Government Monitoring of Electronic Communications

By Ira M. Schwartz
DeConcini McDonald Yetwin & Lacy, P.C.

Biography

IRA M. SCHWARTZ

Ira M. Schwartz is a shareholder in the Phoenix, Arizona office of DeConcini McDonald Yetwin & Lacy, P.C. He practices primarily in the intellectual property area, representing a broad range of clients from large corporations and universities, to small and medium sized high tech businesses, to individual artists, authors and inventors. His practice includes prosecuting copyright and trademark applications, both in the U.S. and internationally, preparing licensing and royalty agreements, manufacturing and distribution agreements, and enforcing and defending patent, trademark, copyright infringement and trade secret misappropriation cases in federal and state courts. Mr. Schwartz lectures frequently on the topics of Computer and Internet Law, Intellectual Property Law and International Arbitration of Intellectual Property Disputes. He is a member of the Board of the International Technology Law Association (ITechLaw) and a past president of the Intellectual Property Section of the State Bar of Arizona. Mr. Schwartz is also a *Judge Pro Tempore* of the Arizona Superior Court. In addition to his active intellectual property litigation practice, he has also handled numerous cases as a mediator and an arbitrator.

Ira M. Schwartz
DeConcini McDonald Yetwin & Lacy, P.C.
7310 N. 16th Street, Suite 330
Phoenix, Arizona 85253
Phone: (602) 282-0500
Email: ISchwartz@dmylphx.com

Government Monitoring of Electronic Communications

By Ira M. Schwartz
DeConcini McDonald Yetwin & Lacy

Presented to the International Technology Association
October 3-5, 2012 – Rome, Italy

In the past when the government wanted to monitor the activities of people, it had to exert considerable effort to do so. It needed people to physically observe a person's activities and movements or physically tap into telephone lines. Now, with the advent of computers, cell phones, the internet and social media, the government can monitor a person's location, movement, activities and communications merely by looking up some computer records. Further, by aggregating data from various sources, the government can compile a detailed dossier without more than a few mouse clicks. The question is: how far can the government permissibly go?

What is the Government Monitoring?

Your cell phone information. According to a recent article in the American Bar Association Journal[1], during 2011 cellphone carriers responded to approximately 1.3 million demands from law enforcement requiring the disclosure of cell phone information.[2] This included both location data and text messages. Keep in mind that for most cell phones the GPS software on such phones cannot be turned off and is active even when the phone is turned off.[3]

Your Emails. In one recent extreme example, the Food and Drug Administration secretly monitored emails of its own scientists, including emails which the scientists sent to their own lawyers and to members of a congressional oversight committee. While the monitoring was originally done to investigate a possible leak of confidential data, the monitoring quickly became a far reaching effort by high

---

[11] Martha Neil, *It Isn't Necessarily Big Brother, But Somebody is Potentially Watching, Virtually All the Time*, ABA Journal, posted July 17, 2012 at http://www.abajournal.com.

[2] Debra Cassens Weiss, *Congressional Inquiry Reveals 'Explosion in Cellphone Surveillance'*, ABA Journal, July 9, 2012 at http://www.abajournal.com.

[3] As of June 2011 there were over 322 Million wireless devices in the United States. Facts cited in *United States v. Jones*, (Supreme Court No. 10-1259 decided Jan. 23, 2012, Justice Alito concurring in the judgment).

ranking FDA officials to quell criticism of the FDA. The monitoring went so far as to log keystroke information on home computers of the scientists, personal email accounts, personal thumb drives, and keystroke monitoring of messages as they were being composed.[4]

Social Media. London's Metropolitan Police Force set up a social media hub and used automation to help spot early signs of riots or demonstrations during the recent Olympics. The U.S. Federal Bureau of Investigation has been investigating companies to help it build social media monitoring apps for similar purposes. [5] In addition, the U.S. Department of Homeland Security has been observing Facebook, MySpace, Twitter, YouTube, Flicker, and even Hulu.[6] Government monitoring does not end with social media websites. The government also monitors websites

[4] Eric Lightblau and Scott Shane, *Vast F.D.A. Effort Tracked E-mails of Its Scientists*, The New York Times, July 14, 2012 at http://www.nytimes.com.

[5] *Tweet with Caution*. Pittsburgh Post Gazette, July 15, 2012 at http://post-gazette.com.

[6] Graeme McMillan, *Big Brother is Watching: Document Reveals Surveillance of Social Media, Blogs, Image-Sharing Sites*, Time Techland, Jan. 12, 2012 at <http://www.time.com...>

such as the New York Times Lede Blog, The Drudge Report, Huffington Post and many others.[7]

The monitoring of online postings has taken on a new dimension recently as schools have started to aggressively monitor the online postings of their students. Schools have been bolstered by new state laws. North Carolina recently enacted a law making it a crime for students to post statements via the internet that "intimidate or torment faculty."[8] The law makes such conduct a misdemeanor punishable by up to a $1,000.00 fine and/or probation.

However, almost as quickly as states are adopting such laws, certain courts are striking them down as unconstitutional violations of the student's First Amendment Rights.[9] Two things should be noted: First, as part of the school's investigations of such conduct, the schools are requiring the students to disclose their Facebook user ID's and passwords, conduct which itself is questionable. Second, the conduct specifically involved information posted online by students

---

[7] Id.
[8] See Steve Eder, *Teachers Fight Online Slams*, The Wall Street Journal, September 17, 2012 at http://www.online.wsj.com.
[9] See Sam Favate, *Court: Student's Facebook Messages are Protected Speech,* The Wall Street Journal, September 18, 2012 at http://www.blogs.wsj.com.

using their personal computers outside of school hours and school activities.

Skype Calls? Recently Skype upgraded its infrastructure. Skype reported that these improvements were made to "improve user experience and reliability." However, technology blogs were speculating that such improvements would allow law enforcement to better monitor Skype calls. Skype admitted that, in appropriate cases, it would pass on messages to law enforcement. However, online blogs raised concerns because Microsoft, which owns Skype, has filed a U.S. Patent for "Legal Intercept," a technology capable of monitoring communication between two entities using VoIP (Voice over Internet Protocol) calls. These events lead to news reports linking the two.[10]

What are the Rules?

Recently, the United States Supreme Court had an occasion to consider how far the government can go in monitoring the activities of a person before they need to obtain a search warrant. In *United States v. Jones*, (S. Ct. Case No. 10-1259

[10] *Skype Denies Police Surveillance Policy Change*, BBC News (Technology) July 27, 2012 at http://www.bbc.co.uk.

decided January 23, 2012) the Court considered whether the government needed a warrant to attach a GPS monitoring device to a suspect's vehicle for the purposes of continuously monitoring his location. For differing reasons, all nine Supreme Court Justices said yes. However, the Court issued three different opinions on the matter and, while all the Justices concurred in the result, there was (in this author's opinion) no clear consensus as to the legal standards for evaluating what constitutes an "illegal search".

The majority opinion, authored by Justice Scalia, held that attaching the GPS device to the suspect's vehicle violated the original intent of the Fourth Amendment because the attachment to the vehicle was a search of an "effect" which required a warrant. Applying an original meaning interpretation of the Fourth Amendment, the attachment to the vehicle was analogous to a trespass to the chattel, namely the vehicle, which required a search warrant.

The government argument, that the suspect had no expectation of privacy in the location of the vehicle because this could be publicly observed, was rejected. The Court majority determined that the "expectation of privacy" test was not the only test under the Fourth Amendment and, therefore, they did not need to address this question.

The Court majority in *Jones* included Justice Sotomayor, who filed a concurring opinion in which she went out of her way to provide several cautionary notes. First, she joined Justice Alito's opinion (which concurred in the judgment) that longer term GPS monitoring would impinge upon the reasonable expectations of privacy, and, therefore, would require a warrant under any type of Fourth Amendment analysis. She also noted that long term monitoring of the GPS position of a person's car would reveal private information. She discussed examples like trips to a psychiatrist's office, an abortion clinic, an AIDS treatment center, a mosque, synagogue or church, or a gay bar, etc. She went on to argue that awareness that the government is watching would chill a person's rights to free association and free expression. Finally, she went on to question whether it may be necessary to reconsider the legal premise that a person has no expectation of privacy in information disclosed to third parties.

Justice Alito wrote a separate opinion, concurring in the judgment, in which he stated that he would have determined the case based upon the expectation of privacy test. It should be noted that three other justices (not including Justice Sotomayor) joined in Justice Alito's opinion. He went on to

note several potential problems that would be created with the majority approach. One of the most interesting is whether physical trespass is required to trigger the Fourth Amendment protection, or whether unwanted electronic contract from one computer to another would be sufficient. As many are aware, there are several reported cases where unwanted computer to computer contact has been considered trespass to chattels.[11]

Interestingly, in a recent decision subsequent to the *Jones* ruling, the Sixth Circuit Court of Appeals in a criminal case determined that a defendant had no expectation of privacy in the location data emanating from his cell phone and that no warrant was required by the police to obtain such data.[12] The Court there determined there was no expectation of privacy in the phones GPS location and that since there was no physical touching of anything by law enforcement, there was no Fourth Amendment violation in obtaining such data without a warrant.

---

[11] *CompuServe, Inc. v. Cyber Promotions, Inc*. 962 F. Supp. 1015 (S. D. Ohio 1997): See also *Register.com, Inc. v. Verio, Inc*., 126 F.Supp.2d 238, (S.D.N.Y 2000).

[12] *U.S. v. Skinner*, (6th Cir., No. 09-6497 decided Aug. 14, 2012).

Who Else is Watching?

According to a report in the Wall Street Journal, the top 50 websites in the United States installed, on average, 64 pieces of tracking technology on to a user's computer when the user visited those sites. In most cases no warning was given to the visitors.[13] This tracking technology in the past was mainly cookies, but now includes cookies, flash cookies, beacons, and other types of tools. In some cases, this even includes some types of cookies that can regenerate themselves after being deleted.[14]

In most cases, these tools do not include personally identifiable information, but instead set up an individual user profile that may include demographic and similar information such as: location, income levels, marital status, home ownership, presence of children in the home, shopping interests, other websites you have visited and other categorical information. This information is used to develop a profile of the computer user, which is then sold by middlemen to advertisers.[15] In some cases, the user profiles are matched by sophisticated statistical algorithms to certain

---

[13] Julia Angwin, *The Web's New Goldmine: Your Secrets*, The Wall Street Journal, July 30, 2010 located at http://online.wsj.com/article/....
[14] *Id*.
[15] Id.

offline data, such as income levels and geography, to try to match ads to the user profile.[16] In other words, if you do an online search for vacation information, the online ads generated for you will be tailored based upon your search information and "educated guesses" about your income level, based on your geographic location and other information in your profile.

What Will the Future Look Like?

The sophistication of our current technology will present several novel legal issues that will have to be answered in the near future. The following appear to be a few that are ripe for resolution[17]:

Reasonable Expectation of Privacy: What is a reasonable expectation of privacy? And does the Fourth Amendment protect our "reasonable expectation of privacy" or is it limited to some type of trespass theory?

Related to this is the question: can one have a reasonable expectation of privacy even when they are acting in public? It can reasonably be argued that most people do not know

[16] Id.
[17] The comments in this section regarding projections for the future are strictly the opinions and comments of the author.

that their cell phone is constantly announcing their location to the world. However, whether we know it or not, does the fact that this happens mean that everyone has the right to know where we are every second of every day? Or can we expect that the government will not be monitoring our every move without at least going through the process of obtaining a warrant based upon probable cause?

Third Party Records Doctrine: I must also note that Justice Sotomayor may have forecasted the next big issue that the Supreme Court will be forced to address. The question that will face them is the extent to which releasing information to a third party means that all expectation of privacy in that information has been waived.[18] As the world progresses, information is moving away from paper maintained in the home to electronic records and information maintained by third parties. As we need to rely on these third parties to store and process this information, we should not thereby automatically lose all privacy rights in that information. In the past, the only third party who had access to such information on a regular basis was the telephone company when we made telephone calls. Further, we were all

[18] See also Orin Kerr and Greg Nojeim, *Crashing the Third Party: Experts Weigh How Far the Government Can Go in Reading Your Email*, ABA Journal, Aug. 1, 2012, available at <http://www.abajournal.com....>

protected by laws that very specifically protected the privacy of those telephone calls. Now there are multiple providers, providing a multitude of services for a variety of types of electronically transmitted and stored information. How these questions are handled will have a significant impact on how privacy laws develop.

I note that there are some particularly interesting and difficult questions that will present themselves as the technology advances. A few of these have already been raised in the media. Others have been framed in the context of science fiction; but science fiction is becoming tantalizingly close to science fact. Consider two related scenarios:

First is the *Minority Report*[19] paradigm. If police monitor someone's web searches and detect a pattern that they believe shows someone is planning a crime, at what point can they act to prevent the crime?[20]

Second, is the potential to use the internet for civil disobedience purposes, especially for objecting to the police power as described in the first scenario. What would happen

[19] Minority Report is a science fiction movie starring Tom Cruise. DreamWorks Pictures, 2002.
[20] See Will Oremus, *Could Cops Use Google to Prevent Murder?*, posted at Slate.com, June 6, 2012.

if hundreds of people in a selected location all perform a Google search for "how to bury a dead body?" merely for some type of political protest against the government monitoring of the internet? What, if anything, should be the response to that?

As the technology develops it is certain that, at least in some fashion, the government will use internet technology to monitor for potential illegal activity. The nature and extent of how far that monitoring will go and what checks and balances we need on that activity will have to be determined.

Ira M. Schwartz is a partner in the Phoenix office of DeConcini McDonald Yetwin & Lacy, P.C. He practices in the fields of intellectual property law, international law and mediation and arbitration of intellectual property disputes. He can be reached at (602) 282-0500 or ischwartz@dmylphx.com.