Colorado Freedom of Information Coalition
coloradofoic.org
coloradofoic@gmail.com
720-274-7177
@CoFOIC

Disappearing transparency: How public officials' use of ephemeral messaging apps undermines open government laws

Researched and written by Mackenzie Coupens
University of Denver, Sturm College of Law, J.D. 2023
mcoupens23@law.du.edu

July 2023

EXECUTIVE SUMMARY

Overview

Federal and state open records laws are intended to ensure an informed citizenry, but it is impossible to achieve that purpose when public officials evade disclosure requirements by engaging in official communications on disappearing and encrypted messaging apps. However, most open records laws do not directly address the legality of official communications taking place on these apps and whether such communications fall within the definition of "public records." Perhaps not surprisingly, the use of apps that can automatically delete messages is becoming more prevalent. While a few states have taken steps to address this issue, Colorado has not yet implemented any amendments to its open records or records retention laws to prevent state and local officials from engaging in official business on private messaging apps.

Current Legal Landscape

- **Michigan House Bill 4778** directs state departments and agencies not to use any app or technology that prevents them from maintaining or preserving electronic public records as required by law.
- In ***Sansone v. Governor of Missouri***, the Missouri Court of Appeals for the Western District held that the governor's use of disappearing messaging apps was not a violation of the sunshine laws because no messages were retained so there was no public record to be produced.
- **Texas Senate Bill 944**, enacted in 2019, requires government officials to preserve text messages sent from or received on their personal devices that concern public or official business. However, the law does not directly address the use of disappearing or encrypted messaging apps.
- **Kansas Executive Order 18–06** requires governor's office employees to conduct official business on their official state email accounts; accordingly, any use of a disappearing or

encrypted messaging app for official business would be in violation of the executive order.

Colorado Recommendation

Colorado should adopt new legislation addressing the legality of public officials' use of disappearing and encrypted messaging apps. Because Michigan House Bill 4778 is currently the only piece of state legislation to directly address this issue, that language should be mirrored in Colorado and applied to members of state and local public bodies as well. The following language would make it a violation of state law for any public official to use disappearing or encrypted messaging apps to conduct official business:

All state and local departments, all state and local government entities, and all elected and appointed officials of state and local government entities, agencies and public bodies must not use any app, software, or other technology that prevents it from maintaining or preserving a public record as required by law on an electronic device that is used to create a public record.

Contents

I. Introduction 5

II. Overview of Current Document Disclosure and Retention Laws 6

a. The Freedom of Information Act 6

b. State Open Records and Retention Laws 7

1. Colorado Open Records Act 7

2. Colorado Uniform Records Retention Act 8

3. State Archives Statute and Public Records Law 9

III. Disappearing and Encrypted Messaging Apps 11

a. Overview of Confide and Signal 11

b. Limits on the Use of Encrypted Messaging Apps in Federal Agencies 12

c. Use of Disappearing and Encrypted Messaging Apps by Public Officials 14

IV. Policy Issues Surrounding Public Officials' Use of Encryption Apps 16

a. Use of Ephemeral Messaging Apps Eliminates Government Transparency 16

b. The Use of Ephemeral Messaging Apps Impedes Litigation 17

V. Current Legal Landscape 20

a. Michigan House Bill 4778 20

b. District of Columbia Bill 24-0692 20

c. Missouri: Sansone v. Governor of Missouri 22

d. Texas Senate Bill 944 23

e. Kansas Executive Order 18–06 24

VI. Colorado: Legality of Use Under Transparency Laws and Prevalence of Use 25

a. Colorado Transparency Laws do not Address Messaging Via Encryption Apps 25

b. Prevalence of the Use of Encryption Apps in Colorado 26

VII. Colorado Recommendation 27

VIII. Conclusion 28

I. Introduction

Federal and state open records laws exist to ensure that the public is informed through transparency and access to government records.[1] These laws serve as a mechanism to prevent corruption and ensure the government is held accountable.[2] Open records laws allow the public to request access to public records unless the records fall into certain exceptions within federal or state laws.[3] However, open records acts generally apply only to records that are in existence at the time a member of the public requests access to them; these laws do not require the making of a new record, nor the production of records that no longer exist. Other statutes and policies, extraneous to open records laws, dictate the period of time that a public record must be maintained prior to destruction ("retention period").[4]

Recent developments in technology have proven that the reach of open records laws is not sufficient. In the first wave of technological advancements, the laws had to address whether emails and text messages were within the definition of "records." Today, one of the prevalent issues in connection with these laws and transparency is that many federal and state public officials are using disappearing or encrypted messaging apps. These apps immediately (or after a very short interval of time, following receipt) delete communications and no records of the communications are kept.[5] Because no records are kept, official communications that would otherwise be within the realm of document production laws are not subject to production because there is no *existing* record to be produced.

This paper will: 1) provide an overview of federal and state open records laws; 2) explain the purpose for and use of disappearing and encrypted messaging apps; 3) discuss the policy concerns surrounding the use of these apps for official business; 4) provide an overview of the

[1] *See What is FOIA?*, FREEDOM OF INFORMATION ACT, https://www.foia.gov/about.html (last visited Mar. 25, 2023).
[2] *See* NLRB v. Robbins Tire & Rubber Co., 437 U.S. 214, 242 (1978).
[3] *See* 5 U.S.C. § 552(b) (providing the list of exemptions within the Freedom of Information Act); *see, e.g.*, *Law Summary: Colorado Open Records Act - "CORA,"* COLORADO OFFICE OF LEGISLATIVE LEGAL SERVICES (Dec. 1, 2022), https://leg.colorado.gov/sites/default/files/colorado-open-records-act-cora.pdf (explaining the Colorado Open Records Act and the exceptions within the Act).
[4] *See e.g.*, COLO. REV. STAT. § 6-17-101 et seq. (Colorado Uniform Records Retention Act); COLO. REV. STAT. § 24-80-101 et seq. (Colorado State Archives Statute).
[5] *See* CONFIDE, https://getconfide.com (last visited Mar. 29, 2023); *see* SIGNAL, https://signal.org/#signal (last visited Mar. 29, 2023).

current legal landscape on the legality of using these apps for official business; 5) demonstrate the prevalence of the use of these apps by public officials in Colorado; and 6) propose recommended language for legislation to address this issue in Colorado.

II. Overview of Current Document Disclosure and Retention Laws

a. The Freedom of Information Act

The federal law governing the production of records pertaining to the affairs of the United States government is the Freedom of Information Act (FOIA).[6] The overarching purpose of FOIA is "to ensure an informed citizenry, vital to the functioning of a democratic society, needed to check against corruption and to hold the governors accountable to the governed."[7] The law encourages "public disclosure of information so citizens may understand what their government is doing," enabling the public to "have access to government information that is unnecessarily shielded from public view."[8]

FOIA provides any person the right to request access to federal agency records or information, and those records must be produced unless they are protected from disclosure.[9] There are nine exemptions in the law that exclude certain types of information from disclosure.[10] Additionally, Congress has provided that three narrow categories of law enforcement and national security records are excluded from FOIA.[11] Aside from the information protected from disclosure, all documents are subject to disclosure under FOIA if

[6] 5 U.S.C. § 552.
[7] NLRB v. Robbins Tire & Rubber Co., 437 U.S. 214, 242 (1978).
[8] Miccosukee Tribe of Indians of Fla. v. United States, 516 F.3d 1235, 1244 (11th Cir. 2008).
[9] 5 U.S.C. § 552(a).
[10] 5 U.S.C. § 552(b) (The following nine categories of information are protected from disclosure: 1. classified information for national defense or foreign policy, 2. internal personnel rules and practices, 3. information that is exempt under other laws, 4. trade secrets and confidential business information, 5. inter-agency or intra-agency memoranda or letters that are protected by legal privileges, 6. personnel and medical files, 7. law enforcement records or information, 8. information concerning bank supervision, and 9. geological and geophysical information).
[11] The Freedom of Information Act, U.S. DEP'T OF STATE, https://foia.state.gov/learn/foia.aspx (last visited Mar. 29, 2023) ("The first exclusion protects the existence of an ongoing criminal law enforcement investigation when the subject of the investigation is unaware that it is pending and disclosure could reasonably be expected to interfere with enforcement proceedings. The second exclusion is limited to criminal law enforcement agencies and protects the existence of informant records when the informant's status has not been officially confirmed. The third exclusion is limited to the Federal Bureau of Investigation and protects the existence of foreign intelligence or counterintelligence, or international terrorism records when the existence of such records is classified.").

they are "agency records," which the Supreme Court has defined as records created or obtained by the agency and in the agency's control.[12] Based on the Supreme Court's definition of "agency record," any electronic communication, such as emails or text messages sent or received by a federal government employee, would be subject to disclosure under FOIA so long as the subjects of communication do not fall under the exemptions laid out within the Act or by Congress.

b. State Open Records and Retention Laws

Because FOIA only governs federal agencies, the law does not apply to state and local governments.[13] Accordingly, each state has its own laws governing retention and production of government records.[14] In Colorado, the Colorado Open Records Act (CORA), the Colorado Uniform Retentions Act, and the Colorado State Archives Law govern the retention and production of government records.[15]

1. Colorado Open Records Act

The Colorado Open Records Act requires that most public records be made available to the public upon request.[16] Similar to the definition of an "agency record" under FOIA, CORA defines "public records" as "all writings made, maintained, or kept by the state, or any political subdivision thereof . . . for use in the exercise of functions required or authorized by law or administrative rule."[17]

CORA does not provide any guidance about retention periods for public records. While CORA "directs records custodians to adopt a policy regarding the retention, archiving and destruction of records kept 'in miniaturized or digital form,' it doesn't outline any specifications for such a policy."[18] Accordingly, a policy requiring that all of an agency's emails be deleted

---

[12] 5 U.S.C. § 552(a)(4)(B); U.S. Dep't of Just. v. Tax Analysts, 492 U.S. 136, 144–46 (1989).
[13] *See* 5 U.S.C. § 551, 552.
[14] *See e.g.*, COLO. REV. STAT. § 24-72-201 et seq.; NEV. REV. STAT. § 19-239 et seq.; CAL. GOV'T CODE §§ 6250 – 6268.
[15] COLO. REV. STAT. § 24-72-201 et seq. (Colorado Open Records Act); COLO. REV. STAT. § 6-17-101 et seq. (Colorado Uniform Records Retention Act); COLO. REV. STAT. § 24-80-101 et seq. (Colorado State Archives Statute).
[16] COLO. REV. STAT. § 24-72-201 et seq.; *Colorado Open Records Act (CORA)*, COLORADO SECRETARY OF STATE, https://www.sos.state.co.us/pubs/info_center/cora.html (last visited Mar. 14, 2023).
[17] COLO. REV. STAT. § 24-72-202(6)(a)(I) (2019).
[18] Jeffrey A. Roberts, *CFOIC Research: 'What Colorado Needs to do to Preserve the Modern Public Record*,' COLORADO FREEDOM OF INFORMATION COALITION (October 1, 2019), https://coloradofoic.org/cfoic-research-what-colorado-needs-to-do-to-preserve-the-modern-public-record/.

upon receipt would not violate the plain language of CORA because the agency followed guidelines and adopted a retention policy.[19]

With the evolution of technology, CORA was amended to include provisions about electronic communications, but the provisions only apply to the monitoring of public employee email systems and require that agencies using email communications "adopt a written policy on any monitoring of electronic mail communications and the circumstances under which it will be conducted."[20] Furthermore, Section 24-72-204.5 requires that the agency policy "include a statement that correspondence of the employee in the form of electronic mail may be a public record under the public records law and may be subject to public inspection."[21] While the amendment addressed electronic mail communications, the Colorado Supreme Court has held that text messages are considered public records under CORA if they are made or maintained for the purpose of conducting public business.[22]

2. Colorado Uniform Records Retention Act

The Colorado Uniform Records Retention Act states that records required to be kept under state or local law, such as CORA, "may be destroyed after three years from the date of creation, unless such law or regulation establishes a specified records retention period or a specific procedure to be followed prior to destruction."[23] The Uniform Records Retention Act was enacted to "minimize the paperwork burden associated with the retention of business records for individuals, small businesses, state and local agencies, corporations, and other persons," with the intent to "minimize the costs of collecting, maintaining, using, storing, and

[19] Jill Beathard, *But the Emails… What Colorado Needs to do to Preserve the Modern Record*, COLORADO FREEDOM OF INFORMATION COALITION (Oct. 2019), https://coloradofoic.org/wp-content/uploads/2019/10/ButTheEmails_Oct2019.pdf; *see Law Summary: Colorado Open Records Act - "CORA,"* COLORADO OFFICE OF LEGISLATIVE LEGAL SERVICES (Dec. 1, 2022), https://leg.colorado.gov/sites/default/files/colorado-open-records-act-cora.pdf ("CORA does not contain a specific requirement regarding the length of time a custodian must maintain a public record. Custodians and agencies can make their own determination of the appropriate length of time a record must be kept or archived.").

[20] COLO. REV. STAT. § 24-72-204.5 (2019).

[21] COLO. REV. STAT. § 24-72-204.5 (2019).

[22] Denver Pub. Co. v. Bd. of Cnty. Comm'rs of Arapahoe, 121 P.3d 190, 192 n.1 (Colo. 2005) (explaining that while the text messages sent in the case "do[] not fit into the traditional notion of computer-to-computer e-mail", they are treated as "electronic mail" for the purposes of CORA).

[23] COLO. REV. STAT. § 6-17-104 (2019).

disseminating information and business records."[24] Given that the Uniform Records Retention Act prescribes only how long the records must be retained before destruction but does not itself provide any mechanism for the public to access those records,[25] it does not appear to be terribly concerned about maintaining government transparency. The statute seems more concerned with not overburdening state and local records storage repositories.

3. State Archives Statute and Public Records Law

Along with CORA and the Colorado Uniform Records Retention Act, the Colorado State Archives Statute provides guidance on the retention of public records and requires that each state agency adopt a records retention policy.[26] The States Archives law defines "records" as

> all books, papers, maps, photographs, or other documentary materials, regardless of physical form or characteristics, made or received by any governmental agency in pursuance of law or in connection with the transaction of public business and preserved or appropriate for preservation by the agency or its legitimate successor as evidence of the organization, functions, policies, decisions, procedures, operations, or other activities of the government or because of the value of the official governmental data contained therein.[27]

Section 24-80-102.7 requires state agencies to "[e]stablish and maintain a records management program for the state agency and document the policies and procedures of such program."[28] The State Archives Statute allows for discretion on the part of the agency for what types of electronic messages and communications are considered records. For example, emails are specifically excluded from the definition of "records," unless such messages have been "previously segregated and stored… as evidence of the organization, functions, policies, decisions, procedures, operations, or other activities of the government or because of the value of the official governmental data contained therein."[29] Accordingly, whether electronic communications are considered "records" for the purposes of the State Archives Law hinges on

[24] COLO. REV. STAT. § 6-17-102 (2019).
[25] *See generally* COLO. REV. STAT. § 6-17-101 et seq. (2019).
[26] COLO. REV. STAT. § 24-80-101 et seq. (2019).
[27] COLO. REV. STAT. § 24-80-101(2) (2019).
[28] COLO. REV. STAT. § 24-80-102.7(2)(a) (2019).
[29] COLO. REV. STAT. § 24-80-101(2)(f) (2019).

the content of the messages rather than the type or form of message,[30] as is true for whether an electronic or digitized communication constitutes a "public record" under CORA.

The Office of State Archives has promulgated model retention schedules for state agencies that "give state agencies the legal authorization to retain and dispose of common kinds of records created by state government," and it has promulgated similar retention schedules for local governments.[31] For example, the State Archives recommends that administrative records of state agencies be retained according to the following classification of records: records of enduring or long term value[32] should be retained permanently; records of routine value[33] should be retained for two years; and records of transitory value[34] should be retained for 90 days or until the material has been read.[35] Recommended schedules are provided for other agency records as well, such as budgeting records, communications records,

[30] Jill Beathard, *But the Emails… What Colorado Needs to do to Preserve the Modern Record*, COLORADO FREEDOM OF INFORMATION COALITION (Oct. 2019), https://coloradofoic.org/wp-content/uploads/2019/10/ButTheEmails_Oct2019.pdf.

[31] *State Agency Records Management*, COLORADO STATE ARCHIVES, https://archives.colorado.gov/records-management/state-agency-records-management (last visited Mar. 29, 2023).

[32] COLORADO STATE ARCHIVES, RECORDS MANAGEMENT MANUAL STATE GOVERNMENT AGENCIES: SCHEDULE NO. 1 ADMINISTRATIVE RECORDS 4, https://drive.google.com/file/d/0B-21ETcKVa4LZlotaVpYSVpZY3dhNzB6NDB0U0VDZFhrOWRF/view?resourcekey=0-F9AakdoN-sSE63IiXqGTBQ (explaining that records of enduring or long term value include "[d]ocumentation or correspondence, including e-mail messages, with lasting long-term administrative, policy, legal, fiscal, historical or research value; records that relate to policy issues and actions or activities in which an important precedent is set; records of historic events; and other similar records and documentation.").

[33] COLORADO STATE ARCHIVES, RECORDS MANAGEMENT MANUAL STATE GOVERNMENT AGENCIES: SCHEDULE NO. 1 ADMINISTRATIVE RECORDS 4, https://drive.google.com/file/d/0B-21ETcKVa4LZlotaVpYSVpZY3dhNzB6NDB0U0VDZFhrOWRF/view?resourcekey=0-F9AakdoN-sSE63IiXqGTBQ (explaining that records of routine value include "[r]outine operating documentation or correspondence with limited administrative, legal, fiscal, historical, informational or statistical value. Includes routine e-mail messages, letters or memoranda, reading or chronological files that contain duplicates of memos or letters also filed elsewhere, routine requests for information, transmittal documents, etc.").

[34] COLORADO STATE ARCHIVES, RECORDS MANAGEMENT MANUAL STATE GOVERNMENT AGENCIES: SCHEDULE NO. 1 ADMINISTRATIVE RECORDS 4, https://drive.google.com/file/d/0B-21ETcKVa4LZlotaVpYSVpZY3dhNzB6NDB0U0VDZFhrOWRF/view?resourcekey=0-F9AakdoN-sSE63IiXqGTBQ (explaining that records of transitory value are "[g]eneral documentation or correspondence of extremely short-term interest that has no documentary or evidential value. Includes transmittal correspondence, copies of replies which require no administrative action, no policy decision, and no special compilation or research for reply; and quasi-official notices such as for holidays, charity, and fund appeals, bond campaigns, and other similar papers.").

[35] COLORADO STATE ARCHIVES, RECORDS MANAGEMENT MANUAL STATE GOVERNMENT AGENCIES: SCHEDULE NO. 1 ADMINISTRATIVE RECORDS, https://drive.google.com/file/d/0B-21ETcKVa4LZlotaVpYSVpZY3dhNzB6NDB0U0VDZFhrOWRF/view?resourcekey=0-F9AakdoN-sSE63IiXqGTBQ.

and financial records.[36] Because the model schedules do not cover all types of records, "state agencies must develop retention schedules with the archives to authorize legal retention and destruction of those records."[37] Similar to the Colorado Uniform Records Retention Act, the State Archives Law governs only the retention of public records but does not provide an avenue for the public to request access to those records, which is the exclusive province of the CORA.

III. Disappearing and Encrypted Messaging Apps

a. Overview of Confide and Signal

Ephemeral and encrypted messaging apps are becoming more prevalent given their ability to delete messages and keep communications private. Two components distinguishing these messaging applications "from other electronic communication media are: (1) automated disposition of message content on the sender's application *and* that of the recipient; and (2) E2E (end-to-end) encryption functionality."[38] The ability of these applications to automatically delete messages results in the deletion of the underlying metadata.[39] Additionally, "[e]ncryption involves the use of cryptography to take a plain text and, through use of keys and algorithms, transforms that plain text into coded text that cannot be read."[40] The combination of disposition of content and encryption results in no maintained record of communications.

Two commonly used disappearing messaging apps are Confide[tm] and Signal[tm]. These apps promote themselves by highlighting their privacy and secrecy components. Confide claims that through the use of "encrypted, self-destructing, and screenshot-proof messages, [it] gives you the comfort of knowing that your private communication will now truly stay that way," and the confidential nature of the app allows users to "[d]iscuss sensitive topics, brainstorm ideas or

[36] *State Agency Records Management*, COLORADO STATE ARCHIVES, https://archives.colorado.gov/records-management/state-agency-records-management (last visited Mar. 29, 2023).
[37] *State Agency Records Management*, COLORADO STATE ARCHIVES, https://archives.colorado.gov/records-management/state-agency-records-management (last visited Mar. 29, 2023).
[38] The Sedona Conference, *The Sedona Conference Commentary of Ephemeral Messaging*, 22 SEDONA CONF. J., 437, 446 (2021).
[39] The Sedona Conference, *The Sedona Conference Commentary of Ephemeral Messaging*, 22 SEDONA CONF. J., 437, 446 (2021).
[40] The Sedona Conference, *The Sedona Conference Commentary of Ephemeral Messaging*, 22 SEDONA CONF. J., 437, 447 (2021).

give unfiltered opinions without fear of the Internet's permanent, digital record and with no copies left behind."[41] Confide "prevents anyone from saving, forwarding, printing or taking a screenshot of the message."[42] Similarly, Signal promotes its "[s]tate-of-the-art end-to-end encryption… [that] keeps your conversations secure," and emphasizes privacy because the company and the public cannot read your messages or listen to your calls.[43]

While Confide and Signal both use encryption methods, there are slight differences between them. Confide messages are deleted immediately upon opening them; Signal allows users to set a timer and determine how long the messages are retained after opening them.[44] Despite minor differences, both apps have the same essential purpose of enabling the sending and receiving of encrypted messages that can "self-destruct" or evaporate, automatically, to avoid preservation of the communications.

b. Limits on the Use of Encrypted Messaging Apps in Federal Agencies

The concern surrounding the use of disappearing messaging apps goes beyond the impact this technology has on compliance with open records laws. The Securities and Exchange Commission (SEC), for example, "specifically prohibit[s]" registered investment advisors from using "apps and other technologies that can be readily misused by allowing an employee to send messages or otherwise communicate anonymously, allowing for automatic destruction of messages, or prohibiting third-party viewing or back-up."[45] The prohibition is an effort to enforce compliance with Advisers Act Rule 204-2, which "requires advisers to make and keep certain books and records relating to their investment advisory business, including typical accounting and other business records as required by the Commission."[46]

---

[41] CONFIDE, https://getconfide.com (last visited Mar. 29, 2023).
[42] Jason Hancock, *Appeals Court Hears Arguments Over Greitens' Use of Self-Destructing Text Message App*, MISSOURI INDEPENDENT (May 16, 2022), https://missouriindependent.com/2022/05/16/appeals-court-hears-arguments-over-greitens-use-of-self-destructing-text-message-app/.
[43] SIGNAL, https://signal.org/#signal (last visited Mar. 29, 2023).
[44] Robert W. Wilkins, *Client Litigation Risks When Using Ephemeral Messaging Apps*, JONES FOSTER (Mar. 5, 2020), https://jonesfoster.com/our-perspective/pbcba-messaging-app-article.
[45] Office of Compliance Inspections and Examinations, *Observations from Investment Adviser Examinations Relating to Electronic Messaging*, SECURITIES AND EXCHANGE COMMISSION, https://www.sec.gov/files/OCIE%20Risk%20Alert%20-%20Electronic%20Messaging.pdf (Apr. 19, 2023).
[46] Office of Compliance Inspections and Examinations, *Observations from Investment Adviser Examinations Relating to Electronic Messaging*, SECURITIES AND EXCHANGE COMMISSION, https://www.sec.gov/files/OCIE%20Risk%20Alert%20-%20Electronic%20Messaging.pdf (Apr. 19, 2023).

The Department of Justice (DOJ) has also provided guidance on "how it will evaluate whether companies have implemented appropriate guidance and controls on the use of personal devices and third-party and ephemeral messaging platforms."[47] In contrast with the SEC's "hardline stance against the use of ephemeral messaging," the DOJ guidelines require a fact-specific analysis.[48] The DOJ, within the Foreign Corrupt Practices Act, instructs companies to implement

> appropriate guidance and controls on the use of personal communications and ephemeral messaging platforms that undermine the company's ability to appropriately retain business records or communications or otherwise comply with the company's document retention policies or legal obligations.[49]

New guidance from the DOJ states that, when evaluating whether a corporation's policies for investigating and reporting misconduct and violations of law, "prosecutors should consider a corporation's policies and procedures governing the use of personal devices, communications platforms, and messaging applications, including ephemeral messaging applications."[50] Specifically, the prosecutor should consider whether use of messaging applications — including ephemeral messaging apps — has impaired "the organization's compliance program or its ability to conduct internal investigations or respond to requests from prosecutors or civil enforcement or regulatory agencies."[51]

The guidelines implemented by both the SEC and the DOJ demonstrate that concerns regarding the use of disappearing messaging apps for official business are prevalent throughout governmental agencies. They make it clear that the concern of such use by public officials to evade transparency laws is more than superficial.

---

[47] Vinson & Elkins LLP, *Updated DOJ Guidance on Devices and Ephemeral Messaging*, LEGOLOGY (MAR. 16, 2023), https://www.lexology.com/library/detail.aspx?g=a454c972-b6cb-42da-b6cc-2b9919da385a.
[48] Vinson & Elkins LLP, *Updated DOJ Guidance on Devices and Ephemeral Messaging*, LEGOLOGY (MAR. 16, 2023), https://www.lexology.com/library/detail.aspx?g=a454c972-b6cb-42da-b6cc-2b9919da385a.
[49] 15 U.S.C. §§ 78dd-1, et seq.9-47.120 - FCPA Corporate Enforcement Policy - https://www.justice.gov/jm/jm-9-47000-foreign-corrupt-practices-act-1977
[50] DEPARTMENT OF JUSTICE: CRIMINAL DIVISION, EVALUATION OF CORPORATE COMPLIANCE PROGRAMS 17 (Mar. 2023), https://www.justice.gov/criminal-fraud/page/file/937501/download.
[51] DEPARTMENT OF JUSTICE: CRIMINAL DIVISION, EVALUATION OF CORPORATE COMPLIANCE PROGRAMS 17 (Mar. 2023), https://www.justice.gov/criminal-fraud/page/file/937501/download.

c. Use of Disappearing and Encrypted Messaging Apps by Public Officials

The use of disappearing and encrypted messaging apps such as Confide and Signal has become prevalent among public officials across the country. There may well be valid reasons, in certain circumstances, for public officials to use encryption apps.[52] For example, when public officials are traveling outside of the United States, they rely on their communications being encrypted because "any other country could lawfully eavesdrop on anything [these officials] are doing on their cellphones."[53] However, inside the United States, where such foreign surveillance technology is far less present, public officials appear to be using encryption and automatic deletion apps not to avoid the interception of their communications, but to evade states' open records laws.[54] It follows then, while there are legitimate uses for these encryption apps, the public cannot be expected "to just trust that [state and federal elected officials] are not using this encrypted capability to [avoid the application of] open records laws."[55]

According to a news report from 2019, nearly a third of Colorado legislators were using either Confide or Signal at that time.[56] Political staffers and other Colorado public officials also were found to be using these apps.[57]

Much more recently, in July 2023, two Colorado lawmakers filed a lawsuit against the state House of Representatives and the Democratic and Republican House caucuses, alleging in part that legislators' regular use of Signal to discuss public business amongst themselves — outside of public view — violated the Colorado Open Meetings Law,[58] which declares that "all meetings of two or more members of any state public body at which any public business is discussed" are "public meetings open to the public at all times."[59] These electronic communications "were not available to the public for contemporaneous observation and were set for automatic deletion via a disappearing messages function." Further, "[t]he self-

[52] On-background interviews with Colorado journalists.
[53] On-background interviews with Colorado journalists.
[54] On-background interviews with Colorado journalists.
[55] On-background interviews with Colorado journalists.
[56] Alex Burness, *Holes in Colorado Open Records Law Grow as Technology Changes*, DENVER POST, https://www.denverpost.com/2019/10/26/colorado-open-records-confide-signal/ (October 26, 2019, 9:08 AM).
[57] Alex Burness, *Holes in Colorado Open Records Law Grow as Technology Changes*, DENVER POST, https://www.denverpost.com/2019/10/26/colorado-open-records-confide-signal/ (October 26, 2019, 9:08 AM).
[58] Epps and Marshall v. Colorado House of Representatives, Denver District Court (2023).
[59] COLO. REV. STAT. § 24-6-402(2)(a) (Colorado Open Meetings Law);

destructing writings transmitted among House members were not retained, and therefore were not available for public inspection as is required by the Colorado Open Records Act."[60]

Additionally, Colorado journalists interviewed on background for this paper provided the names of dozens of state legislators, legislative staffers and state agency officials and staffers, including some in the governor's office, who appear in their Signal contacts.[61]

In 2022, Maryland governor Larry Hogan and his administration "were found to be using a messaging app that deletes messages after 24 hours, keeping his internal communications with staff members private and out of the state archives."[62] The governor's office was communicating on a different end-to-end encryption app called Wickr and the "[c]hat rooms used by Hogan were set to a timer called 'Burn-on-Read' which deletes the messages after 24 hours."[63] The messages showed that Hogan was discussing a wide range of topics that would have otherwise been subject to document production laws "including the state's response to the pandemic, coordinating with staffers and complaining about media."[64]

In 2017, it was alleged that the former Missouri governor, Eric Greitens, and his staff were communicating through Confide, allowing them to circumvent Missouri's transparency laws.[65] The lawsuit was premised on arguments that "Greitens conspired to destroy records to ensure they could not be produced pursuant to an open records request."[66] However, the attorney representing Greitens argued that no affirmative action was taken to destroy records because

[60] Epps and Marshall v. Colorado House of Representatives, Denver District Court (2023).
[61] On-background interviews with journalists.
[62] Brad Dress, *Hogan, Administration Found Disappearing Messaging App to Communicate with Staff*, THE HILL (January 1, 2022), https://thehill.com/regulation/administration/587856-hogan-administration-found-to-use-disappearing-messaging-app-to/.
[63] Brad Dress, *Hogan, Administration Found Disappearing Messaging App to Communicate with Staff*, THE HILL (January 1, 2022), https://thehill.com/regulation/administration/587856-hogan-administration-found-to-use-disappearing-messaging-app-to/.
[64] Brad Dress, *Hogan, Administration Found Disappearing Messaging App to Communicate with Staff*, THE HILL (January 1, 2022), https://thehill.com/regulation/administration/587856-hogan-administration-found-to-use-disappearing-messaging-app-to/.
[65] Jason Hancock, *Appeals Court Hears Arguments Over Greitens' Use of Self-Destructing Text Message App*, MISSOURI INDEPENDENT (May 16, 2022), https://missouriindependent.com/2022/05/16/appeals-court-hears-arguments-over-greitens-use-of-self-destructing-text-message-app/.
[66] Jason Hancock, *Appeals Court Hears Arguments Over Greitens' Use of Self-Destructing Text Message App*, MISSOURI INDEPENDENT (May 16, 2022), https://missouriindependent.com/2022/05/16/appeals-court-hears-arguments-over-greitens-use-of-self-destructing-text-message-app/.

the application used, Confide, prevented any records from being retained at all.[67] The court agreed with Greitens' attorney and held that the use of Confide did not violate Missouri's transparency laws because no record was kept.[68]

The prevalence of lawmakers and public officials using these platforms for official communications begs the question of whether such use is legal under state or federal transparency laws and how to implement changes to maintain both government transparency and an informed citizenry.

IV. Policy Issues Surrounding Public Officials' Use of Encryption Apps

The use of disappearing and encrypted messaging apps by public officials proves incredibly problematic for a number of reasons.

a. Use of Ephemeral Messaging Apps Eliminates Government Transparency

Most notably, the use eliminates an entire level of transparency and openness that public records laws are designed to provide. Open government laws are intended to ensure an informed citizenry,[69] but it is impossible to achieve that purpose when public officials evade disclosure requirements by the use of encrypted and disappearing messaging apps. Because messages and communications on encryption apps are not addressed by open records laws and, thus, are not subject to disclosure, it is enticing for public officials at both the state and federal levels to communicate through these apps and purposely avoid being within the bounds of open records laws. This actively creates an avenue for communications to be kept private when they would otherwise be available to the public upon filing a FOIA or state open records request. It also permits members of public bodies to engage in private conversations about public business that should otherwise be held in open forums under the requirements of state open meetings laws.

---

[67] Jason Hancock, *Appeals Court Hears Arguments Over Greitens' Use of Self-Destructing Text Message App*, MISSOURI INDEPENDENT (May 16, 2022), https://missouriindependent.com/2022/05/16/appeals-court-hears-arguments-over-greitens-use-of-self-destructing-text-message-app/.

[68] Sansone v. Governor of Mo., 648 S.W.3d 13, 21–23 (Mo. Ct. App. 2022).

[69] *See What is FOIA?*, FREEDOM OF INFORMATION ACT, https://www.foia.gov/about.html (last visited Mar. 25, 2023); *Guide to Colorado's Open Records and Open Meetings Laws*, COLORADO FREEDOM OF INFORMATION COALITION, https://coloradofoic.org/open-government-guide/ (last visited Mar. 30, 2023) (explaining that CORA allows the public to inspect public records of state agencies to create transparency).

Notably, public officials may communicate with one another in person or over the phone and keep those communications private because no writing memorializes the conversation.[70] However, if officials use technology that creates writing — including ephemeral messaging apps, email, or text — they cannot dispose of the written communications or have their devices dispose of the messages without affecting their availability under open records laws.

b. The Use of Ephemeral Messaging Apps Impedes Litigation

If state and federal laws are not amended to govern the use of encrypted messaging apps for official communications, there will be a continued impact on litigation. The use of these apps effectively slows and impedes litigation because there is an abundance of communications that are not discoverable as they are destroyed and never retained.[71] The common law duty to preserve evidence is well recognized federally and among the states.[72] It is well understood that "[t]he obligation to preserve evidence arises when the party has notice that the evidence is relevant to litigation or when a party should have known that the evidence may be relevant to future litigation."[73] While there is an obligation to preserve all evidence that is potentially relevant to pending litigation to prevent the spoliation of evidence,[74] and "even though [messages via] self-destruct apps fall within the scope of discovery",[75] deleted encrypted messages that should have been preserved are unrecoverable because no records of the

---

[70] *See e.g.*, COLO. REV. STAT. § 24-72-202(6)(a)(I) (2019) (defining "public record" as "all *writings* made, maintained, or kept by the state").

[71] Dalila Hoover, *Ephemeral Messaging Apps Users: Use Caution During Anticipated or Ongoing Litigation*, AMERICAN BAR ASSOCIATION (Feb. 28, 2020), https://www.americanbar.org/groups/litigation/committees/pretrial-practice-discovery/practice/2020/ephemeral-messaging-apps-users-use-caution-during-anticipated-or-ongoing-litigation/?login

> While [ephemeral messaging apps] offer substantial benefits for their corporate and individual users, they present unique discovery challenges that are inconsistent with the duty to preserve evidence because of their ephemeral features… Their use is likely to place many organizations at risk for failure to satisfy electronically stored information (ESI) preservation considering that a large portion of their workforce uses EMAs for business-related communications."

[72] Robert W. Wilkins, *Client Litigation Risks When Using Ephemeral Messaging Apps*, JONES FOSTER (Mar. 5, 2020), https://jonesfoster.com/our-perspective/pbcba-messaging-app-article.

[73] Zubulake v. UBS Warburg LLC, 220 F.R.D. 212, 216 (S.D.N.Y. 2003).

[74] Zubulake v. UBS Warburg LLC, 220 F.R.D. 212, 216 (S.D.N.Y. 2003) (quoting West v. Goodyear Tire & Rubber Co., 167 F.3d 776, 779 (2d Cir.1999)) (Spoliation is "the destruction or significant alteration of evidence, or the failure to preserve property for another's use as evidence in pending or reasonably foreseeable litigation.").

[75] Agnieszka McPeak, *Self-Destruct Apps: Spoliation by Design?*, 51 AKRON L. REV. 633, 640 (2018).

content exists.[76] With no records of communications, "there is less access to potentially relevant content in civil discovery."[77]

The issue of whether the use of encryption apps constitutes spoliation of evidence arose in 2018 ahead of the *Waymo v. Uber*[78] trial during the discovery process.[79] Waymo discovered that Uber employees were instructed to use an encryption app to discuss their self-driving technology efforts, which were the subject matter of the suit.[80] The judge presiding over the case ruled that Uber "could have reasonably expected that Google would file suit," and Waymo argued that "Uber preemptively covered its tracks, and in so doing, inappropriately interfered with legal proceedings by deleting evidence."[81] However, the judge did not directly claim the use of ephemeral messaging apps constituted spoliation; instead he stated that "while Waymo [could] mention in court that Uber used Wickr 'as a possible explanation for why Waymo [had] failed to turn up more evidence of misappropriation in this case,' it [could not] use that evidence to 'invite improper speculation [or] vilify Uber without proving much else.'"[82] While the judge did not directly find that Uber's actions constituted spoliation, "employers should

[76] Robert W. Wilkins, *Client Litigation Risks When Using Ephemeral Messaging Apps*, JONES FOSTER (Mar. 5, 2020), https://jonesfoster.com/our-perspective/pbcba-messaging-app-article; Agnieszka McPeak, *Self-Destruct Apps: Spoliation by Design?*, 51 AKRON L. REV. 633, 640 (2018).

[77] Agnieszka McPeak, *Self-Destruct Apps: Spoliation by Design?*, 51 AKRON L. REV. 633, 640 (2018).

[78] Waymo LLC v. Uber Techs. Inc., No. C 17-00939 WHA, 2018 WL 646701 (N.D. Cal. Jan. 30, 2018).

[79] Caroline O'Donovan, *The Legal Consequences of Sending Disappearing Messages at Work*, BUZZFEED NEWS (Feb. 1, 2018), https://www.buzzfeednews.com/article/carolineodonovan/waymo-uber-wickr-ephemeral-messaging-apps-ruling.

[80] Caroline O'Donovan, *The Legal Consequences of Sending Disappearing Messages at Work*, BUZZFEED NEWS (Feb. 1, 2018), https://www.buzzfeednews.com/article/carolineodonovan/waymo-uber-wickr-ephemeral-messaging-apps-ruling.

[81] Caroline O'Donovan, *The Legal Consequences of Sending Disappearing Messages at Work*, BUZZFEED NEWS (Feb. 1, 2018), https://www.buzzfeednews.com/article/carolineodonovan/waymo-uber-wickr-ephemeral-messaging-apps-ruling; Waymo LLC v. Uber Techs. Inc., No. C 17-00939 WHA, 2018 WL 646701, at *15 (N.D. Cal. Jan. 30, 2018) ("[T]he record clearly shows (and this order finds) not only that a reasonable party in Uber's circumstances would have reasonably foreseen this litigation in January 2016, but also that Uber *actually* foresaw this litigation in January 2016 when it commenced the process of acquiring Otto.").

[82] Caroline O'Donovan, *The Legal Consequences of Sending Disappearing Messages at Work*, BUZZFEED NEWS (Feb. 1, 2018), https://www.buzzfeednews.com/article/carolineodonovan/waymo-uber-wickr-ephemeral-messaging-apps-ruling; Waymo LLC v. Uber Techs. Inc., No. C 17-00939 WHA, 2018 WL 646701, at *3 (N.D. Cal. Jan. 30, 2018) ("[E]vidence of Uber's litigation misconduct or other bad behavior may be relevant and admissible insofar as it reasonably bears on actual claims and defenses in this case… Such evidence will *not* be permitted, however, to the extent that it becomes cumulative, invites improper speculation, vilifies Uber without proving much else, or threatens to overwhelm the trial and distract from the merits of the case.").

nonetheless take the order as a warning when it comes to using ephemeral messaging apps at work" and recognize the risk in using such apps.[83]

In another case, *FTC v. Nolan*,[84] the Federal Trade Commission motioned for spoliation sanctions because the defendant began using Signal to hide evidence after being made aware of an impending subpoena.[85] The court again did not directly find spoliation of evidence but issued a general adverse inference against the defendant.[86] Additionally, the court held that the defendant demonstrated an intent to deprive and violated their preservation duty because "the plaintiff asked the defendants to suspend any deletion of relevant data and the defendants intentionally disobeyed."[87] The courts' holdings from both *Waymo v. Uber* and *FTC v. Nolan* demonstrate that this problem could arise in all types of litigation, but specifically may arise in cases regarding government transparency and compliance with state open records laws, as evidenced in *Sansone v. Governor of Missouri*,[88] which will be discussed in Section V.

It is important to note that "[w]hile companies should not be permitted to use ephemeral apps in bad faith to destroy or conceal relevant business records, communicating via ephemeral app alone is not improper."[89] However, there is a concern that "businesses will use ephemeral apps to impede discovery of potentially damaging records,"[90] which reflects the concern that public officials may use ephemeral messaging to evade the open records laws.

---

[83] Caroline O'Donovan, *The Legal Consequences of Sending Disappearing Messages at Work*, BUZZFEED NEWS (Feb. 1, 2018), https://www.buzzfeednews.com/article/carolineodonovan/waymo-uber-wickr-ephemeral-messaging-apps-ruling.

[84] Fed. Trade Comm'n v. Noland, No. CV-20-00047-PHX-DWL, 2021 WL 3857413 (D. Ariz. Aug. 30, 2021).

[85] Mike Hamilton, *Case Law Alert: Use of Ephemeral Messaging Leads to Adverse Inference Sanction*, EXTERRO (Mar. 11, 2022), https://www.exterro.com/blog/case-law-alert-use-of-ephemeral-messaging-leads-to-adverse-inference-sanction.

[86] Mike Hamilton, *Case Law Alert: Use of Ephemeral Messaging Leads to Adverse Inference Sanction*, EXTERRO (Mar. 11, 2022), https://www.exterro.com/blog/case-law-alert-use-of-ephemeral-messaging-leads-to-adverse-inference-sanction; Fed. Trade Comm'n v. Noland, No. CV-20-00047-PHX-DWL, 2021 WL 3857413, at *12 (D. Ariz. Aug. 30, 2021) ("The FTC has easily carried its burden of showing that the Individual Defendants acted with the intent to deprive the FTC of the information contained in the Signal and ProtonMail messages. The most decisive factor is the timing of the installation and use of Signal and ProtonMail. The Individual Defendants installed these apps in late May 2019, *one day* after Noland discovered the FTC was investigating him and SBH.").

[87] Mike Hamilton, *Case Law Alert: Use of Ephemeral Messaging Leads to Adverse Inference Sanction*, EXTERRO (Mar. 11, 2022), https://www.exterro.com/blog/case-law-alert-use-of-ephemeral-messaging-leads-to-adverse-inference-sanction.

[88] Sansone v. Governor of Mo., 648 S.W.3d 13 (Mo. Ct. App. 2022).

[89] Agnieszka McPeak, *Self-Destruct Apps: Spoliation by Design?*, 51 AKRON L. REV. 633, 644 (2018).

[90] Agnieszka McPeak, *Self-Destruct Apps: Spoliation by Design?*, 51 AKRON L. REV. 633, 644 (2018).

V. Current Legal Landscape

While FOIA and state open records laws govern the production of agency documents, these laws did not contemplate certain technological advancements and how they would impact the efficacy of document production when they were enacted. Document production laws did not consider the development of messaging apps that erase messages upon delivery which prevents the retention of those communications. Accordingly, transparency laws do not address the legality of federal and state governments using these apps for official communications. Although most states have not addressed this problem, a few states have recently touched on the legality of public officials using disappearing and encrypted messaging apps.

a. Michigan House Bill 4778

In 2021, Michigan enacted new legislation that directly addressed the issue of state departments and agencies using encryption apps or software.[91] Michigan House Bill 4778 declares that "all state departments and all state agencies must not use any app, software, or other technology that prevents it from maintaining or preserving a public record as required by law on an electronic device that is used to create a public record."[92] The Michigan legislature passed the bill for the purpose of banning the use of text messaging encryption apps on state-issued phones as a method of evading the Michigan Freedom of Information Act.[93] The bill is the first piece of legislation in the United States to directly address the issue of disappearing messaging apps being used for official communications and establish that such use is in violation of state laws.

b. District of Columbia Bill 24-0692

On March 1, 2022, the District of Columbia passed Bill 24-0692[94] emphasizing "that communications created or received electronically in the course of official business are subject

[91] *See* H.B. 4778, 101st Leg., Reg. Sess. (Mich. 2021).
[92] H.B. 4778, 101st Leg., Reg. Sess. (Mich. 2021).
[93] *See* H.B. 4778, 101st Leg., Reg. Sess. (Mich. 2021).
[94] B. 24-0692, 24th Council (D.C. 2022) (amending provisions codified at D.C. CODE §§ 2-1701(13), 2-1706(a)(1)).

to existing record retention obligations."[95] The bill focused on encryption apps and found that the use of such apps "with their ability to destroy or delete communications or keep them hidden or obscured, is contrary to the District's emphasis on governmental transparency, and makes public access to these records significantly more difficult, if not impossible (in cases where certain communications are deleted)."[96] Recognizing the negative impact on governmental transparency, the Bill amended the District of Columbia Public Records Management Act (PMRA) to clarify that "public records" under the PMRA include "electronic mail or other communications transmitted electronically, including through any electronic messaging service."[97] Section 2-1706(a)(1) of the PMRA was also amended to require that

> [a]ny record created or received by the District in the course of official business, including records created or received electronically, is the property of the District and…shall not be destroyed, sold, transferred, or disposed of in any manner, including through the enabling of settings on electronic devices that allow for the non-retention or automatic deletion of records.[98]

These amendments effectively provide that any official communications through encrypted messaging apps are "public records" under the PMRA and such messages cannot be destroyed or disposed of.[99]

Prior to the amendments, communications via ephemeral messaging apps allowed public bodies to evade D.C. FOIA. "Since public bodies cannot deliver what they do not retain, the use of *ephemeral* texting indirectly circumvents D.C. FOIA by effectively treating a written conversation as a phone call," since the "writing" is eradicated as soon as the parties

[95] Niquelle M. Allen, Applicability of D.C. FOIA to Text Messaging, Off. of Open Gov't, Op. No. 2022-001 (2022), https://www.open-dc.gov/sites/default/files/FOIA%20Advisory%20Opinion_Text%20Messages_OOG%202022-001_03162022.pdf.
[96] Niquelle M. Allen, Applicability of D.C. FOIA to Text Messaging, Off. of Open Gov't, Op. No. 2022-001 (2022), https://www.open-dc.gov/sites/default/files/FOIA%20Advisory%20Opinion_Text%20Messages_OOG%202022-001_03162022.pdf.
[97] D.C. CODE § 2-1701(13).
[98] D.C. CODE § 2-1706(a)(1).
[99] Niquelle M. Allen, Applicability of D.C. FOIA to Text Messaging, Off. of Open Gov't, Op. No. 2022-001 (2022), https://www.open-dc.gov/sites/default/files/FOIA%20Advisory%20Opinion_Text%20Messages_OOG%202022-001_03162022.pdf.

disconnect.[100] Additionally, there is even less of a trace of communication via encryption apps; while phone records provide evidence that some communication took place, these ephemeral apps keep no records of communications whatsoever. Accordingly, the Office of Open Government Advisory Opinion recommends that the District of Columbia prohibit "the use of ephemeral messaging applications to conduct District government business"[101] because "[m]odernization and innovation in technology should be used to create and retain *more*, not less, transparency in the spaces where public officials and employees exercise public trust."[102]

c. Missouri: *Sansone v. Governor of Missouri*

In 2022, the Missouri Court of Appeals for the Western District addressed the issue of public officials' use of encrypted messaging apps. In *Sansone v. Governor of Missouri*,[103] the governor's office was requested to provide all documents or phone records showing that the governor or any of his employees downloaded or used any application that automatically destroys messages or other forms of communication after the communication is sent or received.[104] Additionally, the governor's office was asked to produce all messages sent or received by the governor or his employees using a disappearing messaging application.[105] In response to these requests, the governor's office explained that these documents could not be produced because the applications do not allow the recipient to "retain opened messages; sent messages are deleted from the sender's phone upon the opening of a new message; and the last unopened sent message is no longer on the sender's phone after 48 hours."[106] In analyzing the issue, the court stated that the Missouri Sunshine Law "only requires that governmental agencies provide access to records then in existence, and in the agencies' possession or under

[100] Niquelle M. Allen, Applicability of D.C. FOIA to Text Messaging, Off. of Open Gov't, Op. No. 2022-001 (2022), https://www.open-dc.gov/sites/default/files/FOIA%20Advisory%20Opinion_Text%20Messages_OOG%202022-001_03162022.pdf.
[101] Niquelle M. Allen, Applicability of D.C. FOIA to Text Messaging, Off. of Open Gov't, Op. No. 2022-001 (2022), https://www.open-dc.gov/sites/default/files/FOIA%20Advisory%20Opinion_Text%20Messages_OOG%202022-001_03162022.pdf.
[102] Niquelle M. Allen, Applicability of D.C. FOIA to Text Messaging, Off. of Open Gov't, Op. No. 2022-001 (2022), https://www.open-dc.gov/sites/default/files/FOIA%20Advisory%20Opinion_Text%20Messages_OOG%202022-001_03162022.pdf.
[103] Sansone v. Governor of Mo., 648 S.W.3d 13 (Mo. Ct. App. 2022).
[104] Sansone v. Governor of Mo., 648 S.W.3d 13, 16 (Mo. Ct. App. 2022).
[105] Sansone v. Governor of Mo., 648 S.W.3d 13, 16 (Mo. Ct. App. 2022).
[106] Sansone v. Governor of Mo., 648 S.W.3d 13, 18 (Mo. Ct. App. 2022).

their control," so if records are never possessed or controlled by an agency they are not governed by the law.[107] The court held that the messages were never officially retained because they were automatically deleted by the Confide application, so the messages were not considered public records under the state's sunshine laws.[108]

The court's reasoning indicates that the use of any disappearing or encrypted messaging apps by Missouri public officials will not be in violation of the state's sunshine laws. While this may seem aligned with the Missouri Sunshine Law because the documents were never "retained," this holding allows public officials to avoiding producing official communications that would otherwise be subject to the Sunshine Law (if communicated via email or text message) and available to the public. This outcome is problematic as open document laws are intended to keep the public apprised of official communications and actions of the government.

d. Texas Senate Bill 944

In 2019, a Texas law went into effect requiring government officials to preserve text messages sent from or received on their personal devices that concern public or official business.[109] The purpose of the bill, which is an amendment to the Texas Public Information Act (PIA), was to ensure that an employee of a "governmental agency who creates or receives records on a privately-owned device or account provides that information to the government's public information officer… [to] protect[] that information and ensur[e][] transparency."[110] Section 552.004 of the PIA now states that

> (b) a current or former officer or employee of a governmental body who maintains public information on a privately owned device shall: (1) forward or transfer the public information to the governmental body or a governmental body server to be preserved as provided by subsection (a); or (2) preserve the public information in its original form in a backup or archive and on the privately owned device for the time described under subsection (a).[111]

[107] Sansone v. Governor of Mo., 648 S.W.3d 13, 22 (Mo. Ct. App. 2022).
[108] Sansone v. Governor of Mo., 648 S.W.3d 13, 21–23 (Mo. Ct. App. 2022).
[109] *See* S.B. 944, 86th Leg., Reg. Sess. (Tex. 2019).
[110] *FAQ: How Does S.B. 944 Affect Us?*, THE TEXAS RECORD (Sept. 6, 2019), https://www.tsl.texas.gov/slrm/blog/2019/09/faq-how-does-s-b-944-affect-us/.
[111] Texas S.B. No. 944, Sec. 522.004(b).

Additionally, the amendment requires that "if an officer or employee possesses records on a personal device that have not been provided to the government's control, they must surrender or return that information to the governmental body not later than the 10th day" after a public information officer requests that information to be surrendered.[112] In response to the new state law, some cities and counties in Texas have enacted their own policies that align with the law. For example, public employees in Brazos County are required "to use county-issued cellphones equipped with Smarsh software that archives text messages and makes them searchable if they need to be provided in response to open records requests."[113]

While Senate Bill 944 requires records on an official's personal device to be turned over upon request, it does not directly solve the issue of public officials using disappearing messaging apps. Even under the new amendment, an official may use a disappearing messaging app, and the messages may not be considered "records" under the ruling of a Texas court if the judge holds that the records were never kept and are not subject to the Act.

e. Kansas Executive Order 18–06

In 2018, the former Kansas governor, Jeff Colyer, signed an executive order intended to "promote executive branch transparency… that… require[s] employees in the governor's office to use official email accounts to perform state business."[114] The executive order requires all officers and employees of the Office of the Governor to execute the Policy Regarding Use of Private email Accounts.[115] The policy requires that

> [a]ll officers and employees within the Office of the Governor shall conduct official state business only on their official State of Kansas e-mail accounts. If a message regarding official state business is received on a private e-mail account, that message should immediately be forwarded to the recipient's official e-mail account, and the sender of the message should be notified that the recipient's official e-mail account is the proper address for official state business.[116]

---

[112] *FAQ: How Does S.B. 944 Affect Us?*, THE TEXAS RECORD (Sept. 6, 2019), https://www.tsl.texas.gov/slrm/blog/2019/09/faq-how-does-s-b-944-affect-us/.
[113] Jeffrey A. Roberts, *Private-Messaging Apps CORA's Accountability Mandate*, COLORADO FREEDOM OF INFORMATION COALITION (Nov. 7, 2019), https://coloradofoic.org/private-messaging-apps-undermine-coras-accountability-mandate/.
[114] Tim Carpenter, *Colyer Signs Four Executive Orders to Improve Transparency*, TOPEKA CAPITAL-JOURNAL, https://www.cjonline.com/story/news/politics/state/2018/02/08/gov-jeff-colyer-signs-four-executive-orders-to-improve-openness-to-executive-branch/15282076007/ (Feb. 8, 2018, 11:27 PM).
[115] Executive Order 18-06 (Kan. 2018), https://kslib.info/DocumentCenter/View/6889/EO-18-06?bidId=.
[116] Executive Order 18-06 (Kan. 2018), https://kslib.info/DocumentCenter/View/6889/EO-18-06?bidId=.

Furthermore, "[a]ll officers and employees within the Office of the Governor shall not use private e-mail accounts to conduct official state business, except in the event of a failure or outage of official e-mail accounts."[117] Tangentially, this executive order addresses use of disappearing messaging apps by employees within the office of the governor in Kansas. Given that the policy requires all employees to conduct official business on their official state email accounts, any use of a disappearing or encrypted messaging app for official business would be in violation of the executive order.

As evidenced by the above discussion, some states have taken steps in the right direction by requiring public officials to conduct official business on official email accounts or requiring the retention of official communications that are conducted on personal devices. However, the only state that has directly addressed the issue in a straightforward way is Michigan with House Bill 4778. Outside of the examples of new legislation from the District of Columbia, Texas, Michigan, and Kansas, the majority of states have taken no steps to address the issue in any capacity. With the language in most open records laws, courts would likely reach the same conclusion as *Sansone v. Governor of Missouri* and find that communications on disappearing messaging apps like Confide or Signal are not covered by open records laws because the records were never actually "retained."

VI. Colorado: Legality of Use Under Transparency Laws and Prevalence of Use

a. Colorado Transparency Laws Do Not Address Messaging Via Encryption Apps

The Colorado Open Records Act does not address the legality of using disappearing or encrypted messaging apps. CORA acknowledges that some electronic records are considered public records and subject to disclosure under the act, but there is no further guidance on what procedures must be followed.[118] Section 203 of CORA requires agencies to adopt policies "regarding the retention, archiving, and destruction" of digital records, but it does not specify how long those records must be retained.[119] Moreover, as discussed above in Section II(b),

[117] Executive Order 18-06 (Kan. 2018), https://kslib.info/DocumentCenter/View/6889/EO-18-06?bidId=.
[118] Alex Burness, *Holes in Colorado Open Records Law Grow as Technology Changes*, DENVER POST, https://www.denverpost.com/2019/10/26/colorado-open-records-confide-signal/ (October 26, 2019, 9:08 AM).
[119] COLO. REV. STAT. § 24-72-203(b)(I) (2019).

neither the Colorado Uniform Records Retention Act nor the Colorado State Archives Law addresses the issue and legality of whether communication via disappearing or encrypted messaging apps constitute records and therefore must be retained. Accordingly, while electronic records must be kept, if those records do not exist because they are immediately deleted upon receipt with the use of a disappearing messaging app, Colorado courts would likely hold, like in *Sansone v. Governor of Missouri*, that CORA does not apply because there was never a retained public record. With this outcome, the purpose of CORA is diminished because there is no government transparency.[120]

b. Prevalence of the Use of Encryption Apps in Colorado

Unfortunately, the problems that arise from the use of encryption apps are not theoretical; the use of disappearing messaging apps is prevalent among Colorado legislators and other public officials. As discussed in Section III(c), nearly a third of Colorado legislators were using Confide or Signal in 2019,[121] and journalists more recently have found dozens of state lawmakers, other elected officials and government staffers in their Signal address books.[122] The previously referenced lawsuit filed by Representatives Elisabeth Epps and Robert Marshall alleges that "both the Democratic and Republican Caucuses (of the Colorado House) utilized Signal to discuss public business outside of public view."[123]

In response to the knowledge of certain Colorado public officials and lawmakers having accounts on Confide or Signal, the Colorado Freedom of Information Coalition (CFOIC) submitted CORA requests to the Governor, Secretary of State, Attorney General and Denver Mayor offices to try to ascertain how these apps are used.[124] However, the CFOIC was met with either no response to its requests, a response of "no responsive records" or a response requiring an extremely steep payment for the production of the requested records.[125] The responses to these CORA requests demonstrate both the inaccessibility of the open records

[120] Alex Burness, *Holes in Colorado Open Records Law Grow as Technology Changes*, DENVER POST, https://www.denverpost.com/2019/10/26/colorado-open-records-confide-signal/ (October 26, 2019, 9:08 AM).
[121] Alex Burness, *Holes in Colorado Open Records Law Grow as Technology Changes*, DENVER POST, https://www.denverpost.com/2019/10/26/colorado-open-records-confide-signal/ (October 26, 2019, 9:08 AM).
[122] On-background interviews with journalists.
[123] Epps and Marshall v. Colorado House of Representatives, Denver District Court (2023).
[124] Colorado Freedom of Information Coalition CORA requests.
[125] Colorado Freedom of Information Coalition CORA requests.

laws, indicated by the payment required to obtain records, and the difficulty in obtaining records on the use of disappearing messaging apps, if any such records may exist.

While simply having Signal or Confide does not guarantee that public officials are having official communications on these apps, there is no way to assure the public that official business is not being discussed. Furthermore, the Colorado Open Meetings Law, which is part of the state Sunshine Law, states that "[a]ll meetings of two or more members of any state public body at which any public business is discussed or at which any formal action may be taken are declared to be public meetings open to the public at all times."[126] Accordingly, any communication by two or more members of a state public body (or for a local public body, a quorum or three or more members, whichever is fewer)[127] on an encrypted messaging app is in violation of the Colorado transparency laws if it concerns public business. The public would have no knowledge of these communications nor the ability to access the records. With that in mind, despite the legitimate reasons for legislators and public officials to use these apps for personal communications, the public deserves more certainty and transparency from its elected officials and should not have to question whether encryption apps are being used to avoid disclosure requirements.

VII. Colorado Recommendation

The Colorado Open Records Act requires the production of requested public records by state and local government entities unless the records fall under certain exceptions in the law. However, if those records do not exist because they are immediately deleted upon receipt, Colorado courts would likely hold that CORA does not apply because a public record was never

[126] COLO. REV. STAT. § 24-6-402(2)(a) (2019).

[127] *See, e.g.*, DENVER, COLO., MUN. CODE, ch. 2, art. III, § 2-32(b) (defining a meeting as "[a]ny assemblage of a quorum of any public body, whether in person, electronically, or by other means of communication, whose central purpose is the discussion of public business or the adoption of any proposed policy, position, resolution, rule, regulation, standard, ordinance, or other official action or enactment. The term "quorum" shall mean that portion of a public body defined by its by-laws or rules as the minimum number of its members who must be present at a meeting for business to be transacted legally."); § 2-33(a) (requiring all meetings to be open to the public). Accordingly, under the Municipal Code of the City and County of Denver, any city or county meeting must be open to the public, so communication via encryption apps would be in violation of the code.

retained. This loophole allows public officials to avoid accountability mechanisms imposed by CORA and the Colorado Open Meetings Law.

Accordingly, new legislation should be enacted to directly address this issue and curtail the use of these apps by public officials. As discussed in Section V(a), Michigan House Bill 4778 is currently the only piece of state legislation to directly address this issue, making it a violation of the law for public officials to use encryption apps for official communications.[128] Accordingly, language that mirrors the Michigan legislation, while also including elected officials, would make it illegal for Colorado public officials to use encrypted messaging apps for official business. The following language, nearly identical to that of Michigan House Bill 4778, would address the issue head-on and prevent public officials from using encryption apps to evade the requirements of Colorado transparency laws:

All state and local departments, all state and local government entities, and all elected and appointed officials of state and local government entities, agencies and public bodies must not use any app, software, or other technology that prevents it from maintaining or preserving a public record as required by law on an electronic device that is used to create a public record.

VIII. Conclusion

Public officials' use of disappearing and encrypted messaging apps has thwarted the purpose of state and federal transparency laws by allowing communications to evade being "kept" under these laws and thereby eliminating the ability of the public to access otherwise producible public records. The use of these apps by members of public bodies may also circumvent the requirements of open meetings laws. Currently, only a handful of states have addressed the legality of the use of encryption apps by public officials. Colorado, however, has not addressed this problem. CORA, the Uniform Records Retention Act, and the State Archives Statute do not address the legality of public officials using these apps or whether communications via these apps are considered "records." Accordingly, Colorado should enact

[128] H.B. 4778, 101st Leg., Reg. Sess. (Mich. 2021).

new legislation, a broadened version of Michigan House Bill 4778, making it a violation of state law for public officials to use any encrypted or disappearing messaging apps for official business.