



# Modern Surveillance Methods and Public Trust

Nicholas Proferes

*Networked devices present new dilemmas to the legal system. The use of these devices can challenge the preconceived notions of what is public and what is private. One might ask, do the same rules for monitoring traffic operations among public and private roads apply to monitoring a telecommunications infrastructure that is made up of public and private networks? Should wiretapping laws written to apply to telephone conversations apply to voice communications over an IP network? Does an individual's right to privacy end when that person walks out his front door? Does he even have to leave his house, but instead just sign in online? Is surveillance the same thing as search and seizure? The rapid evolution of technical capabilities available in new technology is spurring more questions than answers. When courts are asked these types questions, they routinely have to answer based on law and regulation that was created with old technology in mind. This can and has led to legal challenges regarding the use of these technologies, and can further lead to a public mistrust of these networked devices and systems. This paper looks to explore the relationship between ubiquitous technologies today, the aging policy that is often used to explore and exploit it in the legal arena, and the concept of public trust.*

In the 1967 Supreme Court case *Katz v. United States*, it was the Court's opinion that, "What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection, but what he seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected."<sup>1</sup> Given the evolution of what is considered public and private space in today's society, and the rapid changes occurring within technology, this statement's validity can come under question. Networked devices present new dilemmas to the legal system. The use of these devices can challenge the preconceived notions of what is public and what is private. One might ask, do the same rules for monitoring traffic operations among public and private roads apply to monitoring a telecommunications infrastructure that is made up of public and private networks? Should wiretapping laws that may have been written to apply to telephone conversations apply to voice communications over an IP network? Does an individual's right to privacy end when

---

<sup>1</sup> *Katz v. United States*, 389 U.S. 347 (U.S. Supreme Court 1967)..

that person walks out of the front door? Does that even have to leave the house, but instead just sign in online? Is surveillance the same thing as search and seizure?

The rapid evolution of technical capabilities available in new technology is spurring more questions than there are answers. When courts are asked these types of questions, they routinely have to answer based on law and regulation that was created with old technology in mind. This can and has led to legal challenges regarding the use of these technologies, and can further lead to a public mistrust of these networked devices and systems. It is important to explore this relationship between ubiquitous technologies today, the aging policy that is often used to explore and exploit it in the legal arena, and the concept of public trust.

Some of these questions stem from uncertainty about the rights an individual has in a public space. The constitutional basis for the right to privacy is found within the Fourth Amendment: “The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.” Houses, papers, and effects are things normally considered private spaces, or can be found in private spaces. But does this right to secure in our persons apply in public spaces? The answer depends on how invasive the search process is. In 1991, “the Court of Appeals for the Ninth Circuit held that individuals videotaped in public view have no reasonable expectations of privacy.”<sup>2</sup>

At the same time that the judicial system hands out rulings similar to this, courts also recognize the issue of public trust created by surveillance. In fact, in a ruling by the U.S. Fifth Circuit stated that video surveillance was, “reminiscent of the 'telescreens' by which 'Big Brother' in George Orwell's 1984 maintained visual surveillance of the entire population.”<sup>3</sup> If this sort of surveillance causes such concern as to draw a comparison to a fictional but totally panoptic society, why would the judicial system allow it to proceed?

Video surveillance or closed circuit television (CCTV) can help municipalities, private companies, or law enforcement monitor public areas for the purposes of crime prevention, traffic congestion monitoring, or criminal prosecution. CCTV is often more cost effective and efficient than hiring police officers to patrol the same streets. For these reasons, video surveillance appears to be a technology that could help the public feel safe in their surroundings. Within the framework of safety, and feeling secure in one's self, the public begins to put trust in these systems.

The judicial system often has to rule about the legality of a use of a new technology from law and policy that was not written in a time when the technology was foreseen, as was the case with CCTV and video surveillance. The Omnibus Crime Control and Safe Streets Act of 1968 did not specifically reference video surveillance in statutory language when addressing the use of electronic surveillance. It was, however, the legal framework for the decision that would come later in 1984 in *United States v. Torres*. This case found that video surveillance could fall within the guidelines for use set out in Omnibus Crime Control and Safe Streets Act.

After this ruling, policy makers set out to clarify and adapt. In 1986, the Electronic Communications Privacy Act was passed. This spelled out clearly, and in explicit terms, that video surveillance could be used for purposes of public safety. Congress believed there was no reasonable expectation of privacy in a public setting, partially due to the ruling two years earlier, and since CCTV was not an intrusive device, it would be analogous to having an automaton police officer. A result of this opinion is the plain view rule. “If a person does something illegal in plain view, an officer would

---

<sup>2</sup> *United States v. Taketa*, 923 F.2d 665, 677 (9th Cir. 1991)

<sup>3</sup> *United States v. Torres*, 751 F.2d 875, 877 (7th Cir. 1984)

not need a warrant to search that person to find the incriminating evidence.”<sup>4</sup> In this case though, instead of it being an officer, it would be a video camera.

There are some caveats that come with video surveillance and CCTV, however. In order to comply with the law surrounding wiretaps and audio recordings, public video surveillance must be done without audio. This is done in order to not run afoul of the Electronic Privacy Act of 1986. Devices that can record audio and video can still be installed, but they require a warrant.

This leads to a question about the nature of surveillance itself. Is surveillance analogous to search and seizure that is described in the Fourth Amendment? According to an article by Marcus Nieto, “The Supreme Court has developed a test to determine if such surveillance violates the Constitution: 1. Does the surveillance occur from publicly navigable airspace? 2. Is the surveillance conducted in a physically non-intrusive manner?”<sup>5</sup>

Keeping this test in mind, consider this illustration, which implements more modern technologies. A person is sitting in a public park with his laptop, accessing a publicly available wireless (Wi-Fi) network. Very simply put, the way a Wi-Fi connection works is analogous to two radio stations talking to each other, the two radio stations being the laptop with a wireless card, and a wireless router, respectively. However, because these messages are “broadcasted” like a radio, it is very easy for a third party to intercept these messages. In this example, the third party is also sitting in the park, and ‘overhears’ the conversation. Was this a violation of the Fourth Amendment? Under the test above, the surveillance occurred in a publicly navigable airspace, and the surveillance was not conducted in a physically intrusive manner. The result? No violation.

To illustrate the change in traditional public and private boundaries, a slight change can be made to this scenario. Instead of the person sitting in a park, accessing the publicly available wireless network, consider what might happen if he is instead in his own home, accessing the publicly available network. Surely because the Fourth Amendment contains an explicit statement that a person has the right to be secure in his own home, this would break the Fourth Amendment. But no, the results of the test remain the same. The surveillance conducted by the third party is still occurring from a publicly navigable airspace, and the surveillance is still being conducted in a non-intrusive manner.

The ability to access public networks from the home is not a new phenomenon. Radio, television, and the telephone have all brought the technologies inside the front door, but in each of these cases, the technology has come with specific restrictions. Shortwave radios, FM and AM, as well as broadcast television have traditionally been one-way communication methods. Because there is no two-way communication, intercept is pointless. The same content can be accessed next door with the same technology. Telephone technologies, however, brought about a whole host of legal issues regarding two-way communication that could connect two private residences over a commercial network. It is important to discuss the legal issues surrounding the telephone, not because it is the same technology that is of concern today, but because the tort law and law created by the Congress concerning it have been applied to data communications as they first existed with modems.

Part of the logic used to underpin modern wiretap laws originated in the 19<sup>th</sup> century: “it was held that a sealed letter entrusted to the mail is protected by the amendments. The mail is a public service furnished by the government. The telephone is a public service furnished by its authority. There is, in essence, no difference between the sealed letter and the private telephone message...”<sup>6</sup>

<sup>4</sup> Nieto, M. (1997, June). *Public Video Surveillance: Is It An Effective Crime Prevention Tool?*. Retrieved April 19, 2007 from California Research Bureau Web site:

<http://www.library.ca.gov/CRB/97/05/crb97-005.html>

<sup>5</sup> *Ibid.*

<sup>6</sup> Solove, D., Rotenburg, M., Schwartz, P. (2006). *Privacy, Information, and Technology*. New York, NY: Aspen Publishers. p. 67

Subsequent court rulings further protected an unwarranted wiretap by making it clear that it did not matter where the physical tap occurred, but simply that a tap occurred at all. In fact, it was considered illegal to place a wiretap without a warrant. It was determined later that this same logic applied to data communications that took place over phone lines as well. Since modem communications can be considered private communications, it may be a commonly held belief that all data communications must be private. This creates a sense of public trust.

This belief may or may not be justified, however. “In *Goldman v. United States*, the police placed a device called a “detectaphone” next to a wall adjacent to a person’s office. The device enabled the police to listen in on conversations inside the office. The Court concluded that because there was no trespass, there was no Fourth Amendment violation.”<sup>7</sup> This follows the surveillance test described earlier.

How does *Goldman v. United States* apply to current technologies? The detectaphone worked by capturing audio information from another room, without actually having to access the network that the audio data in the next room was transmitting over. In actuality, it was a hyper-sensitive microphone. With the exception of audio information that may come out of a computer’s speakers, it may seem as though this case has little to do with modern computer technology. But remember, unlike the phone system that is a closed system, wireless communications (Wi-Fi) are broadcasted. This means that the information that one sends out over the network could be “overheard” by an unintended recipient in the room next door, or by the actual intended target, the wireless router. Suddenly, there is a public trust issue. The data being communicated on a wireless network is the same as if it were being communicated on a modem, yet the protections that each have now been granted have shifted dramatically.

Today, the Electronic Communications Privacy Act of 1986 (ECPA) is considered modern wiretapping law. It defines three specific types of communications that have different levels of protection: wire communications, which are defined as “aural transfers that travel through a wire or similar medium”; oral communications; and electronic communications, which can consist of all non-wire non-oral communication.<sup>8</sup> Interestingly, the act does not necessarily apply to electronic communications that are not conducted over phone lines. This creates a loophole for Internet communication.

Consider the scenario discussed earlier. The person sitting in the park is using a publicly available Wi-Fi network, with a third party capturing the data that is being broadcasted back and forth. Because the wiretapping section of the ECPA does not cover this type of “electronic communication,” there is neither a violation of the person’s Fourth Amendment rights, nor any restrictions governing wiretapping. Taking this a step further, suppose the person on his laptop on the public network is using a voice-over-IP service, which allows him to hold an audio conversation over the wireless data network. Suddenly, determining if the third party is acting legally becomes highly confusing. It is still an electronic communication, but it may also be considered an oral communication.

The nature of the third party who monitors others may also be changing. In considering video surveillance, who would setup and monitor those cameras? Generally, it was a representative of a municipality, law enforcement personnel, or business. The cost of setting up CCTV in a public space was generally prohibitive for the general public, although recently, private use in homes has grown tremendously. The public also may have access to view some of the cameras, such as traffic congestion

---

<sup>7</sup> *Ibid.*

<sup>8</sup> United States Code (1986). *Electronic Communications Privacy Act: Chapter 119 - Wire and Electronic Communications Interception*. Retrieved April 16, 2007 from , Web site: <http://floridalawfirm.com/privacy.html>

monitoring. A public authority, business, or municipality generally does the monitoring, though sometimes these networks are available for public use. The third party in the Wi-Fi example could be anyone. It does not take much investment to be able to capture data on a public Wi-Fi network. All that is required is a computer with a wireless network card and a piece of software called a packet sniffer (which can generally be found for free).

What is the motivation for monitoring a public Wi-Fi network? For authorities, the justification for implementing video surveillance could be to prevent criminal activity, to monitor network traffic and congestion, or to prosecute crime after it has happened. However, since the ability to monitor is not limited to public authorities, there are an entire host of other reasons for capturing information on a network such as: the ability to obtain personal information such as usernames and passwords; the ability to capture information which may not include illegal information, but potentially embarrassing information, such as health information; or the ability to pirate or intercept intellectual property which may otherwise not be accessible. Since there is no crucible and no warrant required, no reason has to even be given to obtain the information.

Is a Wi-Fi surveillance scenario possible? While many Wi-Fi networks today are privately owned and operated, Philadelphia, San Francisco, and New Orleans each have plans to roll out free citywide wireless networks which would be available for use by anyone. Additionally, there are many private businesses that offer free Wi-Fi as a “perk” to shop or eat at that location. Many airports now offer free Wi-Fi as an incentive for businesspersons to fly at those locations.

In fact, there is an entire online culture that surrounds finding and mapping wireless networks. This is a process known as “war driving.”<sup>9</sup> War driving gets its name from an older process called “war dialing,” which involved calling up phone numbers sequentially via computer to see if there was a pick-up, and to see if that pick-up was a computer. War driving is very similar in concept. It involves getting in a car and driving around an area to find wireless networks that are accessible. When done in conjunction with a GPS system, it is possible to create a map of where Wi-Fi access can be granted. War driving may not necessarily include accessing the network, but instead just collecting the information about it.

There are several distinctions that need to be made about Wi-Fi networks and war driving. Many of the networks that are found and can be accessed may still be “private” networks. They may be networks that people are operating within their homes and are not networks that are being offered for public use. Some networks may also require authentication to ensure that the person accessing the network is allowed to be on it.

Due to the properties of the wireless networks themselves, if there is no authentication required on a wireless network, it is nearly impossible to tell if a wireless network is being offered for public use or is simply a private network that has not been properly secured. This ambiguity leads to a legal loophole for entities to potentially access private networks without “proper” authorization and capture information from that network.

While there have been criminal cases which involved unauthorized use of a wireless communication network, they usually surround an illegal activity that a person was conducting while on that network. To date, no case has specifically addressed war driving. The practice is generally seen as entirely legal. From the information gained through war driving, it is possible to essentially gain a map of locations where network traffic can be captured legally.

The ambiguity surrounding wireless communication has led to some public distrust of wireless systems. However, because many people may not understand this issue because it is confusing and

---

<sup>9</sup> (2004). *War Driving: About/Definition*. Retrieved April 16, 2007 from Web site: <http://www.wardriving.com/about.php>

new, or because there have been no court cases which have explicitly dealt with the practice, there has not been a strong public outcry which could lead to changes in the law.<sup>10</sup>

There are some protections that do exist for wireless networks, though they are not necessarily under the guise of privacy. Earlier, it was mentioned that some Wi-Fi networks require “authorization.” This authorization is actually a pass phrase. Knowing the pass phrase allows you access to the network. Thanks to many state laws, an attempt to break into a network that requires a pass phrase is considered illegal. In Florida, it is considered unauthorized access to a computer network, which is a felony. This pass phrase can also be used for another mechanism called encryption, which allows for a greater degree of security on a network.

Encryption is an important tool relating to wireless networks, privacy, and the law. In considering the reasoning behind the wiretap legislation and the logic used to create the modern wiretap laws (ex parte Jackson, 96 U.S. 727 (1877)), “it was held that a sealed letter entrusted to the mail is protected by the amendments. The mail is a public service furnished by the government. The telephone is a public service furnished by its authority. There is, in essence, no difference between the sealed letter and the private telephone message...” There is an important characteristic of the letter defined here, and that is the “seal.” The seal on a letter is a mechanism that keeps others from reading the material because the letter is no longer “in plain sight,” as per the plain sight rule. Encryption acts in the exact same manner. It “seals” the data packet that is being sent over the wireless network. The only manner in which one could read the data is to break the encryption, similar to how one might break the seal on an envelope. It may not be incredibly hard to do, but the act itself may be considered illegal. As a result, persons using encryption may also believe that they have a reasonable expectation of privacy, which may then be protected under the Fourth Amendment.

Encryption also affords a person using it another legal protection which may seem as though it has very little to do with privacy. In 1998, the Digital Millennium Copyright Act (DMCA) was signed into law. The act was a version of law originally intended to help people protect their copyrights and prosecute those who violate copyrights.<sup>11</sup> Copyright holders often use encryption as a means to control the distribution, replication, and consumption of their work. The DMCA made it illegal to circumvent or break an encryption mechanism in order to help protect copyrights. Incidentally, attempting to circumvent or break the encryption on a wireless network packet could be held as a violation of the DMCA. Encryption can help those who may not have trusted a wireless network to safeguard their privacy.

Encryption is not only limited to private networks which require a pass phrase. It is possible through the use of “tunneling,” to encrypt information that is transversing a public wireless network. The process of tunneling involves creating a connection between the laptop on the public wireless network and a machine elsewhere that is not on a public network. A person sitting in the park on his laptop happens to have an armchair interest in privacy issues, and happens to know that his communications may not be secure. In order to make himself more secure, this person can set up an encrypted connection between the laptop and his home computer, which is on a secure private network. When the person sitting in the park surfs the web, the request to view a homepage will travel encrypted from his laptop through the network, to his machine at home. The machine at home will then un-encrypt the request, transverse the private network to request the webpage. The webpage will then be returned

---

<sup>10</sup> Wakefield, J. (2005, July 28). *Wireless hijacking under scrutiny*. Retrieved April 16, 2007 from BBC News, Web site: <http://news.bbc.co.uk/2/hi/technology/4721723.stm>

<sup>11</sup> US Copyright Office (2003, October 28). *Rulemaking on Exemptions from Prohibition on Circumvention of Technological Measures that Control Access to Copyrighted Works*. Retrieved April 16, 2007, from Web site: <http://www.copyright.gov/1201/2003/index.html>

to the home computer, and then will be encrypted, and sent back to the laptop. A common implementation for this connection mechanism is called “Virtual Private Networking” or VPN for short. Setting up a VPN network gives users nearly the same protections as if they were on that private network in their home, with the same protections that are given to encrypted materials on a private network.

While it may appear that video surveillance and Wi-Fi network surveillance are only marginally intertwined by the legal precedents that had been set before each technology even existed, the legality of the uses of these technologies is likely to become more intertwined as time progresses and technology develops further. In 2005, the Real ID Act was included as part of the Emergency Supplemental Appropriations Act for Defense, the Global War on Terror, and Tsunami Relief.<sup>12</sup> The intent of this act was to create a national ID system that would make it difficult to obtain a fraudulent ID card. The national ID card would contain a certain amount of required information such as name, birthdate, location of residence, a photograph of the cardholder, gender, and signature of the cardholder. This information is generally located on most state driver’s licenses. There is a clause in this law though which is important to note. A characteristic of the ID card is that the information it contains must be in “common machine-readable format.”

The definition of what a common machine-readable technology is not given. In the worst-case scenario from a privacy perspective, a machine-readable technology could be a radio frequency identity (RFID) tag. A RFID is a technology that transmits information stored within the tag over a short distance via radio frequency to a receiver. RFID technologies are vulnerable to being “overheard” or picked up, similar to how Wi-Fi packets can be picked up. Also similar to Wi-Fi networks, some types of RFID do not employ encryption techniques to mask the information. If a national ID card was instituted with extremely poor RFID technology, it could theoretically be possible to determine exactly who was in park at a given time, assuming everyone in the park had their national ID on their person.

The worst-case scenario yields two results. First, the possibility for “personalized surveillance.” When combined with video surveillance, it could be possible to track where individual people were at all times, as long as they were in a public space. If they were still in the public space, it could be possible to view them on demand, and if they were not in a public space, it could be possible to identify the last location from which they exited a public setting. The second result is that not everyone would necessarily carry their national ID. In fact, a person who commits a criminal act might be better off not carrying an ID at all. This association of tracking identity and behavior could give choosing not to carry a national ID card a nearly criminal connotation. Either result is a far closer representation of the Orwellian state that the U.S. Fifth Circuit Court of Appeals had mentioned earlier. However, RFID technology would still pass the Fourth Amendment test, as it occurs in a publicly navigable airspace, and is not an invasive search.

The best-case scenario for a machine-readable ID card is that the machine-readable information would only be used to verify the validity of the ID itself. Additional safeguards could include requiring that no records be retained that an ID was ever scanned. This would require that the machine-readable area of the card be printed with ink (such as a barcode) or perhaps an electronic solution that would require physical contact with the card to instigate data transfer. While this may seem as though it would solve many of the privacy and trust concerns, according to the privacy group EPIC, “Requiring a common machine-readable technology exposes individuals to identity theft, and turns the driver’s license into surveillance and tracking system beyond a simple identification system. Making IDs easily machine-readable changes the nature of the interaction when we identify ourselves. When another

---

<sup>12</sup> US Code, Emergency Supplemental Appropriations Act for Defense, the Global War on Terror, and Tsunami Relief, 2005, Pub. L. No. 109-13, 119 Stat. 231 (May 11, 2005).

person visually checks your ID, they look to see if you match your ID. When a machine does it, it records the information on the card. Thus what used to be an ID check is now a recording, and thus, surveillance and data collection.”<sup>13</sup>

In fact, a *Star Ledger* article says this is already occurring with state licenses that are already machine-readable. “Club managers love the gadget, and it's rapidly becoming standard issue at the bigger clubs in Manhattan, New Jersey and elsewhere. But the box does more than just check birth dates. It also retains the customer's name, address, license number -- even height, weight, and eye color. All that information then can easily be downloaded into a computer system. Most patrons have no idea their information is being electronically stored -- nor are they asked if they mind.”<sup>14</sup> There are also no laws concerning what businesses can do with this information, since the data may or may not fall under the Drivers Protection Privacy Act. This could potentially create large public trust issues concerning the use of these technologies.

The RFID scenario may seem somewhat far-fetched; however, the United States recently altered the construction of its passports to include a RFID. Only time will tell how this may affect the privacy rights of the individuals who hold these IDs in a public space.

The Real ID Act and the RFID tags now found in U.S. passports garnered a significant amount of media and public attention. There has been increasing pressure from the states to make it difficult or impossible for an ID card proposed under the Real ID Act to be implemented. While there was a significant amount of resistance (and even some online guides on how to disable the RFID) to the passport program, it has been implemented. Because of the attention to RFID technologies, including the discussion of the inappropriate uses of it, there seems to be a large amount of distrust in the systems as it related to privacy concerns.

The main privacy issue surrounding these technologies is that the laws surrounding them are often vague, and predicated upon laws which had not forecasted technological growth. These technologies are shifting what is considered public and private space. Sometimes, the rules that govern one technology may crash into another. Wiretapping laws were not written for wireless network communications and the intricacies surrounding them. The practice of video surveillance and the laws created as a result of it greatly influenced the laws and rules that can be applied to public networks, not just public places. And while courts may decide that individual technologies do not violate an individual's Fourth Amendment rights, when used in combination with other technologies, the results can cause great distrust and concern about potential abuse. The concern about abuse may also transcend the fear of an Orwellian government, and the rights that others have, namely to have the ability to legally perform surveillance on a public wireless network. There are solutions that will emerge, such as encryption, and some may even become legislative mandates. These solutions can help build trust in the security of these technology systems. Ultimately, public trust can dictate whether a system or a technology survives, or fails.

---

<sup>13</sup> Electronic Privacy and Information Center (2007, February 2). *REAL ID and Domestic Violence*. Retrieved April 16, 2007 from Web site: [http://www.epic.org/privacy/dv/real\\_id.html](http://www.epic.org/privacy/dv/real_id.html)

<sup>14</sup> Star Ledger (2006, November 6). *Clubs Scan Licenses*. Retrieved April 16, 2007 from Web site: <http://www.nj.com/search/index.ssf?/base/news-5/1164261389312610.xml?starledger?nnj&coll=1>