



330 Main Street, Hartford, Connecticut 06106
860-523-9146 | www.acluct.org

Testimony Supporting House Bill No. 5640, An Act Concerning Compelled Disclosure of Cellular Telephone and Internet Records

March 22, 2016

Senator Coleman, Representative Tong and distinguished members of the Judiciary Committee, my name is David McGuire. I am the Legislative Policy Director of the American Civil Liberties Union of Connecticut and I am submitting this written testimony in support of House Bill No. 5640, An Act Concerning Compelled Disclosure of Cellular Telephone and Internet Records. This bill is the product of extended discussions between our organization, the Office of the Chief State's Attorney and the Office of Chief Public Defender. House Bill 5640 would bring Connecticut's cell phone surveillance laws into compliance with the Fourth Amendment and Supreme Court jurisprudence while allowing legitimate police investigations to proceed.

The ACLU of Connecticut strongly supports liberty and justice for all. This includes the right to privacy and freedom from baseless searches. The Fourth Amendment mandates that the government may not invade and search places where we have a reasonable expectation of privacy, unless the search is conducted pursuant to a search warrant issued by a neutral magistrate with the place and time of search specified in the warrant. Today, it is hard to imagine a place more private, and with more private information, than our cell phones. The average American sends or receives 32 text messages per day, and most of us use our phones to communicate everything from cat videos to revelations to close confidants. We entrust information about our banking, shopping, fitness, dating, and more to our phones, and we keep our phones with us in order to determine where we are and how to navigate elsewhere, at all times. House Bill 5640 will protect individuals' privacy rights by requiring police to prove that they have probable cause to believe that a crime has been or is being committed or that exigent circumstances exist before tracking a person by their cell phone or accessing cell phone content.

In 2012, the U.S. Supreme Court ruled in *U.S. v Jones* that the government violated the Fourth Amendment when it used a GPS device to track a suspect's location for 28 days without a valid warrant.¹ The majority of the justices recognized that such close and persistent long-term monitoring of a person's movements, no matter what technology law enforcement officials use, impinges on an individual's reasonable expectation of privacy. In a concurrence endorsed by four justices, Justice Alito urged

¹ <http://www.supremecourt.gov/opinions/11pdf/10-1259.pdf>

legislators to address location privacy issues, writing: "In circumstances involving dramatic technological change, the best solution to privacy concerns may be legislative...A legislative body is well situated to gauge changing public attitudes, to draw detailed lines, and to balance privacy and public safety in a comprehensive way."

Unfortunately, current law has not kept up with technology and police have pushed the limits. Connecticut General Statutes § 54-47aa(g) was passed in 2005, and has been used by law enforcement to track a person by his or her cell phone, based only upon law enforcement stating a reasonable and articulable suspicion that a crime has been or is being committed. Since 2005, police have used the law more than 14,000 times. To the best of our knowledge, Connecticut courts have never rejected a cell phone surveillance request from law enforcement, largely because the standard is so low.

As a result, scores of Connecticut residents have had their Fourth Amendment privacy rights violated through warrantless cell phone tracking—often without their knowledge. Police have used court orders to get historical location information, to track a person's location in real time, and to obtain emails, text messages and Facebook messages. Requiring police to show probable cause before obtaining this sensitive data comports with the Fourth Amendment and would allow legitimate investigations to proceed, while protecting people in Connecticut from intrusions into their privacy.

We encourage this committee to pass this bill, which will bring Connecticut General Statutes § 54-47aa(g) into conformity with the Fourth Amendment by expressly requiring police to obtain a warrant in order to access cell phone geolocational data. In the last three years, states including Maine and Utah have passed laws requiring police to get a warrant before accessing historical cell phone data. The bill helps Connecticut's laws to keep up with technology by requiring law enforcement agents to show probable cause in order to obtain an ex parte to track people through information obtained from their cell phone provider or an internet service provider such as Comcast, Facebook or Hotmail.

In addition, advances in cellular surveillance technology, including "stingrays" devices that can track a cell phone if it is in a certain area, make it possible for law enforcement agents to obtain information about where someone is, based on cell phone location, in real time without court oversight or the telecommunication carrier's assistance. When someone powers it on, a cell phone constantly sends detailed location data to its cellular carrier. Even phones without a GPS function leave a trail of contact with cell phone towers. Like GPS technology, this provides law enforcement agents with a powerful, inexpensive mechanism to track individuals over an extended period of time, in an unlimited expanse of space, and in public and private areas. Some manufacturers have also started marketing surveillance devices that can place malware on phones, diminish their battery charge, or otherwise interfere with their use. Cell phone tracking is an even more invasive location tracking method than the GPS transponder at issue in the *Jones* case. After all, almost every teenager and adult in Connecticut carries a cell phone all day long. Additionally, unlike GPS data, cellular location data is available to law enforcement retroactively, as a historical record of an individual's movements.

CGA § 54-47aa(g) requires law enforcement officials to notify people by mail that they have been tracked under an ex-parte order, so that they can move to challenge the order. The ACLU of Connecticut

followed up with several people who were subjects of an order obtained under the existing law. We found that many people were never charged with a crime and were never informed that police had obtained their personal cell phone data. This lack of notice is an extremely troubling due process violation and likely explains why more people are not complaining about being tracked in a fishing expedition. This bill's amendment to subsection (g) would help ensure notification by requiring that police file a copy of the mailed notice with the court.

Lastly, this bill would prohibit law enforcement officials from storing disclosed data for longer than fourteen days, unless the data relates to an ongoing criminal investigation. This would prevent police from holding onto innocent people's sensitive data while allowing police to keep the data as long they are still engaged in an active investigation.

The need for House Bill 5640 is real and immediate. The ACLU of Connecticut agrees with Justice Alito that, in this time of rapid technological change, it is especially appropriate to regulate the use of surveillance technology by government. The probable cause requirements for all cell phone and internet account tracking strike the appropriate balance, ensuring that legitimate investigations can go forward without eroding the privacy rights of people in Connecticut. We urge the committee to pass this bill.