October 2020 | Memorandum 1164

CITIZENS RESEARCH COUNCIL OF MICHIGAN
UNBIASED POLICY RESEARCH

Statewide Ballot Proposal 20-2:

Protection of Electronic Data and Communications

In a Nutshell

Proposal 2 is an amendment to the Michigan Constitution that would add electronic data and electronic communications to the existing protections against unreasonable government search and seizure.

If Proposal 2 is Adopted The Michigan Constitution would provide specific protections to electronic data and communications. Law enforcement would be required to obtain warrants to access information stored in these formats.

If Proposal 2 is Rejected Law enforcement would continue the current practice of seeking warrants to access electronic data and communications based on interpretation of the "Searches and Seizures" provision of the Michigan Constitution and the Bill of Rights in the U.S. Constitution.

Major Issues to Consider Article I of the Michigan Constitution contains many of the personal protections found in the Bill of Rights in the U.S. Constitution. While neither constitution explicitly protects electronic data and communications, Michigan law enforcement agencies mostly treat this information the same as the protections for "persons, houses, papers, and effects/possessions" found in the U.S. and state constitutions. Proposal 2 attempts to remove any ambiguity.

Introduction

With the proliferation of modern technology, the amount and personal value of the data stored on an individual's phone, computer, hard drive, etc. can be considerable. As each day passes, our lives become more and more integrated with technology.

On November 3, 2020, voters in Michigan will be presented with a legislatively proposed amendment to the state Constitution to add language explicitly stating that electronic data and communications are protected against unreasonable search and seizure. The proposed amendment aims to afford electronic property some of the same protections that have long existed for tangible property.

Proposal 2 would amend Article 1, Section 11, of the Michigan Constitution to read as follows:

> The person, houses, papers, ~~and~~ possessions, **electronic data, and electronic communications** of every person shall be secure from unreasonable searches and seizures. No warrant to search any place or to seize any person or things or **to access electronic data or electronic communications** shall issue without describing them, nor without probable cause, supported by oath or affirmation....[a]
>
> [Proposed language to be deleted is struck through. Proposed language to be added is bolded.]

Article I of the Michigan Constitution, entitled "Declaration of Rights", sets forth basic individual liberties that state government shall not impair.

[a] The last sentence of this section allows allows for the use of evidence seized outside of a person's house. It has been ruled invalid because it conflicts with the Fourth Amendment to the U.S. Constitution. In *People v Pennington*, (383 Mich 611; 1970), the Michigan Supreme Court held that this sentence, which allowed certain evidence to be admitted into criminal proceedings, violated the federal exclusionary rule as enunciated by the U.S. Supreme Court in *Mapp v Ohio*, (367 US 643;1961). See Michigan Constitutional Issues: Article I – Declaration of Rights, Citizens Research Council Report 360-04 (March 2010) https://crcmich.org/wp-content/uploads/rpt36004.pdf

Many of these individual liberties were modeled after those found in the federal Bill of Rights. Both Article I and the Bill of Rights accord the right to equal protection of the laws, peaceful assembly, religious worship, and freedom of expression and of the press. Both prohibit depriving a person of life, liberty, or property without due process of the law. Indeed, both provide the right to be secure in your persons, houses, papers, and effects/possessions.

The Fourth Amendment to the U.S. Constitution reads as follows:

> 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 searched, and the persons or things to be seized.

Value of Redundancy in State Constitutions

Since many individual protections are established by the Bill of Rights, some may wonder why states would repeat these protections in their constitutions.

Originally, the federal Bill of Rights was intended to serve as a limitation only upon the federal government. Thus, the First Amendment begins, "Congress shall make no law...." For the protection of individual liberties against impairment by state action, it was thought that a citizen should look to the constitution of the state wherein he or she resided and not to the federal government. It was not until 1925 that the U.S. Supreme Court held that the Fourteenth Amendment to the U.S. Constitution "incorporated" the Bill of Rights and made those protections applicable to the states.

The final authority to interpret and fix the meaning of a state constitution rests with the supreme court of each state. Thus, the supreme court of a state has the discretion, within judicial boundaries, to interpret that constitution in such a manner as to accord the citizens of that state more rights than they enjoy under the U.S. Constitution.

Since the provisions of the U.S. Constitution, as currently interpreted, supercede conflicting provisions of state constitutions, state constitutions can enhance federal protections, but not diminish them. In 1961, the U.S. Supreme Court's decision in *Mapp v. Ohio* held that it is a violation of the guarantees provided by the U.S. Constitution for any state to admit into evidence in any criminal proceeding in its state courts any evidence illegally obtained by an unreasonable search and seizure.[1]

The characteristics of electronic property are nuanced, complex and ever-changing with technological advancements. Courts have had difficulty contending with the extent to which the Fourth Amendment protects against the search and seizure of electronic property. Few cases have risen to the U.S. Supreme Court to become binding precedent. Inclusion of more specific protections in the Michigan Constitution, therefore, serves to further define the federal protections without relying on federal court precedent. Of course, decisive actions by states do not preclude the possibility of later court decisions nullifying those state-adopted provisions.[2]

CRC Board of Directors

ALEKSANDRA A. MIZIOLEK, Chair
MICHAEL P. MCGEE, Vice Chair
LAURA APPEL, Treasurer
ORLANDO BAILEY
LAURA BASSETT
BETH BIALY
LARRY BLUTH
CHASE CANTRELL
MEGAN CRESPI
STEVE CURRIE
DAN DOMENICUCCI
RICK FAVOR JR.
ANN FILLINGHAM
MARY LYNN FOSTER
CARL GENBERG
JUNE HAAS
RON HALL
JASON HEADEN
KEVIN HEARD
RENZE HOEKSEMA
MICHAEL HORRIGAN
WIN IRWIN
TOM KYROS
ANNE MERVENNE
JAMES POLEHNA
KIRK PROFIT
NEIL SHERIDAN
CAROLEE SMITH
CHRISTINE SONERAL
TONY STAMAS
KATHLEEN WILBUR
MICHAEL WILLIAMS
DIANE YOUNG

Search Warrants

Law enforcement agencies must comply with specific procedures when investigating alleged crimes. Specifically, they must obtain a warrant if the collection of evidence necessitates searching a person, that person's location, and specific items. A valid search warrant must meet four requirements:

1. it must be filed in good faith by a law enforcement officer;
2. it must be based on reliable information showing probable cause to search;
3. it must be issued by a neutral and detached magistrate; and
4. it must state specifically the place to be searched and the items to be seized.[3]

Defining Terms

The scope of what would currently be included in a definition of electronic data and electronic communications and covered by Proposal 2 is broad.

Obviously, electronic communications would include email and text messages. Electronic data would include user files related to word processing, spreadsheets, pictures, accounting, and similar files and images.

Electronic data and communications are very broad categories, and law enforcement is able to dig deeply into electronic devices to access other forms of electronic data and communications, including: telephone call records; participation in online chatrooms; Internet search histories; IP addresses; location data; and the time and length of use of individual apps.

As technology evolves, new forms of data and communications also may fall within the bounds of the proposed language. Just as the terms and concepts mentioned above would have been alien to citizens adopting the 1963 Constitution, law enforcement and the courts 20 or 30 years from now may wrestle with access to forms of electronic data and communications that seem farfetched to us today.

"Electronic data" could refer solely to content or it could mean both content and metadata. *Content* is whatever is found on drives or files, email messages, or other electronic data. *Metadata* is information that is related to this content. As an analogy, when sending a letter to someone, the content would be the written letter and the metadata would be the address of the recipient; or in an electronic context, content might be the contents of an electronic file, and the corresponding metadata would be the file's size, date of creation, date of last edit, and so on.

Current Protections

Even though electronic data and communications are not explicitly recognized in the U.S. Constitution, aspects of them have been protected by a rigorous vetting processes requiring law enforcement to obtain warrants. For the most part, electronic information is considered an "effect" in the language of the Fourth Amendment, and it is widely analogized as closed containers by the federal courts.[b] [4]

Congress has enacted several laws applying to Fourth Amendment protections and the need for search warrants. Among these are the Pen Registers and Trap and Trace Device Statute that restricts collection of metadata concerning telephone and Internet communications.[5] The Electronic Communications Privacy Act protects email and other subscriber data stored by Internet service providers from disclosure without appropriate warrants.[6]

Just as is the case for tangible evidence, statutes and case law require warrants for electronic information to be specific in the desired evidence and its location.[7] For example, in *United States vs Carey*, some evidence was suppressed because searchers went beyond the scope of their warrant when gathering evidence from the defendant's computer.[8]

Even with electronic data and communications already being protected without explicit reference to it in the Fourth Amendment, some grey area still exists with regard for searching and seizing electronic information. For instance, while the U.S. Supreme Court decision in *Carpenter v. United States* (2018) held that the government violated the Fourth Amendment by accessing historical records containing the physical locations of cellphones without a search warrant, it has not yet addressed how to handle email communications.[9]

[b] As it relates to the Fourth Amendment, the courts have differentiated items in plain view from those contained in closed containers. In overly simplified terms, identifying property in *plain view* involves no invasion of privacy, but property in *closed containers* is generally assumed to be private.

The Benefits of Clearer Boundaries

This amendment might help both law enforcement agencies seeking warrants and those individuals, families and organizations who may face unjust searches and seizures of electronic devices. Although some law enforcement professionals may see this provision as a hindrance to investigating and prosecuting crimes, it seems that most already treat electronic data and communications the same as tangible property and effects.

Proposal 2 aims to create clear boundaries for law enforcement officials in Michigan. If it is successful doing this, it could save money for law enforcement agencies by relieving them of the burden of defending unlawful searches or electronic data seized without a warrant.

Clearer boundaries could promote a more equitable legal structure. The proposed amendment may help to protect the less affluent from the necessity of dedicating scarce financial resources to fighting legal battles. If they are faced with questionable searches and/or seizures, but do not have the time nor the resources to carry out legal battles, they would have to endure the unconstitutional injustice with no compensation. If Proposal 2 can define clear boundaries for law enforcement, it could reduce or eliminate the need for expensive legal challenges.

Other States

If Michigan adopts Proposal 2, it would join Alaska, Arizona, California, Florida, Hawaii, Illinois, Louisiana, Montana, Missouri, New Hampshire, South Carolina, and Washington, all of which have clauses in their state constitutions that protect electronic data from unreasonable search and seizure.[10]

Most of these other state constitutions are oriented toward privacy, which can touch upon law enforcement's need for search warrants but extends to the actions of Internet businesses to use browser and location history, monitor conversations, and use other privacy infringements to market goods and services. For instance, the California Consumer Privacy Act gives consumers more control over the personal information that businesses collect about them.[11]

Michigan's proposed amendment would be similar to Missouri's, because they both explicitly mention electronic data in their constitutional provisions related to search and seizure.[12]

Issues to Consider

At first blush, it appears Proposal 2 will do little to change how law enforcement treats electronic data and communications. It already is common practice for police to seek a warrant before attempting to access information stored in these formats. If nothing else, the proposed constitutional amendment would eliminate any ambiguity in state law.

Electronic information is already protected under the U.S. Constitution, even though it is not explicitly stated. Previous court decisions have clarified how law enforcement must treat various aspects of electronic data and communications; however, very few of those cases have made it to the U.S. Supreme Court to create precedents. Even if the Court does eventually establish precedents, future cases may work to reverse that precedent. The rapidly evolving nature of technology further complicates this legal uncertainty at both the federal and state levels.

While Proposal 2 might not be seriously impactful at this current point in time, it could become more influential in the future. Technology and electronic data have rapidly become an integral part of everyday life. Just over ten years ago, Apple released the iPhone, and for many, this began the process of the intermingling of personhood and electronic information. Today, many people's professional and personal identities are inextricably tethered to electronically stored information.

Some of the current political discourse addresses varied opinions about police actions and personal rights. While some may see Proposal 2 as an infringement on law enforcement, most police officers already seek warrants for the search and seizure of electronic data and communications. More than just law enforcement and those suspected of committing crimes, the proposed amendment could serve to provide stronger protections to citizens concerned about their privacy.

Endnotes

1 *Mapp v. Ohio*, Decision No. 236 October term, 1960, Supreme Court of U.S.

2 See Citizens Research Council of Michigan Memorandum 1136, A Reminder to Clean Up the Michigan Constitution (July 2015) https://crcmich.org/publications/reminder_clean_michigan_constitution-2015

3 Justia, Search and Seizure Frequently Asked Questions (accessed 20 Aug, 2020) https://www.justia.com/criminal/docs/search-seizure-faq/#q3

4 U.S. Department of Justice, Computer Crime and Intellectual Property Section - Criminal Division, Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations, https://www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/01/14/ssmanual2009.pdf, 3

5 18 U.S.C. §3121 et seq. See Rand Corporation, Sean E. Goodison, Robert C. Davis, Brian A. Jackson, Digital Evidence and the U.S. Criminal Justice System, https://www.ncjrs.gov/pdffiles1/nij/grants/248770.pdf

6 18 U.S.C. §2701 et seq. See Rand Corporation, Sean E. Goodison, Robert C. Davis, Brian A. Jackson, Digital Evidence and the U.S. Criminal Justice System, https://www.ncjrs.gov/pdffiles1/nij/grants/248770.pdf

7 U.S. Department of Justice, Computer Crime and Intellectual Property Section - Criminal Division, Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations, https://www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/01/14/ssmanual2009.pdf, 64

8 U.S. Department of Justice, Computer Crime and Intellectual Property Section - Criminal Division, Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations, https://www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/01/14/ssmanual2009.pdf, 18

9 *Carpenter v. United States* No. 16-402, 585 U.S. ____ (2018) https://www.scotusblog.com/case-files/cases/carpenter-v-united-states-2/

10 National Conference of State Legislators, New Hampshire Voters Approve Constitutional Amendment on Privacy (November 14, 2018) https://www.ncsl.org/blog/2018/11/14/new-hampshire-voters-approve-constitutional-amendment-on-privacy.aspx

11 California Attorney General Xavier Becerra, California Consumer Privacy Act (CCPA) https://oag.ca.gov/privacy/ccpa

12 Article I, Section 15 of the Missouri Constitution https://www.sos.mo.gov/CMSImages/Publications/CurrentMissouriConstitution.pdf

A Fact Tank Cannot Run on Fumes

Do you find this report useful and want to support analysis that will lead to better policy decisions and better government in Michigan? Your support of Citizens Research Council of Michigan will help us to continue providing policy makers and citizens the trusted, unbiased, high-quality public policy research Michigan needs.

Please visit www.crcmich.org/donate or fill out the form below and send it to:

Citizens Research Council of Michigan
38777 Six Mile Road, Suite 208
Livonia, MI 48152-3974

You can learn more about the organization at www.crcmich.org/about.

YES! I want to help fill Michigan's Fact Tank and support sound public policy in Michigan!

NAME _____

ADDRESS _____

EMAIL / PHONE _____

- I wish to make a one-time, tax-deductible gift of: $ _____
- I wish to pledge a total of $ _____ with an initial payment of $ _____ .
- I would like my contribution to support: _____ Annual Fund _____ Endowment
- Please mark my gift:
  - ☐ Anonymous
  - ☐ In Honor Of: _____
  - ☐ In Memory Of: _____
- Gift will be matched by: _____

Or donate online at www.crcmich.org/donate