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

October 22, 2019

Joint Committee on the Judiciary
Senator James Eldridge & Representative Claire Cronin, Chairs

SUPPORT FOR H.3422 & S.861
AN ACT TO PROTECT ELECTRONIC PRIVACY

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

On behalf of the ACLU of Massachusetts, we write in strong support of H.3422 & S.861, two versions of An Act to Protect Electronic Privacy.

The Electronic Privacy Act: What it does

The Electronic Privacy Act would apply to our digital lives the same basic rules and standards that have traditionally governed law enforcement searches 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, our calendars, our address books, and all of our cloud-stored files, emails, and other documents. In addition, there's all the information companies maintain about their customers for their own commercial purposes, such as our internet search terms and records of the articles we read or the links we 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 clarifies and updates Massachusetts law in 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.

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.

We need strong statutes, not just patchwork case law.

Eventually, when given the chance, courts usually affirm basic constitutional principles about search and seizure in the digital age. For example, in 2014, the U.S. Supreme Court ruled that police may not search an arrested person's cell phone without first obtaining a warrant.[2]

As Chief Justice John Roberts wrote in *U.S. v. 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."

And in 2018, the Court ruled that law enforcement officials must get a warrant to obtain historical cell site location data from phone companies.[3]

But these cases were decided decades after virtually every American began to use cell phones, and they still do not provide a comprehensive framework for law enforcement access to various aspects of our digital lives.

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

---

[1] Both the House and Senate versions of this legislation include these fundamental provisions. S.861 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.

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

[3] *Carpenter v. United States*, No. 16-402, 585 U.S. ____ (2018).

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 has 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.[4]

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.

---

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