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

February 15, 2022

Joint Committee on the Judiciary
Sen. James Eldridge & Rep. Michael Day, Chairs

OPPOSITION TO H.4347
EXPANSION OF WIRETAP POWERS

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

The ACLU of Massachusetts opposes expansion of our state wiretap law in the strongest terms. There are many pressing needs facing the Commonwealth and its residents. Authorizing the government to listen in on private communications in new ways and for new reasons is not one of them.

We live in the Golden Age of Surveillance

Ours is the golden age of surveillance.[1] Never before has it been so easy for the government to track and monitor every person's habits, associations, and patterns of life. The ubiquitous presence of digital devices and apps creates unprecedented quantities of extremely revealing content and metadata, the vast majority of which is accessible to law enforcement through subpoenas, court orders, warrants, or emergency requests. It is now possible—and in many cases far too easy[2]—for investigators to access this wealth of data to gather information about every criminal suspect's movements, associations, private text and email conversations, and activities.

In the past, law enforcement struggled to investigate a suspect's past movements and actions, cobbling together potentially unreliable witness interviews with credit card receipts and other miscellanea. Today, finding out where a suspect was physically located, and with whom they communicated, at any given moment in recent history is as easy as securing a routine warrant and sending it to a telecommunications company. And unlike witnesses, metadata always remembers, and it never lies.

Every day, new technologies expand government's reach into the private lives of millions of Massachusetts residents. If there is a crisis in Massachusetts pertaining to the government's ability to peer into our digital devices and the personal information they contain, it's that electronic surveillance is far too *easy* to conduct, and subject to too *few* restrictions to protect individual privacy and other basic freedoms.

Current wiretap law strikes the right balance by focusing on coordinated criminal activity—"organized crime"

---

[1] Peter Swire, "The Golden Age of Surveillance," Slate, July 15, 2015. https://slate.com/technology/2015/07/encryption-back-doors-arent-necessary-were-already-in-a-golden-age-of-surveillance.html.

[2] Michael Levenson, "Power to seize phone, Net records is a 'sanctioned fishing expedition,' critics say," Boston Globe, July 16, 2017. https://www.bostonglobe.com/metro/2017/07/16/concerns-raised-over-prosecutors-power-seize-phone-internet-records/JKdVWqjFNUSMkaboOoAhZK/story.html.

Massachusetts residents should be proud that our state wiretap law is among the most protective in the nation. When it was enacted, lawmakers took an appropriately limited approach to authorizing government agents to listen in to private phone calls and to install listening devices in people's private homes, cars, and businesses—a particularly invasive form of government intrusion into private affairs.

As the general court found when it originally established the wiretap statute: "[T]he uncontrolled development and unrestricted use of modern electronic surveillance devices pose grave dangers to the privacy of all citizens of the commonwealth. . . .The use of such devices by law enforcement officials must be conducted under strict judicial supervision and should be limited to the investigation of organized crime."[3] Monitoring the content of personal communication is a tool best suited to identifying and disrupting serious criminal activity coordinated among multiple parties, which is exactly what the current statute enables.

Proponents of wiretap expansion have claimed that an SJC decision supports major changes to the law, but such claims are significantly misleading. In a concurring opinion in *Commonwealth v. Tavares* (2011), two justices expressed their view that the wiretap law should be amended to make electronic surveillance more generally available to investigate and prosecute "shootings and killings by street gangs." The concurrence does *not* suggest that the current law should be amended so that *individuals* can be investigated, with wiretaps and monitoring of a vast array of electronic communications for offenses not associated with organized crime.

The bill before this committee represents a sweeping and gravely dangerous expansion of the wiretap law. The legislation would authorize government agents to install bugging devices in the private businesses and homes of individuals suspected of minor crimes like selling small amounts of drugs. Massachusetts should not authorize government agents to secretly enter a person's home to install a listening device merely because they are suspected of a non-violent crime like petty drug selling.

Indeed, these bills go far beyond any changes contemplated by *Tavares* and the stated goals of its proponents. The legislature should reject any approach that enables government agents to listen in to the private conversations or digital communications of people not engaged in criminal conspiracies.

Any expansion of surveillance powers to enable wiretapping of private communications in investigations not related to "organized crime" would have far-reaching negative effects and open up a Pandora's box of potential unintended consequences, including political harassment and intimidation. The ACLU of Massachusetts respectfully asks the committee to recommend that these bills ought NOT to pass.

Sincerely,

Gavi Wolfe, Legislative Director
Kade Crockford, Technology for Liberty Program Director

[3] G.L. c.272, §99, paragraph third.