

CCDLA
"READY IN THE DEFENSE OF LIBERTY"
FOUNDED IN 1988

Connecticut Criminal Defense
Lawyers Association
P.O. Box 1766
Waterbury, CT 07621
(860) 283-5070 tel/fax
www.ccdla.com

March 20, 2015

Senator Eric Coleman, Co-Chair
Representative William Tong, Co-Chair
Judiciary Committee
Room 2500, Legislative Office Building,
Hartford, CT 06106

Re: Testimony in support of Senate Bill 1092 - *An Act Concerning Compelled Disclosure of Cellular Telephone and Internet Records.*

Dear Senator Coleman, Representative Tong and Committee Members:

The CCDLA is a not-for-profit organization of approximately three hundred lawyers who are dedicated to defending persons accused of criminal offenses. Founded in 1988, the CCDLA is the only statewide criminal defense lawyers' organization in Connecticut. An affiliate of the National Association of Criminal Defense Lawyers, the CCDLA works to improve the criminal justice system by insuring that the individual rights guaranteed by the Connecticut and United States constitutions are applied fairly and equally and that those rights are not diminished.

The CCDLA urges this committee to **vote favorably on SB 1092**. This bill would amend Conn. Gen. Stat. § 54-47aa, by requiring probable cause before a judge signs an ex-parte order for "cell-location" data and "metadata". C.G.S. § 54-47aa applies when:

- A law enforcement official is conducting a criminal investigation, and;
- Wants to get data from phone providers regarding the *location* of phone calls, also called "cell-site records" or "cell-location" data and/or;
- Wants to get data from phone providers regarding the ownership of phone numbers, the list of numbers that called a particular number, the list of numbers that were called from a particular number, the duration of the calls, the timing of those calls and the credit card or other bank information used to pay for that phone service, commonly referred to as "metadata" and/or;
- Wants to get data from internet service providers like Facebook, Instagram, Twitter, Google+, Gmail, Yahoo!, Hotmail, Snapchat, Comcast, Cox, Verizon, etc.

about the ownership of a particular account, when someone registered or created an account and how they pay for that account.

Of course digital data stored on electronic devices or online provides law enforcement with a powerful investigative tool for solving crimes, a tool it should be permitted to use to make the residents of Connecticut safer and solve crimes. But there must be a balance between security and privacy. That balance has traditionally been struck by requiring law enforcement obtain a search warrant before they can access private information.

Currently, a judge must find only *reasonable and articulable suspicion* before such an order may be granted. An investigation conducted by NBC Connecticut last year revealed that since 2005, over 13,000 ex parte orders have been granted and there is no record that any of them were rejected.¹

This bill would amend the standard to raise it to require a showing of *probable cause*. Probable cause is the same standard required to obtain a search warrant. **Probable cause is a more stringent standard** that requires individualized showing that the person whose records are being sought is engaged in criminal activity. The *reasonable and articulable suspicion* standard is most frequently encountered in investigative detentions on the street, when officers are asking brief questions or patting down for weapons.

The **difference between reasonable suspicion and probable cause** is that reasonable suspicion is a lower standard and can arise from information that is less reliable than that required to show probable cause. *Alabama v. White*, 496 U.S. 325 (1990). For instance, an unverified tip from a known informant may not be reliable enough to establish probable cause to arrest an individual or search his person or his home, but can be sufficiently reliable to justify a brief investigative detention on the street or a stop-and-frisk for weapons. *Adams v. Williams*, 407 U.S. 143 (1972).

It is critical that tracking and searches by law enforcement of “cell location data” and “metadata” be permitted only upon a showing of reliable information that a crime has been committed by the individual whose records are being sought, because of the wealth of information that can be gathered:

“Cell location data” or “historical cell-site data” is the trail left by every cell phone as it connects with various cell towers in its immediate vicinity. This data can be gathered

¹ <http://www.nbcconnecticut.com/investigations/Are-Police-Collecting-Your-Digital-Records-246976931.html>

and collected by law enforcement over a number of days to track the location and movements of an individual. In United States v. Jones, 132 S.Ct. 945 (2012), the United States Supreme Court said that similar long-term tracking of an individual's car via a GPS device violated the Fourth Amendment if done without a warrant based on probable cause.

“Metadata” is all the information that can be gleaned from an individual's phone or internet accounts without reading the content of those conversations or communications. It is, however, more than just abstract numbers without any content. “Metadata” is just as revealing as if law enforcement were permitted to eavesdrop on what was being said. For instance, an hour-long call at 3A.M. to a suicide prevention hotline; a thirty-minute call to an alcohol addiction hotline on New Year's Eve; or a fifteen-minute call to a phone-sex service all reveal information that virtually anyone would consider exceptionally private. Disclosure of metadata from a handful of calls can yield equally sensitive information about a caller. For example: a person makes a series of calls first, to an HIV testing service; then, a doctor; then to a loved one; and then, an insurance company paints a clear picture of someone with a relatively new HIV diagnosis.²

The United States Supreme Court has recognized the importance of obtaining a warrant in the digital age with its opinion in Riley v. California, 134 S. Ct. 2473 (2014), in which it held that law enforcement must obtain a warrant based on probable cause before looking at the contents of an individual's cell phone. In doing so, it recognized the wealth of information available on a cell phone, the pervasiveness of the devices and the near ubiquitous use by people today.

The CCDLA urges this committee to recognize those same concerns and vote favorably on **Senate Bill 1092**.

Respectfully submitted,
Tejas Bhatt
Executive Board Member
CCDLA

² EFF and ACLU *amicus* brief filed in Klayman v. Obama, accessed online at <https://www.eff.org/document/eff-and-aclu-amicus-brief-klayman>; see also a 2014 Stanford study, accessed at <http://webpolicy.org/2014/03/12/metaphone-the-sensitivity-of-telephone-metadata/>