The Historical Society *of the* New York Courts

Joshua Pawlikowski

2013 David A. Garfinkel Essay Contest
NYS Community College Grand Prize

# *A Slow Eclipse: The Fourth Amendment In The Age Of Counter-Terrorism*

Faculty: David R. Katz III, Professor of Political Science
Mohawk Valley Community College (SUNY System)

**A Slow Eclipse: The Fourth Amendment In The Age Of Counter-Terrorism**

As in any age, our modern world has come to be largely shaped and defined by major historical forces. The emergence of global threats such as cyber-crime and widespread terrorism has caused a shift in the priorities of governments around the world, including the United States. While such threats should be taken seriously, it will be very important going into the future for such states to ensure that they do not develop methods for dealing with these threats which come into conflict with, or outright nullify, certain rights, liberties, and protections which have come to be expected in modern liberal societies. These liberties, such as the people's right to privacy and security "in their persons, houses, papers, and effects, against unreasonable searches and seizures" as enshrined in the Fourth Amendment to the United States Constitution, are more and more frequently clashing with the increasing ability of the government to perform surveillance on citizens. This ability comes not only from recent advances in technologies such as drones, GPS devices, and the Internet, but also through a growing legal framework which some criticize as giving far too much surveillance power to the government—while at the same time lacking any mechanisms for meaningful oversight, control, or protections for our Fourth Amendment rights.

Recently, the use of GPS devices for surveillance purposes has become something of a legal contest between the executive branch, asserting that it has the legal authority to order covert GPS surveillance of a person under various anti-terrorism statutes, and members of both the judicial and legislative branches who feel that such surveillance tactics are either questionably justified, or are outright unconstitutional as currently implemented. The current row over GPS tracking comes after *United States v. Jones*, a 2012 Supreme Court ruling which stated that the Fourth Amendment protects a person's vehicle from warrantless tracking by law enforcement, as the vehicle is private property and is therefore to be protected against unreasonable search and seizure. According to the Obama administration, the use of such "slap-on" GPS tracking devices by law enforcement agencies is not a violation of privacy—or at the very least, the violation would be "minimal". To prohibit the use of such devices without first attaining a warrant would not only inhibit traditional law enforcement, the administration asserted in a recently-filed brief, but would also "seriously impede the government's ability to investigate drug trafficking, terrorism, and other crimes." Furthermore, the

administration disagreed with the Supreme Court's original ruling, arguing that the “automobile exception” cited in their decision—a provision which allows police officers to search a car for contraband and other illegal material—applies to both items within the car and any data which would indicate the location or movements of that vehicle.[1] The Supreme Court, however, is not alone in its disagreement with the administration's assertion of authority.

In fact, the program has been a matter of public contention for quite some time. Several cases of citizens discovering themselves subject to GPS surveillance have gained media attention over the last few years. In 2010, for example, then-20-year-old Yasir Afifi, an American-born citizen and college student, discovered a suspicious device on his car after having taken it to a mechanic for a routine oil change. Afifi removed the device from his vehicle and, suspicious of being targeted by the authorities due to his ethnicity and family history, posted pictures of the device online (Afifi's family has lived in Egypt since 2003 after moving there from the United States, and his father was a president of the Muslim Community Association).

Within two days, Afifi received confirmation that the troubling object was, in fact, a GPS tracking device. This confirmation came in the form of a visit from federal agents, who proceeded to demand the return of the device and then questioned him about a threatening blog post supposedly written by a friend. During the questioning, he learned that he had been under close surveillance for some time; one agent at the meeting congratulated him on a new job which he had been hired for only very recently. Afifi had previously suspected that he was on a federal watchlist, as he was regularly subjected to extra screening at airports during his frequent business trips. Also, six months prior to his encounter with the authorities, a former roommate told Afifi that he had been contacted by FBI agents responding to an anonymous tip that the young student was a possible “threat to national security”. Yasir Afifi was contacted by the American Civil Liberties Union shortly after posting about his experiences online, and gained legal representation in a suit against the government for violations of his civil liberties. He has since requested a stay on his case in the wake of the current uncertainty over the legality of such warrantless GPS tracking. [2]

In 2011, another young man reported finding a different GPS device on his vehicle after a trip to the mechanic. The man (wishing to be known only as “Greg” in a single interview with Wired magazine)

discovered the GPS device after buying a car from a cousin who later turned out to be under investigation in a criminal case involving drugs. However, Greg insisted that not only was he not involved in any illegal activities related to his cousin's legal troubles, but he did not even find out about the investigation until after he had already purchased the vehicle. Whether or not the tracking device was planted with a warrant is not certain. En route to an interview with Wired reporter Kim Zetter, scheduled in order to document the presence of the GPS device on Greg's car, the reporter found herself being followed by a trio of police cars to the interview location previously agreed upon. The two decided to relocate their interview nearby, and quickly found themselves followed again to the new location. Such overt and seemingly intimidating maneuvers by the authorities is a cause of concern for Zahra Billoo, the attorney for the aforementioned Yasir Afifi. The mere existence of such technology is not problematic on its own, “[b]ut it shouldn't be unchecked authority on the part of police officers. If law enforcement doesn't care to have their authority checked,” according to Billoo, “then we're in a lot of trouble.” [3]

Many have criticized such locative surveillance techniques as being needlessly invasive and arbitrary, and also feel that such activities should have much clearer guidelines for acceptable use than the current warrantless system. One recent piece of legislation, the Geolocation Privacy and Surveillance Act (also known simply as the GPS Act), seeks to clarify the circumstances in which geolocation data can be used. According to a recent press release from Utah Congressman Jason Chaffetz, who is a cosponsor of the act, the increasing technical ease with which a person's locational data can be retrieved does not mean that the government should simply be able to access such private information without a warrant. Rather, supporters of the GPS Act argue that the government should do even more to protect citizens' privacy from what they believe to be unreasonable searches under the Fourth Amendment.

According to Chaffetz and others, legislation such as the GPS Act is necessary since “the Department of Justice is still arguing in court that they do not need a warrant to track someone’s movements using GPS devices or technology. This highlights the need for Congress to step in and provide clear and reasonable guidelines.” [4] Such “reasonable guidelines” would include provisions forcing law enforcement agencies to obtain a warrant before acquiring GPS information for an individual, and would carry criminal penalties for

“surreptitious”, warrantless use of geolocation technology for both law enforcement and companies. The act would also prohibit the revelation of an individual's GPS data by commercial service providers to outside parties such as AT&T, who were sued by the Electronic Frontier Foundation for allegedly sharing customer information with the National Security Agency without customer consent. [5] The passage of legislation like the GPS Act would certainly be a positive step towards allaying the impression some glean from warrantless government surveillance—namely, that of a government willingness to ignore the rights of its citizens in favor of the ability to spy on them without inhibition.

GPS data is not the only source of concern for privacy advocates; drones are another rapidly-evolving technology that will have wide-ranging effects on citizens' expectations of Fourth Amendment privacy protections. While the public perception of drones largely centers around their deployment by the military in various combat operations in the Middle East, this is in fact a rather narrow view of their use. In the near future, drones are expected to expand both in their surveillance capabilities and range of operation. Troublingly for some, this widened range includes U.S. airspace. The combination of these two factors has the potential to seriously impact Americans' “right to be left alone”.

Perhaps the most chilling example of this is the ARGUS-IS drone surveillance system. Recently developed by DARPA as a tool for “wide area persistent surveillance”, the ARGUS system consists of a 1.8 gigapixel sensor array (composed essentially of 368 separate 5-megapixel cell phone cameras) which allows for an unprecedented level of surveillance. From altitudes of up to 20,000 feet, ARGUS is capable of recording video over an area equivalent to around half the size of Manhattan. The system is also able to track incredibly small objects from such a height (as small as six inches, in fact) and has a massive data storage capacity of 6,000 terabytes. For comparison, most of the larger computer hard drives available commercially have a storage capacity of only 1 to 4 terabytes. In effect, the ARGUS drone surveillance system would confer upon the government not only the ability to record the activity of a small city in incredible detail, but also a massive backlog of recorded activity which could later be sifted through at leisure.

The privacy implications of such technology should be readily apparent; not only would the near-certainty of having one's every move passively surveilled as soon as one steps out the door practically eliminate

the “right to be left alone”, but the backlog of activity ARGUS provides would allow for authorities and analysts to retroactively record, track, and scrutinize a person's every move through an area for days, looking for “suspicious” activity without either their knowledge or consent. This would clearly violate Fourth Amendment expectations against unreasonable search. [6] Some may argue that this would be no different than being seen on camera anywhere in public—in a store or at the bank, for example. However, this is a spurious argument at best. While people may expect to be seen on camera in such establishments for the purpose of preventing theft, one would be hard-pressed to find many people who expect to have their every move recorded across an area the size of a small city—to say nothing of being comfortable with the idea. In fact, it could be argued that this pervasive surveillance capability would not only fly in the face of Fourth-Amendment protections against unreasonable searches, but would actually qualify as a search outright. In *Katz v. United States*, the Supreme Court ruled that the Fourth Amendment protects all areas where a person has a “reasonable expectation of privacy”. It also established this expectation of privacy as essentially being considered reasonable by society at large. [7] While it is reasonable to conclude that a person is visible when out in public, and therefore not necessarily in a private place, it has yet to be demonstrated that this therefore justifies the type of near-complete, retroactive and invasive surveillance provided by use of the ARGUS-IS system.

While today's drones do not currently have the advanced surveillance capabilities of ARGUS, what they lack in ability could soon be made up for in numbers, as the presence of drones in American airspace is slated to greatly increase in the near future. The Federal Aviation Administration, for example, announced last year that plans were underway which would see small unmanned aircraft (defined as those under 55 pounds) in the air by 2014. Larger aircraft would likely be cleared for takeoff the following year, and tests will soon be performed in order to determine how best to add drone traffic to America's busy skies.[8] These new drones would also be able to take off from any one of sixty-four planned bases scattered across the country. [9] This is not a troubling development in and of itself, of course. Drones will have many uses which should cause no concern for privacy advocates; search-and-rescue operations, fighting wildfires, geographical surveys, and meteorology are just a few areas where drone proliferation would be of undeniable benefit, and more uses will likely become apparent in coming years. However, when paired with the development of programs such as ARGUS, the impending

acceleration of drone deployment by law enforcement agencies, and the general lack of current legislation aimed at protecting citizens' Fourth Amendment rights in the face of such powerful surveillance tools, the idea of widespread drone proliferation becomes rather troubling. [10]

The use of unmanned drones and warrantless GPS tracking are enough to worry anyone who is concerned about the future of our right to privacy. Unfortunately there are many other developments, in terms of both technology and national policy, which threaten to undermine the rights enshrined in the Fourth Amendment. Two rather disconcerting trends are included in these developments. Firstly, there is the steadily increasing ability and willingness of the government to conduct widespread surveillance on nearly all private communications, as well as a penchant for doing so with little to no justification or oversight. Secondly (and perhaps even more worrisome), we see a seemingly simultaneous growth of public apathy or ignorance about these surveillance methods. In fact, such a broad lack of widespread understanding or concern among the general public could present just as great a danger to our Fourth Amendment rights as the surveillance itself.

As previously mentioned, there is a wide range of techniques with which various government agencies conduct surveillance on the American population. Perhaps the most infamous of these is a National Security Agency program colloquially known as the “warrantless wiretap program”, conducted under the authorization of then-President George W. Bush. While many of the details have yet to be revealed, the spy program allowed for the collection of “hundreds, perhaps thousands” of international phone calls and emails made by people within the United States. Ostensibly, the NSA carried out such surveillance in order to track possible communications with al Qaeda. However, after the program was revealed in a groundbreaking 2005 *New York Times* article, controversy soon followed. [11] Many were uncomfortable with the precedent set by the NSA, arguing that since the surveillance was carried out without first seeking a warrant, it violated both the requirements of the Foreign Intelligence Surveillance Act and the Fourth Amendment rights of those spied upon under the program.

In a ruling as controversial as the program itself, Judge Anna Diggs Taylor ruled that such electronic surveillance was unconstitutional since “[t]he President of the United States . . . has indisputably violated the Fourth in failing to procure judicial orders as required by FISA, and accordingly has violated the First

Amendment Rights of these Plaintiffs as well." However, even amongst those who agreed with the overall outcome of the ruling, the legal justifications for the decision were criticized as "innovative" yet ineffective since it relied on the argument that plaintiffs may have felt intimidated in expressing their First Amendment right to free speech, rather than relying on existing jurisprudence. [12] The decision was later overturned.

Even more frustrating to those concerned with the growing prevalence of such surveillance, the collusion of telecommunications corporations such as AT&T in the aforementioned "warrantless wiretap" program has been repeatedly protected from both scrutiny and legal action. Mark Klein, a former AT&T employee, joined the Electronic Frontier Foundation in suing the company in 2006 for allegedly allowing the NSA to access customer phone calls and divert internet traffic into a room installed per the NSA's request at a switching center in San Francisco. According to the employee's statement, the NSA also installed a data-sifting device (a Narus STA 6400, specifically) which is "known to be used particularly by government intelligence agencies because of its ability to sift through large amounts of data looking for preprogrammed targets". This revelation only served to increase the skepticism of many as to the nature and scope of the NSA's surveillance programs. The agency's installation of such data-mining equipment in a room built especially for that purpose indicated to Klein that "unlike the controversy over targeted wiretaps of individuals' phone calls, this potential spying appears to be applied wholesale to all sorts of internet communications of countless citizens." [13]

Such concerns, unfortunately, would go largely unaddressed. In 2008, the Bush administration succeeded in gaining immunity for companies like AT&T against any litigation stemming from their involvement in such surveillance programs. This immunity was later upheld by the Supreme Court in 2012, and the Obama administration sided with the Court's decision "in order to encourage cooperation in efforts to fight terrorism". [14] The defense that such seemingly obvious violations to citizens' Fourth Amendment rights are justified in order to combat terrorism have only escalated in recent years, and the methods with which surveillance is carried out have also expanded.

In somewhat stark contrast to AT&T's outright compliance with government surveillance, tech giant Google has recently come forward with information regarding how often the government collects information on citizens through Google's services. Specifically, Google has revealed how often the Federal Bureau of

Investigations demands customer information (ostensibly in pursuit of cases related to preventing terrorism) through national security letters. Also known as NSLs, these documents allow the FBI to gather a plethora of information, ranging anywhere from online contacts and sites visited to the content of what a person has said online. The possibility that an individual's supposedly private and anonymous activities on the Internet (such as posting political opinions) can be retrieved at any time by the FBI should be troubling enough. However, there is even more cause for concern with the practice, as the government not only has the supposed authority to demand this information, but also prevents companies who have received a national security letter from disclosing to customers that such information has even been collected at all. Not only can these practices violate a person's right to privacy, but they may never even find out that their Fourth Amendment rights have been violated in the first place. [15]

In another surprising potential victory for privacy advocates, a California federal judge recently ruled that the use of such national security letters and their subsequent gag orders is an unconstitutional violation of the First Amendment. The ruling also stated that the use of such letters is a threat to the separation of powers amongst the branches of government, as it "impermissibly attempts to circumscribe a court's ability to review the necessity of nondisclosure orders," which would basically nullify the judicial branch's ability to check certain actions of the executive branch. [16]

Another government surveillance method which has drawn recent criticism is its frequent use of a piece of equipment known colloquially as a "Stingray". Essentially, the Stingray is a device which mimics a cell phone tower, allowing the user to determine the location of targeted cell phones as well as intercept calls made on that phone. The device is not as specific as it would at first appear, however. Since it functions by mimicking a mobile tower, a suspect's phone attempt would not be alone in connecting to the Stingray—it would be joined by every cell phone in the area that would connect to the type of tower the Stingray is mimicking. This essentially allows for passive data collection of innocent citizens who would be completely unrelated to the subject of surveillance—which would, again, violate their Fourth Amendment right to unreasonable search and seizure. Even more troubling, the use of such "omnivorous" data capture devices is on the rise and seeing more widespread application. The Los Angeles Police Department, for example, used Stingray technology at least 21

times during what would be considered “routine” operations, such as investigations into murder, theft, and drug-related crimes. [17] This illustrates the corrosive nature of the argument that it is justifiable to ignore Fourth Amendment concerns about privacy in order to “stop terrorism”, as the LAPD example was completely unrelated to terrorism—and yet, Fourth Amendment rights were still apparently violated.

It also seems the devices may have been used rather surreptitiously by law enforcement. In a series of recently-released emails from the Department of Justice, it is revealed that in many cases, federal agencies were requesting permission to conduct electronic surveillance without specifically mentioning their intention to deploy Stingray devices in their applications to the court. In a recent and ongoing case involving the use of these surveillance methods, the government claimed that this was an unintentional omission by agents “using a relatively new technology”. While this may in fact be the case, it does little to mitigate the serious privacy concerns raised by the growing use of data-mining technologies such as the Stingray or the Narus that was deployed within the offices of AT&T.

The use of the aforementioned technologies and programs—which are designed to gather massive amounts of data on citizens—raises a question which is incredibly relevant to concerns about the future of our Fourth Amendment rights. Namely, *what is being done with this information?* Especially if they are determined to be innocent during an investigation, or are unknowingly “swept up” in such widespread dragnet policies? The answer is, unfortunately, rather daunting.

An investigation conducted in 2012 by the *Wall Street Journal* uncovered a forthcoming policy which represents “a sea change in the way that the government interacts with the general public”. Dubbed the National Counterterrorism Center (or NCTC), this new initiative allows for activities which would come into direct conflict with the protections guaranteed in the Fourth Amendment. Specifically, the NCTC is authorized to conduct dragnet surveillance on American citizens, regardless of whether or not they are even suspected of a crime. The agency is now able to compile and keep records on the public (copied wholesale from various government databases) for up to five years, as well as sift through that massive cache of data for any activity which could be considered “suspicious”. Furthermore, if a person is “reasonably believed to constitute terrorism information”, their records may be kept permanently. This data could also be shared with foreign governments

for independent analysis. Such widespread sharing of data between government agencies was once prohibited by the Federal Privacy Act, which prevented inter-agency sharing of information for reasons irrelevant to why such was originally collected. Apparently, this is no longer the case as long as an agency files a notice with the Federal Register—an exception which seems to function as little more than a rubber-stamping mechanism for such widespread data sharing.[18]

The Fourth Amendment implications of a surveillance program of such magnitude are astounding and, frankly, somewhat disturbing. A program in which almost any data collected about a person by myriad government agencies can be gathered together, investigated for vaguely-defined "suspicious activity" regardless of their innocence, and kept for up to five years—or perhaps forever— seems to completely nullify the Fourth Amendment expectation that a person has the right to be secure "in their persons, houses, papers, and effects, against unreasonable searches and seizures".

Even more troubling than the breadth and scope of the surveillance programs and methods described above is the reaction to them from the public at large—or specifically, the relative *lack* of a reaction. While groups such as the American Civil Liberties Union, the Electronic Frontier Foundation, and others have a relatively long history of addressing the corrosive influence surveillance has been exerting on our Fourth Amendment rights, it seems that a majority of the general public remains almost completely unaware of these critical issues. Furthermore, it seems that whatever attention is paid to matters of privacy is misdirected into relatively trivial matters. For example, a recent fiasco arose over changes to Facebook's privacy policy and received a great deal of attention from both the public and the media. Around the same time, the FISA Amendments Act was passed, which granted prosecutorial immunity to telecommunications companies for the NSA's warrantless wiretapping program (as discussed earlier). [19] While this may have received some attention in the news media, the Facebook privacy changes received far more public scrutiny despite being almost completely inconsequential with regards to their Fourth Amendment rights.

This state of affairs must change if we are to maintain our Fourth Amendment right to privacy and security against unreasonable search and seizure. Public apathy and ignorance about the various surveillance programs, techniques, and technologies currently being deployed by our government is the main factor in

allowing such activities to alter our right to privacy. If there is to be any hope of preventing a “sea change” in our understanding of that right, a greater public understanding must be reached of the Constitutional threats posed by the gross misapplication of GPS, drone, and cellular tracking technologies.

At the close of the Constitutional Convention, when asked about the sort of government our fledgling nation was to have, Benjamin Franklin reportedly quipped “a Republic, if you can keep it.” In the face of such broad and seemingly insurmountable threats to our current understanding of our Fourth Amendment rights, our stewardship of the Republic may become far more difficult to maintain.

Endnotes

1 Webster, Stephen C. "Obama Administration: Warrantless GPS Tracking Needed." Obama Administration: Warrantless GPS Tracking Needed to Fight Terrorism | The Raw Story. March 19, 2013. Accessed March 20, 2013. http://www.rawstory.com/rs/2013/03/19/obama-administration-warrantless-gps-tracking-needed-to-fight-terrorism/.

2 Zetter, Kim. "Caught Spying on Student, FBI Demands GPS Tracker Back." Wired.com. October 05, 0010. Accessed March 23, 2013. http://www.wired.com/threatlevel/2010/10/fbi-tracking-device/all/.

3 Zetter, Kim. "Busted! Two New Fed GPS Trackers Found on SUV." Wired.com. November 06, 2011. Accessed March 23, 2013. http://www.wired.com/threatlevel/2011/11/gps-tracker-times-two/all/.

4 "Chaffetz Works to Protect Privacy with GPS Act." Welcome to Congressman Jason Chaffetz. March 21, 2013. Accessed March 23, 2013. http://chaffetz.house.gov/press-release/chaffetz-works-protect-privacy-gps-act.

5 "EFF's Case Against AT&T | Electronic Frontier Foundation." Electronic Frontier Foundation. Accessed March 21, 2013. https://www.eff.org/nsa/hepting.

6 Kopstein, Joshua. "The Verge." The Verge. February 1, 2013. Accessed March 21, 2013. http://www.theverge.com/2013/2/1/3940898/darpa-gigapixel-drone-surveillance-camera-revealed.

7 "Facts and Case Summary." USCOURTSGOV RSS. Accessed March 24, 2013. http://www.uscourts.gov/EducationalResources/ClassroomActivities/FourthAmendment/CellPhoneSurveillance/FactsAndCaseSummary.aspx.

8 Gallagher, Sean. "ArsTechnica." Ars Technica. August 8, 2012. Accessed March 21, 2013. http://arstechnica.com/tech-policy/2012/08/faa-chief-dont-fear-the-reapers-or-predators-global-hawks-other-drones/.

9 Franceschi-Bicchierai, Lorenzo. "Revealed: 64 Drone Bases on American Soil." Wired.com. June 11, 2012. Accessed March 23, 2013. http://www.wired.com/dangerroom/2012/06/64-drone-bases-on-us-soil/.

10 Stone, Andrea. "Drone Program Aims To 'Accelerate' Use Of Unmanned Aircraft By Police." The Huffington Post. May 22, 2012. Accessed March 21, 2013. http://www.huffingtonpost.com/2012/05/22/drones-dhs-program-unmanned-aircraft police_n_1537074.html.

11 Risen, James, and Eric Lichtblau. "Bush Lets U.S. Spy on Callers Without Courts." The New York Times. December 16, 2005. Accessed March 24, 2013. http://www.nytimes.com/2005/12/16/politics/16program.html?pagewanted=all.

12 Liptak, Adam. "Many Experts Fault Reasoning Of Judge in Surveillance Ruling." The New York Times. August 19, 2006. Accessed March 24, 2013. http://www.nytimes.com/2006/08/19/washington/19ruling.html?ex=1313640000.

13 Singel, Ryan. "Whistle-Blower Outs NSA Spy Room." Wired.com. April 7, 2006. Accessed March 23, 2013. http://www.wired.com/science/discoveries/news/2006/04/70619.

14 Baynes, Terry. "Supreme Court Won't Review Telecom Immunity for Surveillance." Reuters. October 09, 2012. Accessed March 24, 2013. http://www.reuters.com/article/2012/10/09/us-usa-court-telecom-idUSBRE8981F920121009.

15 Abdo, Alexander. "American Civil Liberties Union." American Civil Liberties Union. March 7, 2013. Accessed March 24, 2013. http://www.aclu.org/blog/national-security-technology-and-liberty/googles-report-nsls-what-we-still-dont-know.

16 Valentino-Devries, Jennifer. "Judge Strikes Down Secretive Surveillance Law." Wall Street Journal. March 15, 2013. Accessed March 24, 2013. http://online.wsj.com/article/SB10001424127887324532004578362710014676902.html?mod=WSJ_hpp_LEFTTopStories.

17 Timm, Trevor. "As Secretive "Stingray" Surveillance Tool Becomes More Pervasive, Questions Over Its Illegality Increase." Electronic Frontier Foundation. February 12, 2013. Accessed March 24, 2013. https://www.eff.org/deeplinks/2013/02/secretive-stingray-surveillance-tool-becomes-more-pervasive-questions-over-its.

18 Angwin, Julia. "US Terrorism Agency to Tap a Vast Database of Citizens." Wall Street Journal. December 13, 2012. Accessed March 23, 2013. http://online.wsj.com/article_email/SB10001424127887324478304578171623040640006-lMyQjAxMTAyMDEwMzExNDMyWj.html#

19 Masnick, Mike. "People Freak Out About Privacy On Facebook, But Ignore Widespread Government Surveillance." Techdirt. January 2, 2013. Accessed March 13, 2013. http://www.techdirt.com/articles/20121229/02225421522/people-freak-out-about-privacy-facebook-ignore-widespread-government-surveillance.shtml.