-terrorism activities. Technologies that geeks invent are driving governments to radically change the way they handle themselves.

As the 9/11 attacks clearly showed, terrorists are making full use of the Internet and other digital technologies. They use these technologies and applications to collect money, educate and recruit young people, broadcast agitating messages, and develop their plots in collaboration with one another. Not only plain e-mail messages but also cryptographic and steganographic messages are embedded in web-based BBSs or wikis. Terrorist web sites are frequently relocated and are difficult to follow. Terrorists have managed to intrude government computer systems and steal confidential information. They have become adept at concealing their malicious acts online.

Normal Internet-based activities are traceable, much more so that most people realize. Terrorists know this, and so they take care to avoid leaving footprints. It is a cat-and-mouse game between terrorists and intelligence agencies. That is reason why the Bush administration decided to undertake massive eavesdropping over the Internet with the cooperation of all of the major telecommunications carriers. Technological development is a factor that intelligence agencies wish they could forget, because a stable world is a much easier one for tracking targets. In the world in which we now live, however, they need to follow moving targets armed with fast changing technologies.

Most geeks have traditionally not cared about national security issues, and are fundamentally opposed to government intervention into the Internet community. They pursue the development of cyberspace as an independent, egalitarian world. Now that commercialization of the Internet has taken place, it is impossible to fully exclude the government, and tension between geeks and governments is thus rising. Geek-developed technologies will continue to complicate and hinder national and international security, and governmental agencies will continue to contaminate the open and free world that geeks are tying to create.

In order to achieve real international security, a better relationship between geeks

and governments must be forged. This point is largely ignored in most security policy recommendations. Organizational reforms are not enough. What is needed is the formation of flexible and responsive organizations that can keep pace with changing technologies, services and governance.

The Internet community and the Intelligence community are focused on opposing elements of human nature. Geeks believe in freedom and openness, and the intelligence agency personnel are focused on more secretive natures. The Internet community is open to anyone; it places the highest value on information sharing, and is organized on the themes of the common good and voluntarism. The intelligence community is open only to qualified persons, places its highest value on information control, and is organized on the themes of authority and order. These two entities had previously had existed independently of each other, but terrorists are now connecting these two communities.

Confrontation with geeks will only worsen the situation. Inclusion is a far more intelligent and effective approach. The NSA has been able to maintain a degree of supremacy because of its overwhelmingly high level of technology and capable people. If a group came up to surpass it in these ways, though, the result would be a grave threat to the authority of governments everywhere.

Reference

- Bamford, James, *The Shadow Factory: The Ultra-Secret NSA from 9/11 to the Eavesdropping on America*, New York: Doubleday, 2008.
- Cerf, Vinton G., "Prepared Statement of Vinton G. Cerf," United States Senate Committee on the Judiciary Hearing on Reconsidering our Communications Laws, Wednesday, June 14, 2006 available at <http://judiciary.senate.gov/testimony.cfm?id=1937&wit_id=5416> (access: April 12, 2007).
- Clark, David D., "A Cloudy Crystal Ball -- Visions of the Future," Presentation given at the 24th Internet Engineering Task Force, July 16, 1992.
- Electronic Frontier Foundation, "EFF Analysis of the Provisions of the USA Patriot Act

that Relate to Online Activities," available at <http://www.eff.org/Privacy/Surveillance/Terrorism_militias/20011031_eff_usa_patriot_analysis.html> (access: October 31, 2001).

- Katz, Jon, *Geeks: How two Lost Boys Rode the Internet out of Idaho*, New York: Broadway Books, 2001.
- Risen, James, and Eric Lichtblau, "Bush Lets U.S. Spy on Callers without Courts," *New York Times*, December 16, 2005.
- Risen, James, *State of War: The Secret History of the CIA and the Bush Administration*, New York: Free Press, 2006.
- Scheuer, Michael, *Imperial Hubris: Why the West is Losing the War on Terror*, Herndon, Virginia: Potomac Books, 2007.
- Sharma, Dinesh C., “Indian president says Google Earth 'aids terrorists'” CNET <http://news.cnet.co.uk/software/0,39029694,39193293,00.htm> October 18, 2005 (access: January 23, 2009).
- Turner, Stanfield, *Secrecy and Democracy: The CIA in Transition*, New York: Perennial Library, 1985.
- John Yoo, *War by Other Means: An Insider’s Account of the War on Terror*, New York: Atlantic Monthly Press, 2006.