PACIFIC LEGAL FOUNDATION

October 3, 2019

Via E-Mail

The Honorable Senator James Runestad
Senate Committee on Judiciary and Public Safety
kvincent@senate.michigan.gov

Re: Legal Analysis of Senate Joint Resolution G (2019)

In response to a request from your office, Pacific Legal Foundation is pleased to provide our legal opinion on the need for the protection of electronic privacy and an analysis of the effectiveness of Senate Joint Resolution G (2019) (SJR G) to achieve its intended purposes. By own our publication of this letter and with any further publication you may assist with, we hope our analysis will both aid the Committee and help educate Michigan citizens on the value and importance of this type of reform. In that regard, we'd be happy to provide more formal testimony at a Committee hearing if that would also be helpful.

An amendment to Article I, Section 11 of the Constitution of Michigan to ensure the security of electronic data and communications against unreasonable searches and seizures is a strong step forward for Michiganders' privacy in the face of case law that leaves substantial doubt as to the bounds of the federal Fourth Amendment's application to digital data and telecommunications. By inclusion of language like that in SJR, Michigan would take guesswork from the hands of the judiciary and instead deliver to the courts a message that intrusion by the state into the emails, metadata, and phone records of its citizens will not be tolerated without a warrant supported by probable cause.

While the Founders could not have predicted the technologies prevalent in America today, the language they drafted for the Bill of Rights nonetheless guarantees certain freedoms against their use in government hands. Just as freedom of the press extends to social media platforms, and the Second Amendment extends beyond black powder muskets, so too does the language of the Fourth Amendment and Michigan's Article I, Section 11 extend beyond physical papers, possessions, and effects. Yet, the courts have been slow to adopt protections surrounding new technologies.

Since the 1920s, law enforcement agencies have used the emergent technologies of the day to engage in clandestine surveillance that invades places previously thought private and secure against intrusion except by physical means. Yet, it was not until 1967 that the Supreme Court of the United States recognized such practices invade an expectation of privacy that society deems reasonable, and thereby extended the protections of the Fourth Amendment against such intrusions.[1]

Again, it wasn't until 2014, more than three decades after the widescale adoption of cell phones and six years after the release of Apple's first iPhone, that the Supreme Court clarified a warrant must be acquired to search through a person's handheld phone without their consent.[2] And it took the Court until 2018, approximately 40 years after the invention of GPS technologies, to announce that the Fourth Amendment likewise protects Americans' location data gathered by telecommunications providers.[3] And even then, the Court's opinion was narrow.[4] These decisions still leave many open questions about the privacy of Americans' electronic data and communications, particularly depending on where and how they are stored.[5]

Neither the Fourth Amendment nor Michigan's state analog contain the word "privacy". Yet, these provisions defend it by guaranteeing the security of Americans in particular places and things. Thus, the outlines of constitutional privacy are drawn by reference to the definitions of a "person," "house," "paper," and "effect" (or "possession" in Michigan).[6]

---

[1] Justice Harlan's concurrence from *Katz v. United States*, 389 U.S. 347, 360 (1967), became the landmark rule of law that courts would apply going forward. This case redefined a "search" under the Fourth Amendment as a government action that invades a person's expectation of privacy that society deems reasonable. It involved a bugging device planted on a telephone booth used by a person dealing in illicit interstate gambling. The use of an electronic device to eavesdrop on a person who had shut the door to a telephone booth and reasonably expected that his conversation would remain private, ruled the Court, invaded a protected Fourth Amendment privacy interest by technological means.

[2] *See* Riley v. California, 575 U.S. 373 (2014).

[3] *See* Carpenter v. United States, 138 S. Ct. 2206 (2018).

[4] Instead of overturning the third-party doctrine, which holds that information shared with a third party forfeits all expectations of privacy, the *Carpenter* decision merely limited this rule to "commercial" as opposed to personal information. *See id*. at 2219-20.

[5] Legal standing in the Fourth Amendment context has become an open question in many instances as more electronic data generated by Americans' use of the Internet and mobile devices has placed information in the hands of third-party service providers such as software, website, and telecommunications companies.

[6] The Fourth Amendment to the United States Constitution reads,

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searches, and the persons or things to be seized.

U.S. Const. amend. IV. Michigan's analogous constitutional provision reads,

The test relied upon by most courts since 1967 does not look exclusively at whether one of these items was intruded upon, but instead depends on assessing whether Americans deem a particular place or thing to be reasonably private.[7] Thus, in the wake of leaks about intrusive government surveillance techniques, these societal expectations of privacy can deteriorate, resulting in a lower standard of protection under the prevailing judicial standard. But constitutional rights should not wax and wane with majoritarian sentiment, particularly when such sentiment can change on the basis of government malfeasance.

Reform language like that in SJR G would sidestep the need to rely on this self-defeating standard by clearly establishing that a warrant must be acquired to access electronic data and communications. Thus, a Michigan court need not guess about whether a majority of Americans consider emails, social media messages, or browser search histories to be private. Under SJR G's reforms, they would be protected from search or seizure except upon the issuance of a warrant following proper judicial procedures. This would allow the courts in Michigan to focus on the more important task of defining what constitutes a "person," "house," "paper," "possession," "electronic data", and "electronic communication" in the digital age.[8] The prevailing expectation of privacy standard from

---

> The person, houses, papers and possessions of every person shall be secure from unreasonable searches and seizures. No warrant to search any place or to seize any person or things shall issue without describing them, nor without probable cause, supported by oath or affirmation. The provisions of this section shall not be construed to bar from evidence in any criminal proceeding any narcotic drug, firearm, bomb, explosive or any other dangerous weapon, seized by a peace officer outside the curtilage of any dwelling house in this state.

Mich. Const. art. I, § 11 (1963). The amendment would add "electronic data" and "electronic communications" to both the list of items secured by the Michigan constitution against unreasonable search and seizure as well as the enumeration of items against which a warrant issued must be supported by probable cause and circumscribed by particularity. While probable cause defends against the spurious and undiscerning issuance of warrants, the particularity component of the text ensures that government agents and officers do not wield the type of unbridled discretion to search and seize that presents fertile ground for tyranny.

[7] Before this new legal definition of a "search", the Supreme Court relied upon the principle of trespass, deciding when a search or seizure occurred by looking at whether government action had physically intruded into a house. *See*, *e.g.*, Silverman v. United States, 365 U.S. 505 (1961) (holding attachment of a microphone to a heating duct running into suspect's home violated the Fourth Amendment). After the Court developed the new *Katz* standard in 1967, litigants began using this new test and the trespass doctrine withered on the vine. But in 2012, the Supreme Court decided *United States v. Jones*, in which it held narrowly that attachment of a GPS device to a car by the police constituted a search under the trespass doctrine. 565 U.S. 400 (2012). This case affirmed that *Katz* did not replace the trespass doctrine, but instead supplemented it. In *Carpenter v. United States*, Justice Gorsuch lamented that litigants are not sufficiently relying on this doctrine to vindicate Fourth Amendment interests in the context of modern technologies. *Carpenter*, 138 S. Ct. at 2269-72 (Gorsuch, J., dissenting).

[8] This should result in a more robust jurisprudence defining the contours of when governments conduct trespasses on electronic and digital property, rather than questioning whether people think it should be private in the first place.

the 1960s has derailed this effort and curtailed the role of the courts in defending data created by contractual relationships between end users and electronic service providers.

At their core, the Fourth Amendment and Michigan's Article I, Section 11 defend people and property against government intrusion. For too long, the courts have tried to find out what "privacy" means at the expense of defining whether electronic data and communications are "effects," "possessions," or "papers", and what government conduct constitutes a trespass against them. SJR G would be effective in setting the record straight and announcing that the government in Michigan must get a warrant to access the vast troves of electronic data collected by service providers on Americans conducting their everyday lives. This is a step forward for property rights, privacy, and the rule of law.

Sincerely,

Daniel T. Woislaw
Attorney*
Pacific Legal Foundation
**Licensed in the Commonwealth of Virginia*

Cf. Carpenter, 138 S. Ct. at 2268 ("[T]he fact that a third party has access to or possession of your papers and effects does not necessarily eliminate your interest in them.") (Gorsuch, J., dissenting). This will enable clarity in the law and less guesswork for law enforcement agencies over whether they need a warrant in any given context.