ACLU
Michigan

To: Senate Judiciary & Public Safety Committee
From: Kimberly Buddin, ACLU of Michigan
Date: May23, 2019
RE: SB 341, 342
Position: Support

In this time of rapid technological change, this legislature has an important role to play in regulating the use of surveillance technology by law enforcement. With the advancement of technology, consumers increasingly rely on electronic devices, like cell phones to work, communicate, search the internet, or call for transportation, track and collect sensitive location information. Unfortunately, our laws have not kept pace with these new technological developments – resulting in confusion among the courts, law enforcement officials, and the public over the protections that apply to location information. ACLU of Michigan supports SB 341 and 342 because they provided the public critical privacy protections.

SB 341 Provides Necessary Fourth Amendment Protections In the Use of Cell Site Simulators

Currently, through the use of cell-site simulators, police are able to collect the cellphone location information of anyone in the vicinity of the device. Location tracking enables law enforcement to capture details of someone's movements for months on end, unconstrained by the normal barriers of cost and officer resources.[1] This is not limited to the targets of police investigations and includes passersby suspected of no wrongdoing. Law enforcement is able to routinely collect this information without a probable cause warrant or other appropriate privacy protections. As this has become an increasing problem, similar measures to SB 341 have passed all over the country.

The availability of information and the length of time this information is stored varies with the policies of each mobile phone carrier. Verizon has reported storing location information for one year;[2] T-Mobile keeps historical cell site information for six months;[3] Sprint reportedly stores information from 18 to 24 months,[4] and AT&T retains location information for up to five years.[5] This is why limitations around retention are critical.

Law enforcement must be required to obtain a probable cause warrant to access past or real-time location information to ensure adequate Fourth Amendment protections. The intimate nature of the information that might be collected by this technology—even the limited collection of location information—can reveal intimate and detailed facts about a person. This privacy invasion is multiplied many times over when law enforcement agents obtain this information for prolonged periods of time. As the Supreme Court explained, "[s]ociety's expectation has been that law enforcement agents and others would not -- and indeed, in the main,

---

[1] *See United States v. Pineda-Moreno*, 617 F.3d 1120, 1124 (9th Cir. 2010) (Kozinski, J, dissenting from denial of rehearing en banc) ("The modern devices used in Pineda- Moreno's case can record the car's movements without human intervention—quietly, invisibly, with uncanny precision. A small law enforcement team can deploy a dozen, a hundred, a thousand such devices and keep track of their various movements by computer, with far less effort than was previously needed to follow a single vehicle.").

[2] Letter from William B. Peterson, General Counsel, Verizon Wireless to the Honorable Edward J. Markey, United States Senator 3 (Oct. 3, 2013), available at http://www.markey.senate.gov/imo/media/doc/2013-12-09_VZ_CarrierResponse.pdf.

[3] U.S. Dep't of Justice, Retention Periods of Major Cellular Service Providers (Aug. 2010), available at https://www.aclu.org/cell-phone-location-tracking-request-response-cell-phone-company-data-retention-chart.

[4] *Id.*

[5] Letter from Timothy P. McKone, Executive Vice President, Federal Relations, AT&T to the Honorable Edward J. Markey, United States Senator (Oct. 3, 2013), available at http://www.markey.senate.gov/imo/media/doc/2013-10-03_ATT_re_Carrier.pdf.

ACLU
Michigan

simply could not -- secretly monitor and catalog every single movement of an individual's car, for a very long period."[6] There have always been facets of life which have been uniquely safeguarded from the intrusive interference and observation of government. Location tracking threatens to make even those aspects of life an open book to law enforcement.

Michigan's residents deserve better. They deserve to be protected and have more control over how and when police use surveillance and greater accountability for the police.

SB 342 Safeguards Privacy Interests Against the Use of Facial Recognition

Facial recognition software can identify faces in photographs of demonstrations posted on social media platforms and match them to persons with open warrants. Use of facial recognition in this context has obvious chilling effects on the exercise of First Amendment freedoms, particularly given the imperfections in both computer and human facial matching, which recent studies[7] show have an error rate of 50 percent. And the claimed use of facial recognition in protests about police misconduct raises questions about whether the technique is being used in a racially disparate way, as well as whether the "probable cause" standard is being adhered to.

A growing body of evidence, including a report released by the Center on Privacy & Technology at Georgetown Law,[8] suggests that law enforcement use of face recognition technology is having a disparate impact on communities of color, potentially exacerbating and entrenching existing policing disparities. Face recognition systems are powerful—but they can also be biased. SB 342 safeguards Americans' privacy interests.

Such facts are particularly disturbing given that face recognition technology is increasingly being used by federal, state, and local law enforcement for routine investigations, and face recognition networks have grown to include half of all American adults. According to the Georgetown report, more than 117 million American adults are included in face recognition networks across the country, and at least one in four state or local police departments can run facial recognition searches through their own network or the network of another agency. Thus, face recognition technology is rapidly being interconnected with everyday police activities.

Face recognition technology has enormous civil liberties implications and its use must be closely examined to ensure that it is not violating Americans' civil rights.

We urge this legislature to pass SB 341 and 342.

Respectfully submitted,

Kimberly S. Buddin
Policy Counsel
American Civil Liberties Union of Michigan
kbuddin@aclumich.org

---

[6] *Id.* at 964 (Alito, J., concurring).

[7] White D, Dunn JD, Schmid AC, Kemp RI (2015) Error Rates in Users of Automatic Face Recognition Software. PLOS ONE 10(10): e0139827. https://doi.org/10.1371/journal.pone.0139827.

[8] Garvie C, Bedyoa A, Frankle J (2016) Perpetual Line-Up: Unregulated Police Face Recognition in America. Georgetown Law Center on Privacy & Technology. https://www.perpetuallineup.org/.