ACLU of Massachusetts
One Center Plaza, Suite 850
Boston, MA 02110
617-482-3170
www.aclum.org

July 13, 2023

Joint Committee on Advanced Information Technology, the Internet and Cybersecurity
Rep. Tricia Farley-Bouvier and Sen. Michael O. Moore, Co-Chairs

Testimony in Support of S.27
An Act to Protect Private Electronic Communication, Browsing, and Other Activity

Dear Representative Farley-Bouvier, Senator Moore, and members of the committee:

The ACLU of Massachusetts offers our strong support for S.27, *An Act to Protect Private Electronic Communication, Browsing, and Other Activity* (the "bill"), sponsored by Senator Eldridge.[1] This legislation would apply the same safeguards to our personal digital records (all our information held by the companies that provide us online services) that already protect our physical papers and effects, including by protecting against dragnet searches. It is time to ensure that privacy from government intrusion thrives in the digital age.

Massachusetts Residents Deserve Robust Digital Privacy Protections

Everything we do online leaves a trail of detailed records, most of which are retained by companies like telecommunication providers, internet services, and tech companies. These records include but are not limited to messages people send over apps; information showing who we call, when, and how long our calls last; banking and credit card information; our physical locations; our internet searches; documents and files we store on tech company servers; records of each time someone logged in to a service like Facebook or Gmail; metadata pertaining to every picture we take, including place, time, and date; and more.

Today, law enforcement and prosecutors can too often access these records about our digital lives and online personas without showing probable cause or going to a judge. Even worse, these searches can take place in complete secrecy, with the target never even learning that their digital papers and effects were seized by the government. This is very different from the analog world, where the U.S. Constitution and Article 14 of the Massachusetts Declaration of Rights have long required a warrant when law enforcement agencies search our physical property and seize our personal effects[2] and barred police from issuing dragnet warrants to search hundreds or thousands of homes in search of evidence of one person's alleged wrongdoing. But without clear prohibitions on similarly intrusive methods in the digital realm, the government has turned to novel methods, using dragnets that would be unthinkable in the physical world.

This discrepancy between how police treat digital and physical searches makes little sense. Indeed, the digital data trails we leave contain information more revealing and voluminous than the contents of our desk drawers and our home closets. To address this discrepancy, the legislature should ensure our electronic records receive the same protections as their physical counterparts.

---

[1] An identical bill, H.1653, filed by Rep. Jay Livingstone, has been assigned to the Joint Committee on the Judiciary.

[2] Constitutional privacy protections also apply to searches and seizures of our personal electronic devices. See. *Riley v. California*, 573 U.S. 373 (2014), in which the U.S. Supreme Court ruled that police must obtain a warrant to search a cellphone even during an arrest. A primary goal of the proposed legislation is to ensure similar protections for the digital information we generate that is held by communications companies and online service providers.

Privacy Law for the 21st Century

An Act to Protect Private Electronic Communication, Browsing, and Other Activity brings Massachusetts law into the 21st century by requiring police and prosecutors to obtain warrants before demanding our digital papers and effects, and prohibits the use of dragnet digital warrants.[3]

Require a Warrant to Search and Seize Our Digital Papers and Effects

Probable cause warrants are the gold standard of American justice and privacy protection — a standard that should apply to our electronic and subscriber information stored by telecoms, service providers, and tech companies. To that end, **the bill requires a warrant based on probable cause, or exigent circumstances, to access these records and does away with the current practice of using administrative subpoenas**.[4]

Massachusetts residents deserve to be protected from warrantless search and seizure, no matter who holds their sensitive information. For example, if the government seeks access to a person's physical checkbook, they must obtain a warrant before rummaging through their files. The bill applies the same standard to financial transaction information held digitally by companies like banks and app developers. Likewise, just as police are required to obtain a warrant before seizing a person's physical calendar or address book from their home office, the bill mandates the government obtain a warrant to access similar digital files stored on a company's cloud servers.

Massachusetts would not be the first state to require the government to obtain a warrant before demanding access to such records. In 2018, California passed the California Electronic Communications Privacy Act (CalECPA), which among other things requires police and prosecutors to obtain a warrant before demanding access to communications content and metadata.[5]

The proposed legislation also includes transparency provisions requiring courts to report information about the warrants they issue. This will help the legislature and the general public understand how often law enforcement demands that companies turn over our personal electronic records.

Prohibit Dragnet Warrants

In recent years, police across the country have taken advantage of gaps in privacy law and begun to conduct fishing expeditions for broad categories of potential criminal activity by using novel, dragnet warrants sometimes known as reverse location and keyword demands.[6] These demands cast a wide

---

[3] The bill also provides an important protection to public library users by establishing that data about their library use is not a public record, and it is subject to the same warrant requirements that the bill applies to other personal digital information. This testimony provides a broad overview of the legislation. For a detailed section-by-section analysis of the bill, please contact Emiliano Falcon-Morano at efalcon@aclum.org.

[4] Administrative subpoenas are demand letters prosecutors and law enforcement send to communications and internet providers like Verizon, Google, Facebook, and Twitter, seeking sensitive information about our communications and online activities. Administrative subpoenas do not require probable cause or even a suspicion of criminal activity. Instead, they merely require that the records sought be "relevant and material" to a criminal investigation. Judges are not involved in the issuance of administrative subpoenas, and there is no notice provided to the person whose records are being requested.

[5] California Electronic Communications Privacy Act (CalECPA) - SB 178, ACLU of North California, April 2018, https://www.aclunc.org/our-work/legislation/california-electronic-communications-privacy-act-calecpa-sb-178

[6] Although the information on the use of reverse warrants is hard to come by, data released by Google for reverse location warrants it received from 2018 to 2020 illustrates this troubling trend. See https://services.google.com/fh/files/misc/supplemental_information_geofence_warrants_united_states.pdf (general

net, seeking information about tens, hundreds, or even thousands of people, none of whom is individually suspected of criminal activity. That's because rather than seeking the information of a particular person suspected of a particular crime, like with traditional warrants, these dragnet demands seek information about an unidentified group of people who may have shared a common location or searched for a similar term online.

In other words, reverse court orders are the 21st-century equivalent of colonial general warrants. These dragnet demands subject large numbers of people to search merely because they queried a particular term online or were thought to be physically present in a neighborhood where a crime was committed – even though they are not individually suspected of criminal activity.

The United States and the Commonwealth have a long and proud tradition of opposition to the use of general warrants. Indeed, outrage in Boston about the British Crown's use of general warrants served as inspiration for Article 14 of the Massachusetts Declaration of Rights, which in turn inspired the Fourth Amendment to the United States Constitution. Opposition to the use of general warrants in the United States dates to the pre-Revolutionary War era.[7]

This bill builds on these long-standing American privacy principles in the digital age by prohibiting reverse-location and reverse-keyword court orders and searches.

Require a Warrant to Use a Cell Site Simulator Device

The bill would also require law enforcement to obtain a warrant before intercepting digital data or identifying the location of our cellphones when we are using them. Cell-site simulator devices, commonly known as stingrays, are surveillance devices that mimic cellphone towers and trick cellphones into communicating with the surveillance device, including by sending information revealing the physical location of a phone. Some models are also capable of intercepting communications content like text messages and voice call data from cellphones.

Rulings of the Massachusetts Supreme Judicial Court and United States Supreme Court require law enforcement to get a warrant to demand cellphone location information from cellphone companies, except in emergencies. But no current statute mandates that police get a warrant to use a stingray to track the physical location of a phone. Worse still, no law requires police to delete data from non-target phones acquired during stingray surveillance deployments.

The bill would impose a statutory warrant requirement on the use of stingrays, except in exigent circumstances. It also establishes that all data from phones that are not the target of surveillance must be deleted within twenty-four hours. When stingrays are used to track a suspect's mobile phone, they collect data from all the phones in a broad area, and all bystanders' information should be purged.

Ensure Enforcement

Finally, Massachusetts privacy laws must have a strong enforcement mechanism or they will be merely words on paper. For this reason, the proposed legislation includes a private right of action. If rogue government actors disregard the law's protections, a person whose rights have been violated can bring a civil claim to vindicate their rights in court.

---

reporting) and https://services.google.com/fh/files/misc/geofence_warrants_by_jurisdiction_2018_through_2020.zip (state-by-state data)

[7] See Stanford v. Texas, 379 U.S. 476, 484 n.13 (1965).

Conclusion

Massachusetts residents' personal information and records revealing their relations, habits, and other intimate details deserve the same protection regardless of whether that information exists physically in their homes or is generated and stored digitally.

We respectfully urge this Committee to advance S.27 with a favorable report, and we would welcome the opportunity to work with you on this legislation.