

# The Neighborhood Network Watch

**Emery Caleb Martin**

Interactive Telecommunications Program

New York University

721 Broadway, 4<sup>th</sup> Floor

New York, NY 10012

+1 626 354 2713

emartin@dhsnnw.org

## **ABSTRACT**

In this paper, I will be discussing means by which to increase awareness about network security and power relations embedded within networks. This will serve as an entry point to look at how data transferred over networks can be used by hegemonies and as a means by which to engage the public in critical discourse about technology, the malleability of information, and power relations.

## **Keywords**

art, activism, domestic surveillance, education, information manipulation, network security, politics, power relations, public, simulation, terrorism, text analysis, ubiquitous computing

## **INTRODUCTION**

Given the continued proliferation of networkable devices within the context of the everyday, the topic of network security will also be entering the everyday and the discussion of how politics and power are embedded within networks. Why haven't these issues risen to the forefront of public discourse to a degree proportionate with the proliferation of these technologies? In conjunction, how can the entities that own, control, access, and exert power over networks use the data that is being transferred over them? Why are not the embedded power relations within networks, the usage of data and information by entities of authority, and authority and power itself not being questioned critically by the public?

## **BACKGROUND**

Having grown up using computers from an early age, I have always enjoyed working with them and technology in general. By middle school I became interested in networking computers and would eventually create one for

My own household. This resulted in me eventually working for the computer lab at my middle school and doing some work with the Los Angeles Unified School District. By high school I began to be interested in network exploits and security. However I found myself no longer having time to stay abreast on the topic while pursuing my undergraduate degree.

My interest was reinvigorated while attending the Interactive Telecommunications Program, specifically with a class taught by Raffi Krikorian. The class discussed the implications of our every day usage of technology, primarily situated within the context of investigating TCP/IP networking protocol. This included how vulnerable networks are to eavesdropping especially wireless networks.

I will begin by discussing how Local Area Networks (LAN) function as well as the origins of the Internet in order to contextualize both the governing ideas behind the different network topologies but also to lay the groundwork to begin to discuss the vulnerabilities to eavesdropping.

## **Local Area Networks**

Local Area Networks are the smallest and lowest level form of networks, the type that are typically found in many of our homes. They are typically comprised of a hub, switch, or router that connects multiple networkable devices together via physical Ethernet connections (see Figure 1). Today wireless or WiFi (802.11x) routers have risen to become the prominent [42] type of router populating homes in conjunction with the trend towards using laptops over desktops and the introduction of many WiFi enabled devices. These wireless routers operate in the same way as a typical wired router (see Figure 2), only it does not require a direct physical wired connection to each client connected, rather all communications are broadcasted on a radio frequency through the air. These types of networks are often referred to as Wireless Local Area Networks

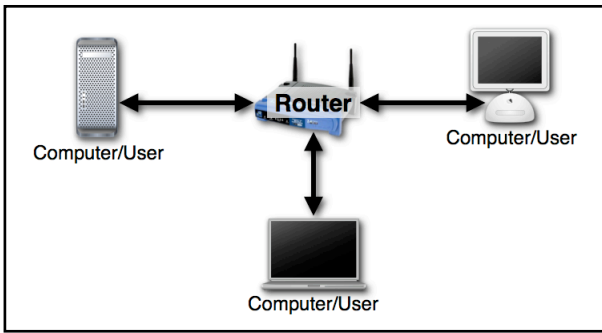


Figure 1. Local Area Network (LAN) Diagram

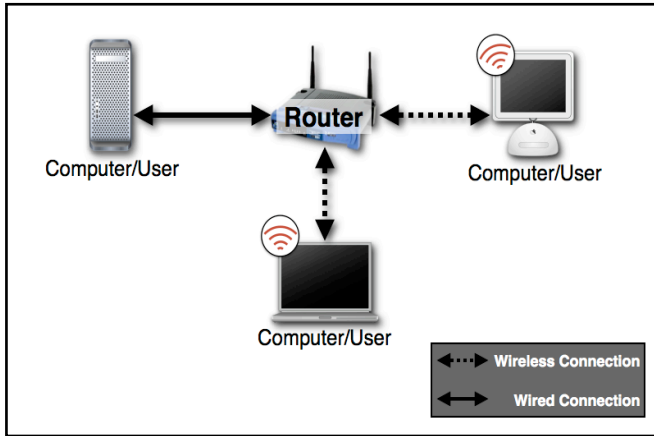


Figure 2. Wireless Local Area Network (WLAN) Diagram

(WLAN). WLAN's have the benefit of being easier to install, since physical cables no longer need to be used to connect each computer as well as providing a fairly large amount of geographical freedom for the user to stray considerable distances from the router. You can see that the LAN requires geographical centralization whereas the WLAN allows more flexibility and allows for geographical decentralization. However, all traffic is still routed through the centralized router. These routers often times still contain wired connections to connect computers that are stationary or lack WiFi connectivity, and hence are a hybrid of sorts, operating both a LAN and WLAN simultaneously. In addition all of these routers generally have a Wide Area Network (WAN) connection that allows a DSL or cable modem to be connected for access to the Internet.

### The Internet Origins and Topology

The Internet for all intents and purposes was designed and built as a response to the potential of a nuclear attack on the U.S. telecommunications infrastructure. After World War II the U.S. conducted research on the effects of the bombing campaigns both on the European and Pacific fronts. This was conducted by the U.S. Strategic Bombing Survey, which came to the conclusion that aerial bombing had been most effective when it was applied to centralized production centers that supplied materials to

other industries [25]. In addition the survey also saw that U.S. cities were constructed in a similar fashion to those of the Japanese cities that had been bombed with atomic bomb [25]. They concluded that American cities should be designed differently to withstand nuclear attack. A move towards decentralization of both U.S. cities and industries was needed in order to minimize damage in the event of a nuclear attack. By decentralizing areas of production and population by geographical dispersion, it would increase the number of targets yet at the same time decrease the effects of a nuclear strike since not all targets could be struck at a given time, hence allowing much critical infrastructure to remain intact.

Therefore, this also meant communication infrastructure would also have to be made nuclear proof through a similar decentralization; such a scheme was tasked to Paul Baran at the RAND Corporation. "His job was to develop a scheme that would ensure the survival of the U.S. telecommunications infrastructure through a Russian first strike—a vital link not only for domestic communications, but also for command and control." [25] Baran would be one of the co-developers of packet switching networks that would eventually lead to the creation of ARPANET and the Internet, which were and are distributed networks not unlike the highway system in the United States [25][26] that were created during the same period, the late 1950's through the 1960's. In a distributed network data is free to flow from one point to another through any available path. It is like the highway system in that it allows similar freedom, as pointed out by Alexander Galloway, "The highway system is a distributed network because it lacks any centralized hubs and offers direct linkages from city to city through a variety of highway combinations." [26] There are no centers there only nodes that connect to and through each other and therefore even if you damage, destroy or remove nodes you will likely still have other nodes to route through in this network structure.

This shift from centralized networks to decentralized and or distributed networks happened around the same time as the shift from modernism to post modernism was beginning. With modernity primarily being concerned with creating universal systems that have one point of view, which centralize and consolidate power [29] and post modernity inverting this to allow multiple vantages and points of view, which decentralizes and reduces centralized power [29]. You can see this transition to post-modernity through the coordinated shifting of telecommunication and industrial infrastructures to decentralized and distributed models. Yet, is power really being reduced? This question goes hand in hand with the question of whether or not post-modernism is actually a shift or rather just another permutation or extension of modernism. Rather it would seem they are dependent upon one another, since post modernism may be seen as simply a reactionary position

taken against modernism that is unable to stand on its own, since it relies on modernism to define itself. Is post modernity, modernity's means to maintain hegemony and reproduce its own ideology? It is possible that it is liken to the McLuhan egg chicken question, "Instead of asking which came first, the chicken or the egg, it suddenly seemed that a chicken was an egg's idea for getting more eggs." [38]

In many ways this is the exact situation with the Internet as a distributed networking system. The model for the Internet was created out of necessity to prevent the breakdown of communications in the event of a nuclear attack. Therefore, decentralization and distribution becomes a necessary means or tactic by which to continue centralized control and hegemony, liken to the egg's usage of the chicken to continue the production of more eggs. How can this be though if the Internet is distributed and allows communication between any node and has no beginning or end liken to Deleuze and Guatarri's rhizome [13][26]? Upon further investigation into the actual construction of the Internet the answer to this question is revealed. Centralized power still exists within the Internet. It exists on multiple levels both at the topological level as well as at the protocol level. [26]

The network topology of the Internet can be described as a, "...system of interconnected packet networks...interconnected using packet-switching computers called 'gateways' or 'IP routers' by the Internet community, and 'Intermediate Systems'..." [30] This can be simplified to mean that the Internet is a series of networks [30] of varying scopes and sizes that may include nested networks within them, branching out like tree branches that are all interconnected through main routers and switches, the "gateways" and "IP routers." These networks at the bottom most level are for instance the Local Area Networks (LAN) found in our homes. These networks connect to Wide Area Networks (WAN) that are operated by Internet Service Providers (ISP) that provide our LANs' access to networks beyond our home, which includes other ISPs and the Internet (see Figure 3). Often times when sending information from one geographical location to another data will travel through multiple networks since its destination maybe outside of the scope of the LAN, ISP, etcetera. For example in order for a computer in Taiwan to connect to France, it cannot directly connect locally obviously and in fact it likely cannot connect directly even at the ISP level, since the ISP's network does not cover these distances between the two countries. Therefore the ISP ends up connecting to other ISPs, that eventually could connect to Tier 1 ISPs that make up the backbone of the Internet, which means they have access to the entire Internet from their networks (see Figure 4). Currently much of this backbone is geographically situated in the United States therefore traffic from Taiwan to France,

would potentially get routed from Taiwan to and through the United States and then on to France. Since the mainstay of the Internets backbone is geographically situated within the United States, it might be apt to point out that the topology of the Internet is not completely distributed and decentralized.

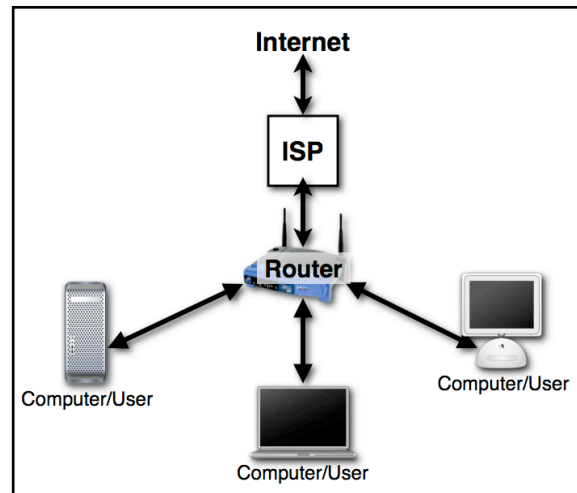


Figure 3. Local Area Network (LAN) to Internet Diagram

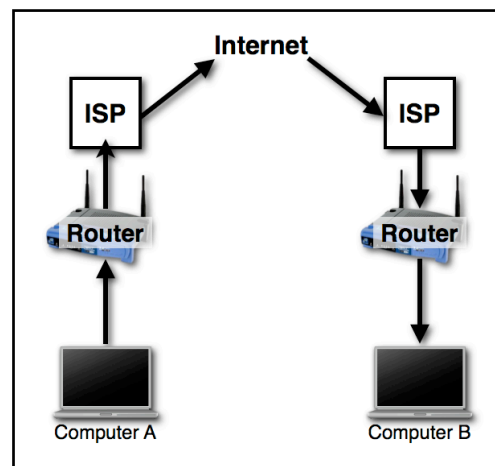


Figure 4. Computer-to-Computer Communication Diagram

This is not unlike distribution of wealth or the rate of modernization that has occurred and is continuing to occur in developing nations. Richard Florida discusses the sharp disparities that still exist despite the so-called flattening of the world brought on by globalization, "By almost any measure the international economic landscape is not at all flat. On the contrary, our world is amazingly 'spiky.' In terms of both economic horsepower and cutting-edge innovation, surprisingly few regions truly matter in today's global economy." [20] This same unequal distribution can be seen in the geographical situation and ownership of the backbone of the Internet and bandwidth. You can see just how uneven, undistributed, and centralized global routes,

bandwidth, and in turn Internet backbone are in Figure 1 in Appendix 1 [46]. In the end the Internet may be a distributed network, however it is not nearly as equally distributed or democratic as Deleuze and Guattari's rhizome. Therefore the common description of the Internet, "...as an unpredictable mass of data—rhizomatic and lacking central organization..." [26] is a fallacy, which also means that, "...the world is..." [26] not "...witnessing a general disappearance of control..." [26] However, there is another layer of where power is being situated that needs to be investigated, this being at the level of the protocols that are used to govern communication on the Internet.

The protocol level in relation to technology can be defined as, "...standards governing the implementation of specific technologies." [26] Essentially it is the law that governs how communication is to be conducted, this is not very different from other previous uses of protocol that range from less formalized social codes to highly formalized codes that would include items military chain of command. These protocols which, govern the Internet, are written and are made available through Request of Comments (RFC) documents [26]. In the RFC Requirements for Internet Hosts, it states the following, "This RFC enumerates standard protocols that a host connected to the Internet must use..." [30] As you can see RFC's are not suggested uses but rather mandates on how you must communicate. Therefore, you can see that at the protocol level the Internet is not at all free from centralized power, but rather maintains the same command and control that it was previously said to be moving away from.

### The Panopticon and Panopticism

Since we have now discussed that the Internet is not free from centralized control or power let us step back a moment to look at similar developments previously in history that started as centralized structures of power and eventually would develop into decentralized or flexible models for control. In 1787, Jeremy Bentham conceived of an architectural model for a prison that would be less abusive, more transparent, and above all economical. This prison was the Panopticon, which was never built during Bentham's life but would be constructed with elements of his vision later on. The Panopticon is essentially a circular prison with the perimeter of the circle being composed of individual cells for individual inmates, constructed in such a manner that they cannot communicate with one another (See Figure 5). The outer walls of each cell include large windows to illuminate the cell at all times, thus keeping the prisoner visible at all times. In the center of the circle there is a central watchtower or lodge, where an inspector may inspect all the inmates from. The lodge is constructed in a fashion so that no inmate can ever discern where the inspector's gaze is directed as well as if the inspector is in the lodge inspecting. The fact that the prisoners cannot view the inspector or determine where he is gazing at any

given moment coupled with the fact that you can always see where the inspector would be is the key to how the Panopticon functions. "The essence of it consists, then, in the centrality of the inspector's situation, combined with the well-known and most effectual contrivances for seeing without being seen." [7]

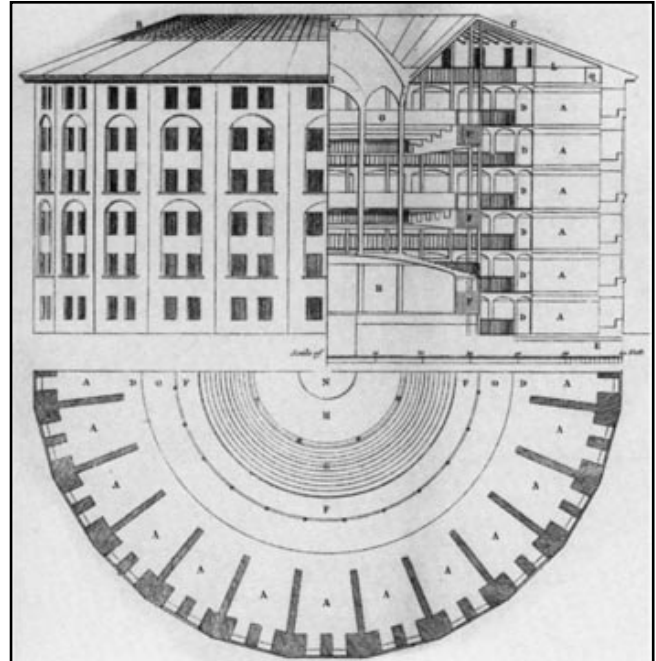


Figure 5. Diagram of the Panopticon

By preventing the inmates from every being able to verify that they are being watched at any given moment, it forces them to self discipline themselves and watch their actions accordingly, since they could be watched at any time, it is essentially a deterrent. In fact Bentham believed that this concept was of the most important aspect and effect of the Panopticon as articulated here, "...the most important point, that the persons to be inspected should always feel themselves as if under inspection, at least as standing a great chance of being so, yet it is not by any means, the only one." [7] In turn this idea that the inmate is not necessarily the only one being watched at a given time combined with the fact that they are likely being watched begins to endow an almost omnipotent and all seeing attribute to the inspector and his lodge. Foucault sums up the main effect of the Panopticon as, "...to induce in the inmate a state of conscious and permanent visibility that assures the automatic functioning of power. So to arrange things that the surveillance is permanent in its effects, even if it is discontinuous in its action..." [23] Here we can see that the Panopticon is not merely a disciplinary mechanism which forcibly confines people, or a Repressive State Apparatus [1] (RSA), but rather it is also an Ideological State Apparatus [1] (ISA), since it affects the consciousness of the inmate as well. In addition it would seem that the

inspector is not necessarily needed for this system to continue to operate once established or possibly at all, since the architectural model is so efficient in generating discipline through the fear of being watched that in turn reinforces the power relations that have been established. Since the inspector is not needed the system operates on its own and is automated to maintain power, "...this architectural apparatus should be a machine for creating and sustaining a power relation independent of the person who exercises it; in short that the inmates should be caught up in a power situation of which they are themselves the bearers." [23] It also allows power to be disindividualized [23] since power is not ascribed to any one person or body, it has been generalized to be the fictitious inspector or the inspectors lodge, which is undefined and therefore could be perceptibly replaced by anything or anyone and in fact was designed to accommodate even the general public [7]. At the same time since, the Panopticon situates power in such a way that it is always, "visible and unverifiable," [23] it begins to articulate and reveal the nature of power relations in the more general sense. "A real subjection is born mechanically from a fictitious relation." [23] This relation that Foucault talks of here is one of power. Here it is mechanically constructed and embedded by and within this architectural model of the Panopticon, yet it also can be applied outside of this context. In fact Bentham saw that the principles that governed the Panopticon directly applicable to many other areas of society, such as hospitals, schools, and workshops [7] all of which require a level of monitoring that would be able to be executed with the utmost efficiency and economy with the application of the panoptic principle. The Panopticon itself was simply a platform that operates in the general sense and hence could be duplicated and replicated. "The panoptic arrangement provides the formula for this generalization. It programmes, at the level of an elementary and easily transferable mechanism the basic functioning of a society penetrated through and through with disciplinary mechanisms." [23]

Bentham's Panopticon is not very different in many ways from a router that may occupy one's home. The router is a centralized node with all computers surrounding it not unlike the inspector's lodge being surrounded by the cells containing inmates. Of course a large difference is that the router allows communication between computers and in fact facilitates it. However, the router is still the centralized point that has command over all the computers in this network. In addition what the router does is for the most part unknown to most users and owners, it is visible but what it actually does is not necessarily readily verifiable, it is automated and generalized, just like the Panopticon. The router is in many ways a perfect example of an apparatus that is highly specialized and in turn become impenetrable, or what many people would refer to as a "black box." We may own the router and setup the router but are we being reduced to mere laborers for the router itself? "The

functionary controls the apparatus thanks to the controls of its exterior (the input and output) and is controlled by it thanks to the impenetrability of its interior. To put it another way: Functionaries control a game over which they have no competence." [21] This would seem to potentially be the case for a large amount of the public that owns routers.

### **Swarming and the Shift Towards Distributed Control**

With the further generalization of the Panopticon and its guiding principles, the Panopticon began to move further from its origin as a prison. This in turn caused the identification of power within the system to begin to disappear from sight as well as the direct linkage with government to dissolve as it became de-institutionalized and disassociated from its origins. In turn this allowed the principles of the Panopticon to develop and spread out, moving from singular centralized inflexible mechanism of discipline to a network of smaller flexible mechanisms of discipline that began to manifest in the everyday. Bentham had hoped this would be the case for the Panopticon. "Bentham dreamt of transforming into a network of mechanisms that would be everywhere and always alert, running through society without interruption in space or in time." [23] In essence Bentham already saw that the move towards generalization, decentralization, and deinstitutionalization as the next logical step for disciplinary apparatuses. Foucault describes this development as, "The swarming of disciplinary mechanisms." [23] These new devices operate ubiquitously within the everyday. For example they become embedded into the fabric of schools and hospitals [23], where the exterior motivations are to provide public services and its interior motivations is to perform surveillance, intelligence gathering, and data mining on the public for the state. "While, on the one hand disciplinary establishments increase, their mechanisms have a tendency to become 'de-institutionalized', ...and to circulate in a 'free' state; the massive, compact disciplines are broken down into flexible methods of control, which may be transferred and adopted." [23] From here Deleuze, in his *Postscript on the Societies of Control*, moves us one step further beyond the now decentralized methods of flexible control that can be situated with modernity, to distributed modulating control that is of the post modern order or the "societies of control." Deleuze defines this new form of control being, "...based on protocols, logics of 'modulation,' and the 'ultra-rapid forms of free-floating control...'" [26] Since, the Internet operates under a set of defined protocols, it may be apt to say that the Internet itself is prime example of "modulating control."

### **Eavesdropping on Networks**

We have not discussed surveillance however or inspections, as it were. Can the router inspect the data we send over the network? Yes, absolutely, in fact many routers have built

in filtering for both incoming and outgoing traffic some of which must be configured by the user and others that are existing as its normal or default state. This can be done further up at any point along the route that data maybe traveling say on its way to a computer outside our network or to a website. During its route from our computer to our router, to our ISP, through their infrastructure, onto other ISPs, to the gateways to the backbone of the Internet and back down again, the data being sent can be inspected. Any of these centralized points or pathways are places where surveillance may be carried out. It can be done without the knowledge of those sending and receiving often times and therefore it is unknown when or where eavesdropping may occur, liken to where the gaze of the inspector is situated, in the Panopticon.

What can be seen though and how? Let us first start with the how and then move onto the what. Surveillance on networks can be carried out using a number of methods however I will focus on one of them that being a technique known as “packet sniffing.” “Packet sniffing,” allows someone to view the packets of information being sent across a network. This includes information such as whom the packet is from and whom it is addressed to as well as the contents of the packet or payload. “Packet sniffing” can be carried out by using software that is used for analyzing networks which are sometimes called network analyzers, protocol analyzers or simply packet or network sniffers. Sniffer software allows a network card on a computer to attempt to listen and capture all packets that are being transferred over the network, whether they are addressed to the computer running the sniffer or not. The computer operating the sniffer must be connected to the network. Since wireless networks transmit data by broadcasting the network traffic to and from users on a specific radio frequency, sniffing a wireless network only involves listening in on the correct frequency to capture the packets being transferred. In many cases this has been seen as a security liability and issue with wireless networks since they broadcast data through the air and do not require a physical connection and presence that is geographically local.

“Wireless networks are always open – Physical media does not protect them. Any device that implements the same radio interface can access a wireless network...Attacks are not limited by location or distance. The distance from where the attacker can reach the wireless network is only limited by the power of the transmitter.”[42]

The sniffer, once operating can essentially view or capture all information being transferred over the network, which would include things like, emails, websites, login information, passwords, etcetera. Just like the inmate within the Panopticon, which is always in view of the

inspector, a packet sniffer can view the computers and data being transferred and received over a network at any given time. Of course packet sniffers may drop at times not receive all packets of data being transferred, also known as dropped packets, but they are able to capture most if not all of them. Very quickly you can see the type of eavesdropping that can be used, where it can be used, and what it can see.

One might then infer that “packet sniffers” must be only available to entities like the government, corporations, and trained technicians, who know how to operate them as well as operate them in ways that are not nefarious. This is not the case at all, many network diagnostic tools are open source and free, in fact they are often times built right into the operating system as in the case of Unix based operating systems. TCPDUMP is one of the most common and readily available networking-debugging tools that include packet sniffing. It is a command line based tool, so it is not necessarily the easiest application to use and in fact this may operate as a deterrent to usage by non-professionals, that works on almost any UNIX based operating system and is often built into the operating system as is the case with the Mac OS X operating system from Apple Inc. TCPDUMP is also available for Windows as well and therefore TCPDUMP is nearly available to any operating system. It allows for traffic to be outputted in real time as well as to be written or dumped to a file for later analysis.

During the course of my time at ITP, I eventually became quite proficient with TCPDUMP as well as other tools such as Ethereal and KisMac. Once I was able to penetrate the unwelcoming exterior of TCPDUMP it quickly became evident to me that network eavesdropping in many ways was incredibly easy and simple. Even more so with wireless networks since you did not even need a physical connection to a gain access to a network. Upon learning and realizing how easy it was to eavesdrop on wired and wireless network traffic with free, readily available, and at many times built in software tools, I began to ask the question of, if eavesdropping on network traffic can be easily and readily done by a normal user what could a skilled user, company, or government use these tools or more advance software packages and technologies for?

This question of course cannot live or be separated from the current climate within post September 11<sup>th</sup> America that has been dominated by the war on terror. Civil liberties have become a frequent casualty throughout the ongoing war, with the justification being always the same, defending our nation from terrorist and terrorism. With this have come legislation, policy, and programs ranging from the Patriot Act to the NSA domestic eavesdropping operations.

To set the stage, prior to the September 11<sup>th</sup> attacks, back in 1997, the FBI deployed an application called, Omnivore, which was a packet sniffing application used for digital wire tapping. The application targeted emails from the suspects IP address and collected accordingly. This system was discontinued in 1999, for a new system known as the DragonWare Suite, which had the capability to collect and reconstruct emails, files, and websites from the targeted individual. Collection of the data was handled by Omnivore's direct successor, Carnivore, which was a regular packet sniffer with customized Perl scripts used to filter out what data should be captured from what data to not capture, in accordance with a court wiretap order. Donald Kerr, former Assistant Director of the FBI stated the following about Carnivore, "The Carnivore device works much like commercial "sniffers" and other network diagnostic tools used by ISPs every day, except that it provides the FBI with a unique ability to distinguish between communications which may be lawfully intercepted and those which may not." [22] After having obtained a court order presumably, the FBI would install a computer operating the Carnivore software on the suspect/s ISP's network and would leave it to collect data, which could potentially be used in court. However, early on Carnivore came under fire when it was found that it was actually collecting more data than it was supposed to be doing, thus violating the court orders, making the collected data un-permissible in court, along with potentially also collecting data from people not covered by the court order, therefore raising questions about violations of 4<sup>th</sup> Amendment rights. Many of these details are uncertain since the program for the most part was kept secret from the public, in fact the former page on the program has been removed from the FBI website. Another question was whether or not the data collected was being sent by the suspect or rather someone else using that computer, as well as the archives of data that may contain actual email contents when a court order had not allowed collection and monitoring of the contents. [24] The FBI eventually changed the name of the application to be more benign, DSC 1000, in order to try and adjust public opinion however by 2001 the usage of the application would be discontinued. The biggest and most pertinent questions coming from the FBI's Carnivore end up being how much and what portions of traffic can be collected, whether the contents of traffic can be data mined, and a questioning of whether or not the current system or issuing court orders, that had been previously used for phone tapping, could be applicable or need to be changed for computer based communications.

These issues would come back to the forefront along with others, with the current class action suit, *Hepting v. AT&T* [18], brought forth by the Electronic Frontier Federation (EFF), in January of 2006. The case accuses AT&T and the National Security Agency (NSA) of unlawfully monitoring communications made through

AT&T's networks, without warrant or judicial oversight. In turn these may have infringed upon both 1<sup>st</sup> and 4<sup>th</sup> Amendment rights as well as breaching AT&T's privacy agreement with its customers.

The monitoring of communications was done by splitting the data stream for the main fiber optic backbone for the Internet, flowing through an AT&T switching station in San Francisco, California, which allowed of the data stream to be copied. This allowed the full data stream to be monitored, analyzed and data mined in addition the hardware that was installed to monitor the traffic also made possible on the fly analysis for known targets suspects. The program began potentially as early as 2001 and has been widely associated with the whistleblower Mark Klein, a former AT&T communications technician that discovered room 641A, which housed the equipment for the joint NSA AT&T domestic eavesdropping operation. Mark Klein's 2005 memo, "AT&T's Implementation of NSA Spying on American Citizens," stated the following in regards to the usage of the splitter on the AT&T network at the San Francisco facility, "...it's only purpose is to enable a third party to examine the data flowing between sender and recipient on the Internet." [33] In regards to the equipment being used in the operation, Brian Reid, the Director of Engineering and Technical Operations at Internet Systems Consortium, stated the following,

"This infrastructure is capable of monitoring all traffic passing through the AT&T facility (some of it not even from AT&T customers), whether voice or data or fax, international or domestic. The most likely use of this infrastructure is wholesale, untargeted surveillance of ordinary Americans at the behest of the NSA." [43]

In addition it is likely that similar rooms were installed at fifteen to twenty other AT&T facilities [43] (see Appendix 2).

This sort of generalized, non-specific and widespread surveillance that likely was being conducted at the AT&T switching station, is particularly troubling not only due to the obvious illegal and unconstitutional nature of these activities but rather due to the ideology behind conducting such a vast operation. This ideology sees all people as potential suspects and targets, and singles them out based on algorithmic criteria, from which they can then assemble the evidence typically needed to initiate these sorts of eavesdropping activities in the first place. Gone are the days of establishing probable cause and gaining judicial approval prior to conducting invasive wiretaps, in this sort of climate with operations now being undertaken in a broad an extralegal manner. Rather it seems that the map has begun to precede the territory, or rather the wiretap prior to

authorization, probable cause, or even suspicion. Which may lead one to infer further into the logic of this ideology and its progressions that would seem to be rooted in a spirit of deterrence by engendering fear and by generalizing all people as potential suspects. In turn this reveals the artificial and constructed quality of the logic that is prevailing in this climate, whose end goal is to simulate and systematically manufacture threats that likely never existed in order to legitimize and as Louis Althusser put, it as the need to, "...reproduce the conditions of its production..."[1] This of course allows the system to be maintained upheld and survive, since without perpetuating the cause for action there can be no continued action. "Simulation is no longer that of a territory, a referential being or a substance. It is the generation by models of a real without origin or reality: a hypereal."[5]

Near the onset of the case, there was a motion put forth by the U.S. government to dismiss the case under the State Secrets Privilege, since the case could potentially endanger national security efforts. In recent years the State Secrets Privilege has been exercised often and freely to the extent that it would begin to seem that there may actually be no threat to national security at all but rather an attempt to avoid embarrassment or scandal. The Supreme Court case *United States v. Reynolds*[45], in 1953, established the government's right to exercise this privilege, after the U.S. government refused to disclose the reports from a B-29 aircraft crash that had three civilian contractors on board. However, once the classified documents that were in question were declassified in 2000, it was found that there was little to no top secret information contained within the withheld documents and rather was an attempt to hide the poor condition of the aircraft that crashed. It would seem that the case, that established the precedent for the usage of the State Secrets Privilege, could be seen as a pretense for the expansion of government power and more importantly establish a government ideology that operates in an opaque extralegal manner. David Lyon, points out that, "...Secrecy feeds upon itself. It increases power without increasing accountability, but often requires more secrecy as greater power accumulates."[35] *United States v. Reynolds* then may have simply be one of the gateways that has enable the climate and culture that is dominating the U.S. government, which has become increasingly more opaque.

The newest and one of the largest cabinet departments, the United States Department of Homeland Security (DHS), can be seen as a prime example of a government body that operates in a particularly opaque fashion. I have had a personal fascination with the DHS since I saw its first iteration as the Office of Homeland Security, created while I was in high school studying U.S. government that involved me actively writing on current events and drawing political cartoons. My fascination began first with the

seemingly unclear, undefined, and overly broad definition of what the Office of Homeland Security was tasked with. The Office of Homeland Security had been given the following mission,

"...To develop and coordinate the implementation of a comprehensive national strategy to secure the United States from terrorist threats or attacks. The Office will coordinate the executive branch's efforts to detect, prepare for, prevent, protect against, respond to, and recover from terrorist attacks within the United States."[41]

I saw the scope of this mission impractical from the onset and the OHS, was indeed ill equipped to actually carry out these tasks since it lacked the actual abilities to implement and coordinate with agencies like the Federal Bureau of Investigation (FBI) and Central Intelligence Agency (CIA). Therefore, how is such an ill defined and overly broad mission statement useful for other than assuring failure? Well it becomes the gateway for the expansion of power through failure to fulfill said mission statement. The founding of a cabinet department, the Department of Homeland Security, would be the first step towards this expansion.

In order to justify the flexing of the DHS' new powers as a cabinet department it would need an identifier to hold up to the public. The Homeland Security Advisory System (HSAS) would become just this. The advisory system was aimed to deliver information about the probability of a terrorist attack occurring, that was broken into five levels of alert, both color coded and named. The system though is completely closed and there is no way to assess its accuracy or even the legitimacy of the system itself. This has been the point that has fascinated me most about the DHS, the complete unverifiable nature about the majority of the claims it makes that seemed to be aimed at simply disseminating fear to substantiate the needs for expanding surveillance, searches, and restrictions on the United States' domestic population. The HSAS functions as reference to legitimize new invasive procedures however the HSAS has yet to be quantified in any way to give it legitimacy, however the DHS has seemed to hold it up as an artifact, a system on which to base decisions off of.

Of course that is not everything the DHS is fueled by, things like Michael Chertoff's intuition or "gut feeling"[3] and the so-called shoe bomber, Richard Clover Reid, would be all things that justify actions and policy. The shoe bomber would precipitate into in the Transportation Security Administration's (TSA) mandate on the removal of shoes when passing through airport security as well as the 3-1-1 rules[49] on liquids, despite the feasibility of being able to combine liquids to create an explosive, such



as TATP, being highly unlikely if not impossible[27]. This has not stopped the DHS from having the TSA continue these regulations that continue to frustrate and hamper travelers and possibly expand and drive the travel size and 3-1-1 specific goods market.[15][52] Since these are regulations, laws, protocols, or codes that have been instated by the DHS and TSA, it would then seem that these frivolous and arbitrary security procedures are simple forms of control, modulated control, that in turn gently reminds us that the DHS and the TSA can have us do just about anything.

This includes who and who cannot fly based on the “No Fly List” which is maintained by the FBI’s Terrorist Screening Center (TSC) which has on occasion used data collected by the TSA. Prior to September 11<sup>th</sup>, the list had a total of sixteen names on it[50]. As of October of 2006, there were 44,000 names on the list, as reported by 60 Minutes[32]. However, the criteria, for the construction for this list, has yet to be articulated concretely or made available to the public or even members of Congress. Therefore it begs the question of is this list based in any sort of reality? Does it have anything to do with terrorism, as it is being positioned as? Is this simply the systematic manipulation and misuse of data and power on behalf of government? All good questions, however I find the manipulation of data the most interesting of the three.

### **Manipulation of Data**

Having done my undergraduate degree in film, focusing on experimental animation, I learned how to effectively use various media, methods and tactics in order to create films. One of the most invasive tactics I found was editing, despite the fact that its exterior is often evasive, seamless and invisible it is none the less still a construction of individual shots. Due to this editing can be seen at times as being coercive, manipulative, and even propagandistic. Early Soviet montage filmmaking has often been seen as coercive and manipulative propaganda due to its glorification of the Soviet state. The verb form of manipulative, manipulation is defined as the following, “The action or an act of managing or directing a person, etc., esp. in a skilful manner; the exercise of subtle, underhand, or devious influence or control over a person, organization, etc.; interference, tampering.”[37] In the case of editing it is not dealing with persons directly rather it is dealing with shots. Therefore, I have always taken issue with Soviet montage films as being simply branded as propaganda, since any form of editing ends up being a manipulative act since the editor exercises power and control by way of choosing shots and assembling shots in order to convey or communicate something, the very definition of manipulation. In fact I would say that Soviet montage films are transparent since there is no disguise that the film you are watching is a complete synthetic construction, whereas Hollywood filmmaking which

employees the principles of continuity editing attempts to hide the hand of the editor, which in many ways is an attempt at deceiving the audience. In the end editing by nature is manipulation and therefore any byproducts of it would be and should be considered the same and not differentiated as being more or less manipulative.

This same idea could be expanded to the handling of any type of data or information not solely that of a filmic nature. Therefore, the U.S. government’s handling of information and data as of recent to generate and construct everything from lists, to the appropriate color code to issue based off of terrorist threats, etcetera, can all be seen as manipulations, manipulations of data. There is a selection or analysis process that is undertaken and guided by some rubric presumably in order to arrive at a destination. However, how and who and what is defining the rubric and the destination is often left undisclosed and shrouded in secrecy, which could be the governmental version of continuity editing, since it is only the polished end goal that matters and is visible.

The results of these processes are purported as truth and reality, despite the potentially highly constructed and manipulated nature of these items that are produced. In fact in many ways these processes and the code that governs them can be seen as highly creative, liken to the accounting practices of Enron. The process though is often rendered opaque, therefore there is no way to examine further and deconstruct, there is no conversation, and since it is purported as reality it becomes so, based solely on the who and/or what that presents it and the way it is presented. Therefore, hegemony is free to define and generate reality at whim and this has been done so. In other cases this process is automated and carried out by an apparatuses, typically technologically advanced and hyperspecialized, which function as diversions from who is exercising control and power. Through this distancing and removal from the process it effectively removes questions about politics and power and replaces them with questions about technology and accuracy. That in turn generates the need for more technology or apparatuses that are more accurate, which creates an infinite spiral directing away from the medium that is inscribed with the ideology to maintain power and control. “For the ‘content’ of a medium is like the juicy piece of meat carried by the burglar to distract the watchdog of the mind.”[38]

### **Agency**

The situation as it sounds seems in many ways utterly lost, hopeless and devoid of any agency. Therefore, where can agency be found if there is any? Well one of the first steps is education and critical questioning. Without this it is nearly impossible to penetrate these system of control and power without being diverted by some, “juicy piece of

meat.” However, education and critical thinking and questioning only allows for penetration of a system to understand it but not engage it. How does one then attempt to engage it when it would seem that there is only a binary, either for or against, 0 or 1? Ambivalence, ambivalence to power and control becomes the key. In Baudrillard’s, *Requiem for the Media* he stated the following about the effects of ambivalence on such a binary system, “But as soon as one posits ambivalent relations, it all collapses. There is no code for ambivalence; and without code, no more encoder, no more decoder...”[4] An ambivalent stance does not recognize the binary and hence does not invest in the fictitious power relations that have been constructed, the binary, and hence can operate externally of them with agency. Essentially one must no longer view power as immutable and absolute and instead must engage it with impunity.

There are a number of artists and artist collectives who I have seen who have used this approach in order to engage with certain issues that would normally be out of the scope of art or even question. Simultaneously I have myself personally made works that have used this same approach.

On May 11<sup>th</sup> of 2005, Megan Collins, Roman Jaster and myself installed a freeway sign, “Honk For Clean Air,”[8][10][31][39] of our design on Interstate 5 South, in Valencia, California. The sign looked nearly identical to a regular traffic warning sign however, the sign did not display a sanctioned message, instead displaying the following, “HONK FOR CLEAN AIR.” (See figure 6).



Figure 6. Photograph of “Honk for Clean Air” – McBean Parkway onramp, Interstate 5 South, Valencia, CA. - 5/12/05

The sign was designed to critique the mass commute from the Valencia to Los Angeles, which had become increasingly filled with sport utility vehicles. It had been inspired by an episode of *South Park* and Richard

Ankrom’s, “Freeway Signs.”[2] Ankrom’s, “Freeway Sign,” is so called “guerrilla public service” as Ankrom calls it. Ankrom created a California Department of Transportation (Caltrans) spec guide sign that was placed on the gantry 23100 to aid motorists in finding the Interstate 5 freeway north since there was no overhead sign. Caltrans did not realize the sign had been placed on the freeway and in fact thought it was actually the work of Caltrans yet later found out and decided to implement Ankrom’s revision coupled with a statement, advising people not to engage in such activities. Our sign stood for five days in contrast, which was much longer than expected. It left some of the public pondering its existence on community forums as well as initiating the occasional honk that could be heard from the nearby overpass. It was successful at blending into its landscape despite it being an unsanctioned foray into the domain of the Caltrans since it was not met with prompt removal. However, the implementation did not produce anyway to gauge any other results beyond this, and it was not possible to assess whether the sign was able to raise awareness or connect with the issue we were exploring. Personally it was my first step into working outside of a sanctioned domain that mirrored the tactics of power and relied on them in order to operate.

This parasitic relationship or mirroring of established institutions has been a tactic employed by a number of artists over time. The Yes Men are probably the best known for this tactic in regards to art and activism, which is sometimes referred to as tactical media. The Yes Men engage in what they call identity correction. Essentially they impersonate, “...big-time criminals in order to publicly humiliate them.”[48] The Yes Men take on the appearances of their targets, assume their languages, and generate spurious look-a-like websites, all in order to allow them to operate as their target, effectively co-opting their identity. They have done this on numerous occasions with probably their best known being when they assumed the identity of Dow Chemicals and publicly apologized and took for responsibility for the Bhopal Union Carbide incident on the BBC’s World Service[48].

Another artist who has worked in a similar manner at times is Coco Fusco, with her performance piece “A Room of One’s Own: Women and Power in the New America” along with the accompanying book *A Field Guide For Female Interrogators*. Fusco takes on the role of a U.S. interrogator at Guantanamo Bay, in order to engage the issues of detention, torture, the War on Terror, women in the military, and Feminism. Her performance primarily consists of herself addressing an audience in a formal and deadpan manner in order to discuss the new opportunities for women as interrogators, since they are able to employ new techniques such as gender and the female body in order to extract information from detainees.[24]

The artist collective Finishing School, takes a similar approach but pushes things a bit further with their 2002 performance and installation, "Today It's Voluntary." [19] The collective took on the role of being a security task force that subjected the patrons to the Huntington Beach Art Center to violations of their privacy and person through data collection, physical searches of belongings and person, and even DNA samples. All of this was done to the patrons under the pretense that it was a new security measure that was for their protection and was voluntary so they could opt out at any time. The performance in many ways was possibly more of a simulation, since actual data was collected, which ranged from address to Social Security numbers to DNA even. They had computer databases to cross check information that was submitted that made usage of public information on criminals. In many ways there are not many things that can be seen as differentiating them from a real security task force. However, once patrons inside there was an instructional video on the violation of the patrons 4<sup>th</sup> Amendment rights and so forth and adding that in all likelihood this could become the norm if post September 11<sup>th</sup> policy went unchecked. In the end they were able to provide a tangible and localized experience to the viewers regarding the dangers of operating under a condition where anything is permissible if it is helping to protect "freedom." However, the project was potentially so well executed that it did not urge viewers to question power, since only three patrons objected and invoked their right to not be searched, since it was voluntary after all.

Lastly I would like to discuss one of my own works that deals primarily with the deconstruction, de-contextualization, manipulation, and re-contextualization of information. This was my 2006 animated short, "Death, Destruction and the Weather Coming Up Next." [12] I was looking to deconstruct and critique the media's representation of war, specifically the Afghanistan and second Iraq War, and reveal its manufactured and synthetic quality. The project involved collecting news footage that was then edited into a short narrative of my own design that was then made into a series of 742 sequential posters. These posters were printed and hung in indoor private and outdoor public suburban spaces as large-scale temporary installations, in order to create a concretized physical manifestation of the news. These posters were then photographed individually, along with the various spaces they were installed within. These photographs were then remade into sequential image sequences that were then edited into an animated short. The piece was able to generate conversations by those passing by the temporary public installations, however its biggest success has been as a film, having been nominated for a Student Academy Award in 2007 and being shown both within and outside the United States.

## **Methodology**

Being immersed in technology while at ITP I found myself in the position of constantly deconstructing and critiquing technology rather than merely celebrating it. This in many ways was due in part to my previous experience with analyzing art and film, but it was also due to the culture I found myself within. I can only describe it as often fully entranced with the aura of technology and technologically determined. In turn I found myself seeking out classes that were driven by critical theory that investigated technology, socio-political issues and art. With current events progressing as they were I became re-invested in the DHS and all issues regarding abuses of power by the U.S. government, especially items dealing with automated surveillance and computer networks. Also, after having spent nearly three years working part time as a computer technician, for both the Apple Inc. and Tekserve, I realized that people often found technology impenetrable, despite innovations over the years. Therefore, without having an entry point through this exterior they would never be able to think about the politics embedded within the devices they use every day.

Therefore, I felt the need and was compelled by all these sprawling interests to attempt to engage the full gamut in some way. Having identified a general lack of awareness of how networks function by much of the public, I felt that networks would be the best and most pertinent entry point through which to tackle these issues. The project I wanted to undertake would use networks as a gateway to discuss network security, the usage of data flowing over networks, the manipulation of data, power and control that is inscribed within technology, post September 11<sup>th</sup> policy and the U.S. government. I felt that one of the most important parts would be allowing the project to be accessible to a broad audience and to allow for direct interaction with individuals in order to educate, engender critique, and engage in critical discourse.

I decided upon making the project large and sprawling, utilizing nearly every medium I have worked in, with each component acting as a building block to create a cohesive, interconnected and interdependent structure or apparatus. It would be based and situated within tactical media activist art practice.

These criteria lead me to decide on creating a simulation of a fictitious community organization dedicated to carrying out domestic eavesdropping operations upon public networks in order to safeguard them, the community and the nation from terrorist threats. This organization would feed off of current events in order to generate its ideology and historical background. Thus entangling itself with current events, post September 11<sup>th</sup> policy, and the U.S.

government. Due to my fascination with the DHS and its invasive and opaque nature, I would link this community group directly with it, in order to directly critique one of the prime examples of post 9/11 policies and current government ideology.

Since, September 11<sup>th</sup>, the government began to enlist all of us in the War on Terror, by asking every citizen to remain vigilant and to never hesitate in reporting the suspicious, since it would be better to be safe than sorry. In many ways we all were being made into extensions of the intelligence community all in order to protect the homeland while generating a culture of fear, paranoia and mutual distrust for our neighbors, especially minorities. Therefore, it would be apt to associate this community group with prior known models that enlisted the communal base, such as neighborhood watch programs. Thus the Neighborhood Network Watch (NNW) came to be. A group modeled off the neighborhood watch groups that people are familiar with but making slight revisions to the formula.

The group would target computer networks instead of suspicious parties or circumstances with its sole purpose to fight terrorism and terrorists that may be living within the community and making use of community networks. It would share information not just with local law enforcement, but also with groups within the intelligence community. The NNW would not target individuals but would rather simply attempt to find networks and generalized areas in which terrorists maybe operating within. The group would take full advantage of all technological resources that were readily available, which would include: off the shelf computers and consumer electronics to carry out operations and web 1.0 and 2.0 infrastructure and technologies to facilitate coordination, communication, and dissemination. The NNW would also adopt a decentralized and distributed organization models mirroring those used by guerillas and terrorist cells, under the pretense that the only way to effectively combat terrorism was to mirror their tactics. In addition a cohesive and consistent ideology would need to be constructed using similar methods employed in revolutionary guerrilla warfare[51] being applied though from the position of a counterinsurgency being backed by the DHS.

I believed that the project could be effective, however for a number of reasons. The first reason, being that it localized the issue of network security and eavesdropping by specifically making use of real networks within the community as reference points. Instead of the conversation remaining at the very top and abstract level that can be seen in *Hepting v. AT&T*[18], where it becomes difficult to fully comprehend the impact, the usage of the local network, that could be in fact where someone may frequent everyday for their morning coffee, quickly situates these

issues directly within a scope that the public can relate with, connect with and understand. This localization provides the entry point to begin to educate people on networks, technology, and the ease in which network eavesdropping can be conducted with even their own home computer. Since, the project operates as a simulation that is technically feasible and tested, it prevents itself from being simply regarded as satire or parody that at times can become ghettoized as simply being humorous and as a result less salient. In addition since it assumes the position of power operating with similar logic systems, ideology, history, and maintains the aesthetic of power it is able to act as a mirror of the systems it is critique but amplifying it due to the obvious illegal implementation and its invasiveness at the community level. As Baudrillard points out, "Simulation is infinitely more dangerous because it always leaves open the supposition that, above and beyond its object, law and order themselves might be nothing but simulation." [5] In the same case the Neighborhood Network Watch becomes much more salient since it begins to reveal and deconstruct the logic that drives post September 11<sup>th</sup> policy. Since, the project is a simulation of what may be the next logical and frightening next step it is also designed to be the object of harsh critique. This critique once begun is allowed to expand organically to the DHS, U.S. intelligence community, and U.S. government practice etcetera. Therefore, the project allows for favorable conditions for the groundwork for critical engagement on these topics but also to simply engage and activate the public to think critically.

## **PROJECT INFORMATION**

The Neighborhood Network Watch can be broken down into five components: collection, analysis, the web presence, the public service announcement (PSA) series, and lately performances. I will now discuss the various components' constructions, technologies, and their roles.

### **Collection**

Collection is essentially the aggregation of data from public networks, with a focus on wireless networks, in order to eventually determine the amount of "terrorist" related traffic maybe traversing the network. The Neighborhood Network Watch uses small one to three person teams, known as NICDs or NICD teams, that are part of the larger Network Identification and Collection Division (NICD). These teams identify networks within the community using readily available information such as online listings and databases of the locations of wireless networks, WiFi stumbling or WarWalking and local knowledge. Maps are generated of the routes and potential targets that have been defined before collection in order to guide the teams. NICD teams collect data using the network diagnostic tool TCPDUMP that is run off of wireless enabled laptops and modified Apple's iPhone and iPod Touch mobile devices. Information that can be collected includes emails, websites,

instant messages and more. Essentially the NICD teams operate at the ground level operating as the eyes and ears of the group as well as the consumers of data; they are the carnivores. The data collected stored in file for later analysis. Please refer to Appendix 3 for an example of the methods used in regards to the collection procedures.

### Analysis

The data that has been previously collected by the NICD teams is then passed on to the Data Analysis Division (DAD). They take the raw data collected and conduct keyword and contextual analysis, with the usage of the Neighborhood Network Watch Keyword Analysis Application (NNWCAA). The NNWCAA software is a java application I have developed, that looks for words that match a list of flagged words. The list, Neighborhood Network Watch Keyword List (NNWKL), is primarily comprised of an ECHELON wordlist that has been combined with publicly available data from both FBI and INTERPOL. If a flagged word is found it then takes note of this and also takes note of the words preceding and following the flagged word. If a word is not flagged the word is cross checked against a dictionary to make sure that the word being checked is indeed a word, thus eliminating the massive amounts of useless characters found in raw network dumps. A count is maintained of the number of flagged words, the total number of words found, the individual counts for flagged words and contextual words. After the entire file has been read, statistical analysis is undergone. The percentage of flagged words to the total number of words is calculated and is denoted as the "Terror Percentage." Depending on the terror percentage the application will give a suggested rating, which follows the DHS' HSAS five-tier system and is named the Network Threat Advisory System (See figure 7). In addition a list of the top 20 flagged words is generated, which is referred to as the "Hit Parade." The probability for a given contextual word following or preceding a flagged word is also calculated and if it meets a certain criteria it will be elected to be included in the supplementary word list which functions just like the NNWKL, however it grows or learns dynamically over time. The statistical results, "Hit Parade," and elected contextual words are exported to text files after the program is finished.

I must note though the NNWCAA is designed in order to artificially inflate the amount of "terror" found in any data it processes in order to accentuate the fact that software and technology do not inherently produce factual information as well as to accentuate the fact that behind every software and technology there is also ideology. In this case the application is aiming to justify the actions of the Neighborhood Network Watch by generating fear that justify continued operations and the expansion of its power. The aesthetics of the application are built explicitly to make a viewer believe that the software is highly specialized and

technical since it takes many of its design cues from command line based software. This also provides for continuity between TCPDUMP. In addition it offers a guise of transparency since it actually displays each word sequentially as it is processing data and denotes whether it is flagged or not. However, the words change so fast that it is impossible to actually gain any insight into how the application operates and thus remains opaque, an embedded critique on transparency. (See Figures 3-4 in Appendix 4)



Figure 7. Neighborhood Network Watch Threat Advisory System

Both these components of the project are not actually carried out by any person within the public but rather are primarily used to generate mock statistics based off of data collected and to be offered up as artifacts during performances and as part of the history on the website. The artifacts range from various types of maps, charts, and graphs. (See Appendix 5)

### Web Presence

The third component, the web presence, operates as the readily accessible public face of the group. It contains its history, its fictitious results, news on the group's activities, upcoming events, policy and future plans, all of which operate as subtle propaganda. This is primarily situated within the official website of the NNW ([www.dhsnnw.org](http://www.dhsnnw.org)). This site mimics the design of the U.S. Department of Homeland Security's website and in fact often links to it, with the transition often between sites being nearly seamless at times. The site is quite vast with now upwards of 120 individual pages. To see the basic site map please refer to Appendix 6.

As mentioned earlier the NNW also makes usage of current Web 2.0 infrastructure; it has presences on two social networking sites, Facebook and MySpace, as well as posts its public service announcements on two Internet video sites, YouTube and Google Video. The NNW sees itself as one of the few progressive entities within the government that is readily embracing the web. The Facebook and MySpace groups are used to inform members on news

about the group, events (performances), as well as provide a virtual meeting place for them. The presence on video sites operates a tool for spurring interest in the group by targeting people interested in networks, the DHS, and technology.

### Public Service Announcements

The public service announcement series, are short videos typically ranging from two to six minutes in length that discuss a number of topics. Some aim to present the fictitious history and findings of the group while others offer documentation of events attended by the NNW, known as “special presentations.” They are narrated by myself and often incorporate me as a high-ranking official for the NNW. The tone of the PSA’s are typically benign and friendly despite some of the outlandish claims and statements made during them, such as this one in regards to what the NNW’s Home Network Awareness Program enables, “...it lets us know if someone maybe using your own home network, or maybe even your neighbors network, for nefarious purposes. That may impact our nation and your own community.”[40] As noted earlier they are primarily viewed within the contexts of either the NNW’s official website and their presences on YouTube and Google Video. In total there are currently four released PSAs with another two currently in post-production, and two more planned.

### Performances

The last component is the performances that are carried out by myself as the so-called “Neighborhood Network Watch Emissary to the Department of Homeland Security” which incorporate all the various components of the project. The title is a bombastic and inflated title that in actually makes no sense upon investigation, however it sounds official. This is coupled with my outward appearance, which consists of a suit, tie, with American flag lapel pin and a pair of black wire frame glasses. As the emissary I use governmental jargon that is stereotypical of a Republican neo-conservative, the DHS, and the Bush administration. This done in a deadpan and benign manner along with body language and gestures associated with politicians. I always get a short edging towards crew cut, haircut and shave for these performances as well (See figure 8). At this point my appearance can correlate and legitimize my bombastic title.

These performances have been typically conducted in academic, art or technology contexts, where there are multiple projects, works, and or presentations being given and shown. The performances are typically done in one of two ways, either a PowerPoint podium style presentation or a trade show or recruitment style booth setup. With the podium style performances, I typically do either a general overview of the group or I focus on a specific aspect of the group, sometimes highlighting the technology components

of the group and always referring people to the website. Also, I typically will take questions from the audience if they have them or make myself available afterwards for discussion.

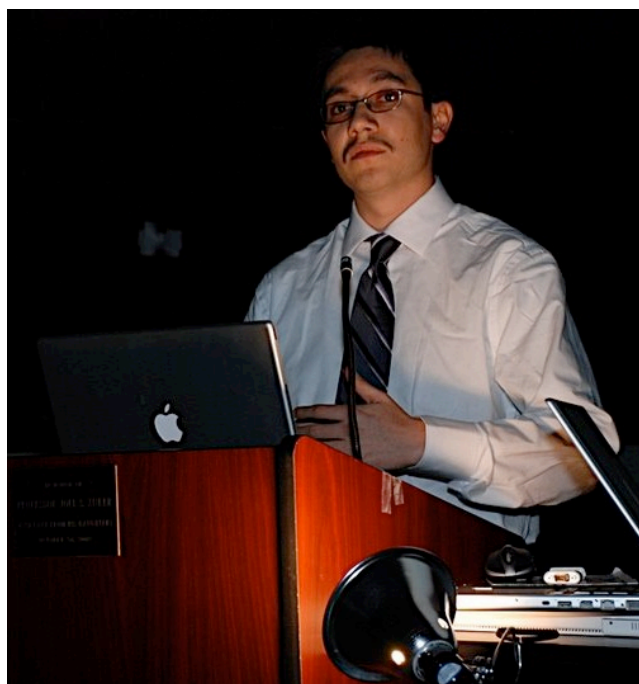


Figure 8. Emery C. Martin as NNW Emissary to the DHS – Hunter College – 11/15/07

With the booth style performances I typically have a long table that will have a computer with the NNW website and PSAs available, a computer demonstrating TCPDUMP and the NNWKAA, visual aids that show the maps and ratings of networks analysis has been conducted on, pamphlets and business cards that are distributed freely and sometimes small memorabilia like buttons (see Figure 3 in Appendix 5). I typically situate myself behind the table in a chair and wait for people to approach the booth before speaking to them. I do not actively try and attract visitors and rather rely on the visuals and the utter lack of cohesiveness with my environment to draw attention. Since, the presentation setups and styles are what are more typical of say a business or governmental meeting or expo, the project ends up standing out since it does not seem to belong within the given context and in turn generates interest. Often times this interest begins as people try and investigate the project from a distance, yet since the information is designed to leave out key information it forces people to begin dialogue with me. At this point the questions often are, “what is this?” or “Why are you here?” At this point I can begin to discuss what the group is, what its mission is, how networks and network eavesdropping can be done, along with how it uses regular consumer technology. I direct their attention to the various visual aids and in fact often urge them to see if they frequent or have friends that

frequent any of the listed locations. A more in depth discussion and at times demonstrations of the technology may sometimes occur. While I am discussing these various aspects I lace it with current policies and events. Throughout this process individuals often begin to raise questions and deconstruct the simulation I have created and presented to them. At this point they come to the realization that these are issues that are important and do have a direct relationship to them and can affect their lives.

## RESULTS

The Neighborhood Network Watch has had numerous results or rather responses. Collection being the first component of the project I will start with it. Collection is a hard area to judge results in since it is a part of the project that has not been readily accessible by the public for the most part and has operated as more of the driving force for the ratings in order to fuel the NNW. In this part it was successful since it was able to provide raw data from thirty-two networks from which ratings could be assessed. Also, the demonstrations of how TCPDUMP works have been fairly effective in demonstrating how a packet sniffer works and how they might be able to use one. Recently the NNW has created a new program known as the Home Network Awareness Program (HNAP)[47] in order to actively teach people exactly how packet-sniffing applications work and how to operate them. Since, the program has just begun no concrete results have yet to be seen on its effectiveness, however it has brought much attention to the project which I will discuss in the section on the web presence.

The analysis portion of the project that has been primarily driven by the development of the NNWKAA, had mixed results early on from the NNWKAA v1-2, however this may potentially be changed with the newest version of the NNWKAA v3.5, which was completed recently. Version 1-2 suffered from being too opaque and closed and hence made the system completely impenetrable and relied on a written or spoken description of what it was doing (see Figures 3-4 Appendix 4). One of the major responses to it during the 2008 ITP winter show was that people wanted to see what words were found that related to terrorism. Version 3.5 has taken this response into account and now presents a highlight of the top 20 flagged words found in the form of the "Hit Parade." Early responses have been mostly positive since it seems that the right balance of transparency, opacity, and feedback has been. The NNWKAA v3.5 is also at a point in development that it maybe allowable to for open distribution to the public, for people to analyze, dismantle and try out on their own with their own data sets.

The Web Presence has been one of the most if not they most successful portions of the project. The social networking presence on Facebook and Myspace has 73

members from all over the U.S. as well as some international members from Canada, Turkey, and Serbia (See figure 9).

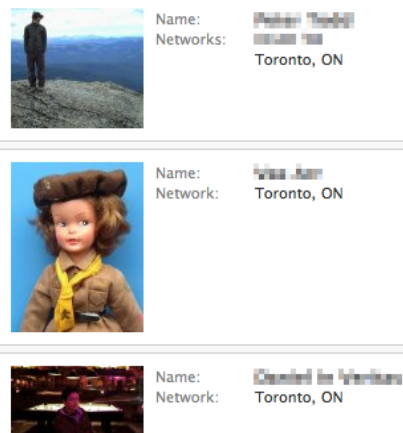


Figure 9. Three Facebook NNW group members from Canada

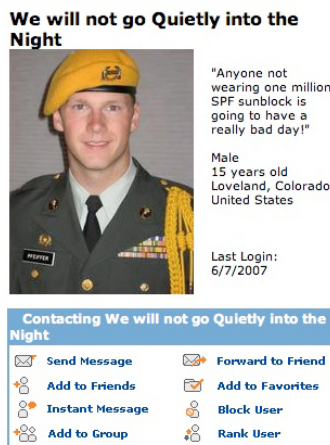


Figure 10. Myspace NNW group member who wanted to learn how he could contribute to the group.

Of these people we have had members who have wanted to actively participate in the groups operations as it were a real government sanctioned group (See figure 10). The Facebook group even has attracted the attention of distinguished members of the network security industry, with one member having been employed as a VP for multiple companies, including 3Com, overseeing network security initiatives and developments. The Public service announcements have been viewed 2,567 times this is excluding the people who have seen them in conjunction with the performances. There have been comments spurred from it that have included quite accurate critiques of the simulation I have created, that have equated it with the Stasi, Gestapo, and Hitler Youth. People have identified that the scariest aspect is the fact that this sort of group is

not entirely far fetched due to the current trend with U.S. policy.

The official website for the group though has had the most success though, having over 20,000 visitors to the site and being referred to by over 600 external sites. A small frenzy began on April 14, 2008, after someone who stumbled upon the site posted it on Reddit[44], the social news site. This began an increase in traffic taking the site from having only a handful of visitors to steadily gaining more traffic.

Simultaneously people began to blog about the site and the group, many believing the group and condemning it and the unethical and illegal manner in which the U.S. government has been operating since September 11<sup>th</sup>. The following week I was contacted by Dan Goodin a reporter from The Register, the United Kingdom (UK) based technology news site, about the website after being tipped off by a reader. The reader who had discovered the site urged Goodin to write a scathing article condemning the continual erosion of privacy in America. Goodin decided to write an article about the project for The Register[28] from which caused yet another wave in traffic which spread news of the group further across the Blogosphere.

This initiated a massive spike in traffic that resulted in over 10,000 visitors within three days (see figures 1-4 in Appendix 8). It has continued to be visited in decent numbers but has fallen off back down to a few hundred visitors a day, which is still well above the numbers prior to April and may change with future events and releases from the group.

In addition the site has gotten traffic from all fifty states in the union and additionally some traffic from overseas, with the UK, Canada, Australia, and Germany being the top four visiting countries outside of the United States (see Figure 5 Appendix 8). I have also seen traffic coming from various elements of the government including the DHS, Department of Defense, FEMA, the Pentagon, as well as more specific groups like the 9<sup>th</sup>, 14<sup>th</sup>, 27<sup>th</sup>, and 377<sup>th</sup> Communications Squadrons. Overall, you can see some of the diversity of those who have visited the site and in turn see that the site has proliferated the project quite well.

The performances have also been a great success for the project. I have since been able to do four performances with one more upcoming currently. They have been at New York University, Hunter College and the Brooklyn art space The Change You Want To See (see Appendix 9). The strategies I had created for the way in order to implement and execute the performances ended up proving to be quite effective.

During the 2007 ITP Winter Show, at New York University, I conducted a booth style performance. The ITP shows are typically quite chaotic affairs, with large amounts of noise, people and typically are not conducive projects that require interactions lasting over a minute or so. However, during the duration of the show, I was able to attract huddled crowds and on average maintained peoples attention for well over five minutes on average. In fact in some cases people talked with me at length for fifteen to twenty minutes at a time. The ploy to design the exterior as to not fit into the atmosphere of the show had worked.

There was one quite unexpected effect that occurred and that was group paranoia and fear that developed as people crowded around while I was already into an explanation of the group. Newly arriving visitors who had not heard the full context for the project would often proceeded to talk with other people trying to gain information. This allowed these visitors to inject their own commentary along with what they knew that only generated more paranoia. This paranoia caused people not to flee but to actually stay longer and ask more questions. The most frequent first questions were, what are you doing, do you really work for the government and why are you here? After answering these questions, often times the next ones were, how are you doing this, you can do this, is this illegal and doesn't this invade my privacy?

Combined these things allowed me the entry point I needed to begin to educate the public about network security and eavesdropping and why they should be concerned. At times visitors began to ask very pointed questions about the criteria and algorithms that were being applied to network traffic as well as who was in control of making these criteria and algorithms. They also began to deconstruct the project, trying to determine whether it was real or not, some of which would leave undecided and discussing this long after they left my booth and the show. I had fellow classmates talk to me after the show letting me know about family members and friends who continued to discuss the project after the show, voicing their concerns and viewpoint on the topics. The pamphlets that were available were taken with a large portion of the buttons by the end of the show. Not all people were able to fully deconstruct the project, however they were still able, to be informed about network security and how it applied to them.

There is another set of results that I will mention that are not a component of the project. These are the personal effects this project has had upon myself. The whole of project quickly became very massive and sprawling and at times quite overwhelming. However, once the major components were established the project began to write itself and in many ways I began to simply play a functionary role. Once the ideology and framework for the



group had been established it became very easy to generate and create all the components. In turn as these parts were created they began to operate not as my own creations but rather as points of references for myself on generating more material for the NNW. For instance I began to reference the website frequently in order to quickly orient myself on how I should write something or determine a course of action. This became frightening at times, since this apparatus, this simulation was starting to operate almost as if it were real. Creation became work for the group.

After doing two performances my character was no longer something that was difficult or hard to maintain. I simply operated according to the ideology of the group; systematically and without hesitation. I am not sure still whether or not my character became an extension of myself or I became an extension of it.

Lastly during the process of generating all the various physical artifacts for the project, such as the business cards, buttons, maps and pamphlets, I found myself deconstructing everyday office supplies. Office Supply stores like Staples became not where I purchased mere functionary office supplies but rather where I purchased instruments of power. All these things I had considered superfluous and useless became necessities to becoming authoritative and exercising power. As a result I will never look at office supplies or office supply stores the same ever again.

#### **FUTURE WORK**

The future of the Neighborhood Network Watch can go in a variety of directions some of which are short term items and some of which are long term or possibly completely separate from the Neighborhood Network Watch. I would like to release the NNWKAA to the public and allow people to actually use it on their own test data whether it is network traffic or just text documents it does not matter. They can start to see exactly how the application works, how it is designed to inflate any threat and also to just simply allow them to use it. This may actually be occurring very soon.

I would like to continue to develop the NNWKAA, but likely move towards making it into a web browser or email client plug-in that would allow it to analyze the sites you visit and emails you send and receive on the fly. Also, in the realm of software I would like to develop a widget to notify them of the rating for the network or general area they are using their computer within.

The Home Network Awareness Program is the area I would like to develop in regards to collection. Currently I have a few friends who are interested in collecting samples from

their own home networks but I would like to expand this and gain a larger base of participants. I think it is important that people not only can conceptually understand how packet sniffing works but also actually attempt it so they can truly understand the ease in which it can be done. With the release of the NNWKAA they could even analyze the data themselves potentially and simply send in the results in to the NNW.

I will be completing the current public service announcements that are in post-production, "How To Watch Terrorist Activity On My Home Network, As Well As My Neighbors" and the latest in the special presentation series, documenting my performance in Brooklyn, New York. In addition I have two other public service announcements that are currently in the planning phase. I also, would enjoy making more of them after this if the project continues.

Lastly I would like to continue to do more performances with larger and more diverse audiences. As well as potentially conducting long format educational and awareness workshops on the various issues raised by the project.

#### **Conclusions**

I believe network security; the usage of networks and who controls them will continue to move to the forefront of society. One of the biggest drivers behind this will be the creation and adoption of networkable devices, especially mobile wireless enabled ones. Networks have and will continue to penetrate further into the everyday and hence these issues pointed to with the Neighborhood Network Watch will continue to be pertinent.

Possibly with the upcoming 2008 U.S. presidential election policy may begin to shift. However, whether all the measures and policy can be or will be rolled back is unknown as well as if this can reverse the damage that has been done. Can the climate of fear and terror be diminished or eradicated within the nation? Maybe it is possible but I do not believe that it will happen overnight and likely, with our current foreign entanglements, the climate will remain for many more years to come. The Neighborhood Network Watch functions to try and raise awareness about the climate and allow people to see just what the costs and ramifications are. Therefore, I believe the Neighborhood Network Watch may remain pertinent in laying the groundwork for beginning to dismantle the current state of fear and terror, even if it has had to engender some fear and terror of its own.

On a personal note I would also like to reflect on the effects the project has had on myself. I have now seen first hand just how an apparatus can begin to move with its own volition and how easy it is to get caught up within it. At times throughout the project I began to reference the items I had created for the group in order to generate more items for the group. What I had created no longer operated as my own but rather it began to work autonomously. I began coming to it for information and guidance rather than relying on myself. It would become a guiding hand that used me as a functionary to write, create and generate new materials for it to sustain itself. This became quite scary at times and left me wondering if I should continue with the project. I am glad though I have seen it through despite at times being lost within it.

### ACKNOWLEDGEMENTS

A very special thanks to Audrey J. Chan, who was always there to support me, always up to talk about and brainstorm about the project, was willing to help me with the production of some of the PSAs and the documentation of the events and to give me tips on my attire. Your help was indispensable and I could not have done it without you. I would like to thank Marisa Olson for her great classes that inspired me and helped fuel the research that would sharpen my own understanding of this project. Raffi Krikorian for his class that spurred me to begin this project. Danny Rozin and Daniel Shiffman for their guidance and support. Thanks to Jonah Bruckner-Cohen, my thesis instructor. Thanks to the two British adjuncts, Rachel Abrams and Sam Howard-Spink. Thanks to Cesar Duran from CSULA, for help with some of the programming. Thanks to all the officers on the Facebook group, Javier Ibanez, Jonathan Kishina, Matthew Muro, and Karen Van Ngo. Thanks to "Team Pizza." Of course thanks to all my friends at ITP especially all those who have been there to encourage me with this project. Thanks to Megan Collins and Roman Jaster who were my collaborators on the street sign and Natalie Bookchin for teaching the Interventions class. Thanks to all my fellow CalArts faculty and alums, who participated and continue to be supportive, especially Robert Dansby. Thanks to my friends back home who have participated and passed around the project. Thank you to Hunter College and The Change You Want To See for allowing me to perform. I would like to thank my family for their continued support. To the Department of Homeland Security and Tom Ridge for inspiration and many laughs, you never cease to amuse me.

### REFERENCES

1. Althusser, Louis. "On the Reproduction of the Conditions of Production." Althusser, Louis. Lenin and Philosophy and Other Essays. n.d.

2. Ankrum, Richard. Freeway Signs. Gantry 23100, Los Angeles.
3. Associated Press. Chertoff remark on terror elicits little alarm. 11 July 2007. 24 Feb 2008 <<http://www.msnbc.msn.com/id/19700127/>>.
4. Baudrillard, Jean. "Requiem for the Media." Baudrillard, Jean. For a Critique of the Political Economy of the Sign. St. Louis: Telos Press, 1981. 164-184.
5. —. Simulacra and Simulations. Ann Arbor: The University of Michigan Press, 1994.
6. —. The Gulf War did not take place. Trans. Paul Patton. Indianapolis: Indiana University Press, 1995.
7. Bentham, Jeremy. The Panopticon Writings. New York: Verso, 1995.
8. Bookchin, Natalie. Interventions 05. 10-05-2005. 06-05-2008 <<http://www.interventions05.blogspot.com/>>.
9. Bush, Rita and Kenneth Kisiel. Information & Behavior Exploitation in Virtual Worlds. Office of Director of National Intelligence; YARPA. Washington D.C.: Office of Director of National Intelligence; YARPA, 2007.
10. Collins, Megan and Emery, Roman, Jaster Martin. Freeway Sign. Interstate 5 / CalArts Interventions 05' Show, Valencia.
11. Critical Art Ensemble. Electronic Civil Disobedience. Brooklyn: Autonomedia, 1996.
12. Death, Destruction and the Weather Coming Up Next. Dir. Emery C. Martin. Prod. Emery C. Martin. 2006.
13. Deleuze, Gilles. "Postscripts on the Societies of Control." October: the Second Decade. Cambridge: MIT Press, 1997.
14. Deleuze, Gilles and Félix Guattari. "A Thousand Plateaus". Minneapolis: University of Minnesota Press, 1987.
15. Easy Traveler Inc. Easy Traveler, Inc. 06-05-2008 <<http://www.easytravelerinc.com/>>.
16. Eisenstein, Sergei. Film Form. New York: Harvest Book, 1949.
17. —. Film Theory and Criticism. Oxford: Oxford University Press, 1992.
18. Hepting v. AT&T. No. CV 06-00672. United States District Court for the Northern District of California. 31 1 2006.
19. Finishing School. Today It's Voluntary. Huntington Beach Art Center, Huntington Beach.
20. Florida, Richard. The Flight of the Creative Class: The New Global Competition for Talent. New York: HarperCollins Books, 2007.
21. Flusser, Vilém. Towards a Philosophy of Photography. London: Reaktion Books, 1983.

22. Forno, Richard. "Who's Afraid of Carnivore Not Me." 05 2000. Cryptome. 06-05-2008  
<<http://cryptome.org/carnivore-rf.pdf>>.
23. Foucault, Michael. Discipline & Punish: The Birth of the Prison. Trans. Alan Sheridan. New York: Vintage Books, 1975.
24. Fusco, Coco. A Field Guid For Female Interrogators. New York: Seven Stories Press, 2008.
25. Galison, Peter. "War against the Center" . Grey Room 4, Summer 2001, p.6-33
26. Gallaway, Alexander. Protocol: How Control Exists After Decentralization. Cambridge: The MIT Press, 2004.
27. Greene, Thomas. Mass murder in the skies: was the plot feasible? 17-08-2006. 06-05-2008  
<[http://www.theregister.co.uk/2006/08/17/flying\\_toilet\\_terror\\_labs/page2.html](http://www.theregister.co.uk/2006/08/17/flying_toilet_terror_labs/page2.html)>.
28. Goodin, Dan. Unmasking the Neighborhood Network Watch. 24-04-2008. 07-05-2008  
<[http://www.theregister.co.uk/2008/04/24/neighborhood\\_network\\_watch\\_unmasked/](http://www.theregister.co.uk/2008/04/24/neighborhood_network_watch_unmasked/)>.
29. Harvey, David. The Condition of Postmodernity: An Enquiry into the Origins of Cultural Change. Cambridge: Blackwell Publishing, 1990.
30. Internet Engineering Task Force. "Requirements for Internet Hosts." RFC 1122 (1989).
31. Jaster, Roman. Interventions. 17 05 2005. 06 05 2008  
<<http://romansinterventions05.blogspot.com/>>.
32. Kroft, Steve. "Unlikely Terrorists on No Fly List." 10-06-2007. CBS News. 06-05-2008  
<<http://www.cbsnews.com/stories/2006/10/05/60minutes/main2066624.shtml>>.
33. Klein, Mark. "AT&T's Implementation of NSA Spying on American Citizens." Dec. 31, 2005. Pdf name is att\_klein\_wired.pdf pg 3
34. Lau, Stephen. "An Analysis of Terrorist Groups' Potential Use of Electronic Steganography." Information Security Reading Room. SANS Institute. 2001.
35. Lyon, David. "9/11, Synopticon, and Scopophilia: Watching and Being Watched." The New Politics of Surveillance and Visibility (2006).
36. —. Surveillance After September 11. Malden: Polity Press in Association with Blackwell Publishing, 2003.
37. "Manipulation Def.4." Oxford English Dictionary. 2nd. 1989.
38. McLuhan, Marshall. Understanding the Media: The Extensions of Man; "The Medium is the Message". New York: Signet, 1964.
39. Measures, Electronic Counter. Jolly Roger Jonesy. 9-17-05-2005. 06-05-2008  
<<http://jollyrogerjonesy.blogspot.com/>>.
40. Neighborhood Network Watch: Home Network Awareness Program Introduction. By Emery C. Martin. Directors. Audrey J. Chan; Emery C. Martin. Performance. Emery C. Martin. 2008.
41. Office of Homeland Security. "National Strategy For Homeland Security." July 2002. U.S. Department of Homeland Security. 22 Mar 2008  
<[http://www.dhs.gov/xlibrary/assets/nat\\_strat\\_hls.pdf](http://www.dhs.gov/xlibrary/assets/nat_strat_hls.pdf)>
42. Petäjäsöja, Sami, Tommi Mäkillä and Mikko Varpiola. "Wireless Security: Past, Present and Future." San Jose: Codenomicon, 1 February 2008.
43. Reid, Brian. "Statement of Telecommunications Expert Brian Reid." EFF. Pdf name reid.pdf pg 1
44. sardis. DHS Neighborhood Network Watch: Snoop on your neighbors wireless and be a patriot. 14-04-2008. 07-05-2008  
<<http://reddit.com/info/6fnm4/comments/>>.
45. United States v. Reynolds. U.S. Supreme Court. 21 Oct 1952.
46. TeleGeography Research. "Late Night Bandwidth Usage." 2007-12-31. i like ellipses. 5-5-2008  
<<http://ilikeellipses.com/2007/12/31/late-night-bandwidth-usage/>>.
47. The Neighborhood Network Watch. Home Network Awareness Program. 18-03-2008. 07-05-2008  
<<http://www.dhnnw.org/hnap.html>>.
48. The Yes Men. Dow Does the Right Thing. 29 11 2004. 06-05-2008  
<<http://www.theyesmen.org/en/hijinks/bbcbhopal>>. The Yes Men. 06-05-2008 <<http://www.theyesmen.org/>>.
49. Transportation Security Administration. 3-1-1 for Carry-Ons. 09-2006. 06-05-2008  
<<http://www.tsa.dhs.gov/311/index.shtml>>.
50. Transportation Security Intelligence Service, U.S. Department of Transportation. "Gordon v. FBI." 12 2002. ACLU. 06-05-2008  
<[http://www.aclunc.org/cases/landmark\\_cases/asset\\_upload\\_file371\\_3549.pdf](http://www.aclunc.org/cases/landmark_cases/asset_upload_file371_3549.pdf)>.
51. Tse-Tung, Mao. Mao Tse-Tung on Guerrilla Warfare. New York: Frederick A. Praeger Inc, Publishers, 1961.
52. 3-1-1 Travel Bag. 3-1-1 Travel Bag. 06-05-2008  
<<http://www.clearbagsystem.com/>>.

# Appendix 1: Unequal Distribution of the Internet's Infrastructure

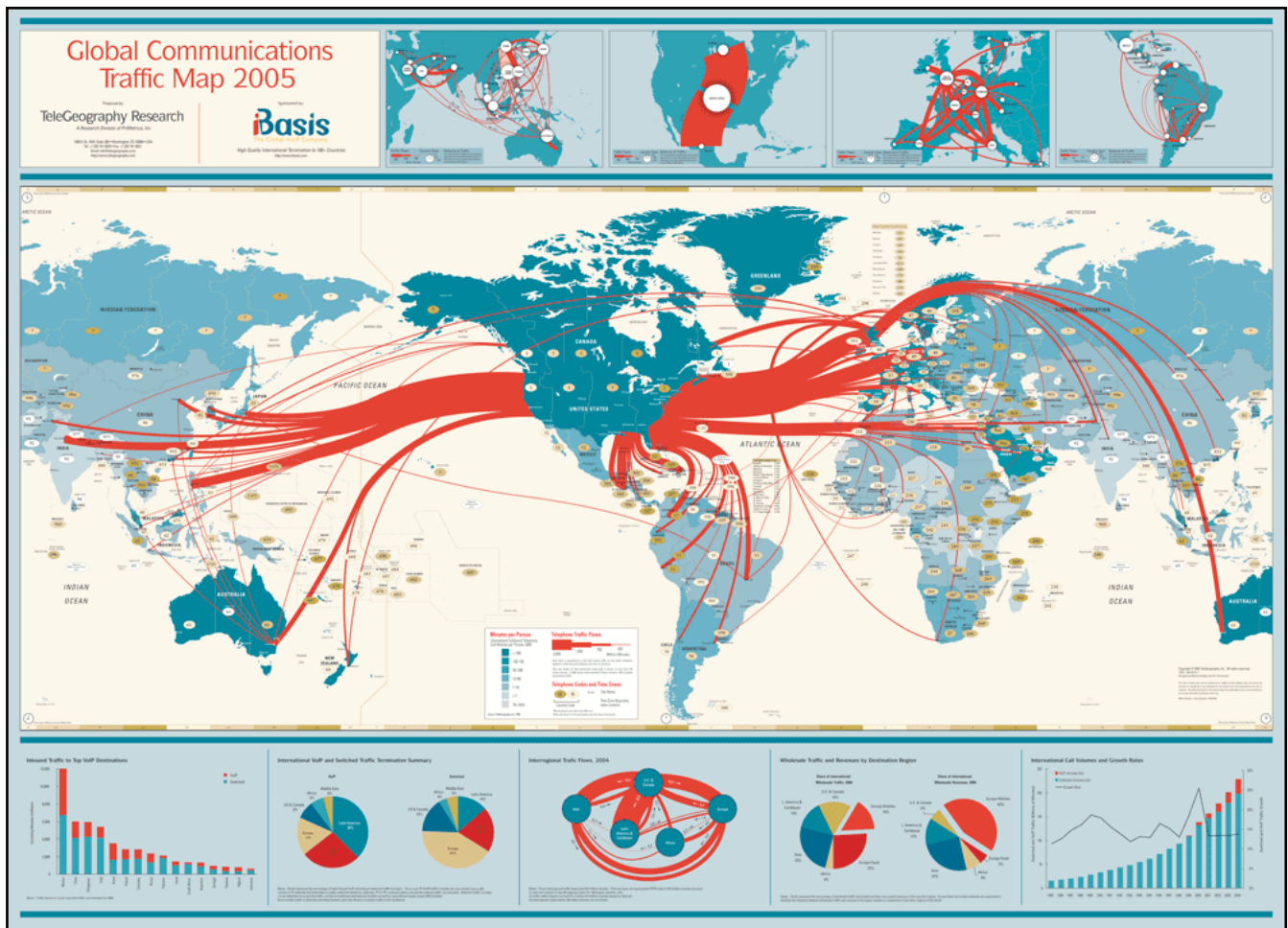
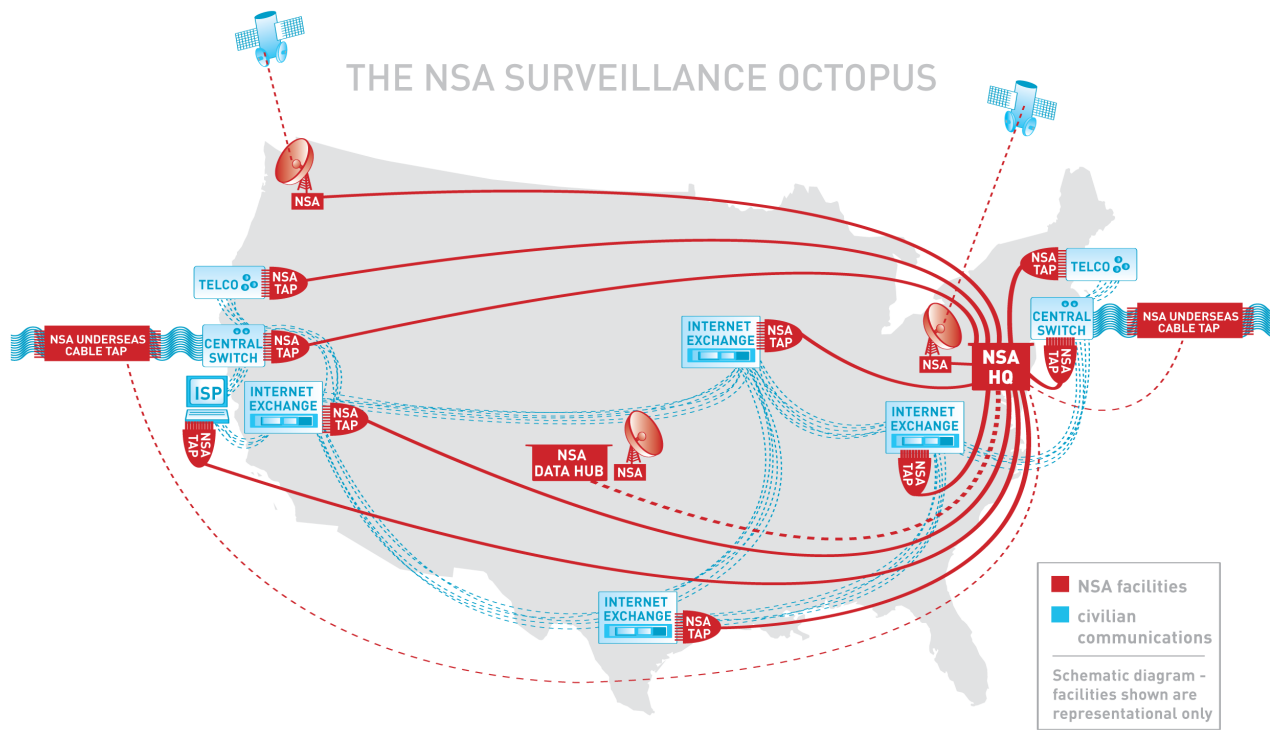


Figure 1. Internet Global Communications Traffic Map-Telegeography (2005) [43]

## APPENDIX 2: ACLU Map on Possible Sites for NSA Intelligence



**Yakima listening post** One way that telephone calls and other communications are sent from the United States to Asia and other destinations is via satellite and microwave transmissions. This NSA satellite facility on a restricted Army firing range in Yakima, Washington sweeps in millions of communications an hour from international communications satellites.



**Sugar Grove listening post** One way that telephone calls and other communications are sent from the United States to Europe and other destinations is via satellite and microwave transmissions. This NSA satellite facility, located in an isolated valley in Sugar Grove, West Virginia, sweeps in millions of communications an hour from international communications satellites.



**Internet Service Provider (ISP)** The NSA may be forcing ISPs to provide it with information in the form of a computer tap (similar to a controversial FBI device dubbed "Carnivore") that scans all the communications that reach that ISP.



**Central switch** These facilities, one in New York and one in Northern California, are operated by major telecommunications companies. They are a primary means by which a mix of voice and data communications, including those that travel over transoceanic undersea fiber optic cables, are routed ("switched") toward their proper destination. Because they serve as central switching points, they offer the NSA access to a large volume of communications.



**Internet exchange** These publicly or privately owned "Internet exchanges" are where Internet traffic is exchanged between the sub-networks that make up the Internet. These public or privately owned facilities are

divided into Tier 1, Tier 2, and Tier 3 exchanges. The Tier 1 exchanges, typically located in big cities, are the ones that have national and global reach and are likely to be of most interest to the NSA.



**Underseas cable tap** According to published reports, American divers were able to install surveillance devices onto the transoceanic cables that carry phone calls and data across the seas. One of these taps was discovered in 1982, but other devices apparently continued to function undetected. The advent of fiber-optic cables posed challenges for the NSA, but there is no reason to believe that that problem remained unsolved by the agency.



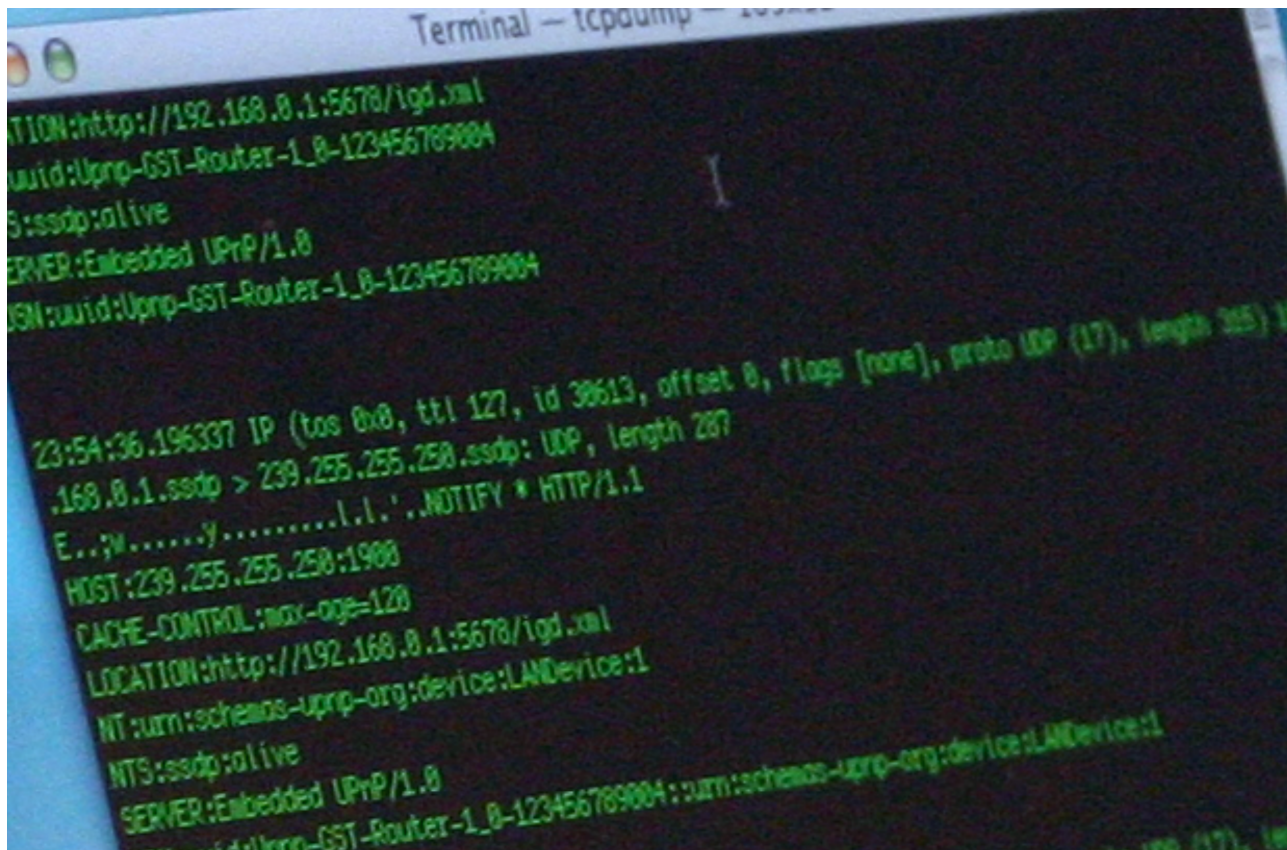
**The NSA's headquarters** Tens of thousands of people, including intelligence analysts, linguists and computer professionals, work at this complex in Fort Meade, Maryland outside of Washington, DC. NSA headquarters is where the millions of intercepted communications are processed and analyzed.



**Telco: Domestic telephone company** The NSA is apparently hooking in to U.S. telephone companies, which have not only networks that can be tapped into, but also records of customer communications.



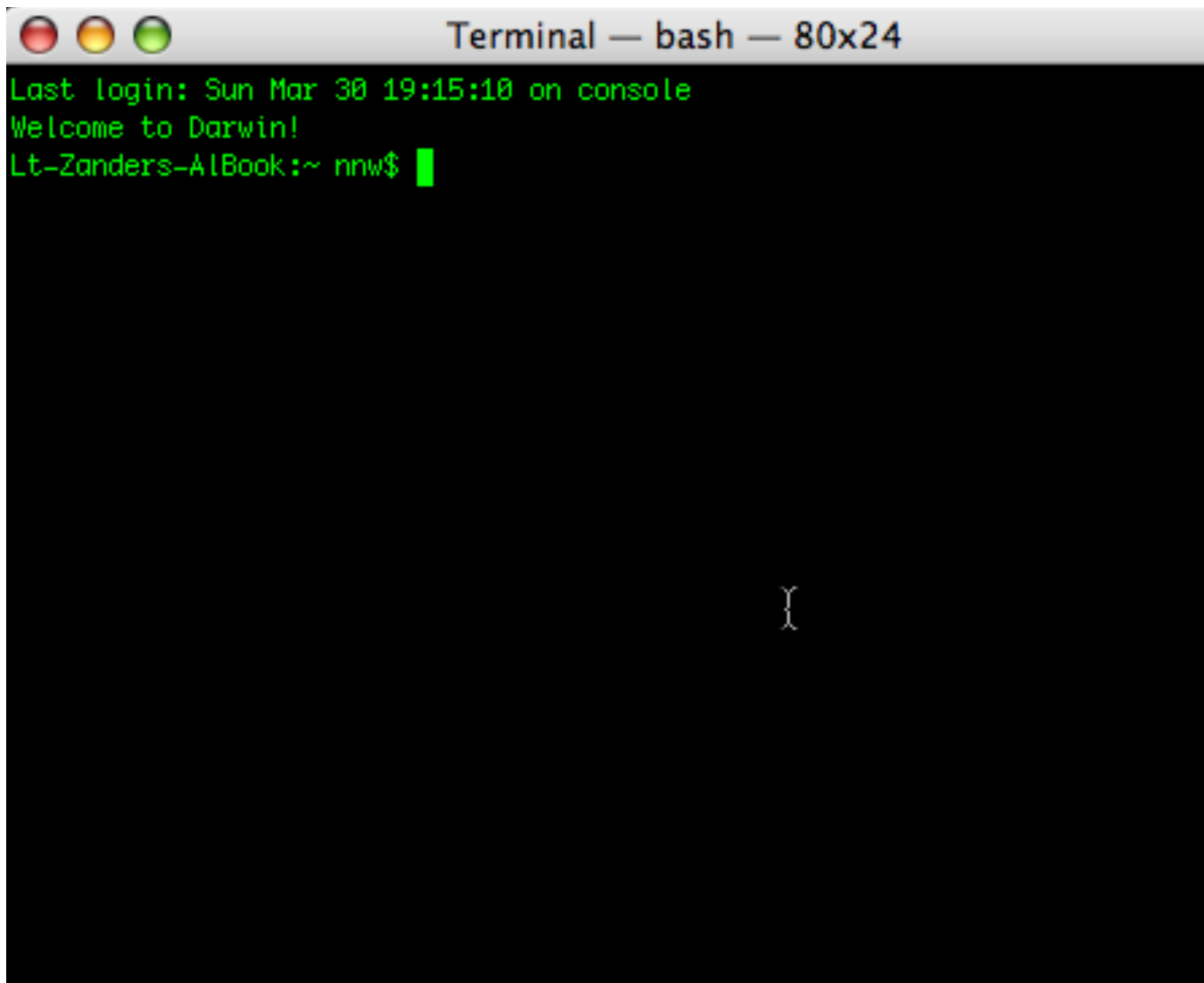
**NSA Data Hub: Domestic Warning Hub and Data Warehouse, Aurora, CO** The NSA is reportedly building a massive data storage facility in this Denver suburb, and also operates a reconnaissance satellite dish here. This may be where the agency's data mining operations take place. A CIA facility and the military's Northern Command (NORTHCOM) are also located here.



## Collecting Network Traffic Or “Sniffing”

The method you will employ for capturing data from a network is commonly known as “packet sniffing.” Every email, instant message, or website you browse is broken up into small packages that contain the data that is being sent and received, these are called packets. A “packet sniffer” allows your networking card to listen to all the packets that are being transmitted across a given network from any computers using this network, along with allowing you to see their contents and store them. Employing a packet sniffer to capture samples of network traffic from a wireless network, is not only effective it is also very easy since it does not require a physical connection to the network since after all it is wireless.

The software that is typically used to do this is network diagnostic software or a dedicated “packet sniffing” application. The Neighborhood Network Watch uses a free Open Source application called TCPDUMP (WinDump for Windows).

A screenshot of a macOS Terminal window. The title bar at the top reads "Terminal — bash — 80x24". The terminal content is as follows:

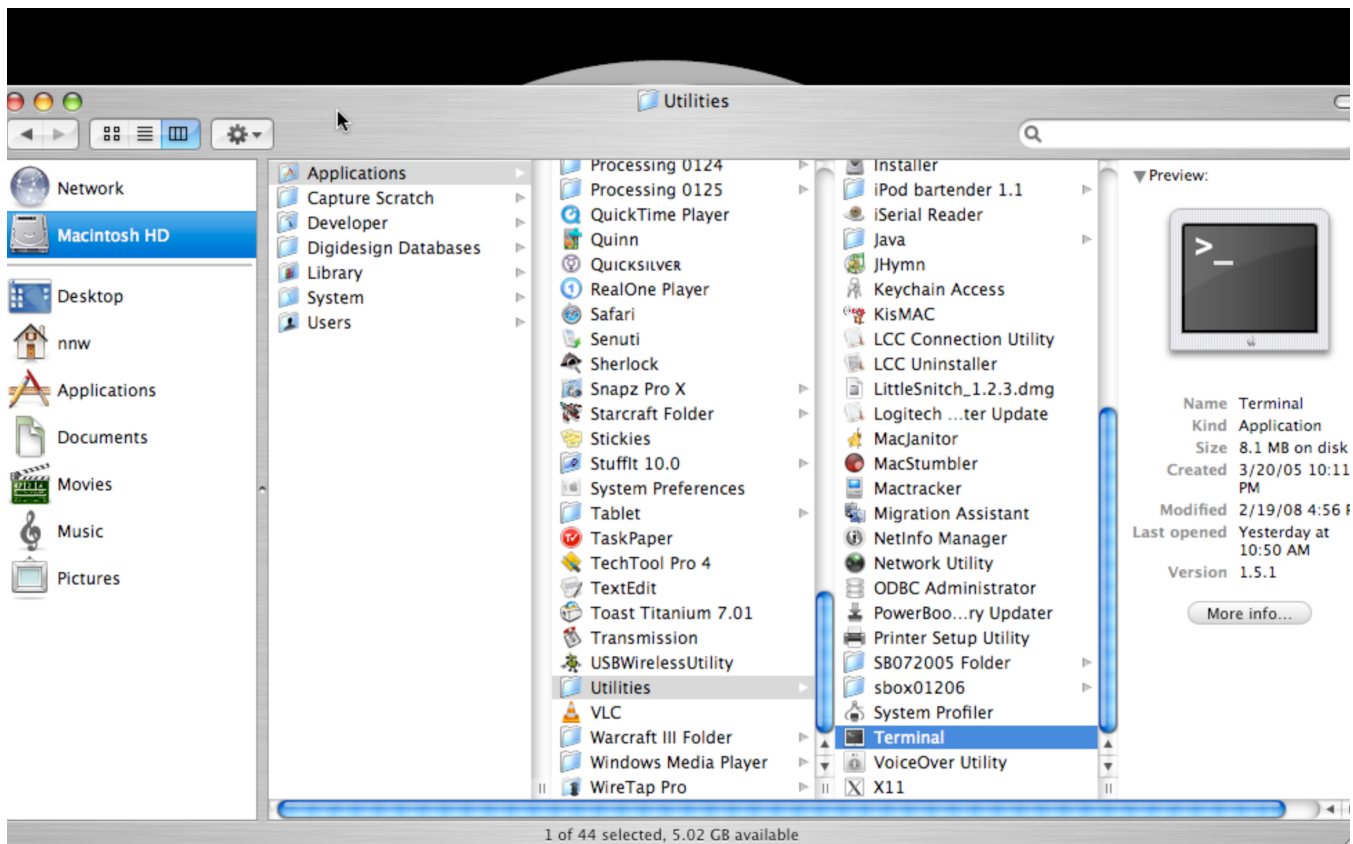
```
Last login: Sun Mar 30 19:15:10 on console
Welcome to Darwin!
Lt-Zanders-AlBook:~ nnw$ █
```

A large, faint, light blue watermark consisting of a pair of curly braces "}" is centered on the terminal background.

## TCPDUMP

TCPDUMP is a command line based application, which means it has no graphical interface and requires you to operate it by using text commands. This may seem intimidating at first but it is really quite simple. Before getting started with teaching you how to operate TCPDUMP you must make sure that you have administration access on your computer or be the administrator of the computer you are using since TCPDUMP requires this.

The following two pages will discuss how to operate TCPDUMP. So, let's get started.



## Where To Find The Command Line

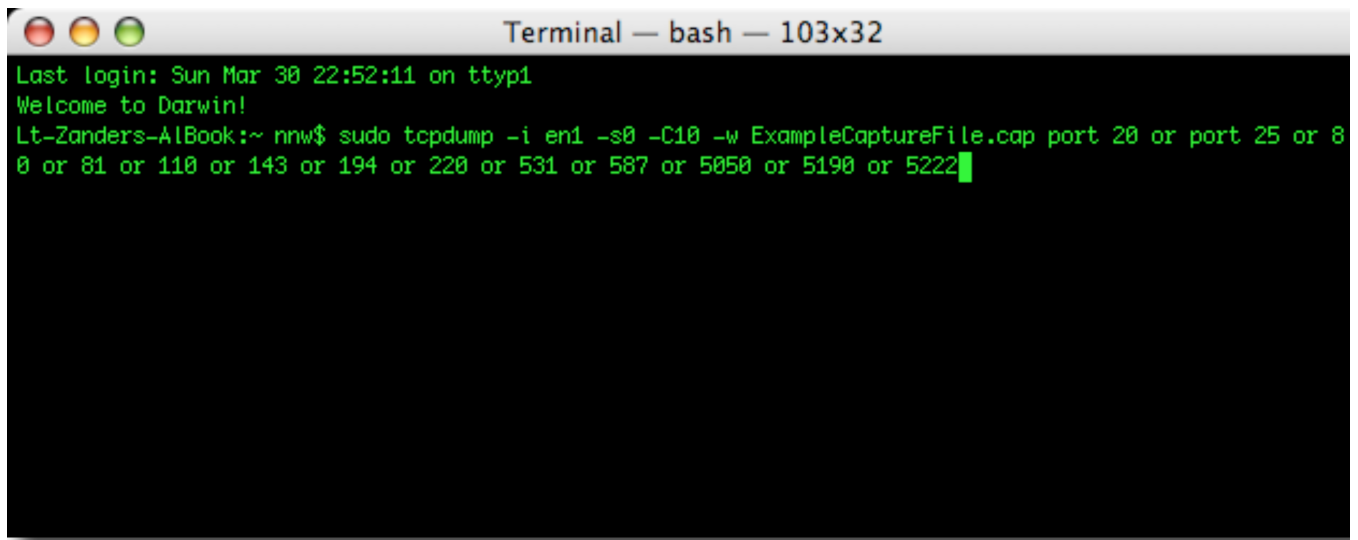
Since, TCPDUMP is a command line application it will be run from the command line. Most operating systems allow you to access the command line through an application that will run at the same time as the normal graphical user interface you are used to.

If you are using the Windows operating system the application will be called "Console" and will be available in the "Applications" part of the "Start" menu.

If you are using the Mac OS X operating system it will be called "Terminal" and will be located in the folder called "Utilities" that resides in the "Applications" folder.

For Unix and Linux users you are likely well acquainted with the command line and if not you will be able to look up directions on how to access the command line by consulting the documentation for your operating system.



A terminal window titled "Terminal — bash — 103x32" with a dark background and green text. The text shows the login process and the execution of a sudo tcpdump command. The command is: sudo tcpdump -i en1 -s0 -C10 -w ExampleCaptureFile.cap port 20 or port 25 or 80 or 81 or 110 or 143 or 194 or 220 or 531 or 587 or 5050 or 5190 or 5222. The cursor is at the end of the command.

```
Terminal — bash — 103x32
Last login: Sun Mar 30 22:52:11 on ttty1
Welcome to Darwin!
Lt-Zanders-AIBook:~ nnw$ sudo tcpdump -i en1 -s0 -C10 -w ExampleCaptureFile.cap port 20 or port 25 or 80 or 81 or 110 or 143 or 194 or 220 or 531 or 587 or 5050 or 5190 or 5222
```

**sudo tcpdump -i en1 -A -s0 -C10 -w  
ExampleCaptureFile.cap port 20 or 25 or 80 or  
81 or 110 or 143 or 194 or 220 or 531 or 587 or  
5050 or 5190 or 5222**

Figure 1a

## The Command

The command in figure 1 will be the full command that you will be typing into your command line to run TCPDUMP to capture all network traffic from the network to a file. TCPDUMP will collect network traffic that is coming from the following types of applications: email clients, instant message clients, instant relay chat clients (IRC), file transfer protocol clients (FTP), and web browsers.

In the following pages we will be breaking down the anatomy of this sequence of commands so you can have a better understanding of what is going on and how to operate TCPDUMP.

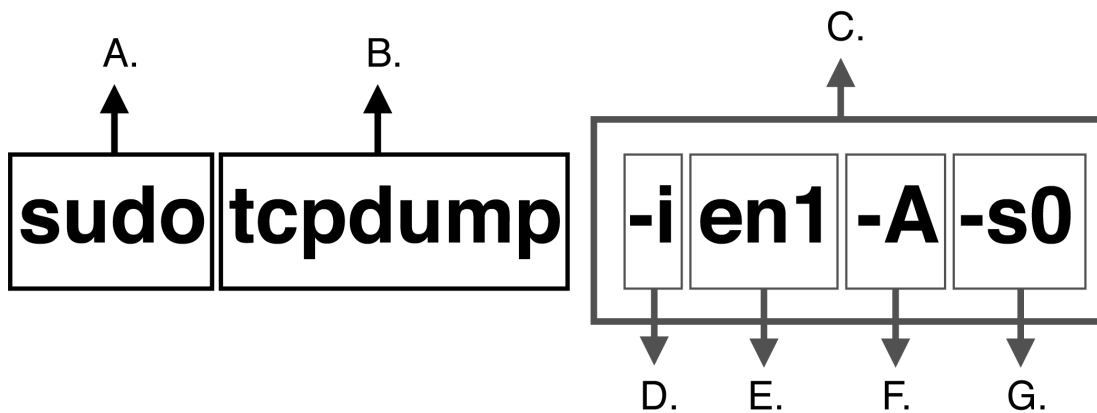


Figure 1b

## TCPDUMP Breakdown Part 1 (figure 1b)

A. Sudo will allow give you the proper authority needed to run tcpdump. You will be prompted for your administration password when you run this command.

B. Tells the computer to run the application TCPDUMP.

C. This is the flag section. Flags basically are parameters that tell the program how operate.

D. “i” - This flag that tells TCPDUMP that I want to designate which networking interface I want to use.

E. “en1” - This flag goes hand in hand with the “-i” flag. This is where the network interface is chosen. Computers often have more than one networking card in them. Typically one that is wired (Ethernet) and another which is wireless (Wireless Ethernet).

These interfaces are given a corresponding number starting with “0” and progressing sequentially. Wired network cards are typically 0 and hence you would use the flag “en0” to run tcpdump on the wired ethernet interface.

Wireless cards are typically “1” therefore you would use the command “en1” when running tcpdump from the wireless networking card.

F. “-A” - This flag tells tcpdump to output the contents of the packets into ASCII, which is a fashion that allows it to be easily read.

G. “-s0” - This flag automatically adjust the amount of information to capture from each packet to its actual size, so nothing gets lost or truncated.

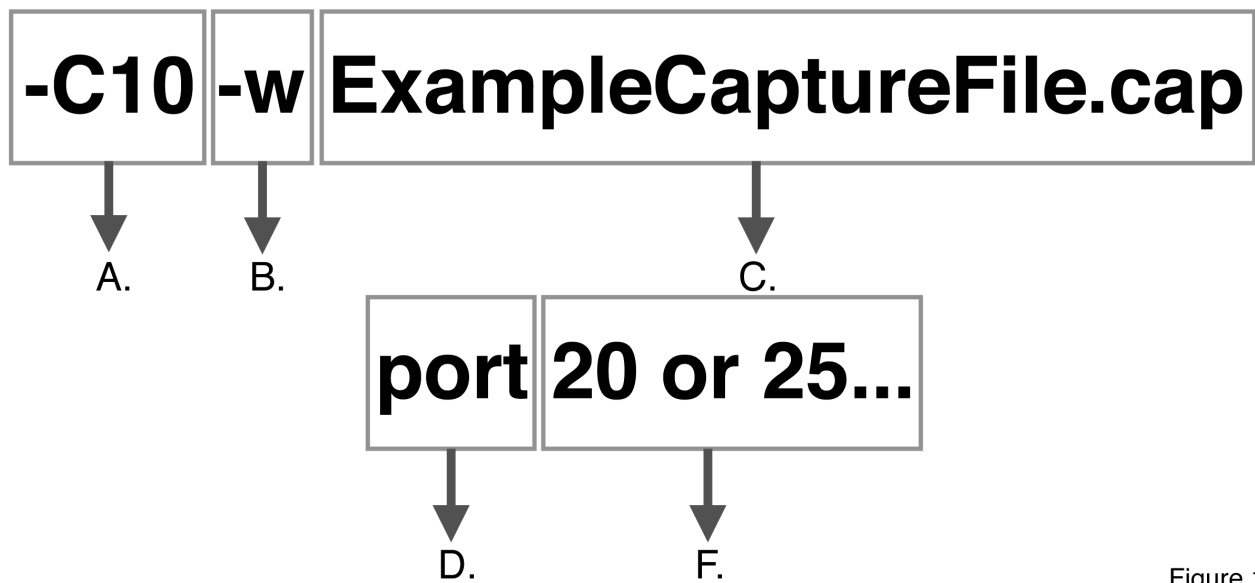


Figure 1c

## TCPDUMP Breakdown Part 2 (figure 1c)

A. “C10” – This flag sets the max size, in megabytes (MB), of the capture files that will be written with the information coming from the network. This is currently set to make 10 megabyte (MB) files. The trailing number can be increased or decreased, however very large files become hard to process or take excessive time and resources. It’s recommended to keep these files under 10 megabytes or under, ie. “C10” or “C5”.

B. “-w” –This flag tells tcpdump to not display the traffic captured but rather write this information out to a file, in the users home directory.

C. “ExampleCaptureFile.cap” – This is the name for the file that will be written. Note it must include the “.cap” extension at the end of the name. This name can be whatever you want, however it’s a good idea to name this after the name of the network as it allows you to keep track of the files with ease. The date is also useful information as well. A better name could look something like this: “BensCafe-01-01-07.cap”.

D. “port” - This flag sets TCPDUMP to only capture traffic from the designated numbered port. If this flag is left out TCPDUMP will capture traffic from every port.

E. “20 or 25” - Are the numbered ports that TCPDUMP will capture traffic from. Most applications use a specific port to transfer data through. Each port number is separated by the word “or”. To see a full list of the ports used refer to Appendix 2.

```
Terminal — bash — 103x32
Last login: Sun Mar 30 22:52:11 on ttty1
Welcome to Darwin!
Lt-Zanders-AlBook:~ nnw$ sudo tcpdump -i en1 -s0 -C10 -w ExampleCaptureFile.cap port 20 or port 25 or 80 or 81 or 110 or 143 or 194 or 220 or 531 or 587 or 5050 or 5190 or 5222
Password:
tcpdump: listening on en1, link-type EN10MB (Ethernet), capture size 65535 bytes
^C32 packets captured
170 packets received by filter
0 packets dropped by kernel
Lt-Zanders-AlBook:~ nnw$ █
```

## Running The Command

After typing in the full command hit the “return” or “enter” key and TCPDUMP will now begin capturing aka “sniffing” traffic with the parameters that were discussed in the previous pages. It will automatically make sequentially numbered files as they hit the file size threshold.

You should collect for a minimum of a half hour, preferably an hour or more if possible. After you are ready to end the capture session, press the “Control” and “C” keys to stop TCPDUMP. TCPDUMP will stop and will let you know how many packets you captured as well as how many were lost or dropped.

That’s it, you have now successfully “sniffed” a network. Congratulations. All that is left to do is to send your files to your local Neighborhood Network Chapter for analysis. If your city does not have a chapter established for your city or town please email your collection files to [hnap@dhsnnw.org](mailto:hnap@dhsnnw.org).

## Appendix 4: Neighborhood Network Watch Keyword Analysis Application (NNWKAA)

Figure 1. Screenshot of NNWKAA v1.0 console

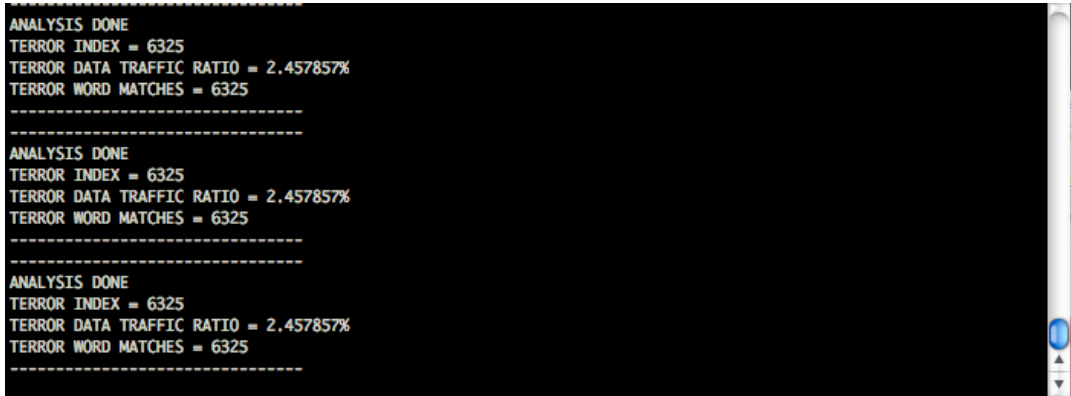


Figure 2. Screenshot of NNWKAA v2.0 Visualization

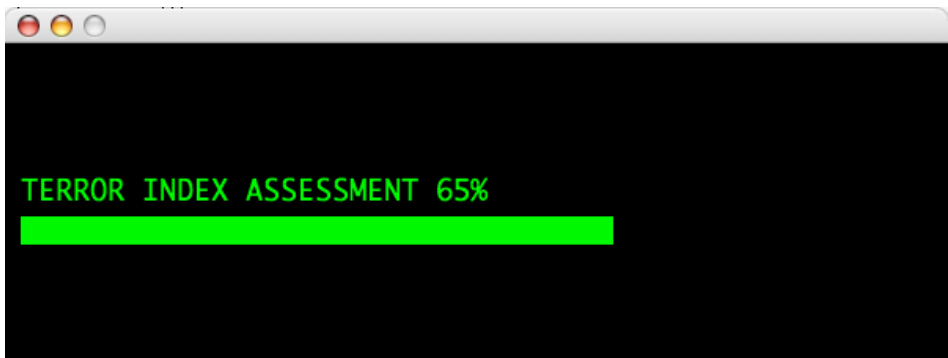
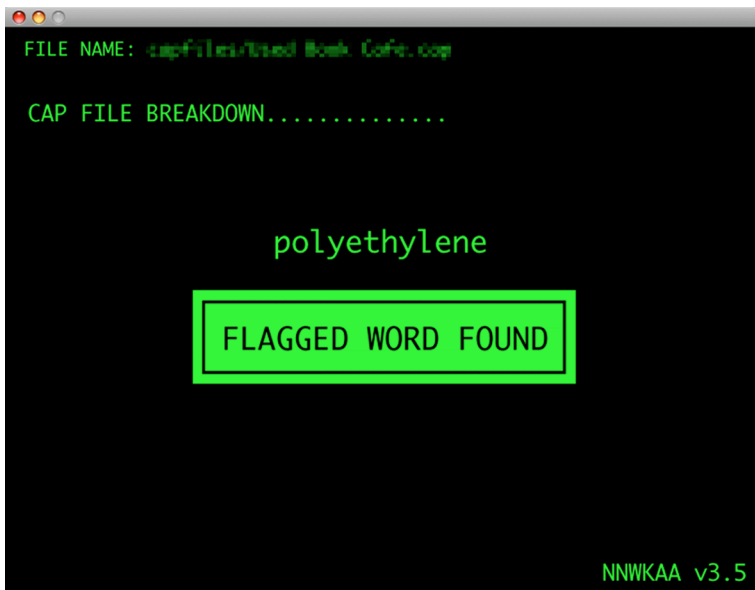


Figure 3. Screenshots of NNWKAA v3.5 Visualization



FILE NAME: zapfiles/Used Book Cafe.doc

STATISTICAL ANALYSIS RESULTS

-----  
TOTAL FLAGGED WORDS = 110173.0  
TOTAL FOUND WORDS = 452983.0  
TERROR PERCENTAGE = 24.321663%  
-----

HIT PARADE OF TOP 20 FLAGGED WORDS

p 22117	at 543
q 21835	the 517
a 21895	macintosh 434
h 23282	in 362
s 22392	ak 358
this 2352	of 338
com 2149	is 274
document 741	id 270
server 697	net 287
engine 672	amp 239

SEVERE

HIGH

ELEVATED

GUARDED

LOW

NNWCAA v3.5

**Appendix 5: NNW Charts and Maps**

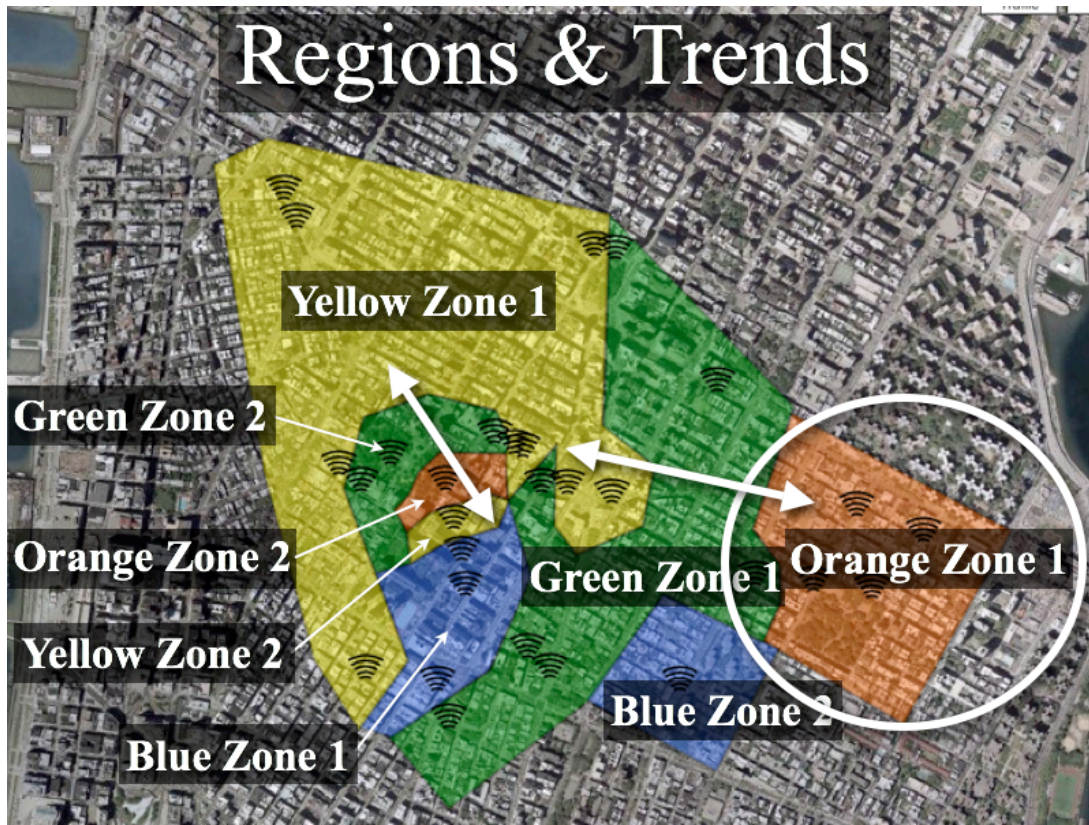


Figure 1. Fall 2007 Region & Trends Map  
 Colors reflect the rating for the given region based off of the NNW Network Threat Advisory System. The circle and large arrows denote regions of interest or conflict.

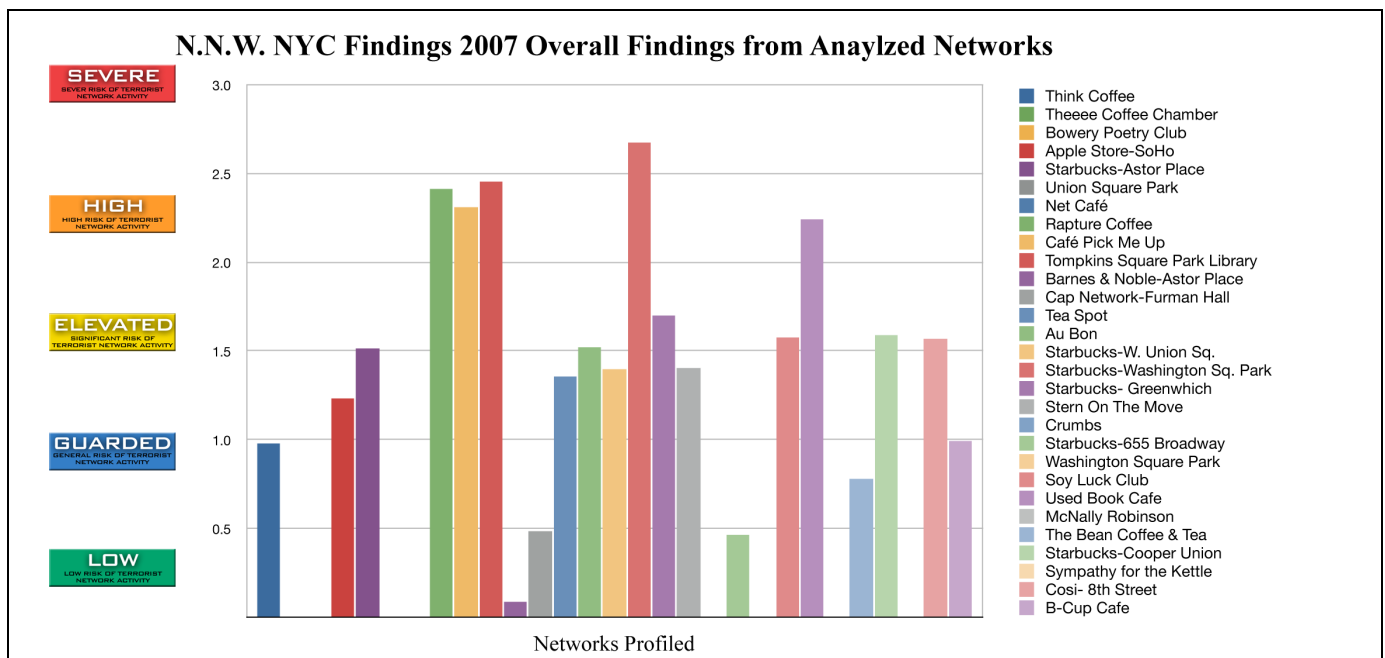


Figure 2. Fall 2007 findings for New York City

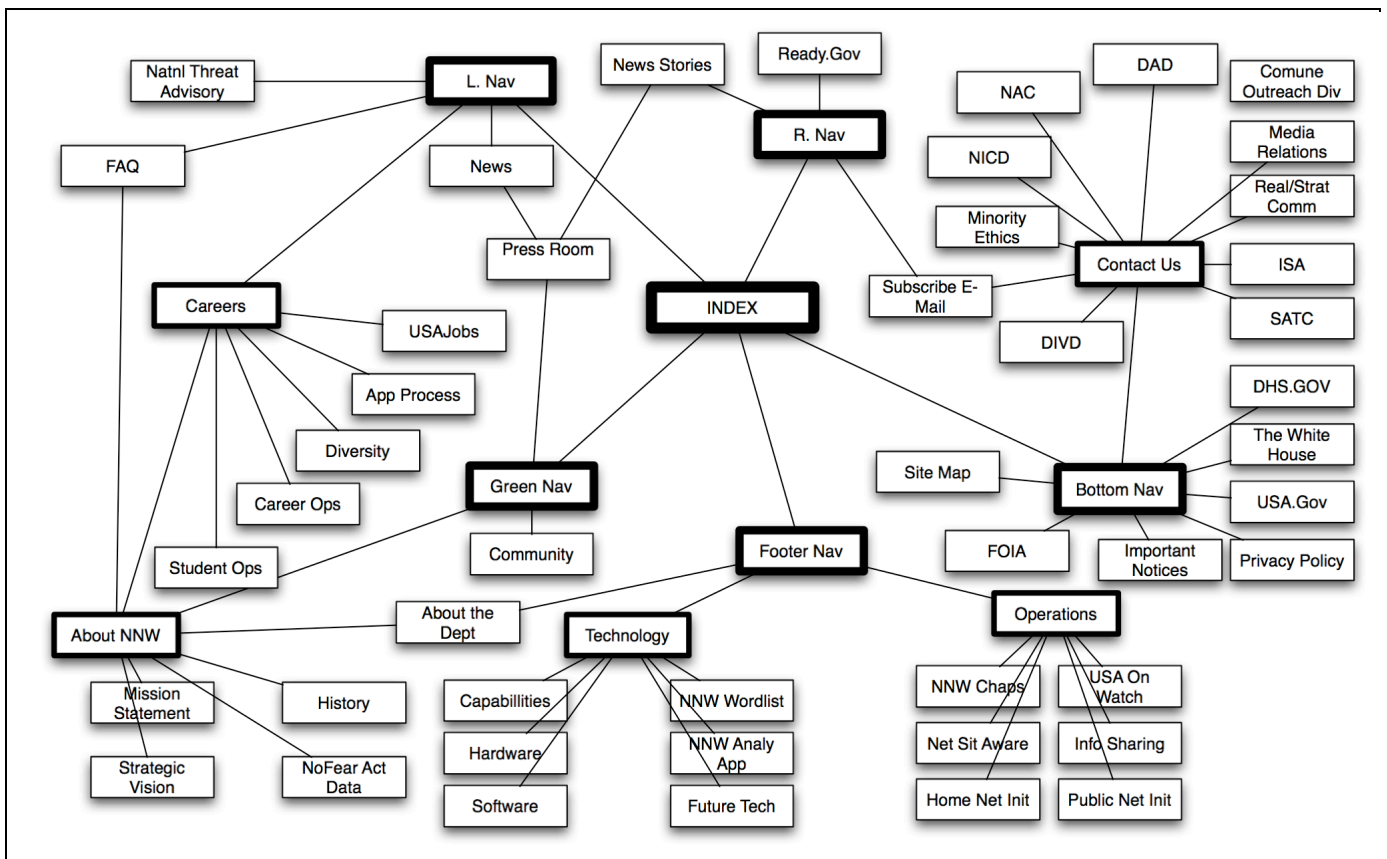


Figure 3. Visual aids on display at ITP 2008 Winter Show

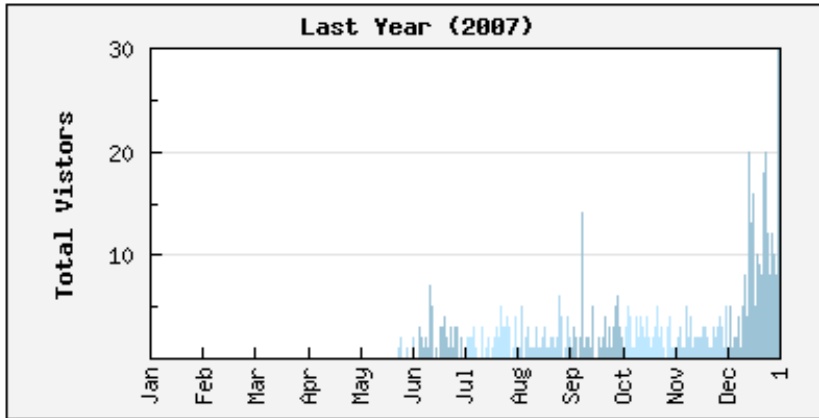


## Appendix 6: Neighborhood Network Watch Early Site Map

Figure 1. Preliminary Site Map for NNW Website - 11/07

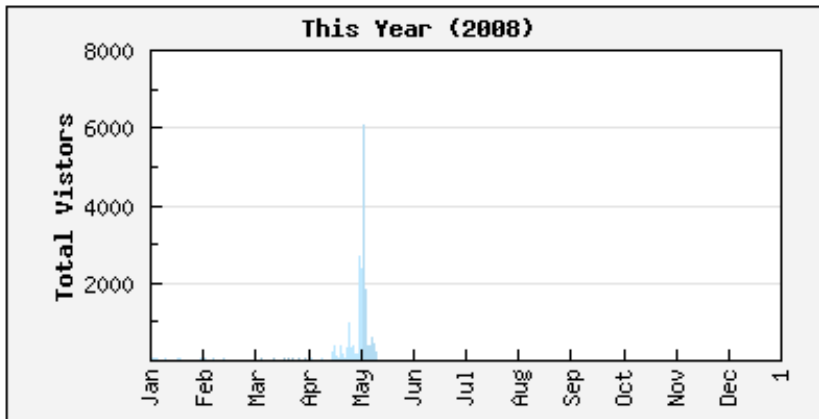


## Appendix 7: Web Traffic Results for NNW Website



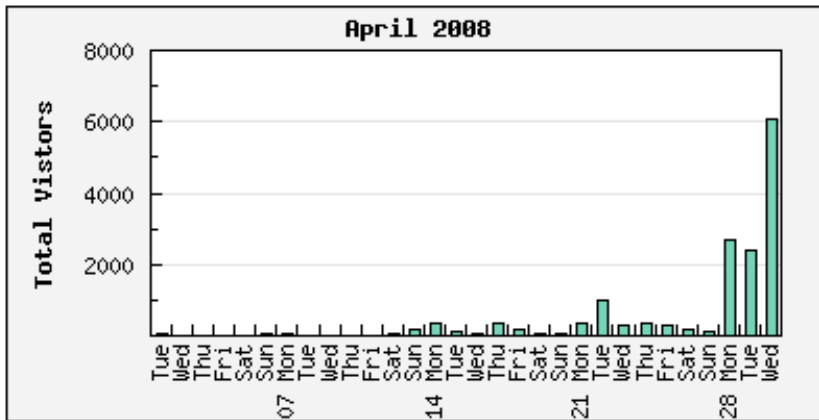
**Graph Summary:**  
*Total Visitors for Year: 629*  
*Average Per Day: 2*

Figure 1. NNW Site Traffic for 2007



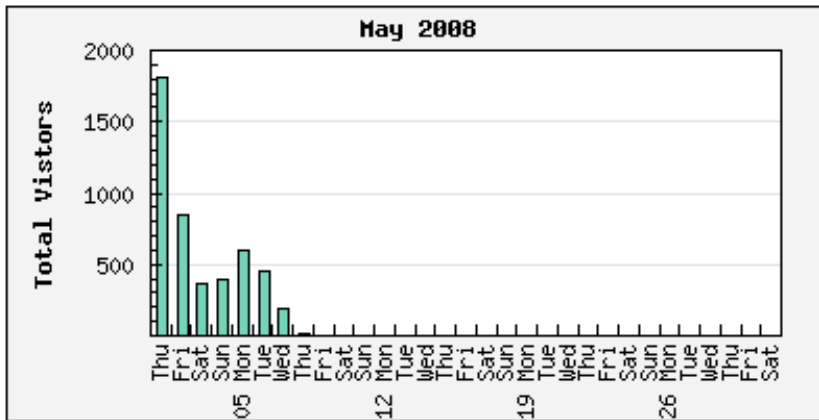
**Graph Summary:**  
*Total Visitors for Year: 21823*  
*Average Per Day: 60*

Figure 2. NNW Site Traffic for 2008



**Graph Summary:**  
*Total Visitors for Month: 15351*  
*Average Per Day: 512*

Figure 3. NNW Site Traffic for April 2008



**Graph Summary:**  
*Total Visitors for Month: 4677*  
*Average Per Day: 585*

Figure 4. NNW Site Traffic for May 2008

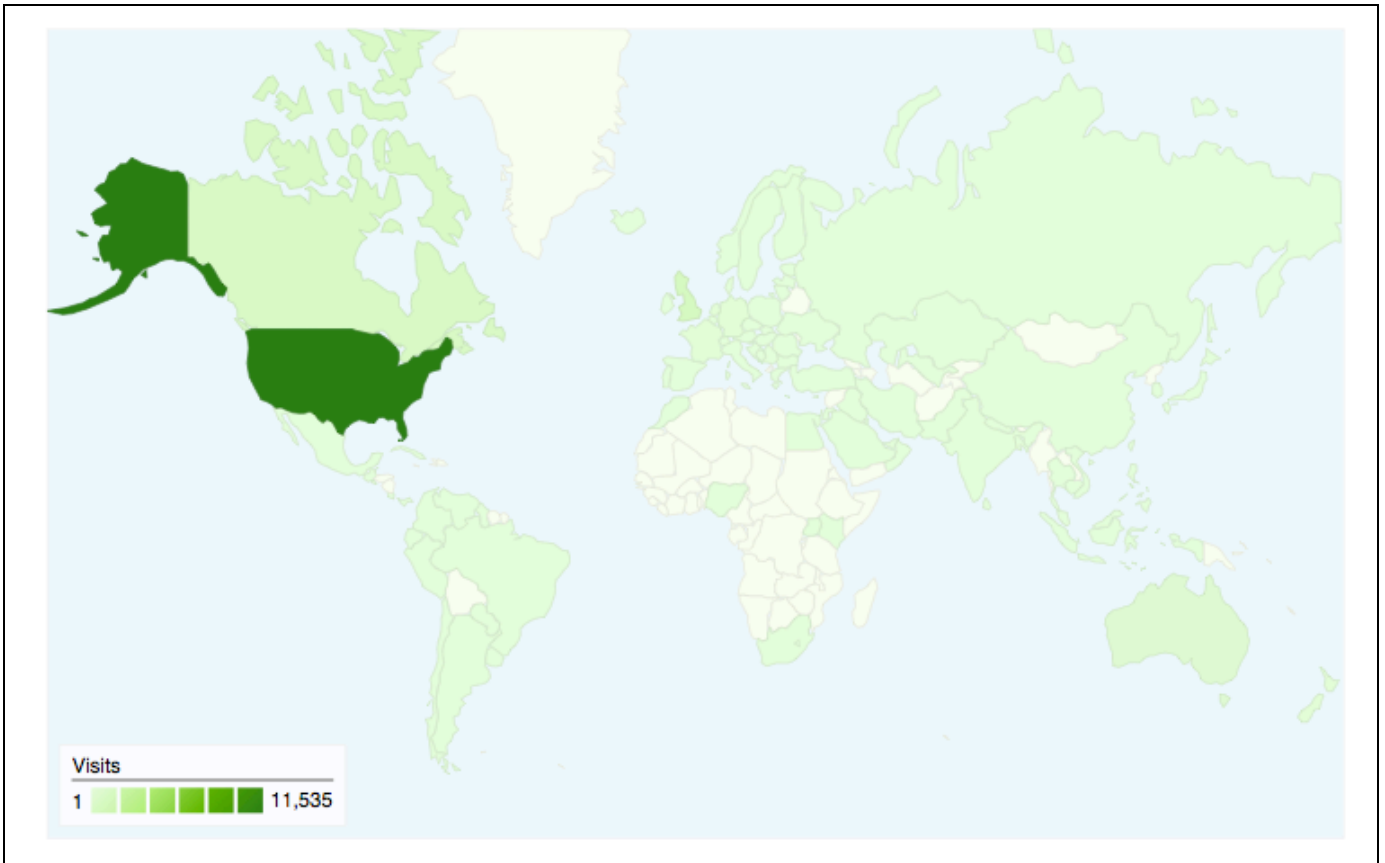


Figure 5. Map of countries who have visited the NNW website.

## Appendix 8: Selected Web & Blog Responses

Figure 1. Reddit.com Post [41] – April 14, 2008

 **reddit** [hot](#) [new](#) [browse](#) [saved](#) [recommended](#) [stats](#)

[ltzanders](#) (1) |  | [preferences](#) | [submit](#) | [help](#) | [blog](#) | [logout](#)

### DHS Neighborhood Network Watch: Snoop on your neighbors wireless and be a patriot

[politics] (dhsnnw.org)  
14 points posted 24 days ago by [sardis](#) 17 comments [unsave](#) [hide](#) [report](#)

[info](#) [comments](#) [related](#) [details](#)

[help](#)

**tonic88** 1 point 22 days ago [-]  
If you aren't doing anything wrong, you have nothing to hide.  
[permalink](#) [report](#) [reply](#)

**dosduros** 1 point 22 days ago [-]  
Who are these people?  
[permalink](#) [report](#) [reply](#)

**TuesdaysMacaron** 1 point 22 days ago [-]  
That's just disturbing. We're losing our privacy every minute.  
[permalink](#) [report](#) [reply](#)

**popmorefizz** 1 point 23 days ago [-]  
THEY'RE READING MY EMAILS DAMMIT >:|  
[permalink](#) [report](#) [reply](#)

**ltzanders** 1 point 23 days ago [-]  
Dude, I dunno, they got a lot of shit on their site. I just starting going through some of it, the sites huge! If it's a hoax it's sure bloody elaborate. You should watch the public service announcements they're creepy as hell.  
[permalink](#) [edit](#) [delete](#) [reply](#)

**greginnj** 3 points 24 days ago [-]  
Ummm, an official fedgov website would be .gov, not .org. That said, this is a brilliant satire site. (The shady-hat logo is a bit too overt, though.)  
[permalink](#) [report](#) [reply](#)

**pn6** 1 point 23 days ago [-]  
not necessarily. maybe the fbi is using this to track paranoia levels, as it used other sites to track pedophiles.  
[permalink](#) [parent](#) [report](#) [reply](#)

**greginnj** 1 point 23 days ago [-]  
Wow, interesting theory! However, I would have to see some more evidence to give it more credence. To accept it, you'd have to believe that they are [this good](#) at satire:  
Q: Isn't this invading my privacy?  
A: In many ways yes, but in a post 9-11 world the government and most communities across the United States, believe that these sorts of measures are necessary to prevent our nation from being attacked by ruthless terrorists. In fact privacy is a relative term with a definition that is constantly being redefined. Especially so in the highly technologically mediated world we live in today.  
I think of the FBI as humorless gits, not capable of this quality of writing, no matter what end they wanted to put it to.  
[permalink](#) [parent](#) [report](#) [reply](#)

**sort by**  
**hot**  
[new](#)  
[top](#)  
[old](#)

**other reddit**  
[politics](#) [reddit.com](#)  
[pics](#) [programming](#)  
[science](#) [worldnews](#)  
[funny](#) [business](#)  
[more >>](#)



[reddit this ad](#)

[greginnj](#) 2 points 24 days ago [-]

check out [the FAQ on this site](#):

Q: Is the Neighborhood Network Watch a government agency?

A: No, despite popular belief the Neighborhood Network Watch is not a government agency. It is affiliated with the U.S. Department of Homeland Security yet is still not a part of them.

Q: If the Neighborhood Network Watch is not a government agency then what is it?

A: The Neighborhood Network Watch is a community based and staffed organization much liken to a Neighborhood Watch, but for network security.

How cute!

[permalink](#) [report](#) [reply](#)

[smssc](#) 2 points 24 days ago [-]

Join the Hitler Youth!

[permalink](#) [report](#) [reply](#)

[bobzibub](#) 1 point 24 days ago [-]

Gots to be april fools. Probably illegal.

[permalink](#) [report](#) [reply](#)

[Khendroc](#) 1 point 24 days ago [-]

I can't believe it advocates and offers instructions on how to log into other people's wireless networks.

[permalink](#) [report](#) [reply](#)

[nouns](#) 1 point 24 days ago \* [-]

Ich Bin nien Stackenblocken!!!!!!

[permalink](#) [report](#) [reply](#)

[alephnul](#) 1 point 24 days ago [-]

OMFG

[permalink](#) [report](#) [reply](#)

[pn6](#) 0 points 23 days ago [-]

Why I don't use wireless.

[permalink](#) [report](#) [reply](#)

[TuesdaysMacaron](#) 1 point 22 days ago [-]

I'm starting to have second thoughts about wireless now...

[permalink](#) [parent](#) [report](#) [reply](#)

[feedback](#) | [bookmarklets](#) | [buttons](#) | [widget](#) | [store](#) | [advertise](#)

 [WIRED.com](#) - [WIRED How-To](#)

Use of this site constitutes acceptance of our [User Agreement](#) and [Privacy Policy](#)(c) 2008 CondeNet, Inc. All rights reserved.

## Unmasking the Neighborhood Network Watch

### Is it art or a plot to spy on America's Wi-Fi networks?

By [Dan Goodin in San Francisco](#) → [More by this author](#)

Published Thursday 24th April 2008 18:41 GMT

Emery Martin is a man on a mission. The 23 year-old resident of Brooklyn has spearheaded the Neighborhood Network Watch, a grassroots group advocating the monitoring by volunteers of open Wi-Fi networks "to make sure that terrorists may not be using your own home network to plan the next attack on our nation or your very own community".

But there's an important catch: Martin's group, which claims to be supported by the US Department of Homeland Security, isn't for real. Rather, it's a sprawling art project and master's thesis cooked up by Martin to stimulate thought about how networks operate and the ability for them to be surveilled.

"The point that I'm making is raising awareness and critical engagement," explains Martin, who is a graduate student in the Interactive Telecommunications Program at New York University's Tisch School of the Arts. "What are the potential things that are lurking in technology itself, and how do they allow control and power?"

The site includes a primer that teaches laymen how to sniff wireless networks using programs like TCPDUMP and WinDump and explains how to use wardriving applications like Net Stumbler and Kismet to find open networks. "Since these networks often times are unsecured or offered as a free service to the public it allows any individual to use them, including terrorists," the site argues. It includes a Wiki that can be used to upload dumps of packets monitored from open networks in a volunteer's vicinity.

With a template that's taken straight from the [DHS website](#), the [Neighborhood Network Watch site](#) was convincing enough to prompt a discussion about it on a Security Focus mailing list.

#### 'Set your watch back 24 years'

"From the 'Set your watch back 24 years' department," one [participant wrote](#), in an apparent reference to the George Orwell novel *1984*. "This has to be invasion of privacy in its purest form," a *Reg* tipster wrote in an email. "Please tell me this schmuck is not affiliated with the Department of Homeland Security."

Indeed, Martin doesn't have any ties to the DHS. But in an environment where Congress is actively considering [handing out immunity to telecom companies](#) that cooperated with warrantless government wiretaps, he doesn't think groups like the one he fabricated are all that far-fetched.

"It could potentially happen in communities that are already invested in that ideology or don't question the motives behind such government policies," he says.

Of course, there are plenty of telltale signs that the site is a hoax. It has no director listed, includes no contact information and the contact listed on whois records for the domain name is a jollyrogerjonesy at a gmail account. Martin also included a video and other statements with rhetoric so over the top that anyone looking long enough would figure out the hoax.

Still, he says the ambiguity, is part of the point.

"The fact [some people don't] get it isn't necessarily a bad thing," he says. "It is based very heavily on generating fear and paranoia. If someone is that concerned about it, that's good. Eventually, they'll be able to figure it out." ®

Figure 3. Archived Email – April 17, 2008 – <<http://www.mail-archive.com/funsec@linuxbox.org/msg06952.html>>

**[funsec] More on the "Neighborhood Network Watch" -- not a joke, but a thesis project?**

Xxxxxxx X. Xxxxx Thu, 17 Apr 2008 14:08:05 -0700

-----Original Message-----

From: [EMAIL PROTECTED]

[EMAIL PROTECTED] On Behalf Of

[EMAIL PROTECTED]

Sent: Thursday, April 17, 2008 4:35 PM

To: [EMAIL PROTECTED]

Subject: [ PRIVACY Forum ] "Neighborhood Network Watch" -- not a joke, but a thesis project?

Greetings. I've been continuing to research the "Neighborhood Network Watch." It remained difficult to see how it could actually be exactly what it claimed to be, and more oddities and inconsistencies appeared the more I dug down, but it all seemed far too elaborate for a joke -- and its technical discussions are not utterly nonsensical.

But use of terms like "ECHELON keyword list" and "emissary to DHS" were red flags. Some readers suggested that the project was the work of some wacko security wannabee (this seemed a definite possibility all along).

Some deep Google searches have now exposed the reality. Not a joke, and not "real" per se, but apparently rather a complicated programming/thesis project presented as a "hoax" organization to critique networking and national security issues.

And while the "project" had notable "screwball" aspects (a la my "Keystone Cops" title), it certainly found its way onto various Web sites and into a number of alarmed e-mails I received "alerting" me to its existence.

Here are links to the relevant NYU blog entries that lay out the "actual" project design:

[http://itp.nyu.edu/blogs/ecm292\\_thesis/2008/02/](http://itp.nyu.edu/blogs/ecm292_thesis/2008/02/)

<http://itp.nyu.edu/blogs/ecm292/2008/02/26/nnwkaa-30/>

Of course, the real point of all this (beyond the programming elements) is that the described operations, despite dubious legal status, are not only largely possible, but in this day and age not something to be dismissed as beyond the pale of actual implementation.

The advisability of publicly presenting a fictional organization in such a manner in this context without any obvious form of disclaimer is an issue for another day.



Figure 4. Direct Email – April 29, 2008

From: [EMAIL PROTECTED]

Subject: Does anyone get it?

Date: April 29, 2008 6:44:14 PM EDT

To: contact@dhsnnw.org

Your site is beautifully done.

I'm curious what type of reaction you've gotten and how many people have actually tried to start sending you data?

I'd love to see any presentations you've got on your experiment to date if you have one.

Thanks and keep up the good work.

-- Xxxxx

--

If you can conceive of morality without god, why can you not conceive of society without government? -- Peter Saint-Andre

## Appendix 9: Select Performance Documentation Images

Figure 1. Documentation of Hunter College Presentation – November 15, 2007

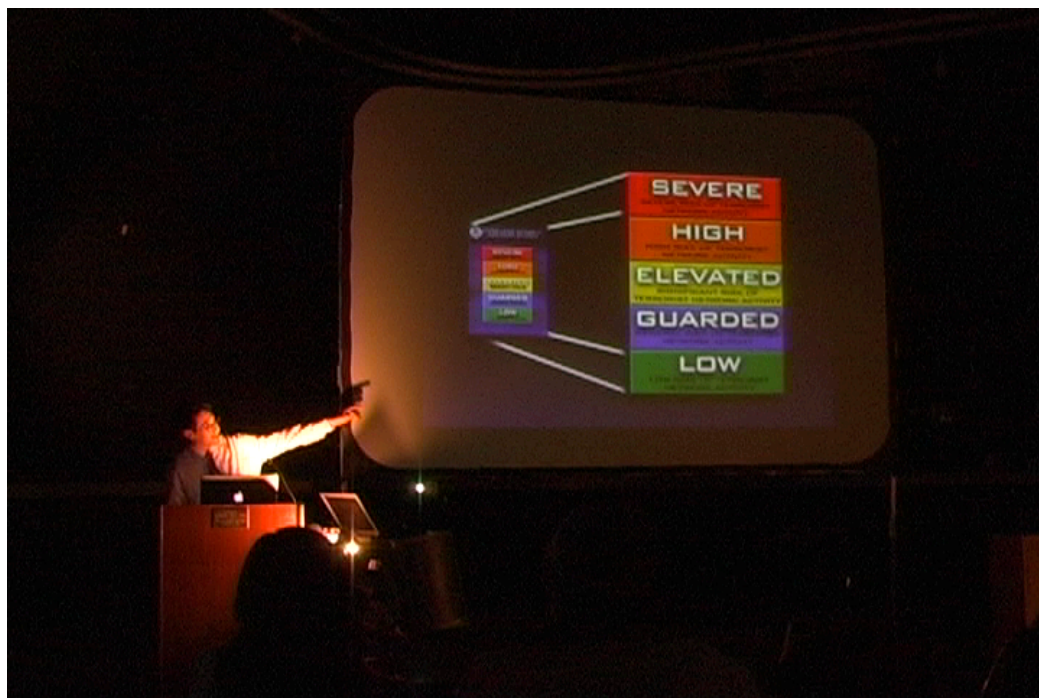
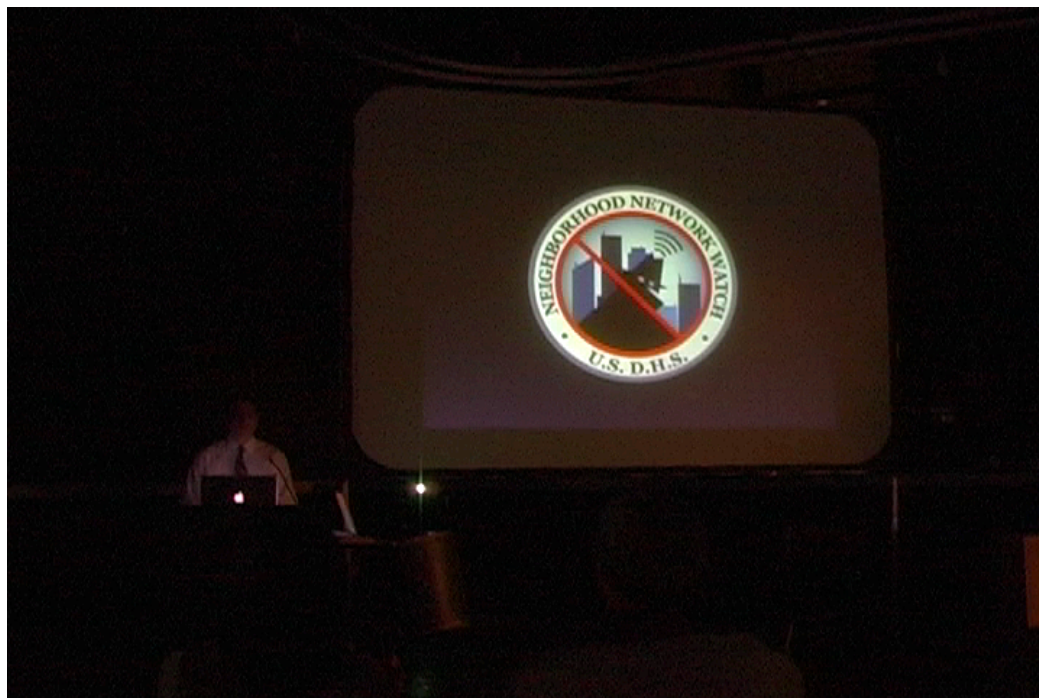




Figure 2. Documentation of 2008 ITP Winter Show – December 16-17, 2008

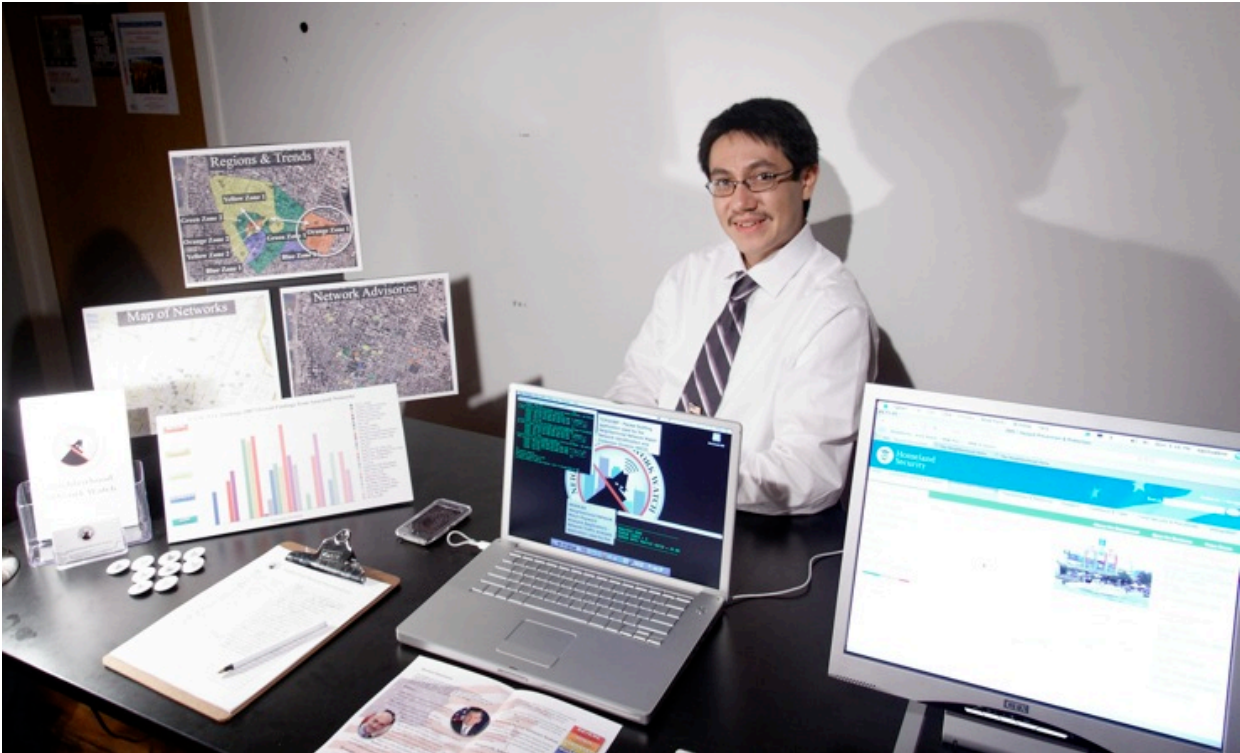




Figure 3. Documentation of Presentation at The Change You Want to See - Brooklyn, NY - April 26, 2008

