ACLU of Massachusetts
211 Congress Street, Suite 301
Boston, MA 02110
617-482-3170 x340
gwolfe@aclum.org

July 9, 2013

Joint Committee on the Judiciary
Sen. Katherine Clark & Rep. Eugene O'Flaherty, Chairs

SUPPORT FOR S.796/H.1684
APPLYING ESTABLISHED STANDARDS AND RULES
TO PROTECT PRIVATE ELECTRONIC COMMUNICATIONS

Dear Senator Clark, Representative O'Flaherty, and members of the committee:

Massachusetts needs to apply the basic rules and standards governing searches of people and property to our personal electronic communications. The ACLU of Massachusetts offers its strongest support for S.796/H.1684, "An Act updating privacy protections for personal electronic information."

The right to be free from unreasonable search and seizure is a fundamental right set forth in Article XIV of the Massachusetts Declaration of Rights and the Fourth Amendment to the U.S. Constitution. That right – born and developed here in Massachusetts and adopted in the Bill of Rights – has served the Commonwealth and the country well for more than 200 years. Today, however, the right to be free from unreasonable search and seizure is at a critical crossroads. We must make sure that our privacy-protective laws fit the way we live in the 21st century, when our "papers and effects" that the Founders and Constitution writers were determined to protect are now largely in digital form. Some of our most private and important personal information is no longer physical property kept in our homes, but rather a combination of deliberately and automatically-generated electronic information held by service providers.

"An Act updating privacy protections for personal electronic information" – the Electronic Privacy Act – was timely filed in January at the start of the session. Recent revelations about continuous, suspicionless, indiscriminate surveillance of every American by the NSA and the U.S. Postal Service have now brought the issue of electronic surveillance front and center. Public concern about government intrusion – particularly, monitoring of individuals' electronic communication – has rarely (if ever) been so focused or intense.

We increasingly lead lives connected via, and expressed in, digital data. It is time to do away with the fictional notion that the data we generate every day as we use our phones, computers, and other electronic devices doesn't belong to us, isn't "ours," and isn't deserving of privacy protection. It's true that some people routinely make personal information about themselves publicly available online: that's their decision. It's essential that individuals retain the ability to make their own choices about whether

and how much information to disclose about themselves, and to whom. We believe we should have and do have a reasonable expectation of privacy from government scrutiny, or, in the words of Justice Brandeis, "the right to be let alone."

When every American is under surveillance, it's clear that we need to restore checks and balances. We can start at home in the Commonwealth by establishing clear and reasonable standards for state and local law enforcement scrutiny of our phone and internet use, and the location information generated by our electronic devices.

The Electronic Privacy Act would protect the privacy interests of all of the Commonwealth's residents in a simple and straightforward manner. It would apply the traditional probable cause warrant standard and procedure to records of our phone and internet use, including our email, and to the location information generated by our electronic devices.

As a preliminary matter, it is necessary to understand some basic facts about the state of the law today. First, federal law in this area generally is woefully inadequate. The Electronic Communications Privacy Act (ECPA), which regulates government access to electronic information, has not been updated since 1986. Its drafters simply could not have anticipated the widespread use of cell phones or the kind of technology, including real-time tracking, that all of our phones and computers are equipped with today. Massachusetts law does little to bridge the gaps, leaving some of our most sensitive and private information vulnerable to unwanted, unwarranted intrusion.

First, **EMAIL**:
Under ECPA, law enforcement does not need to obtain a warrant to obtain private emails in draft form or stored on a server more than 180 days.[1] When Congress passed ECPA, it established the 180-day rule based on then-current technology. In 1986, if a message stayed on a company's server for 6 months without being downloaded, it was perhaps reasonable to consider it abandoned. Today, when web-based email systems allow us to store email indefinitely, everyone agrees that the outdated privacy expiration date is arbitrary and unjustified. Indeed, earlier this year, the Department of Justice testified to that effect before Congress:

> Many have noted—and we agree—that some of the lines drawn by the SCA [the Stored Communications Act, part of ECPA] that may have made sense in the past have failed to keep up with the development of technology, and the ways in which individuals and companies use, and increasingly rely on, electronic and stored communications. We agree, for example, that there is no principled basis to treat email less than 180 days old differently than email more than 180 days old. Similarly, it makes sense that the statute not accord lesser protection to opened emails than it gives to emails that are unopened.[2]

[1] 18 U.S.C.A. §2703 (a)&(b).
[2] Testimony of Acting Assistant Attorney General Elana Tyrangiel Before the U.S. House Judiciary Subcommittee on Crime, Terrorism, Homeland Security, and Investigations, March 19, 2013, http://www.justice.gov/iso/opa/doj/speeches/2013/olp-speech-1303191.html.

Unfortunately, our state law does *nothing* to address this clear gap in privacy protection. Certainly, Massachusetts should not wait for Congress to act. We need to establish uniform, sensible limits on government inspection of residents' email messages without regard to their age. Last month, Texas passed a probable cause warrant requirement for email[3], and Massachusetts should do the same.

Second, **PHONE AND INTERNET RECORDS**:
Currently, police and prosecutors in Massachusetts can obtain significant information about individuals' phone and internet use without obtaining a probable cause search warrant. This includes the details of who calls whom, when, for how long; who sends email or text messages to whom, how frequently; and where such communication takes place. It is information that can reveal all manner of relationships, associations, and personal connections. Instead of applying a meaningful criminal law standard, Massachusetts law states that law enforcement may obtain this information based on their belief that an individual's communication records "are actually or constructively possessed by a foreign corporation that provides electronic communication services or remote computing services"[4] – that is, for example, a mere belief that the individual is a Verizon customer.[5]

This makes no sense. Unless an individual has been arrested, police are prohibited from rifling through his or her phone or computer. Likewise, police should be prohibited from looking at the records service providers hold about an individual's phone and Internet usage if they do not have probable cause to believe he or she is involved in a crime. The lack of a clear, uniform procedure for all Massachusetts agencies puts residents across the state at risk.

Finally, **LOCATION**:
Arguably, the most shocking intrusion into the personal lives of Massachusetts residents is law enforcement's ability to track people's location and movements with data generated by their personal electronic devices. Over the last decade, cell phone use has become ubiquitous. And, with the advent of the smart phone, a person's cell phone creates and preserves a detailed record of its owner's life – including not only call records, text and email messages and pictures, but also a record of everywhere he or she goes.

One's location can reveal strikingly personal information. As D.C. Circuit Judge Ginsburg recently wrote, one's location can reveal "whether he is a weekly church goer, a heavy drinker, a regular at the gym, an unfaithful husband, an outpatient receiving medical treatment, an associate of particular individuals or political groups — and not just one such fact about a person, but all such facts."[6]

---

[3] http://www.capitol.state.tx.us/tlodocs/83R/billtext/pdf/HB02268F.pdf.
[4] M.G.L. ch.276, §1B.
[5] On its face, the same law appears even to allow police to access private information individuals store using any "remote computing services," which could include everything from personal writing to photographs and video. This information should be constitutionally protected. The Electronic Privacy Act would ensure that our statute books clearly and unambiguously spell out a probable cause warrant standard.
[6] *United States v. Maynard*, 615 F.3d 544 (D.C. Cir. 2010).

Cell phone information can provide the real-time location of a person and monitor if a person is stationary or moving. It can provide historical information about where someone has traveled, which phone companies often retain for at least a year.[7] It can also provide broad information identifying all the cell phones that were at a location at any given time.

The geographic location of cell phones can be tracked by phone companies whenever the cell phones are turned on, in at least three ways: (1) by identifying the cell tower from which the phone is receiving the strongest signal and the part of the tower facing the phone; (2) by "triangulating" the precise time and angle at which the cell phone's signal arrives at multiple cell towers; and (3) by using the satellite precision of GPS.

In the past, people have attempted to dismiss concerns about location tracking by saying that tower-based location information was too general to be very intrusive – merely showing a person to be within range of a particular tower. Now it is a rare phone that is not equipped with GPS, and more and more cell towers are being built to satisfy voracious demand for Wi-Fi service, enabling astonishingly granular tracking. In other words, location surveillance transforms an individual's cell phone, tablet, or laptop into a de facto tracking device visible to and readable by the government, without the user's consent or knowledge.

Law enforcement, often without a warrant or showing of probable cause can – and does – obtain real time and historic information about a person or a location from a telecommunications company. Last year, based on an information request from then-Congressman Ed Markey, *The New York Times* reported that in one year cell phone carriers responded to 1.3 million law enforcement requests for sensitive subscriber information, such as text message content and caller location.[8] And this may be just the tip of the iceberg, because a single "bulk" or "tower dump" request can gather location information about hundreds or thousands of individuals in a particular area at a given time.

For some years now, federal and state courts have been grappling with the issue of GPS tracking by law enforcement. Courts have frequently found that people have a privacy interest in not having their location and movements monitored.[9] However, this case law is developing piecemeal, with each ruling arguably limited to the facts of the particular case, creating substantial confusion for both law enforcement and carriers. A statutory structure, with rules and standards, is urgently needed.

Location information is sensitive, and law enforcement agencies should not be accessing it without a warrant. This is not an undue burden. Indeed, individual law enforcement agencies in every geographic region throughout the United States *do* execute probable cause search warrants to obtain location

[7] "Retention Periods of Major Cellular Service Providers." Data gathered by the Computer Crime and Intellectual Property Section, U.S. Department of Justice. Available at: http://www.aclu.org/cell-phone-location-tracking-request-response-cell-phone-company-data-retention-chart.
[8] Eric Lichtblau, *Wireless Firms Are Flooded by Requests to Aid Surveillance*, New York Times (July 8, 2012).
[9] See, e.g., U.S. v. Jones; Commonwealth v. Connolly; and Commonwealth v. Rousseau.

information generated by citizens' electronic devices. It remains a proven, reliable and workable standard.

Montana became the first state to establish this respected standard in a statute applied statewide.[10] Massachusetts should be the next one.

CONCLUSION

In these three critical areas – email communication, phone and internet records, and location tracking – the law today falls far short of the level of protection from intense government scrutiny that citizens of a free society are entitled to expect. Technology now effectively enables protracted, 24/7 monitoring of every move citizens make, in public or private, over a period of weeks or even months—monitoring of a kind that would previously have been prohibitively costly, even at the individual level, and wholly infeasible on the scale that has now become possible.[11]

Such extensive and precise monitoring of email, phone, internet, and location permits government agents to construct an incredibly detailed portrait of an individual's life, associations, and activities, far beyond what would ordinarily be possible through mere observation. Through patterns that emerge from these long-term virtual maps of our lives—especially when multiple such maps are collated—intimate and otherwise undetectable facts are likely to be revealed about our religious observance, sexual and romantic entanglements, medical conditions, and political affiliations. Such exposure implicates not only our right to privacy, but our First Amendment interest in what the Supreme Court has called "expressive association." A free people should not be expected to live as though each of us is being shadowed by a personal, permanent police tail.

Indeed, the government should bear the burden of justifying with particularity any surveillance of ordinary Massachusetts residents. When they have good stated reasons in an application, law enforcement can obtain a warrant. They've been doing that for more than 200 years. It's a familiar system, and it works well. A warrant requirement strengthens public safety AND protects the privacy of law abiding people. Warrants keep law enforcement resources focused on crime, and prevent police from being diverted – and overwhelmed – by extraneous data. And they also ensure that important evidence will be admissible in court, eliminating uncertainty under current law about electronic evidence that is obtained without a warrant.

There is room for improvement in any piece of legislation, and we continue to learn about and absorb new information after the January filing deadline. In this case, we believe the principles of the Electronic Privacy Act can be extended to have a more comprehensive impact by dealing directly with the issue of "administrative subpoenas," which allow prosecutors to issue secret demand letters to

[10] http://leg.mt.gov/bills/2013/BillPdf/HB0603.pdf

[11] It is in part for this reason that the Court of Appeals for the District of Columbia rejected the analogy between GPS tracking and traditional visual surveillance in the case that later reached the Supreme Court as *U.S. v. Jones.* See *United States v. Maynard*, 615 F.3d 544 (D.C. Cir. 2010).

obtain electronic communication information based on a very weak "relevance" standard in place of probable cause, and without any judicial oversight, notice, or other accountability. We urge the Committee to require probable cause warrants in all circumstances in which the government is seeking to access our personal electronic communication information.

* * *

When Massachusetts passes the Electronic Privacy Act, we will establish an excellent model for other states. Our government shouldn't be monitoring our communications and movements without a good reason to believe we are involved in some kind of criminal activity. This is a fundamental tenet of American justice and law – and necessary for a free society. In the 21st century, we need our statutes to reflect, not forsake, our long-standing values.

We would welcome the opportunity to work with the Committee as you consider this critically important proposal, and we urge you to advance it swiftly.

Sincerely,

Gavi Wolfe
Legislative Counsel