LESSONS FROM THE UNITED STATES:
THE PRACTICAL NECESSITY OF THE "INTERNATIONAL PRINCIPLES ON SURVEILLANCE AND HUMAN RIGHTS."

BY: HANNI FAKHOURY

Introduction

The goal of the Principles on Surveillance and Human Rights ("Principles") is to provide a framework by which current or proposed surveillance laws and practices can be evaluated to ensure they are consistent with human rights. The development of these principles provides a unique opportunity to review the United States' experience in regulating government surveillance and access to electronic data to understand the need for the Principles.

This paper hopes to provide a brief explanation of American law as it pertains to each of the Principles. Although American law is developed at both the federal and state level, this paper focuses on federal law. This paper also focuses on the law surrounding domestic investigations, and only briefly discusses foreign intelligence gathering and national security.

Legality

In the United States, the law of electronic surveillance is contained in two legal sources: (1) federal or state constitutions; and (2) federal or state statutory law.

The Fourth Amendment to the U.S. Constitution applies to the federal government and all the states, and prohibits the government from engaging in unreasonable searches and seizures. It requires law enforcement to obtain a "search warrant" before searching a place, including electronic devices and other forms of digital data. A "search" under the constitution is defined as either (1) a government trespass onto private property for the purpose of obtaining information; or (2) a government intrusion into a place where a person has manifested a subjective expectation of privacy that society would accept as reasonable.

Under federal statutory law, the Electronic Communications Privacy Act ("ECPA") governs law enforcement access to many forms of electronic data. ECPA has divisions dealing with specific forms of data; Title I of ECPA amended and updated the Wiretap Act, which regulates how the government can listen to or intercept the contents of a private communication, like phone calls. Title II of ECPA is the Stored Communications Act ("SCA"), which regulates how the government can access the contents of electronic communications (like emails, tweets, text messages, etc.) as well as other non-content information (like cell site location records) from an electronic communications or cloud storage provider. Finally, the Pen Register/Trap and Trace Device ("Pen/Trap") statutes regulate how the government can obtain the routing and transmission information for phone calls, and other forms of electronic content, such as IP addresses and some email headers.

Most states have adopted in whole or in part these provisions of federal law. Generally, states are free to adopt greater statutory protection than what exists under federal law, but cannot provide less privacy protection. A few

states have taken some steps to improve their electronic privacy statutes, and have generally moved much faster than the federal government, which has failed to adequately update ECPA since it was enacted in 1986.

Necessity

Under the Fourth Amendment, a search warrant must be limited as much as possible to prevent general rummaging through a person's belongings, including their electronic data. That includes requiring law enforcement to return to the judge with an inventory of what they have seized, so the court can supervise the police. When it comes to electronic data, one court has warned (PDF) that judges must exercise "greater vigilance" to ensure the government does not collect more data than necessary.

But electronic privacy statutes in the United States have a mixed record when it comes to limiting law enforcement access. The Wiretap Act has strong privacy protection built in, requiring police to minimize the phone conversations they intercept to ensure they are only capturing conversations concerning criminal activity. But the SCA and Pen/Trap statutes don't have similar minimization requirements for the contents of electronic communications or Internet routing information. This needs to be changed – particularly the SCA – which could potentially allow law enforcement wide access to emails and other forms of electronic content.

Adequacy

As explained above and the Petraeus scandal demonstrated, American law enforcement has been anything but restrained when it comes to seizing and searching electronic data.

To make matters worse, there has been great law enforcement pressure on providers and Congress to implement data retention policies for a wide range of data stored by communication providers, like text messages and IP address information. There policies would require providers to keep information solely for the sake of law enforcement's perusal at a later time, oftentimes against the wishes – and business interests – of the providers.

There must be push back against these types of policies, which serve only the government's purpose of surveillance, and as described in more detail below, present security risks.

Proportionality

The Fourth Amendment of the U.S. Constitution requires the police to obtain a "search warrant" in order to conduct a "search" or seize electronic or physical data. To obtain a "search warrant," the police must demonstrate to a judge that they have "probable cause" – that it is more likely than not – that evidence of a crime will be found in the place they want to search. If the judge believes the police have demonstrated probable cause, the judge can issue the search warrant, though the judge must specify what specific places the police may search and what specific items they may seize.

But this probable cause standard only applies if the government is engaging in a "search." And there are many (in fact, too many) exceptions to the search warrant requirement. Moreover, although it is clear the Fourth Amendment applies to data stored on a person's physical device, like their cell phone, there is legal debate on whether it applies to data stored by third parties and in the cloud.

The U.S. government has argued that a person does not have a "reasonable expectation of privacy" in information turned over to someone else, like an ISP or a social media website. Under current Fourth Amendment doctrine, without a "reasonable expectation of privacy," law enforcement is under no constitutional obligation to obtain a search warrant to get customer information and data from companies like Facebook, Twitter or Google. For example, a New York City court ruled that prosecutors did not have to get a search warrant to obtain data from Twitter about Malcolm Harris, an Occupy Wall Street protester, and could instead get information like tweets, and IP address login information with a subpoena since the data belonged to Twitter, not Harris. The same thing happened with the Twitter records of Icelandic Parliament member Birgitta Jonsdottir, which the federal government wanted to see in connection to with its ongoing investigation into Wikileaks. Other courts have disagreed, finding that even though information like email is turned over to third parties, they retain a "reasonable

expectation of privacy," and therefore it is still constitutionally protected and law enforcement must obtain a search warrant to review it.

To make things worse, federal statutory law doesn't require this probable cause standard for all forms of information either. Instead, different legal standards of varying privacy protection apply to different forms of electronic and digital information in the United States.

The strongest privacy protection is in the Wiretap Act, which not only requires law enforcement have probable cause to believe intercepting phone calls will lead to evidence of specific, enumerated crimes, but also requires law enforcement to demonstrate: (1) probable cause that communications regarding the crime will be obtained by the wiretap; (2) normal investigative procedures have been tried and have failed or reasonably appear to be unlikely to succeed if tried or to be too dangerous; and (3) probable cause to believe the phone number or other electronic "facility" where the communication to be intercepted occurs has a connection to the crime or person to be wiretapped.

But the other parts of ECPA do not have the same strong privacy protections contained in the Wiretap Act. The SCA only requires law enforcement to obtain a search warrant to access the contents of electronic communications that are in electronic storage for less than 180 days. Older electronic communications as well as other forms of stored electronic data, however, can be obtained without a search warrant under the SCA.

If the government can demonstrate to a judge "specific and articulable facts" that data is "relevant and material to an ongoing criminal investigation" – a standard far lower than the search warrant's probable cause standard – the SCA allows the government to obtain (1) the contents of electronic communications in electronic storage for more than 180 days (such as an old email siting in an email inbox); (2) contents of electronic communications stored in a cloud storage provider without having to give prior notice to the subscriber (like a PDF stored in Dropbox or Google Drive); and (3) other customer records not including contents (such as IP address information or cell site location information).

And with a only subpoena – which has no judicial supervision at all and may be issued by a lawyer provided it is "relevant" –the government can access (1) the contents of electronic communications stored in a cloud storage provider with prior notice to the customer; and (2) other "subscriber information," including a customer's name, address, local and long distance telephone connection records, or records of session times and durations, type and length of service (including start date), telephone number or other subscriber number or identity, including any temporarily assigned network address; and means and source of payment for the service.

Finally, the Pen/Trap statutes allow the government to obtain routing information if it can prove to a judge the data it wants is "relevant to an ongoing criminal investigation."

Some U.S. courts have found that the SCA does not meet the Fourth Amendment's standard, and required a warrant for this information. However, until this legal dispute is resolved by the courts or an amendment to the statute, the different standards in these statutes create confusion for everyone. Consumers are unsure how much privacy protection they have. Law enforcement, as has been demonstrated, is unclear and inconsistent in using the correct legal standard to obtain data. And courts are struggling to apply cases decided long before the advent of technologies like cell phones and social media networks, to the modern world we live in now.

A uniform standard that applies to all forms of electronic data and which contains strong privacy safeguards, like the one recommended in the Principles, benefits both consumers and law enforcement alike.

Due Process

As explained above, not all law enforcement requests for electronic data require prior judicial authorization. And even when judicial approval is required, the standards for disclosure differ depending on the data being requested. But even more problematic from a "due process" perspective, is the difficulties in proving violations of the law in both criminal and civil contexts.

A defendant in a criminal case can challenge government searches and seizures of electronic data that occur without a search warrant, or if the search warrant was deficient in some way. Most commonly this comes after a person has been charged with a crime and files a motion to suppress evidence. But it is only evidence the government intends to use against the defendant in trial that can be suppressed. All a successful challenge will do is eliminate the government's ability to use certain forms of evidence to convict the person. They may still face prosecution and imprisonment in many instances even without the government's use of the evidence. And although courts will "suppress" evidence taken in violation of the Fourth Amendment, there are many exceptions to the suppression remedy that diminish its effectiveness. For example, evidence will not be suppressed if the evidence was discovered by officers acting in good faith with a reasonable but mistaken belief they were authorized to take the item. Moreover, courts are hesitant to second-guess law enforcement or their judicial colleagues in reviewing the process of searching and seizing items. As a result, suppression isn't very common.

The situation is even bleaker when it comes to proving violations of the statutory restrictions on government access to electronic data. While the Wiretap Act has a statutory suppression remedy, neither the SCA nor the Pen/Trap statutes do. Challenges to the illegal seizure of the contents of electronic communications or routing information must be raised under the Fourth Amendment, not the statutes themselves.

For individuals who have been surveilled illegally, both the Wiretap Act and the SCA permit a private party to sue for improper audio interceptions and seizure of electronic contents. It can be difficult to overcome the many procedural hurdles necessary to bring a civil lawsuit against the government, though possible. For example, one will generally need to show a willful violation, which can be hard to prove. For unlawful seizures, EFF has sometimes turned to the Privacy Protection Act, which limits the government's ability to search or seize items related to publishing a newspaper or other journals and publications, to sue the government.

Sometimes national security concerns can present a difficult barrier. EFF has sued both the National Security Agency and AT&T over the federal government's warrantless wiretap program that started under President George W. Bush with varying levels of success. The case against the NSA has moved slowly, with the government seeking to get the case dismissed on the grounds the litigation would force it to reveal "state secrets." And Congress passed a law providing AT&T with immunity from suit, effectively ending any legal challenges to its role in the president's warrantless wiretapping program.

User Notification

Federal statutory law allows law enforcement to demand providers remain silent about requests for customer data. For example, as part of the post 9/11 PATRIOT Act, the FBI can bypass courts and issue administrative letters, called National Security Letters ("NSLs") (PDF), on their own authority to telecommunications companies. NSLs not only require the companies to disclose information about a customer, but also require the companies to not inform the customer of that demand, and to keep even its receipt of an NSL secret. There have only been a small number of legal challenges to this practice. Even outside the National Security context, the SCA permits the government to delay notice to a user about a government request for the contents of electronic communications and other information for up to 90 days, and law enforcement has the ability to request additional 90 day extensions.

In the absence of any legal limitation on a service provider's ability to notify its users of data requests, companies have a mixed record of informing their customers of law enforcement demands for their digital information. Twitter, for example, has a policy of informing its users of all requests for information prior to disclosure unless prohibited by court order. Facebook's policy is more vague, hinting that law enforcement should obtain a court order to avoid notification, but also permitting nondisclosure if it would "lead to risk of harm."

The importance of user notification cannot be overstated; users should know about requests promptly in order to safeguard their data, assert valid privileges, and seek legal assistance and guidance. Any governmental request for delayed notice should be limited to emergency circumstances, and should be as short as possible. The NSL mechanism of secret, silent access to a user's data should be rejected. So too should the SCA's approach of long,

sweeping periods of delayed notice. Instituting these standards for law enforcement will allow the companies to feel more emboldened to notify their users of law enforcement requests at a greater frequently than they do now.

Transparency about use of government surveillance

American law is lacking when it comes to transparency. With the exception of interception orders under the Wiretap Act, for which the government is required to publish an annual report on the use of wiretaps, there is very little transparency about how frequently the government seek access to electronic evidence (and even the Department of Justice has come under scrutiny for not turning over complete Wiretap Act records and statistics to Congress as required by law). But apart from Wiretap orders, there is little transparency on the part of the government or the providers on how much information the government is gathering, and for what purposes.

As a result, information about government use of various forms of electronic data has only come to light through a Congressional demand for information about requests to cell phone companies, a Freedom of Information Act ("FOIA") request filed by the American Civil Liberties Union ("ACLU") to local law enforcement agencies about their use of cell phone tower location information, and self reporting by companies like Google and Twitter on the number of domestic and international law enforcement requests for user information. Sadly, these reports are the exception, not the norm. Most technology companies do not voluntarily disclose this information. And attempts at the state level to require them to do so have been met with strong opposition by the companies.

Ultimately the picture these informal requests have painted is one of increasing government requests for user data. Thus, increased transparency is necessary to allow users to keep tabs on these growing demands and push back against overreach.

Oversight

In the United States, oversight presumably comes from within the various branches of the government. Law enforcement agencies within the executive branch have inspector generals that review internal practices, while national security agencies report to the Director of National Intelligence. At the legislative branch, congressional oversight committees receive reports from different law enforcement agencies. And the judicial branch hears legal challenges to government surveillance.

But none of these oversight committees are truly independent. And even the committees intended to be "independent" aren't in any meaningful sense of the word. For example, the Intelligence Oversight Board ("IOB") is a Presidentially appointed independent civilian oversight board that ensures the government complies with the law during foreign intelligence investigations. Yet, its actions, including for a time its membership, are shrouded in secrecy. For domestic intelligence, the Privacy and Civil Liberties Oversight Board (PCLOB) was intended to act as an independent check on domestic surveillance practices, but has largely been ineffective, neglected by both Presidents Bush and Obama, and already reorganized (PDF) despite its relatively short existence. Both the IOB and PCLOB exist within and answer to the office of the president, bringing its true "independence" into serious doubt.

Thus, apart from the efforts of various civil liberties organizations like EFF, ACLU, Center for Democracy and Technology ("CDT"), the Electronic Privacy Information Center ("EPIC"), and others to account for domestic government surveillance practices, there is no effective, public independent oversight committee tasked with reviewing domestic practices. And of course despite their best efforts, these organizations are limited in the information they can access. Most of the information is obtained through the court process and FOIA requests, and these organizations are certainly not in a position to review secret or classified information in most instances.

A more formal and truly independent oversight committee, tasked with reviewing the practices of both international and domestic surveillance and intelligence gathering is necessary to prevent civil liberties abuses and shed transparency about government practices.

Integrity of communications and systems

The integrity of network architecture is crucial to a secure digital world. But the American government has long waged a battle seemingly at odds with this goal. Despite obvious security and privacy risks, it has urged Congress

to implement long mandatory data retention periods, pushed for bans on cryptography – a crucial tool to protect electronic communications – all while lobbying to ensure its own backdoor access into communication systems.

The proposal for a backdoor into Internet communications comes from a push to update the Communications Assistance for Law Enforcement Act ("CALEA"). In 1994, Congress passed CALEA, forcing telephone companies to redesign their network architectures to make wiretapping easier. But it specifically excluded data travelling over the Internet. As use of the Internet has expanded, law enforcement has applied increasing pressure on Congress to update CALEA to require communications providers ensure their networks have a backdoor that allows the government to intercept Internet communications as well. This proposed update to CALEA (much like law enforcement's push for data retention) has far reaching and obvious negative consequences for privacy, security and innovation.

Moreover, at times the government has pursued with a heavy hand individuals who have exposed security vulnerabilities and flaws. A researcher was recently convicted under a federal crime prohibiting unlawful access to a computer when he exposed a flaw on AT&T's website that allowed him to obtain the email addresses on AT&T iPad customers by merely visiting an unrestricted website, and not bypassing any technological barriers to access. In another case, the Massachusetts transportation authority attempted to silence researchers who were planning to present research at a conference about vulnerabilities they discovered in the transit fare payment system.

Ultimately, government should encourage technology companies to maintain their customers data securely. But minimizing the risk of disclosure must include government preclusion from backdoor access and limits on data retention. At the same time security researchers who do not illegally access electronic information should not be treated as criminals for simply informing the public of their findings.

Safeguards for international cooperation

Sadly, many countries have attempted to export some of the United States' worse surveillance practices abroad. Unfortunately, countries have used international cooperation as a means to surveil people in violation of their own domestic laws. For example, in the American criminal investigation of the website Megaupload and its founder Kim Dotcom for copyright infringement, it was discovered that New Zealand authorities not only obtained improper search warrants for Dotcom's house there, but also illegally spied on Doctom by monitoring all Internet traffic coming in and out of his house.

That's why it is important to ensure that any law or treaty that legitimizes mass surveillance must be challenged. And any mutual legal assistance treaty (MLAT) must ensure that in the face of conflicting legal standards, the highest, most protective standard should apply.

Preventing illegitimate access

As explained above, individuals who have been the victim of illegal surveillance have civil remedies under both the Wiretap Act and the SCA to sue. But courts and legislatures should ensure that there are not overly burdensome procedural barriers to suit.

Cost of surveillance

Little is known about the cost of government surveillance in the U.S., though service providers have repeatedly insisted they aren't profiting from law enforcement and are merely recouping costs. A comprehensive FOIA request by the ACLU in 2012 revealed in detail the prices companies charged law enforcement for access to wiretaps and cell site records, revealing that the providers charged varying amounts, and many did not charge law enforcement anything in responding to emergency situations.

Ensuring that the costs of surveillance are borne by law enforcement can oftentimes act as a bulwark from government abuse: the more expensive to obtain electronic records and content, the more careful the government will be in what they seek.

Conclusion

Hopefully this primer on American law demonstrates the practical importance of the Principles. As the mistakes of United States law make clear, there are many ways in which privacy can be eroded and unrestrained surveillance can flourish. The Principles are a crucial first step in not only ensuring electronic privacy flourishes internationally, but also to begin the process of filling the privacy protection gaps existing in American law.