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

October 6, 2015

Joint Committee on the Judiciary
Sen. William Brownsberger & Rep. John Fernandes, Chairs

SUPPORT FOR S.903 and H.1531
APPLYING ESTABLISHED STANDARDS
AND RULES TO PROTECT ELECTRONIC PRIVACY

Dear Senator Brownsberger, Representative Fernandes, and members of the committee:

Massachusetts must apply the basic rules and standards governing searches of people and property to the personal electronic records that define our lives in the 21st century. The ACLU of Massachusetts offers its strongest support for S.903 and H.1531, related bills both titled "An Act to protect electronic privacy."

The state of the law in this area is shockingly and woefully obsolete. For example, today, federal statutes state that law enforcement may obtain the entire contents of your email archive as long as the messages are over 180 days old. Indeed, our most sensitive and personal information, from our email messages to our location at any given moment, remain exceedingly vulnerable to warrantless government surveillance.

The Electronic Privacy Act will go a long way to help our laws keep pace with our technology. At a minimum, warrants must be required before law enforcement obtains: (1) the content of your electronic communication such as emails or chats; (2) information stored online in "the cloud," such as photos, documents, digital address books and calendars, or internet search terms; and (3) real-time and historical location information.[1]

We urgently need a statutory structure that provides clear rules, standards, and procedures to law enforcement, gives guidance to companies that hold personal electronic records, and guarantees protections for the public. Courts at every level are faced with constitutional challenges to warrantless surveillance, and they have largely supported robust Fourth Amendment – and, in Massachusetts, Article XIV – protections in the digital age. However, such cases can take decades to develop and be

[1] Both the House and Senate versions of this legislation will accomplish this fundamental task. S.903 would, more comprehensively, require a warrant for *all* personal electronic records, including IP addresses that uniquely identify electronic devices, and "outside of the envelope" information about personal communication, such as who communicated with whom, when, for how long, etc.

decided by the highest courts, while inadequate laws on the books lead to ongoing privacy violations in the interim. Moreover, the judicial decisions that result can be interpreted as applying only to the specific facts of a given case, so many questions remain unanswered. Ultimately, court rulings in this area do not provide clear enough instructions for law enforcement. As Supreme Court Justice Samuel Alito recently said, the question of the Fourth Amendment in the digital age is one of the most important legal questions of our time, and it is best decided not by the courts by but our legislative bodies.[2]

***

What's At Stake

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 – first developed here in Massachusetts and adopted in the Bill of Rights – has served the Commonwealth and the nation well for more than two centuries. But today the right to be free from unreasonable searches and seizures is at a critical crossroads. Our most private and sensitive personal information is no longer physical property kept in our homes. Today, the "papers and effects" that the Founders and drafters of the constitution aimed to protect with the Fourth Amendment are now chiefly in digital form, and they are held by others.

Despite this digital revolution, the law is stuck in the analog 1980s. Technology has fast outpaced the law, creating confusion and an uncertain environment for businesses, law enforcement, and the general public. In order to ensure businesses and individuals can thrive in the new information economy, secure in the knowledge that transactions and information stored in "the cloud" will be protected from warrantless monitoring, we must update and extend our privacy-protective laws to fit the way we live today.

When the ACLU advocates for this electronic privacy update, we are reflecting mainstream America. Because of the widespread use of smartphones, social media, and third party email providers like Google Mail, privacy is popular. In a 2015 Pew survey, 57% of Americans polled said they thought it unacceptable for the government to monitor their communications. 52% of those polled described themselves as "very concerned" or "somewhat concerned" about government surveillance of their data and communications.[3] Collectively, we continue to believe we should -- and do -- have a reasonable expectation of privacy from government scrutiny, or, in the words of Justice Brandeis, "the right to be let alone."

The probable cause warrant -- the gold standard of American justice – has long ensured that our government does not intrude into our personal affairs without good reason and judicial oversight. The

[2] http://abovethelaw.com/2015/09/justice-alito-says-scotus-is-clueless-on-new-tech-which-makes-privacy-cases-even-harder/

[3] http://www.pewinternet.org/2015/03/16/americans-privacy-strategies-post-snowden/

Electronic Privacy Act would update the law to ensure that we maintain our gold standard protection for technologies that are now central to our everyday lives.

The Inadequacy of Current Law

The current landscape regarding electronic surveillance and privacy law is, to put it bluntly, a mess. There are a range of reasons, including an outdated federal statutory scheme, confusing state laws, and a patchwork of judicial decisions that provide only partial answers to the important question of when law enforcement must get a warrant and just what that process should be.

Here are some of the problems.

Outdated Federal Law

Perhaps the most glaring defect is that the federal Electronic Communications Privacy Act (ECPA), which deals with government access to electronic information, has not been updated since 1986. Its drafters did not anticipate the widespread use of cell phones or the kinds of technology that all of our phones and computers are equipped with today. Under ECPA, law enforcement does not need to obtain a warrant to obtain private emails (or potentially other electronic communication, such as online chat messages) in draft form or stored on a server more than 180 days.[4]

The 180-day rule, absurd today, made more sense when Congress passed the statute in 1986, because storing data for lengthy periods was cost prohibitive. Back then, 1GB of storage cost approximately $85,000,[5] so it was unheard of to keep messages on a server for 6 months. 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, the Department of Justice has testified to that effect before Congress: "there is no principled basis to treat e-mail less than 180 days old differently than e-mail more than 180 days old."[6]

Everyone agrees this situation must be fixed, but Massachusetts should not wait for Congress to act. We need to establish uniform, sensible, state law limits on government inspection of residents' email messages without regard to their age. A number of states have already passed a probable cause warrant requirement for email.[7] Massachusetts should enact these protections now.

---

[4] 18 U.S.C.A. §2703 (a)&(b).

[5] http://www.mkomo.com/cost-per-gigabyte

[6] 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.

[7] See, e.g., Maryland (https://govt.westlaw.com/mdc/Document/N13060010034311E49061EA59213A2019), Maine (http://www.mainelegislature.org/legis/statutes/16/title16sec642.html), Utah (http://le.utah.gov/~code/TITLE77/htm/77_23b000400.htm), and Texas (http://www.capitol.state.tx.us/tlodocs/83R/billtext/pdf/HB02268F.pdf).

Imperfect Case Law

The Electronic Privacy Act will also fix problems that case law has failed to adequately address. In Massachusetts, the case law about access to electronic communications and stored content is sparse. And in the area where courts have ruled more recently – namely, government access to location information – the results are incomplete.

In the past two years, the Supreme Judicial Court has issued two important location information decisions. Commonwealth v. Augustine, a 2014 case, ruled that when law enforcement obtains at least two weeks' worth of location information, that constitutes a search that requires the privacy protection of a judicially-approved warrant. In a recently decided follow-up case, Commonwealth v. Estabrook, the SJC ruled that law enforcement must get a warrant to obtain anything more than six hours of telephone call location information from a person's phone company.[8]

These cases were certainly welcome and celebrated by all of us who value privacy and good public safety practice, especially in light of the apparent frequency with which law enforcement has seen fit to seek cell phone data.[9] Yet for two reasons, these court decisions leave a troubling gap in the law, a gap the Electronic Privacy Act is designed to address.

First, although courts are well situated to rule about how constitutional rights must apply in particular cases, they are not generally well equipped to lay out in detail the process and procedure to implement their rulings on the ground. Yet that is exactly what law enforcement needs to ensure that our privacy rights are protected in practice. This is where the legislature must step in: to provide clear steps describing the process that law enforcement officers must follow to lawfully procure location information without violating our constitutional rights.

Second, secretly tracking a person's location is such a serious invasion of privacy that there can be no reason to allow law enforcement to engage in *any* amount of this surveillance without a warrant except in grave emergencies.[10] Even data illustrating an individual's whereabouts over a short period of time, or at a single moment, can be extremely revealing. Consider the implications of knowing that a married man was in the home of a woman other than his wife at 3:52 in the morning, or that a well-known businessperson visits a church for the hour when Alcoholics Anonymous meets there.

---

[8] *Commonwealth v. Augustine*, 467 Mass. 230 (2014); *Commonwealth v. Estabrook*, SJC-11833 (2015).

[9] In 2012, 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. 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. Eric Lichtblau, *Wireless Firms Are Flooded by Requests to Aid Surveillance*, New York Times (July 8, 2012).

[10] In emergencies, law enforcement may exercise a special "exigent circumstances" procedure, which is far preferable to a complete carve-out of the warrant requirement for an arbitrary length of time. Twelve other states require warrants for location information without any temporal exceptions.

In the United States, ordinary people should be able to carry and use the latest technology without worrying about government agents tracking them without any judicial oversight or probable cause. But absent passage of the Electronic Privacy Act, that's exactly what can happen. Indeed, without the Electronic Privacy Act, location tracking remains a threat to every Massachusetts resident with a cell phone.

We need a clear, complete, well-understood standard – the gold standard. If the police want to track our movements through our phones and tablets, they should be required to get 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 information generated by citizens' electronic devices. It is a proven, reliable and workable standard.

Confusing State Statute

Finally, where Massachusetts statutes attempt to establish protocols for law enforcement to follow, they make things more confusing. The state statute that contemplates law enforcement access to remotely held electronic information is puzzling at best, and an invitation to unjustified invasions of privacy at worst. It describes a kind of warrant procedure that is wholly unfamiliar to criminal law practitioners, using the venerable words "probable cause" in a way that bears no relation to the traditional evidentiary standard. Traditionally, a warrant is issued only when prosecutors show they have probable cause to believe that a search of particular property will yield evidence of criminal activity. Yet the Massachusetts statute talks about "probable cause" to believe that an individual's communication records "are actually or constructively possessed by a foreign corporation that provides electronic communication services or remote computing services."[11] Probable cause to believe, for example, that the individual is a Verizon customer.

One hopes that such peculiar statutory language would not lead prosecutors to seek, or judges to issue, warrants based on a mere belief that a company holds personal electronic records about a particular individual. Certainly, our privacy rights should not hinge on non-"standards" like this.

Consider the kinds of significant, sensitive information such companies retain about your digital life. In addition to your email, and in addition to your step-by-step movements, computing services also possess anything you store online, such as photos on Picasa or Shutterfly, or documents in Dropbox or Google Drive. All the information that phone or internet companies store on your behalf to make your digital life run smoothly, such as your calendars and address books. All the information that companies may maintain about you for their own commercial purposes, such as your internet search terms and records of the articles you read or the links you click. Certainly, these kinds of personal electronic records are worthy of a serious, well-written statute that protects our privacy interests.

[11] M.G.L. ch.276, §1B.

Unless they obtain a traditional probable cause warrant, law enforcement is prohibited from rifling through your phone or computer.[12] Likewise, our statute should make crystal clear that the same standards and procedures should be followed to obtain information generated by those devices from a phone or internet company.[13]

CONCLUSION

The government must bear the burden of justifying with particularity its surveillance of ordinary Massachusetts residents, including their personal electronic records.

When they have stated good reasons in an application, law enforcement can obtain a warrant from a court. 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.

When Massachusetts passes the Electronic Privacy Act, we will establish an excellent model for other states. 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,

Carol Rose	Kade Crockford	Gavi Wolfe
Executive Director	Technology for Liberty Program Director	Legislative Counsel

[12] *Riley v. California*, 134 S. Ct. 2473 (2014).

[13] H.1531 describes carefully-drawn conditions for issuing a warrant for personal electronic records, namely: "Upon complaint on oath that the complainant believes (i) that particular identified records or information hereinafter described are in the actual or constructive custody of a Massachusetts or foreign corporation providing electronic communication services, remote computing services, or location information services, and (ii) that such records or information constitute evidence of or the means or instrumentalities of the commission of a specified criminal offense under the laws of the commonwealth."