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

June 5, 2017

Joint Committee on the Judiciary
Senator William Brownsberger & Representative Claire Cronin, Chairs

**SUPPORT FOR H.2332 & S.943**
**AN ACT TO PROTECT ELECTRONIC PRIVACY**

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

On behalf of the ACLU of Massachusetts and its nearly 100,000 members and activists statewide, we write in strong support of H.2332 & S.943, two versions of An Act to Protect Electronic Privacy. While the ACLU has supported similar legislation in past sessions, the need for these updates to the law has increased significantly since the November election. The Trump administration and the Department of Justice under Attorney General Sessions have a very different interpretation of the need to protect basic privacy and Fourth Amendment rights. Accordingly, it's now more important than ever for the state to protect the privacy rights of its residents from inappropriate government intrusion.

**The Electronic Privacy Act: What it does**

The Electronic Privacy Act applies the same basic rules and standards that have traditionally governed law enforcement searches to our digital papers and effects. The bill would protect with a warrant requirement the incredibly detailed and voluminous, sensitive personal information generated when we use our phones and the internet. The digital trails we leave behind us are composed of data that tell the most intimate stories about our lives: the content of our emails and texts, records showing where we've been and when, and all of our cloud-stored files, emails, and other documents. The Electronic Privacy Act brings Massachusetts law into the 21st century by requiring law enforcement get a warrant before obtaining these records from phone or internet companies, and before using an interception device known as a Stingray to trick a phone into divulging information directly. States as politically divergent as California, Connecticut, Montana, Texas, and Vermont have already passed similar legislation.

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. Think of 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. Then there's all the information 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. These kinds of personal electronic records are worthy of the same warrant protections afforded to our communications that exist on paper.

The Electronic Privacy Act would require:

- Warrants for access to stored communications content such as emails, private Facebook messages, and private photographs or documents stored in the cloud;
- Warrants for private location information, including real-time tracking;
- Warrants for the use of Stingray technology, which allows law enforcement to track cell phones without issuing demands to telecom companies;
- Notice to targets of electronic surveillance, which may be delayed with judicial authorization; and
- Reporting on the use of electronic surveillance warrants, on an annual basis, to the legislature.[1]

The legislation contains provisions allowing law enforcement to obtain stored electronic communications and location information without warrants in limited emergencies, using the same emergency exception rules that apply to other kinds of Fourth Amendment searches.

**Context: Obsolete law, fast-moving technology, and federal inaction**

The state of the law in this area is shockingly obsolete. Current federal electronic privacy law was passed in the year 1986, when smart phones didn't exist, and one gigabyte of storage cost approximately $75,000. Since storage was so expensive, Congress wrote the law to allow warrantless law enforcement access to old emails, which they considered abandoned property. As a result, under this statute in the year 2017, state and local law enforcement may claim authority to obtain the entire contents of your email inbox without a warrant as long as the messages are over 180 days old. This is nonsensical and an odious invasion of privacy. Our most sensitive and personal information—from our email messages to our family photo albums to our location at any given moment—remain exceedingly vulnerable to warrantless government surveillance.

During the Obama administration, the Department of Justice issued policy guidance requiring federal agents to obtain warrants before accessing electronic communication content, and issued similar recommendations regarding the use of Stingrays. But these internal, executive branch policies can be overturned with the stroke of a pen, without public notice or accountability. For that reason, there is no reason to believe they remain in effect today. (Furthermore, the DOJ rules only applied to federal agents, not state and local law enforcement.)

**Courts consistently rule in favor of warrants for electronic surveillance**

Some people would like to think the courts will solve these problems. And when given the chance, courts usually do affirm basic constitutional principles about search and seizure in the digital age. But we can't rely on the courts to shape electronic privacy law, both because the courts only rule on the narrow

---

[1] Both the House and Senate versions of this legislation include these fundamental provisions. S.943 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 the source and recipient, date and time, quantum of data transmitted, etc.

issue in front of them, and because it often takes decades for the stars to align in such a way to grant them the opportunity to do so.

In one shining example, the U.S. Supreme Court ruled that police may not search an arrested person's cell phone without first obtaining a warrant.[2] But that case in no way obviates the need for the Electronic Privacy Act; rather, it highlights the prudence of this legislation.

As Chief Justice John Roberts wrote in *Riley*:

> "Modern cell phones are not just another technological convenience. With all they contain and all they may reveal, they hold for many Americans 'the privacies of life'... The fact that technology now allows an individual to carry such information in his hand does not make the information any less worthy of the protection for which the Founders fought. Our answer to the question of what police must do before searching a cell phone seized incident to an arrest is accordingly simple — get a warrant."

While *Riley* protects our physical devices with the gold standard of American Fourth Amendment justice, the probable cause warrant, the very same information that is stored on our cell phones is almost always also stored on the servers of corporations like Google, Facebook, Apple, and Microsoft. If police need to get a warrant, per *Riley*, to search our physical devices when we are arrested, they should also be required to get a warrant to demand from cloud services access to the same information that exists on those warrant-protected devices.

Massachusetts must protect a person's digital privacy even when they are not arrested, and regardless of whether law enforcement wants the data from their physical phone or from their phone company, from their computer, or from an internet company.

Massachusetts case law similarly demonstrates the need for uniform legislation. Two decisions from the Supreme Judicial Court provide imperfect protection for location information generated by cell phones. In these cases, the SJC ruled first that law enforcement must get a warrant to obtain anything more than two weeks of telephone call location information from a person's phone company, and then subsequently narrowed the time period to six hours.[3] Yet data indicating an individual's whereabouts over even a shorter period of time, or at a single moment, can be extremely revealing, and is no less deserving of Fourth Amendment protection. 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 politician visits a church for the hour when Alcoholics Anonymous meets there. A warrant should be required to use technology to track a person's location, whether it's to find out where they've been or to track them in real-time.

---

[2] *Riley v. California*, 134 S. Ct. 2473 (2014).
[3] *Commonwealth v. Augustine*, 467 Mass. 230 (2014); *Commonwealth v. Estabrook*, SJC-11833 (2015).

In another recent case, the SJC came to the conclusion that law enforcement must obtain a warrant to access a person's text messages from their phone company.[4] Yet the decision did not explicitly address the question of email communication, and we cannot assume that prosecutors will follow its logic to what we believe is its natural conclusion—that the Fourth Amendment applies equally to all stored communications content—without explicit instruction from the legislature. This hodge-podge of case law has created an untenable situation. Law enforcement and service providers need clear guidance.

**Updating the law to reflect new technology is a job for the legislature**

Though courts have begun to extend constitutional protection from unreasonable searches and seizures to some digital information, legislative action is needed. Without carefully considered legislation, electronic privacy law develops in patchwork fashion, absent necessary details, and in slow motion. After years of litigation, courts issue decisions that are limited by the narrow facts before them, and they speak to general principles, not specific procedures. 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, but rather by our legislative bodies.[5]

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. It is proven, reliable and workable. The Electronic Privacy Act would update the law to ensure that we maintain our gold standard protection for technologies that are now central to nearly every aspect of our everyday lives.

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.

The ACLU urges this committee to give the Electronic Privacy Act a swift, favorable report. We would welcome the opportunity to work with you to advance this important legislation. Thank you.

Sincerely,

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

---

[4] *Commonwealth v. Fulgiam*, SJC-11674 (2017).

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