Concordia Law Review

Volume 4 | Number 1 Article 9

2019

Now You See It, Now You Don't: The Emerging Use of Ephemeral Messaging Apps by State and Local Government Officials

Kurt J. Starman
Concordia University School of Law

CONCORDIA LAW REVIEW

VOL. 4 **APRIL 2019** **NO. 1**

STUDENT COMMENTS

NOW YOU SEE IT, NOW YOU DON'T: THE EMERGING USE OF EPHEMERAL MESSAGING APPS BY STATE AND LOCAL GOVERNMENT OFFICIALS

Kurt J. Starman[*]

Public access to government-related information is essential in a democracy. The public expects state and local governments to function in an open and transparent manner to ensure accountability. All fifty states have adopted statutes that provide public access to government-related information. However, these statutes have not kept pace with changing technology. The emerging use of ephemeral messaging apps by state and local government officials presents an especially difficult problem. Ephemeral messaging apps are typically used on personal electronic devices, such as privately-owned smartphones. Unlike traditional text messages, however, ephemeral messages cannot be stored and subsequently accessed by the public. Rather, ephemeral messages self-destruct shortly after they are accessed by the recipient. Thus, it is not clear if ephemeral messages are public records—even if the messages pertain to government-related actions. A pending lawsuit in Missouri that pertains to the use of an ephemeral messaging app by former Governor Eric Greitens and members of his staff may be the first case in the nation to address this issue at the state and local level. Two recent state supreme court decisions from California and Washington concluded that traditional text messages that pertain to government-related actions may be public records even when they are retained on personal electronic devices or on third-party servers. These court

[*] 2018-19 Associate Editor, Concordia Law Review. J.D. Candidate, Concordia University School of Law; M.P.A, University of Southern California; M.A. and B.A., California State University, Sacramento. The author first wishes to thank his wife, Jacquelyn, for her unwavering love and support. Additional thanks to Associate Professor Tenielle Fordyce-Ruff for her exceptional instruction on legal writing, as well as to Associate Dean Latonia Haney Keith and Associate Professor McKay Cunningham for their assistance throughout the writing process. Lastly, thanks to the editors of the Concordia Law Review for their hard work, dedication, and professionalism. Any errors are mine.

decisions may provide some useful guidance with respect to ephemeral messages, but there are some key distinctions between traditional text messages and ephemeral messages. To avoid ambiguity and litigation, state legislatures should revise their public records statutes to make it clear that ephemeral messages that pertain to government-related actions are public records. If ephemeral messages cannot be stored and retrieved to ensure public access to this information, state legislatures should restrict the use of ephemeral messaging apps by public officials.

INTRODUCTION

Public access to government-related information is crucial in a democracy. "The people insist on remaining informed [about government decisions] so that they may maintain control over the instruments that they have created."[1] Thus, it follows that state statutes that provide broad access to public records are essential. "Open records laws are critical tools that enable people to learn more about how public officials make decisions, and to hold them accountable."[2]

The federal government enacted the Freedom of Information Act in the 1960s to ensure public access to most federal records.[3] Since that time, "[a]ll 50 states also have [enacted] public records laws which allow members of the public . . . to obtain documents and other public records from state and local government bodies."[4] However, these state statutes have not kept pace with changing technology. As one author noted, "[t]echnology develops

[1] WASH. REV. CODE ANN. § 42.56.030 (West 2018).
[2] MICHAEL HALPERN, FREEDOM TO BULLY: HOW LAWS INTENDED TO FREE INFORMATION ARE USED TO HARASS RESEARCHERS 1 (2015).
[3] *See* 5 U.S.C.A. § 552 (effective June 30, 2016). This article pertains to state statutes that provide public access to state and local government records. The government website FOIA.gov provides an overview of the federal Freedom of Information Act. *See* FOIA.GOV, https://www.foia.gov/about.html (last visited March 16, 2019).
[4] FOIADVOCATES, http://foiadvocates.com/records.html (last visited March 16, 2019). FOIAdvocates assists the public with access to public records. "FOIAdvocates is a project of FOIA attorneys David Bahr [and] Daniel Stotter designed to assist the public in gaining access to records from federal, state and local governments using the federal Freedom of Information Act (FOIA) as well as state and local public records laws." *Id*.

faster than [the] law."[5] This has resulted in ambiguity and, in several instances, litigation.[6]

The emerging use of ephemeral messaging apps by public officials at the state and local level presents an especially difficult dilemma. "Ephemeral messaging is the mobile-to-mobile transmission of multimedia messages that automatically disappear from the recipient's screen after the message has been viewed."[7] In short, an ephemeral message "self-destructs" after the message is read by the recipient.[8] This feature "can be contrasted with [traditional] SMS text messaging and iMessage[s], both of which require the recipient to physically delete messages from the device."[9] Furthermore, ephemeral messaging apps, such as Confide, are typically used on privately-owned smartphones and do not generate a record that can be stored and subsequently accessed by the public.[10] Thus, it is not clear if ephemeral messages that are sent or received on a personal electronic device are public records even when the content pertains to government-related actions.[11]

This Comment examines the use of ephemeral messaging apps by public officials at the state and local level. More specifically, it analyzes whether ephemeral messages are subject to public disclosure under existing state statutes. Part I explores why, from a public policy perspective, states have adopted statutes to ensure public access to state and local government records.[12] It then examines public records statutes from California,[13]

---

[5] James Valvo, *Federal Records Law Must Keep Pace with Evolving Technology*, CAUSE ACTION INST. BLOG (Nov. 3, 2017), https://causeofaction.org/federal-records-law-must-keep-pace-evolving-technology/.

[6] *See* Helen Vera, *"Regardless of Physical Form": Legal and Practical Considerations Regarding the Application of State Open-Records Laws to Public Business Conducted by Text Message*, COMM. LAW., Spring 2017, at 24, 29–30 ("[I]n many states, public officials' denials of access to relevant text messages have been challenged in court.").

[7] Abhinav Jain, *Is Ephemeral Messaging the Future of Messaging?*, QUORA (Mar. 25, 2016), https://www.quora.com/Is-ephemeral-messaging-the-future-of-messaging.

[8] *See id.*

[9] *Id.*

[10] *See generally* CONFIDE, https://getconfide.com/ (last visited March 16, 2019) ("Discuss sensitive topics, brainstorm ideas or give unfiltered opinions without fear of the Internet's permanent, digital record and with no copies left behind.").

[11] *See, e.g.*, Jason Hancock, *Governor's Lawyer Argues Texts Automatically Deleted by App Aren't Public Records*, KAN. CITY STAR, June 19, 2018, https://www.kansascity.com/news/politics-government/article213445529.html.

[12] *See, e.g.*, City of San Jose v. Super. Ct. of Santa Clara Cty., 389 P.3d 848, 852 (Cal. 2017) ("Public access laws serve a crucial function.").

[13] *See generally* CAL. GOV'T CODE §§ 6250–6270.5 (West 2018).

Missouri,[14] and Washington[15] to highlight key features associated with typical public records laws.[16] Part I also addresses some of the conflicting concerns that public officials and open government advocates commonly voice regarding the use of personal electronic devices to send and receive traditional text messages that pertain to government actions.[17] Part I concludes with a brief overview of the emerging use of ephemeral messaging apps by state and local government officials.

Part II analyzes a current lawsuit in the State of Missouri involving an ephemeral messaging app used by state officials.[18] This section highlights the use of the ephemeral messaging app "Confide" by the former governor of the State of Missouri, Eric Greitens, and his staff.[19] Part II reviews the facts and legal issues associated with this litigation, with an emphasis on Missouri's Sunshine Law.[20]

Part III examines two recent state supreme court decisions from California and Washington: *City of San Jose v. Superior Court of Santa Clara County*[21] and *Nissen v. Pierce County*.[22] Both of these cases pertain to the use of traditional text messages on personal electronic devices by local government officials.[23] Traditional text messages are not identical to ephemeral messages; nevertheless, the holdings from *City of San Jose* and *Nissen* provide useful lessons that can be applied, at least in part, to ephemeral messages.[24]

---

[14] *See generally* MO. ANN. STAT. §§ 610.010–610.035 (West 2018).
[15] *See generally* WASH. REV. CODE ANN. §§ 42.56.001–42.56.904 (West 2108).
[16] *See* Vera, *supra* note 6, at 24 ("[E]very state also has some form of open-government law, most with similar scope.").
[17] *See generally* Joey Senat, *Whose Business is it: Is Public Business Conducted on Officials' Personal Electronic Devices Subject to State Open Records Laws?*, 19 COMM. L. & POL'Y 293 (2014) (examining the reasoning put forth to explain why text messages sent or received by public officials on personal electronic devices should or should not be considered public records).
[18] *See* Petition, Sansone v. Greitens, No. 17AC-CC0065 (Cir. Ct. of Cole Cty., Mo. filed Dec. 29, 2017).
[19] *See generally* DARRELL MOORE ET AL., FINAL REPORT: AGO INQUIRY INTO USE OF CONFIDE BY STAFF OF THE GOVERNOR'S OFFICE (2018) ("In late 2017, news media outlets reported that several senior members of the Governor's Office . . . had downloaded Confide to their personal phones. These reports resulted in speculation that the [Governor's Office] may have used Confide to transact public business.").
[20] *Id.; see also* MO. ANN. STAT. §§ 610.010–610.035 (West 2018).
[21] City of San Jose v. Super. Ct. of Santa Clara Cty., 389 P.3d 848 (Cal. 2017).
[22] Nissen v. Pierce Cty., 357 P.3d 45 (Wash. 2015).
[23] *See generally* City of San Jose, 389 P.3d 848; Nissen, 357 P.3d 45.
[24] *See generally* City of San Jose, 389 P.3d 848; Nissen, 357 P.3d 45.

Part IV utilizes the holdings from *City of San Jose* and *Nissen* to develop an analytical framework to determine whether ephemeral messages are subject to existing state public records laws. The Comment identifies six guidelines from *City of San Jose* and *Nissen* that are instructive for this analysis. The analysis in Part IV suggests that at least two of the guidelines from *City of San Jose* and *Nissen* arguably do not apply to ephemeral messages. Consequently, it is possible to make a reasonable argument that ephemeral messages are not covered by existing public records statutes.

Given the outcome of the analysis in Part IV, Part V asserts that there is a need to update and clarify existing public records statutes. Part V outlines public policy reasons that justify treating ephemeral messages as records subject to public disclosure. To ensure transparency, mitigate ambiguity, and reduce litigation, Part V recommends that state legislatures revise their public records statutes to explicitly address the use of ephemeral messaging apps. If it is not possible to retain and retrieve ephemeral messages that pertain to government-related actions, Part V asserts that state legislatures should restrict public officials from using ephemeral messaging apps to conduct the public's business altogether.

Similar concerns exist at the federal level as well, but those issues are beyond the scope of this Comment. As noted above, this Comment addresses the emerging use of ephemeral messaging apps by state and local government officials. Consequently, the analysis below is focused on state public records statutes.

I. IMPORTANCE OF PUBLIC ACCESS TO STATE AND LOCAL GOVERNMENT DOCUMENTS

Democracy demands that state and local governments operate in an open and forthright manner.[25] Citizens have a right to remain informed about government activity.[26] As the California Supreme Court noted:

> Public access laws serve a crucial function. "Openness in government is essential to the functioning of a democracy. 'Implicit in the democratic process is the notion that government should be accountable for its actions. In order to

[25] *See* City of San Jose, 389 P.3d at 852 ("[P]eople have the right of access to information concerning . . . the people's business . . . .").
[26] *See, e.g.*, WASH. REV. CODE ANN. § 42.56.030 (West 2018) ("The people insist on remaining informed . . . .").

> verify accountability, individuals must have access to government files. Such access permits checks against the arbitrary exercise of official power and secrecy in the political process.'"[27]

Open-government laws (frequently referred to as sunshine laws) recognize the importance of public access to state and local government documents. Missouri's Sunshine Law states, for example, that "[i]t is the public policy of this state that . . . records . . . of public governmental bodies be open to the public unless otherwise provided by law."[28] Similarly, the California Public Records Act states that "access to information concerning the conduct of the people's business is a fundamental and necessary right of every person . . . ."[29] The Washington Public Records Act states the case even more forcibly:

> The people . . . do not yield their sovereignty to the agencies that serve them. The people, in delegating authority, do not give their public servants the right to decide what is good for the people to know and what is not good for them to know. The people insist on remaining informed so that they may maintain control over the instruments that they have created.[30]

A. *Open Access to Public Records*

Every state has adopted a statute that enables the public to access state and local government records.[31] Most of these statutes, commonly referred to as public records acts, are similar in scope.[32] To that end, many of these statutes define a public record in a similar manner. For example, Missouri's Sunshine Law defines a public record as:

> [A]ny record, whether written or electronically stored, retained by or of any public governmental body including any report, survey, memorandum, or other document or study prepared for the public governmental body by a consultant or other professional service paid for in whole or in part by public funds, including records created or maintained by

---

[27] City of San Jose, 389 P.3d at 852 (quoting International Fed'n of Prof'l and Tech. Eng'rs, Local 21, AFL-CIO v. Super. Ct. of Alameda Cty., 165 P.3d 488 (Cal. 2007)).
[28] JOSH HAWLEY, MISSOURI SUNSHINE LAW: OPEN MEETINGS AND RECORDS LAW 6 (2018).
[29] CAL. GOV'T CODE § 6250 (West 2018).
[30] WASH. REV. CODE ANN. § 42.56.030 (West 2018).
[31] Vera, *supra* note 6, at 24.
[32] *Id.*

> private contractors under an agreement with a public governmental body or on behalf of a public governmental body. . . . The term "public record" shall not include any internal memorandum or letter received or prepared by or on behalf of a member of a public governmental body consisting of advice, opinions and recommendations in connection with the deliberative decision-making process of said body, unless such records are retained by the public governmental body or presented at a public meeting.[33]

The State of Washington defines a public record more succinctly as "any writing containing information relating to the conduct of government or the performance of any governmental or proprietary function prepared, owned, used, or retained by any state or local agency regardless of physical form or characteristics."[34]

The Washington Public Records Act goes on to state that a writing:

> [M]eans handwriting, typewriting, printing, photostating, photographing, and every other means of recording any form of communication or representation including, but not limited to, letters, words, pictures, sounds, or symbols, or combination thereof, and all papers, maps, magnetic or paper tapes, photographic films and prints, motion picture, film and video recordings, magnetic or punched cards, discs, drums, diskettes, sound recordings, and other documents including existing data compilations from which information may be obtained or translated.[35]

The language utilized in the California Records Act to define a record is similar to the language utilized in the Washington Public Records Act: "[A]ny writing containing information relating to the conduct of the public's business prepared, owned, used, or retained by any state or local agency regardless of physical form or characteristics."[36] The California Records Act defines a writing in a manner that is similar to the definition utilized by Washington, as well.[37]

---

[33] MO. ANN. STAT. § 610.010(6) (West 2018).
[34] WASH. REV. CODE ANN. § 42.56.010 (West 2018).
[35] *Id.*
[36] CAL. GOV'T CODE § 6252 (West 2018).
[37] *See id.* The California Records Act defines a writing as:

> [A]ny handwriting, typewriting, printing, photostating, photographing, photocopying, transmitting by electronic mail or facsimile, and every other

As illustrated by the examples above, the language and definitions associated with public records statutes have not kept pace with changing technology. "Until recently, [many public records] statutes have remained silent regarding access to government-related information created, received or maintained on officials' privately owned electronic devices and personal accounts."[38] Consequently, "[m]any state attorneys general, archival agencies, legislatures, or other official bodies have [been required to] issue[] binding opinions, formal statements, and other guidance providing that [traditional] text messages can be public records under existing laws."[39] The debate regarding whether traditional text messages on personal devices are public records is not yet fully resolved. Only three states explicitly include traditional text messages "within the purview of [their] state open-records laws, either under the statute itself or by regulation."[40] No state has explicitly addressed the use of ephemeral messaging apps either by statute or administrative regulation.

B. *Common Concerns About Traditional Text Messages*

Public officials and open government advocates raise conflicting concerns about the use of personal electronic devices to send and receive traditional text messages that pertain to governmental actions. Those concerns pertain, in part, to: (1) the tension between the desire to protect personal privacy, on the one hand, and the need to provide open access to public records, on the other hand; (2) the real-world challenges associated with retaining and accessing records on personal electronic devices; and, (3) the potential for public officials to utilize personal electronic devices to intentionally circumvent requirements set forth in state sunshine laws.[41] These three concerns permeate the cases and analysis below. Furthermore, these same concerns apply to ephemeral messages. Thus, it is important to briefly explore these three concerns here.

> means of recording upon any tangible thing any form of communication or representation, including letters, words, pictures, sounds, or symbols, or combinations thereof, and any record thereby created, regardless of the manner in which the record has been stored.

Id.

[38] Senat, *supra* note 17, at 298.

[39] Vera, *supra* note 6, at 27.

[40] *Id.* at 25.

[41] *See generally* Senat, *supra* note 17.

First, public officials and government agencies raise concerns about personal privacy. Public officials have claimed, for example, "that disclosure would invade their privacy because personal emails or text messages would be reviewed in the search for those related to government business."[42] As the California Supreme Court acknowledged, "public access to information must sometimes yield to personal privacy interests."[43] Nevertheless, most public records statutes explicitly or implicitly presume that any record that pertains to the business of a public agency is a public record unless exempted by statute.[44] The Washington Supreme Court has noted, for example, that:

> The people enacted the [Public Records Act] "mindful of the right of individuals to privacy," and individuals do not sacrifice all constitutional protection by accepting public employment. Agencies are in the best position to implement policies that fulfill their obligations under the [Public Records Act] yet also preserve the privacy rights of their employees. E-mails can be routed through agency servers, documents can be cached to agency-controlled cloud services, and instant messaging apps can store conversations. Agencies could provide employees with an agency-issued device that the agency retains a right to access, or they could prohibit the use of personal devices altogether. That these may be more effective ways to address employee cell phone use, however, does not diminish the [Public Records Act's] directive that we liberally construe it . . . to promote access to all public records.[45]

Second, public officials raise legal and practical concerns about the ability of government agencies to retain and access records contained on private electronic devices or on third-party servers. "Government bodies have argued that the documents on officials' privately[-]owned electronic devices are not public because the agencies don't possess the documents and don't have a right to access such records."[46] Government officials assert "that ownership of the electronic device on which the information is created, received or stored, and not the substance of the information, should determine

---

[42] *Id.* at 311.
[43] City of San Jose v. Super. Ct. of Santa Clara Cty., 389 P.3d 848, 852 (Cal. 2017).
[44] *See* Senat, *supra* note 17, at 311–14.
[45] Nissen v. Pierce Cty., 357 P.3d 45, 58 (Wash. 2015) (internal citations omitted).
[46] Senat, *supra* note 17, at 314.

whether the public is entitled to the information."[47] Courts and attorneys general have frequently rejected this argument, however.[48] The Washington Supreme Court held that:

> [A]gency employees are responsible for searching their [private] files, devices, and accounts for records responsive to a relevant [Public Records Act] request. Employees must produce any public records (e-mails, text messages, and any other type of data) to the employer agency. The agency then proceeds just as it would when responding to a request for public records in the agency's possession by reviewing each record, determining if some or all of the record is exempted from production, and disclosing the record to the requester.[49]

This holding is similar to the view adopted by other states. Many courts and attorneys general "have rejected the notion that a government official's [private] ownership of a device is more important than the substance of the information."[50]

However, that view is not universally held. In Kentucky, for example, the Attorney General's Office issued an opinion in 2015 stating that communications stored on private devices are not subject to public disclosure because the records are not in the possession of a public agency.[51] The Kentucky Attorney General's Office asserted that:

> In order to determine whether a document is a public record, the threshold question is whether it is in the possession of the agency. Cell phone communications, including calls or text messages, made using a private cell phone that is paid for with private funds, are not prepared by or in the possession of a public agency.[52]

Thus, the Attorney General's Office concluded that the local agency in question "did not violate the Open Records Act in not providing cell phone communications on the private devices of its employees."[53]

---

[47] *Id.* at 322.
[48] *Id.* at 314–22.
[49] Nissen, 357 P.3d at 57.
[50] Senat, *supra* note 17, at 322.
[51] 15-ORD-226, Ky. Op. Att'y Gen. 1, 2 (2015), 2015 WL 9647502.
[52] *Id.*
[53] *Id.*

Given the divergent views espoused by Washington and Kentucky, it is understandable why a "[l]ack of clarity . . . surrounds the applicability of open-records laws to text messages that a state or local government does not 'possess' because the messages are stored on personal devices."[54]

Third, open government advocates raise concerns that public officials and agencies may use personal electronic devices to intentionally circumvent state public records statutes and prevent public access to important government information. "Undergirding the discussion of text messages and other relatively informal electronic communications as public records is the suspicion, in some cases, that these communication formats are not used accidently, but in fact in a purposeful effort to avoid state-open records laws."[55] "If communications sent through personal accounts were categorically excluded from [state public records laws], government officials could hide their most sensitive, and potentially damning, discussions in such accounts."[56]

C. *Concerns About Emerging Technology*

To complicate matters, a new form of technology has recently emerged to shield certain communications. These ephemeral messaging apps are designed to intentionally avoid creating a record that can be accessed at a later date. As one author observed, "the next hurdle may be reaching messages sent using apps that, by design, permanently delete data shortly after it is sent and received."[57] One ephemeral messaging app that is used for this purpose is called Confide.[58] Confide is a "chat app that erases messages as soon as they are read."[59] Confide has been described as follows:

> Confide is a messaging application or "app" for smart phones. While messaging over Confide is substantially similar in many ways to ordinary text messaging, Confide has three principal features that distinguish it from ordinary texting. First, Confide immediately and automatically deletes messages once the recipient has read them, and those messages cannot be recovered. Second, the recipient of a

[54] Vera, *supra* note 6, at 31.
[55] *Id.*
[56] City of San Jose v. Super. Ct. of Santa Clara Cty., 389 P.3d 848, 858 (Cal. 2017).
[57] Vera, *supra* note 6, at 31.
[58] *See generally* CONFIDE, *supra* note 10 ("Discuss sensitive topics . . . without fear of the Internet's permanent, digital record and with no copies left behind.").
[59] Vera, *supra* note 6, at 31.

> Confide message cannot view the entire message at once but instead can view only several words at a time by scrolling his or her finger over the text. This feature is intended to prevent the retention of Confide messages by taking screen shots of the messages. Third, Confide advertises that it uses powerful encryption methods to preserve the security of messages.[60]

Furthermore, Confide "prevents anyone from saving, forwarding, printing or taking a screenshot of the text."[61]

Telegram is another ephemeral messaging app that includes features that are similar to Confide.[62] Telegram allows users, including state and local government officials, to send and receive messages that self-destruct:

> The app . . . was created by a Russian entrepreneur and claims to be 100 percent encrypted. It is one of several apps, including Snapchat, Wickr and Frankly, that offer self-destructing messages. The apps delete messages from the phones of both the sender and the receiver, and they use technology that makes it impractical and sometimes impossible for law enforcement or other third parties to decode.[63]

According to one source, government officials in San Francisco "were using the [Telegram] app to skirt California open records requirements."[64] Local government officials in San Francisco denied those allegations.[65]

No state appellate court has addressed the use of ephemeral messaging apps by public officials, or their application to public records statutes. However, there is pending litigation in the State of Missouri that pertains to the use of an ephemeral messaging app by former Governor Eric Greitens and members of his staff that may serve as an early case study.[66]

---

[60] MOORE ET AL., *supra* note 19, at 1.
[61] Hancock, *supra* note 11.
[62] *See generally* TELEGRAM, https://telegram.org/ (last visited March 16, 2019).
[63] Emily Green, *SF Supervisors Using Messaging App That Lets Texts Vanish*, S.F. CHRON. (Apr. 12, 2016), https://www.sfchronicle.com/politics/article/SF-supervisors-using-messaging-app-that-lets-text-7242237.php.
[64] *Secret Messaging App Used By San Francisco Officials*, CBS S.F. BAY AREA (Mar. 17, 2016, 9:51 AM), https://sanfrancisco.cbslocal.com/2016/03/17/report-san-francisco-officials-using-secret-messaging-app/.
[65] *Id.*
[66] *See* Petition, Sansone v. Greitens, No. 17AC-CC0065 (Cir. Ct. of Cole Cty., Mo. filed Dec. 29, 2017). The use of ephemeral communications tools has recently surfaced in litigation between private sector parties, as well. *See, e.g.*, Aarian Marshall, *The Uber-Waymo Lawsuit*

II. *SANSONE V. GREITENS* SERVES AS EARLY CASE STUDY

Eric Greitens served as the governor of the State of Missouri from January 2017 to June 2018, when he resigned under intense political pressure.[67] In December 2017, the media reported that Governor Greitens and other public officials within the Governor's Office "had downloaded Confide to their personal phones."[68] These reports resulted in speculation that Governor Greitens and his staff may have used Confide to intentionally circumvent Missouri's Sunshine Law.[69] Thus, the Missouri Attorney General's Office opened an inquiry.[70]

A. *Missouri Attorney General's Office Inquiry*

The Missouri Attorney General's Office investigated the use of Confide by the Governor's Office.[71] During the course of the inquiry:

> Eight of Greitens' senior staff members were interviewed by the attorney general's office and admitted they had Confide accounts associated with their personal cell phone: chief of staff Mike Roche, chief operating officer Drew Erdmann, policy director Will Scharf, director of management and budget Jennae Neustadt, deputy chief of staff Nick Maddux, deputy policy director Logan Spena, general counsel Lucinda Luektemeyer and special counsel Sarah Madden.[72]

Governor Greitens was not interviewed by the Attorney General's investigators, however, because the Governor's Office "asserted a blanket

---

Gets A New Star — And Takes a Wild Turn, WIRED (Nov. 30, 2017, 7:00 AM), https://www.wired.com/story/uber-waymo-richard-jacobs-lawsuit/ (alleging Uber used Wickr to send ephemeral encrypted messages to discuss trade secrets stolen from Waymo).

[67] *See* David A. Graham, *The Final Fall of Eric Greitens*, ATLANTIC (May 29, 2018), https://www.theatlantic.com/politics/archive/2018/05/the-final-fall-of-eric-greitens/561473/ ("Most of the state's leading Republicans had called on Greitens to resign, and supported impeachment if he refused.").

[68] MOORE ET AL., *supra* note 19, at 1.

[69] *Id.*

[70] *Id.*

[71] *Id.*

[72] Jason Hancock, *Greitens Admits Using Secret Texting App With Staff But Says He Didn't Violate Laws* (last updated May 15, 2018, 3:56 PM), https://www.kansascity.com/news/politics-government/article211093854.html. [hereinafter *Greitens*].

objection to all questions regarding communications between interviewees and the Governor based on the doctrine of executive privilege."[73]

The Missouri Attorney General's Office published its findings on March 1, 2018, concluding that there was no violation of Missouri's Sunshine Law because the ephemeral communications were transitory in nature.[74] Transitory communications include "[d]rafts or other documents having short-term value and which are not an integral part of administrative or operational records file[s]."[75] The Attorney General's Office noted that communications that are transitory in nature "may be destroyed when no longer needed by the governmental entity."[76] The investigation relied on testimony from officials in the Governor's Office that utilized Confide to make a determination that the nature of the ephemeral messages were not substantive.[77] The Attorney General's Office was not able to independently inspect the ephemeral communications, however, because they no longer existed.[78] As the official report noted, "the nature of Confide necessarily means that no documentary evidence exists to corroborate (or contradict) this testimony."[79]

The Attorney General's Office went on to note that:

> While the use of Confide by [staff in the Governor's Office] does not appear to have violated . . . the Sunshine Law, the [Attorney General's Office] considers it best practice not to use Confide to communicate regarding public business. Most importantly, because Confide automatically deletes messages after they are read, the app prevents public employees from exercising reasoned judgment as to whether a communication must be retained . . . . While the available evidence in this case indicates that messages transmitted over Confide constituted "transitory" communications that need not be retained, it is conceivable that some text messages do fall within record series that require retention. If a public employee were to receive such a communication via Confide, she would be

[73] MOORE ET AL., *supra* note 19, at 1.
[74] *Id.* at 3–4.
[75] *Id.* at 4.
[76] *Id.*
[77] *Id.* at 2.
[78] *Id.*
[79] *Id.*

> unable to retain that communication as required by Missouri law.[80]

The report also noted that:

> After the [Attorney General's Office] launched its inquiry, the [Governor's Office] revised its [internal] Sunshine Law and Records Retention Policy to prohibit the use of Confide for any communications relating to public business. That new policy provides that it is the policy of the Office of the Governor that employees may not use any self-destructing messaging application, for the use of conducting public business, whether it be on a state-issued or personal device.[81]

B. *Public Records Request from the Sunshine Project*

Soon after the media reported that Governor Greitens and members of his staff were using the Confide ephemeral messaging app, attorney Ben Sansone, on behalf of the Sunshine Project, filed several public records requests to obtain copies of the ephemeral messages and related information.[82] "The Sunshine Project [is] a pro bono legal collaboration between the separate law firms of Pedroli and Sansone [that was created] in order to help people submit Sunshine and [Freedom of Information Act] requests and, in some circumstances, file lawsuits if the government refuses to produce the records."[83]

The Sunshine Project filed a total of five written public records requests over several weeks.[84] The first request sought "documents related to the governor's alleged use of text message and communication destroying software, download and use logs, and retention polices."[85] "[T]he Special Counsel for the Custodian of Records [for the Office of the Governor] eventually denied access [to the records] by alternatively claiming that 1) the Office of [the] Governor didn't have the records or 2) the records were closed,

---

[80] *Id.* at 5.
[81] *Id.* at 3 (internal quotation marks omitted).
[82] Amended Petition at 5–9, Sansone v. Greitens, No. 17AC-CC0065 (Cir. Ct. of Cole Cty., Mo. May 1, 2018).
[83] Ben Striker, *St. Louis County Attorneys Remain Persistent In Confide Lawsuit Against Former Gov. Eric Greitens*, MO. TIMES (June 5, 2018). https://themissouritimes.com/51600/st-louis-county-attorneys-remain-persistent-in-confide-lawsuit-against-former-gov-eric-greitens/.
[84] Amended Petition at 5–9, Sansone v. Greitens, No. 17AC-CC0065 (Cir. Ct. of Cole Cty., Mo. May 1, 2018).
[85] *Id.* at 5.

but under information and belief, [the Office of the Governor] retain[s] some, if not all, of the Confide communications."[86]

The Sunshine Project's second public records request sought "[d]ocuments or phone logs that show the date that the governor and anyone employed by the governor's office downloaded any mobile phone and/or computer application which purpose of the application was to automatically destroy text messages and/or other forms of communication after the communication is sent or received."[87] The Custodian of Records responded by stating that "any responsive records would be considered closed . . . as the disclosure of this information would impair the Office of the Governor's Security Division's ability to protect the Governor and his staff, and the interest in non-disclosure outweighs the public interest in disclosure."[88] The Sunshine Project was not persuaded by the Custodian's explanation, however, stating that "[i]n no universe could physical harm possibly befall the governor or his staff if the public knew the date he downloaded Confide."[89]

The Sunshine Project's third public records request sought all "[d]ocuments or phone records that show the mobile phone numbers used by the governor."[90] The Custodian of Records responded by stating that mobile phone numbers are considered closed records.[91]

The fourth public records request pertained to "all SMS messages, text messages, and/or communications sent and/or received by the Governor using the mobile phone application Confide . . . ."[92] The fifth public records request was almost identical to the fourth request, but it pertained to "anyone employed by the governor's office . . . ."[93] The Custodian of Records for the Office of the Governor responded to these last two requests by stating that "the Office of [the] Governor does not have any responsive records to provide . . . ."[94]

---

[86] *Id.* at 6.
[87] *Id.* at 7.
[88] *Id.*
[89] *Id.* at 8.
[90] *Id.*
[91] *Id.*
[92] *Id.* at 9.
[93] *Id.*
[94] *Id.*

C. *Litigation by the Sunshine Project*

As outlined above, the five public records requests filed by the Sunshine Project were denied by the Custodian of Records for the Office of the Governor for a variety of reasons.[95] Thus, Ben Sansone, on behalf of the Sunshine Project, filed a petition with the Circuit Court of Cole County, Missouri, seeking an injunction "enjoining the governor, his staff, and all employees of the governor's office from using the software *Confide* and/or any other automatic communication destruction software."[96] The Sunshine Project also asked the court to order Governor Greitens and his staff to provide a full list of those individuals that "have used or were using text message and/or communication destroying software . . . ."[97]

In response to questions from the Sunshine Project during the early stages of the litigation, attorneys representing Governor Greitens confirmed that the Governor used Confide to communicate with his staff.[98] The Governor's attorneys asserted, however, that Greitens "has only ever used the [Confide] application in a way that the law allows."[99] "Greitens denie[d] he used Confide to communicate with [other State of Missouri] government officials outside his office, with lobbyists, or to discuss pending legislation or policies of the governor's office."[100] However, the Governor "would neither admit nor deny that he used Confide to communicate with political donors, nonprofits, political action committees or staff of the president or vice president's office."[101]

An attorney representing the Governor argued that ephemeral messages are not public records: "If text messages sent using Confide are automatically deleted, then the governor's office can't retain them and thus isn't violating Missouri's open records law by failing to make them public. . . ."[102] The attorney argued that "if the governor's office never possessed the

---

[95] *Id.*
[96] Petition at 4, Sansone v. Greitens, No. 17AC-CC0065 (Cir. Ct. of Cole Cty., Mo. Dec. 29, 2017) (original emphasis).
[97] *Id.* at 5.
[98] *See Greitens*, *supra* note 72.
[99] *Id.*
[100] *Id.*
[101] *Id.*
[102] Hancock, *supra* note 11.

texts, the Sunshine Law doesn't apply."[103] She noted that "[t]he Sunshine Law is designed to allow access to documents that exist."[104]

The trial court judge was "sympathetic to the arguments of the governor's attorney."[105] He noted that, pursuant to Missouri's Sunshine Law, "they only have to produce records they've got."[106] Consequently, the trial judge ruled that the Sunshine Project "cannot move forward with any interviews of current or former Greitens[']staff. Instead, [the Sunshine Project] must issue a subpoena to Confide to see if it can produce copies of the text messages sent using the app by state employees in the governor's office."[107]

D. *Status of Litigation Now Uncertain*

Governor Greitens resigned from office in June 2018 after facing possible impeachment for campaign violations and criminal conduct associated with an extramarital affair.[108] Most of Greitens' staff that utilized Confide also left state employment.[109] Nevertheless, the lawsuit initiated by the Sunshine Project is still active.[110]

One of the attorneys representing the Sunshine Project, Mark Pedroli, asserts that "[e]vidence continues to pour in demonstrating the use of Confide to conduct public business in the Greitens administration."[111] "Pedroli has released copies of screenshots he obtained during discovery that he says show the governor's office used the Confide app to discuss substantial business."[112] It is not clear, however, if the trial court will reverse its previous ruling and

---

[103] *Id.*
[104] *Id.*
[105] *Id.*
[106] *Id.*
[107] *Id.*
[108] *See* Graham, *supra* note 67 ("The scandal-plagued Greitens made [his resignation] announcement in a surprisingly defiant statement . . . in Jefferson City, where he faced possible impeachment.").
[109] Jack Sunstrup, *Attorney Forges Ahead With Greitens Secrecy Probe, Months After Hawley Found No Wrongdoing*, ST. LOUIS POST-DISPATCH (Oct. 10, 2018), https://www.stltoday.com/news/local/govt-and-politics/private-attorney-forges-ahead-with-Greitens-secrecy-probe-months-after/article_271b9d05-f87e-5c18-a42d-226505fb2d10.html.
[110] *Id.*
[111] *Id.*
[112] *Id.*

allow the Sunshine Project to depose the former Governor or his former staff members.[113]

A trial has not yet commenced. The status of the litigation is uncertain given that Greitens resigned and most of his former staff members have departed state government. An injunction directed at Greitens and his former staff at this point may be moot. Thus, it is possible that the suit may be dismissed prior to trial.

III. POTENTIAL APPLICATION OF LESSONS FROM WASHINGTON AND CALIFORNIA

As noted above, no appellate court has addressed the use of ephemeral messaging apps by state and local government officials. However, two recent state supreme court decisions from Washington and California that pertain to traditional text messages on personal electronic devices may provide some guidelines with respect to ephemeral messages.[114]

A. *Nissen v. Pierce County*

In *Nissen v. Pierce County*, Glenda Nissen, a sheriff's deputy, submitted two requests to Pierce County, Washington, seeking public records related to Pierce County Prosecutor Mark Lindquist.[115] Both requests pertained to records associated with Lindquist's personal cell phone.[116] Lindquist personally purchased the phone and he personally paid the monthly service fee.[117] Nevertheless, he often used his personal phone in the course of his employment.[118]

In response to Nissen's records request, Linquist obtained two logs from his cellular service provider.[119] The first log contained a list of calls made and received during the time period in question.[120] The second log contained information about text messages that Lindquist sent and received

---

[113] Hancock, *supra* note 11.
[114] A third case from Vermont may also be instructive. *See, e.g.*, Toensing v. Attorney Gen., 178 A.3d 1000, 1002 (Vt. 2017) ("We conclude that the [Public Records Act's] definition of 'public record' includes digital documents stored in private accounts, but emphasize that it extends only to documents that otherwise meet the definition of public records.").
[115] Nissen v. Pierce Cty., 357 P.3d 45, 49 (Wash. 2015).
[116] *Id.*
[117] *Id.*
[118] *Id.*
[119] *Id.*
[120] *Id.* at 49–50.

during that time.[121] However, the second log did not reveal the content of the text messages.[122] The court noted that "nearly half of the text messages Lindquist sent or received . . . during the relevant period potentially related to his job as the elected prosecutor. The County did not produce the contents of any text message, however, though copies of them exist on Verizon's servers."[123]

Nissen sued Pierce County to obtain the content of the text messages.[124] The trial court determined that, as a matter of law, private cell phone use can *never* contain public records.[125] That decision was subsequently reversed, however, by the Washington Court of Appeals.[126] The Washington Supreme Court then agreed to review the matter.[127]

Pierce County argued that the Washington Public Records Act does not apply to employees "using a private cell phone, even if they use it for public business and even if the same information would be a public record had they used a government-issued phone instead."[128] The Washington Supreme Court disagreed:

> [I]t is clear that an agency's "public records" include the work product of its employees. And we find nothing in the text or purpose of the [Public Records Act] supporting the County's suggestion that only work product made using agency property can be a public record. . . . We hold that records an agency employee prepares, owns, uses, or retains on a private cell phone within the scope of employment can be a public record if they also meet the other requirements of [the Public Records Act].[129]

The Washington Supreme Court then went on to note that:

> When acting within the scope of his employment, Lindquist prepares outgoing text messages by "putting them into written form" and sending them. Similarly, he "used" incoming text messages when he reviewed and replied to them while within

[121] *Id.* at 50.
[122] *Id.*
[123] *Id.*
[124] *Id.*
[125] *Id.* (emphasis added).
[126] *Id.*
[127] *Id.*
[128] *Id.* at 52.
[129] *Id.* at 53.

> the scope of employment. Since the County and Lindquist admit that some text messages might be "work related," the complaint sufficiently alleges that those messages meet all three elements of a "public record". . . .
>
> Transcripts of the content of those text messages are thus potentially public records subject to disclosure . . . .[130]

The Washington Supreme Court recognized there may be practical limitations associated with obtaining public records contained on private devices or third-party servers.[131] Nevertheless, the court determined that the onus must be on the agency and its employees to perform an adequate good faith search for the records requested.[132] The court observed that:

> While a policy easing the burden on employees of preserving public records is certainly helpful, it cannot be a precondition to the public's right to access those records. If it were, the effectiveness of the [Public Records Act] would hinge on "the whim of the public officials whose activities it is designed to regulate."[133]

Nissen does not pertain to ephemeral messages. Nevertheless, the holdings in *Nissen* provide some useful guidelines for other states when determining if ephemeral messages are public records subject to disclosure. First, *Nissen* dispels the notion that records sent or received from a private device can never be public records.[134] If an agency employee uses a private device such as a smartphone to prepare, receive, or retain a work-related record, that record may be a public record if it meets other statutory criteria.[135] Second, the decision in *Nissen* supports the idea that a court may compel an agency employee to produce a transcript of text messages even if those messages are retained by a third party, such as a cellular service provider.[136] The fact that the agency does not have physical possession of the public record does not automatically excuse the agency from complying with a public records request. Lastly, *Nissen* supports the concept that an agency has

---

[130] *Id.* at 55–56.
[131] *See id.* at 56–58.
[132] *Id.* at 57.
[133] *Id.* at 56 (citation omitted).
[134] *Id.* at 55–56.
[135] *Id.*
[136] *Id.* at 58.

a duty to comply with a public records request even if it may be onerous to locate or retrieve the record.[137] A good faith search is required.[138]

None of the holdings from *Nissen* are binding on other states, of course. Nevertheless, *Nissen* provides a framework to evaluate public records requests. More importantly, *Nissen* provides some useful guidelines that may be applicable to certain characteristics associated with ephemeral messages, as well. What *Nissen* fails to address, however, is what obligations state and local government agencies may have, if any, to provide public access to ephemeral messages when no records exist either on the employee's personal electronic device or on a third-party server.

B. *City of San Jose v. Superior Court of Santa Clara County*

In *City of San Jose v. Superior Court of Santa Clara County*, a local resident sought private voicemails, emails, and traditional text messages that related to city business from several city officials.[139] The public records request pertained to:

> [D]ocuments [about] redevelopment efforts in downtown San Jose and included emails and text messages "sent or received on private electronic devices used by" the mayor, two city council members, and their staffs.
>
> The City disclosed communications made using City telephone numbers and email accounts but did not disclose communications made using the individuals' personal accounts.[140]

The California Supreme Court observed that a public record has four important elements: "It is (1) a writing, (2) with content relating to the conduct of the public's business, which is (3) prepared by, *or* (4) owned, used, or retained by any state or local agency."[141] The court acknowledged, however, that the nature of "a writing" has changed over time with advancements in technology. [142] The court recognized that the line between what is a public record and what is a private record may be difficult to discern:

---

[137] *Id.* at 57.
[138] *Id.*
[139] City of San Jose v. Super. Ct. of Santa Clara Cty., 389 P.3d 848, 851 (Cal. 2017).
[140] *Id.*
[141] *Id.* at 853.
[142] *Id.*

> Email, text messaging, and other electronic platforms, permit writings to be prepared, exchanged, and stored more quickly and easily. However, the ease and immediacy of electronic communication has encouraged a commonplace tendency to share fleeting thoughts and random bits of information, with varying degrees of import, often to broad audiences. As a result, the line between an official communication and an electronic aside is now sometimes blurred.[143]

Nevertheless, if a record satisfies the criteria above, it may be a public record subject to disclosure to the public.[144] The court noted that "a city employee's communications related to the conduct of public business do not cease to be public records just because they were sent or received using a personal account."[145] "A writing prepared by a public employee conducting agency business has been 'prepared by' the agency within the meaning of [the Public Records Act], even if the writing is prepared using the employee's personal account."[146]

The City of San Jose argued, in part, that public records "include only materials in an agency's possession or directly accessible to the agency."[147] The City of San Jose asserted that "writings held in an employee's personal account are beyond an agency's reach and fall outside [the Public Records Act]."[148] The California Supreme Court disagreed:

> We likewise hold that documents otherwise meeting [the Public Records Act] definition of "public records" do not lose this status because they are located in an employee's personal account. A writing retained by a public employee conducting agency business has been "retained by" the agency within the meaning of [the Public Records Act], even if the writing is retained in the employee's personal account."[149]

The court went on to explain that:

> Under the City's interpretation . . . a document concerning official business is only a public record if it is located on a government agency's computer servers or in its offices.

---

[143] *Id.*
[144] *See id.* at 853–58.
[145] *Id.* at 858.
[146] *Id.* at 855.
[147] *Id.* at 857.
[148] *Id.*
[149] *Id.*

> Indirect access, through the agency's employees, is not sufficient in the City's view. However, we have previously stressed that a document's status as public or confidential does not turn on the arbitrary circumstance of where the document is located.[150]

The court observed that: "The City's interpretation would allow evasion of [the Public Records Act] simply by the use of a personal account. . . . If communications sent through personal accounts were categorically excluded . . . government officials could hide their most sensitive, and potentially damning, discussions in such accounts."[151]

The California Supreme Court recognized that it may be difficult for a public agency to locate and retrieve records on private devices that are owned and controlled by individual employees.[152] Nevertheless, the court placed that burden squarely on the public agency.[153] Public records "requests invariably impose some burden on public agencies. Unless a records request is overbroad or unduly burdensome, agencies are obliged to disclose all records they can locate 'with reasonable effort.'"[154] With that said, however, "[r]easonable efforts do not require that agencies undertake extraordinarily extensive or intrusive searches . . . ."[155] The court noted that "[i]n general, the scope of an agency's search for public records 'need only be reasonably calculated to locate responsive documents.'"[156]

Similar to the holdings in *Nissen*, the holdings in *City of San Jose* provide some useful guidelines when determining if ephemeral messages are public records subject to disclosure. First, *City of San Jose* makes it abundantly clear, as did *Nissen*, that the fact that a record was originally sent or received on a private electronic device is not dispositive.[157] A record on a personal electronic device may be a public record if it meets the other statutory criteria described above.[158] Second, *City of San Jose* stands for the proposition that a public agency must make a reasonable effort to comply

---

[150] *Id.* at 858.
[151] *Id.*
[152] *See id.* at 859–61.
[153] *See id.*
[154] *Id.* at 860 (citation omitted).
[155] *Id.*
[156] *Id.* (citation omitted).
[157] *Id.* at 857.
[158] *Id.*

with a public records act request.[159] Importantly, however, that does not mean that an agency must undertake extraordinary searches that may be intrusive or overly burdensome.[160] There are undoubtedly limitations as to what actions an agency may be required to take in response to a public records request.

Like *Nissen*, however, *City of San Jose* fails to address what obligations state and local government agencies may have, if any, to provide public access to ephemeral messages when no records exist. It may not be reasonable to require a public agency to comply with a public records request when the record does not exist on the agency's server, the employee's personal device, or a third-party server. Stated differently, it may not be reasonable to require a public agency to produce a record that does not exist.

C. *Important Caveats*

City of San Jose and *Nissen* provide some useful guidance with respect to how courts may view the use of ephemeral messaging apps by state and local government officials. It is important to note, however, that this guidance is limited. First, the holdings in *City of San Jose* and *Nissen* are not binding on other states. Each state supreme court will interpret its state's public records statute as it deems appropriate. Some courts and attorneys general have previously determined, for example, that any record on a personal electronic device cannot, by definition, be a public record.[161]

Second, each state has adopted its own version of a public records statute to provide public access to government records.[162] Most of these state statutes are similar in nature,[163] but they are not identical in every respect. Differences between the public records statutes in California and Washington, on the one hand, and public records statutes in other states, on the other, may limit the impact and applicability of the holdings in *City of San Jose* and *Nissen.*

Finally, the cases from California and Washington pertain to traditional text messages on personal electronic devices, not to the use of

---

[159] *Id.* at 860.
[160] *Id.*
[161] *See, e.g.*, Ky. Opp. Att'y Gen., *supra* note 51 (concluding that communications via a private cell phone that is paid for with private funds are not public records because they are not prepared by or in the possession of a public agency).
[162] *See* Vera, *supra* note 6, at 24.
[163] *Id.*

ephemeral messages. There are similarities between traditional text messages and ephemeral messages generated by apps like Confide. Text messages and ephemeral messages are generated in a similar manner, for example, by using a "keyboard" on a smartphone or other personal electronic device. With that said, however, there are also some important differences between text messages and ephemeral messages.

The most important distinction between traditional text messages and ephemeral messages, of course, pertains to the user's ability to retain and access messages at a later date. Users are able to retain and access traditional text messages on personal electronic devices with relative ease. A text message is typically saved on the sender's personal electronic device until the sender makes a conscious decision to delete the message. Likewise, a traditional text message is normally saved on the recipient's personal electronic device, as well. The text message typically is stored on the device until the recipient makes a conscious choice to delete the message. Even if the sender or receiver of a traditional text message deletes a message, the message is typically stored on a third-party server for some period of time.[164] In other words, a traditional text message is still retained by the user's cellular service provider. Consequently, a traditional text message can be accessed in order to comply with a records request even if the user has inadvertently or deliberately deleted the message from her personal electronic device. That is not the case with an ephemeral message.

When a public official uses an app such as Confide, the message is not retained on her personal electronic device.[165] Rather, it is automatically deleted by the app.[166] Likewise, the recipient of the ephemeral message is not able to retain the message once it has been accessed and read.[167] Apps such as Confide automatically delete the message once the recipient opens the message and reviews the content.[168] And unlike cellular service providers, Confide does not retain any ephemeral messages on its servers.[169] Thus, unlike traditional text messages, ephemeral messages do not result in a record that can be stored and retrieved at a later date.

---

[164] *See* Nissen v. Pierce Cty., 357 P.3d 45, 56 (Wash. 2015).
[165] *See* CONFIDE, *supra* note 10 ("Discuss sensitive topics . . . with no copies left behind.")*.*
[166] *Id.*
[167] *Id.*
[168] *Id.*
[169] *Id.*

Ephemeral messages may be more analogous to "old-fashioned" telephone calls than to traditional text messages. The contents of telephone calls are not typically subject to public records statutes because the conversations that take place over a telephone are transitory and do not result in a record.[170] Similarly, ephemeral messages are used to convey brief messages that are intended to be used only once. Like a telephone call, these fleeting messages do not result in a record that may be accessed later. As the Missouri Attorney General's Office noted, ephemeral messages are transitory in nature.[171] To that extent, at least, ephemeral messages are similar to traditional telephone calls.

In summary, there are similarities between traditional text messages and ephemeral messages; however, there are some important distinctions as well. Given these distinctions, it is not certain whether courts will treat ephemeral messages and traditional text messages in the same manner.

IV. EPHEMERAL MESSAGES AND PUBLIC RECORDS STATUTES

No appellate court has addressed the use of ephemeral messages by state and local government officials. Thus, it is not clear if ephemeral messages sent on apps like Confide are subject to state public records laws. Nevertheless, the two state supreme court decisions described above from California and Washington provide a useful framework to analyze whether ephemeral messages may be subject to public records statutes.[172] *City of San Jose* and *Nissen* include some common themes and questions that are instructive with respect to the analysis of the use of ephemeral messaging apps by state and local government officials.[173] Those themes and questions are explored in more depth below.

A. *Is the Ephemeral Message a Writing?*

The existence of "a writing" is crucial in determining if something is a record. California and Washington both define "a writing" in a similar

---

[170] *See, e.g.*, WASH. REV. CODE ANN. § 42.56.010 (West 2018) (defining a public record as a writing).
[171] MOORE ET AL., *supra* note 19, at 4.
[172] *See* City of San Jose v. Super. Ct. of Santa Clara Cty., 389 P.3d 848 (Cal. 2017); *see also* Nissen v. Pierce Cty., 357 P.3d 45 (Wash. 2015).
[173] *See* City of San Jose, 389 P.3d 848; Nissen, 357 P.3d 45.

manner.[174] The California Public Records Act, for example, defines "a writing" as:

> [A]ny handwriting, typewriting, printing, photostating, photographing, photocopying, transmitting by electronic mail or facsimile, and every other means of recording upon any tangible thing any form of communication or representation, including letters, words, pictures, sounds, or symbols, or combinations thereof, and any record thereby created, regardless of the manner in which the record has been stored.[175]

Other states utilize similar language to define the word "writing" for the purpose of their public records statutes.[176] As noted above, however, only three states explicitly reference traditional text messages.[177] No state explicitly references ephemeral messages.

The California Supreme Court had little trouble in determining that traditional text messages are writings for the purpose of the California Public Records Act.[178] The California Supreme Court conceded that the nature of writings has changed substantially over the past fifty years.[179] Text messages did not exist when the California Public Records Act was adopted in 1968. Nevertheless, the court concluded that traditional text messages are writings.[180] The California Supreme Court did not elaborate on its reasoning; the court simply stated that "[i]t is undisputed that the [text messages] at issue here constitute writings."[181] Parsing the language in the California Public Records Act quoted above is instructive, however.[182] Text messages are typewritten (albeit electronically);[183] they are transmitted via a form of

---

[174] *See* CAL. GOV'T CODE § 6252 (West 2018); WASH. REV. CODE ANN. § 42.56.010 (West 2018).
[175] CAL. GOV'T CODE § 6252 (West 2018).
[176] *See, e.g.*, IDAHO CODE ANN. § 74-101(16) (West 2018) ("'Writing' includes, but is not limited to, handwriting, typewriting, printing, photostating, photographing and every means of recording, including letters, words, pictures, sounds or symbols or combination thereof, and all papers, maps, magnetic or paper tapes, photographic films and prints, magnetic or punched cards, discs, drums or other documents.").
[177] Vera, *supra* note 6, at 25.
[178] City of San Jose v. Super. Ct. of Santa Clara Cty., 389 P.3d 848, 853 (Cal. 2017).
[179] *Id.*
[180] *Id.*
[181] *Id.*
[182] CAL. GOV'T CODE § 6252 (West 2018).
[183] *Id.*

electronic mail;[184] and they contain letters, words, pictures, sounds, and/or symbols.[185] Thus, text messages meet the definition of "a writing".

This test yields a similar result when applied to ephemeral messages like the messages in *Sansone*. First, like traditional text messages, ephemeral messages are typewritten via a smartphone or other personal electronic device. Second, ephemeral messages are transmitted using a form of electronic mail via an app. Lastly, ephemeral messages contain letters, words, pictures, sounds, and/or symbols, just like traditional text messages. Consequently, it is reasonable to conclude that ephemeral messages are writings, at least as the term "writing" is used in most public records statutes.

B. *Does the Ephemeral Message Pertain to the Conduct of the Public's Business?*

"To qualify as a public record, a writing must 'contain[] information relating to the conduct of the public's business.'"[186] As the California Supreme Court noted, however:

> Whether a writing is sufficiently related to public business will not always be clear. . . . Resolution of the question, particularly when writings are kept in personal accounts, will often involve an examination of several factors, including the content itself; the context in, or purpose for which, it was written; the audience to whom it was directed; and whether the writing was prepared by an employee acting or purporting to act within the scope of his or her employment.

The court went on to clarify:

> [T]o qualify as a public record under [the California Public Records Act], at a minimum, a writing must relate in some substantive way to the conduct of the public's business. This standard, though broad, is not so elastic as to include every piece of information the public may find interesting. Communications that are primarily personal, containing no more than incidental mentions of agency business, generally will not constitute public records.[187]

---

[184] *Id.*
[185] *Id.*
[186] City of San Jose v. Super. Ct. of Santa Clara Cty., 389 P.3d 848, 854 (Cal. 2017) (citation omitted).
[187] *Id.*

This test, when applied to the ephemeral messages at issue in *Sansone*, yields ambiguous results. On the one hand, it is undisputed that the ephemeral messages in *Sansone* related to the public's business, at least to some extent.[188] The messages, even if transitory in nature, pertained to activities within the Governor's Office.[189] Furthermore, the ephemeral messages were exchanged between the Governor and his key staff.[190] Thus, the messages were prepared by public officials acting within the scope of their employment.

On the other hand, it is difficult, if not impossible, to ascertain the content, context, or purpose of the ephemeral messages due to the fact that there are no records available to review.[191] The Governor's staff claimed that the messages pertained to mundane and fleeting topics such as scheduling meetings.[192] An attorney representing the Sunshine Project has asserted, however, that at least some of the ephemeral messages pertained to substantive public policy topics.[193]

Regardless of the specific facts in *Sansone*, the cases from California and Washington provide some useful guidance with respect to ephemeral messages in a more general sense. As the Washington Supreme Court noted, text messages can "qualify as public records if they contain any information that refers to or impacts the actions, processes, and functions of government."[194] This rationale applies to ephemeral messages as well. Consequently, it is reasonable to conclude that ephemeral messages that pertain to the conduct of the public's business may be subject to public records laws if other statutory criteria are met.

C. *Was the Ephemeral Message Prepared by an Agency?*

Most public records statutes, by definition, pertain to records prepared by a public agency.[195] As noted above, however, very few statutes explicitly

---

[188] *See* MOORE ET AL., *supra* note 19, at 2.
[189] *Id.*
[190] *See Greitens*, *supra* note 72.
[191] *See* MOORE ET AL., *supra* note 19, at 2.
[192] *Id.*
[193] *See* Sunstrup, *supra* note 109.
[194] *See* Nissen v. Pierce Cty., 357 P.3d 45, 55 (Wash. 2015).
[195] *See, e.g.*, WASH. REV. CODE ANN. § 42.56.010 (West 2018) ("'Public record' includes any writing containing information relating to the conduct of government or the performance of any governmental or proprietary function prepared . . . by any state or local agency . . . .").

address traditional text messages generated or received by a public official on a personal electronic device.[196] Once again, the holdings in *City of San Jose* and *Nissen* provide a useful analytical framework.[197] The Washington Supreme Court held, for example, that "records an agency employee prepares, owns, uses, or retains on a private cell phone within the scope of employment can be a public record if they also meet the other requirements of [the Public Records Act]."[198] The court went on to note that:

> For information to be a public record, an employee must prepare, own, use, or retain it *within the scope of employment*. An employee's communication is "within the scope of employment" only when the job requires it, the employer directs it, or it furthers the employer's interests.[199]

This guideline is helpful when applied to the ephemeral messages at issue in the State of Missouri. In *Sansone*, the Governor and his staff members used personal electronic devices to send and receive ephemeral messages.[200] Most of the devices in *Sansone* were not owned by the State of Missouri.[201] Nevertheless, the ephemeral messages at issue were within each individual's scope of public employment.[202] Furthermore, the ephemeral messages were utilized to advance the employer's interests whether the employer is defined as Governor Greitens or as the State of Missouri.[203] By applying the guidelines set forth in *City of San Jose* and *Nissen*, it is reasonable to conclude that ephemeral messages may be subject to public records statutes if the ephemeral messages (1) were generated in the public official's scope of employment and (2) furthered the employer's interests. Of course, the messages in question would need to meet the other relevant criteria contained in the applicable public records statute as well.

D. *Is the Ephemeral Message Owned, Used, or Retained by an Agency?*

The California Supreme Court noted in *City of San Jose* that:

---

[196] Vera, *supra* note 6, at 25.
[197] *See* City of San Jose v. Super. Ct. of Santa Clara Cty., 389 P.3d 848, 854 (Cal. 2017); *see also* Nissen, 357 P.3d 45.
[198] Nissen, 357 P.3d at 53.
[199] *Id.* at 54 (emphasis in original) (citation omitted).
[200] *See* MOORE ET AL., *supra* note 19.
[201] *Id.* at 2.
[202] *Id.*
[203] *Id.*

> A writing is commonly understood to have been prepared by the person who wrote it. If an agency employee prepares a writing that substantively relates to the conduct of public business, that writing would appear to satisfy the [Public Records] Act's definition of a public record. The City urges a contrary conclusion when the writing is transmitted through a personal account. In focusing its attention on the "owned, used, or retained by" aspect of the "public records" definition, however, it ignores the "prepared by" aspect [of the Public Records Act].[204]

The court then noted that:

> Broadly construed, the term "local agency" logically includes not just the discrete governmental entities . . . but also the individual officials and staff members who conduct the agencies' affairs. It is well established that a governmental entity, like a corporation, can act only through its individual officers and employees. A disembodied governmental agency cannot prepare, own, use, or retain any record. Only the human beings who serve in agencies can do these things. When employees are conducting agency business, they are working for the agency and on its behalf.[205]

The Washington Supreme Court reached a similar conclusion in *Nissen*:

> [Governmental] bodies lack an innate ability to prepare, own, use, or retain any record. They instead act exclusively through their employees and other agents, and when an employee acts within the scope of his or her employment, the employee's actions are tantamount to the "actions of the body itself." Integrating this basic common law concept into the [Public Records Act], a record that an agency employee prepares, owns, uses, or retains in the scope of employment is necessarily a record "prepared, owned, used, or retained by a state or local agency."[206]

Thus, the California Supreme Court and the Washington Supreme Court both concluded that when a public official prepares, owns, uses, or retains any record, that it is tantamount to the government agency preparing,

---

[204] City of San Jose v. Super. Ct. of Santa Clara Cty., 389 P.3d 848, 855 (Cal. 2017).
[205] *Id.* (internal citations omitted).
[206] Nissen v. Pierce Cty., 357 P.3d 45, 52–53 (Wash. 2015) (internal citations omitted).

owning, using, or retaining the same record.[207] This is true even if the public official uses a personal electronic device to create or receive the record so long as the official is acting within the scope of her employment.[208]

When this guideline is applied to the facts in *Sansone*, it is clear that the ephemeral messages sent and received by Governor Greitens and his staff meet most of the criteria set forth in *City of San Jose* and *Nissen*. First, the ephemeral messages were prepared or received by public officials employed by the State of Missouri.[209] Second, the ephemeral messages were owned (albeit only for a brief period of time) by the same public officials. And lastly, the ephemeral messages were used by Governor Greitens and his staff to conduct public business.[210] Governor Greitens and his staff did not retain the ephemeral messages, but that is not essential to the application of this particular guideline. The guideline applies even if only one of the factors is in evidence. Here, three of the factors apply to the ephemeral messages in *Sansone*: preparation, ownership, and use.

E. *Does an Agency Possess the Ephemeral Message?*

In *City of San Jose*, the government agency asserted that " 'public records' include only materials in the agency's possession or directly accessible to the agency."[211] The City of San Jose argued that "writings held in an employee's personal account are beyond an agency's reach and fall outside [the Public Records Act]."[212] The California Supreme Court observed, however, that:

> Appellate courts have generally concluded records related to public business are subject to disclosure if they are in an agency's actual *or constructive* possession. "An agency has constructive possession of records if it has the right to control the records, either directly or through another person."[213]

Thus, the California Supreme Court held that:

> [D]ocuments otherwise meeting [the Public Records Act's] definition of "public records" do not lose this status because

[207] *See* Nissen, 357 P.3d at 52–53; *see also* City of San Jose, 389 P.3d at 855.
[208] *See* City of San Jose, 389 P.3d at 855.
[209] *See* MOORE ET AL., *supra* note 19, at 1.
[210] *Id.* at 2.
[211] City of San Jose, 389 P.3d at 857.
[212] *Id.*
[213] *Id.* (emphasis in original) (internal citations omitted).

> they are located in an employee's personal account. A writing retained by a public employee conducting agency business has been "retained by" the agency within the meaning of [the Public Records Act], even if the writing is retained in the employee's personal account.[214]

The Washington Supreme Court reached a similar conclusion in *Nissen*. The traditional text messages at issue in *Nissen* were not in the possession of the government agency or the public official.[215] Rather, the text messages were retained on a third-party server by the public official's cellular service provider.[216] Nevertheless, the court held that "[t]ranscripts of the content of those text messages [retained by Verizon] are thus potentially public records subject to disclosure . . . ."[217]

Thus, the California Supreme Court and the Washington Supreme Court both concluded that a government agency can "possess" a record even when it does not directly retain or control the record.[218] That is the case when a public official that is employed by the government agency retains access to the record in question even if the record is retained by a third-party that is not directly associated with the government agency.[219]

This guideline is useful when analyzing traditional text messages because those messages are typically stored on a public official's personal electronic device or on a third-party server. That was the case in both *City of San Jose* and *Nissen*.[220] It is difficult, however, to apply this guideline to the facts in *Sansone* or, more broadly, to ephemeral messages in general. In the case of an ephemeral message, the message is not retained by the government agency, the public official, or by a third-party, such as Confide.[221] In fact, the ephemeral message is not retained at all; that is one of the key features of apps like Confide.[222] Thus, the guideline outlined above from *City of San Jose* and *Nissen* does not appear to apply to the facts in *Sansone* or to ephemeral messages in general. That opens the door to a reasonable argument

---

[214] *Id.*
[215] *See* Nissen v. Pierce Cty., 357 P.3d 45, 49–50 (Wash. 2015).
[216] *See id.*
[217] *Id.* at 56.
[218] *See id.*; City of San Jose, 389 P.3d at 857.
[219] *See* City of San Jose, 389 P.3d at 857.
[220] *See generally* City of San Jose, 389 P.3d 848; Nissen, 357 P.3d 45.
[221] *See* CONFIDE, *supra* note 10 ("Discuss sensitive topics . . . without fear of the Internet's permanent, digital record and with no copies left behind.").
[222] *Id.*

that ephemeral messages may not be subject to public records laws. As the attorney representing Governor Greitens asserted, "[i]f text messages sent using Confide are automatically deleted, then the governor's office can't retain them and thus isn't violating Missouri's open records law . . . ."[223]

F. *Can the Ephemeral Message be Retrieved with Reasonable Effort?*

The Washington Supreme Court was cognizant that it may be difficult—and in some cases perhaps impossible—for a public agency to locate and retrieve traditional text messages when those messages are retained on a personal electronic device or on a third-party server.[224] Nevertheless, the court ruled that "[t]he onus is . . . on the agency—necessarily through its employees—to perform 'an adequate search' for the records requested."[225] The court stated that "[t]o satisfy the agency's burden to show it conducted an adequate search for records, we permit employees in good faith to submit 'reasonably detailed, nonconclusory affidavits' attesting to the nature and extent of their search."[226]

The California Supreme Court reached a similar conclusion:

> [Records] requests invariably impose some burden on public agencies. Unless a records request is overbroad or unduly burdensome, agencies are obliged to disclose all records they can locate "with reasonable effort." Reasonable efforts do not require that agencies undertake extraordinarily extensive or intrusive searches, however. In general, the scope of an agency's search for public records "need only be reasonably calculated to locate responsive documents."[227]

The California Supreme Court and the Washington Supreme Court both appear to acknowledge, at least implicitly, that it may be unreasonable in some instances to require a government agency to locate and produce every record that may be responsive to a records request.[228] Thus, both courts employed a reasonableness standard.[229] The onus is on the government agency and its employees to make a good faith effort to comply with a records

---

[223] Hancock, *supra* note 11.
[224] *See* Nissen, 357 P.3d at 57.
[225] *Id.* (citation omitted).
[226] *Id.* (citation omitted).
[227] City of San Jose v. Super. Ct. of Santa Clara Cty., 389 P.3d 848, 860 (Cal. 2017) (internal citations omitted).
[228] *See* City of San Jose, 389 P.3d at 860; Nissen, 357 P.3d at 57.
[229] *See* City of San Jose, 389 P.3d at 860; Nissen, 357 P.3d at 57.

request.[230] With that said, however, a government agency need only make a reasonable effort to locate and disclose the relevant documents.[231]

This guideline is useful with respect to traditional text messages because those messages are typically stored on a public official's personal electronic device or on a third-party server. In most instances it is reasonable to require the public agency, either directly or through its employee, to retrieve the text messages and make them available to the public. That was the situation, for example, in both *City of San Jose* and *Nissen*.[232] It is more difficult, however, to apply this guideline to the facts in *Sansone*. The ephemeral messages that were sent and received by Governor Greitens and his staff no longer exist.[233] The ephemeral messages were automatically deleted by the app that was used to produce and convey the messages.[234] The ephemeral messages in question were not retained by the State of Missouri, Governor Greitens, the Governor's staff, or Confide.[235] Stated more succinctly, the ephemeral messages no longer exist. That opens the door to the logical argument that, using the guideline from *City of San Jose* and *Nissen* described above, it would be *unreasonable* to require the Governor's Office or, more generally, the State of Missouri, to retrieve and deliver a document that does not exist. The Governor's Office could accurately assert that it made a *reasonable search* but that the ephemeral documents do not exist. In fact, that is essentially what the attorney representing Governor Greitens claimed.[236]

In summary, ephemeral messages satisfy some, but not all, of the guidelines set forth in *City of San Jose* and *Nissen*. In the case of ephemeral messages, nobody *possesses* a record. It is not in the possession of the public agency, the public official, or a third-party. Consequently, a *reasonable effort* will never result in the production of the record requested. This suggests that it is possible to make a good faith argument that the holdings in *City of San Jose* and *Nissen* that pertain to traditional text messages do not apply to

---

[230] *See, e.g.*, City of San Jose, 389 P.3d at 859–61.
[231] *See, e.g.*, *id.* at 860.
[232] *See generally* City of San Jose, 389 P.3d 848; Nissen, 357 P.3d 45.
[233] *See* MOORE ET AL., *supra* note 19, at 2.
[234] *Id.*
[235] *Id.*
[236] *See* Hancock, *supra* note 11 ("If text messages sent using Confide are automatically deleted, then the governor's office can't retain them and thus isn't violating Missouri's open records law by failing to make them public . . . .").

ephemeral messages. In other words, it is possible to make a reasonable argument that ephemeral messages are not subject to public records laws.

V. NEED FOR CLARITY

The emerging use of ephemeral messaging apps by public officials creates new questions relative to the public's right to access government records. Ephemeral messaging apps are typically used on personal electronic devices such as smartphones that are privately owned. They do not generate a record that can be stored and subsequently accessed by the public. Thus, it is not clear if ephemeral messages generated on personal electronic devices are public records at all even if the ephemeral messages pertain to government topics. This uncertainty creates ambiguity.

A. *Public Policy Considerations*

There are strong public policy reasons to provide open access to government records. As the California Supreme Court observed:

> "Openness in government is essential to the functioning of a democracy. 'Implicit in the democratic process is the notion that government should be accountable for its actions. In order to verify accountability, individuals must have access to government files. Such access permits checks against the arbitrary exercise of official power and secrecy in the political process.'"[237]

In other words, the public must have open access to government records to effectively monitor government activity and hold state and local government officials accountable for their actions. The public must "remain[] informed so that they may maintain control over the instruments that they have created."[238]

These public policy considerations apply to traditional forms of public records (such as documents generated on paper) and to ephemeral communications alike. The physical form of the record is largely irrelevant for public policy purposes. The public has a crucial interest in the content of ephemeral communications if the messages in question pertain to the conduct of the public's business. Public policy demands open access to ephemeral

---

[237] City of San Jose, 389 P.3d at 852 (internal citations omitted).
[238] WASH. REV. CODE ANN. § 42.56.030 (West 2018).

messages to ensure accountability and to provide a check against potential corruption and other abuses within state and local governments.[239]

B. *Need to Update State Statutes to Reflect New Technology*

Most state public records laws were adopted prior to the widespread use of text messaging and related technology. Some state statutes still refer to antiquated technology, such as magnetic tapes, magnetic cards, punched cards, and diskettes.[240] Only three states explicitly identify text messages as records.[241] And, importantly, no state public records statute identifies ephemeral messages as public records.[242] In short, public records statutes need to be updated to reflect current technology.

The antiquated language in state public records laws has resulted in ambiguity and litigation with respect to the use of traditional text messages sent or received by public officials on personal electronic devices.[243] The emerging use of ephemeral messaging apps by public officials on personal electronic devices will undoubtedly generate similar questions and concerns. That is already the situation in Missouri.[244] "While state laws and policies have yet to catch up with text messages [and ephemeral messages], technology marches forward. With increasing frequency, messaging apps are [being] used in the workplace."[245]

To ensure transparency and reduce ambiguity, state legislatures should revise their public records statutes to explicitly address the use of ephemeral messaging apps. There are strong public policy reasons to treat ephemeral messages sent or received on personal electronic devices in a manner similar to other, more traditional records. Public officials and agencies should be required to retain these ephemeral messages for a reasonable period of time if the content would otherwise be subject to that state's public records statute. Ephemeral messages should be made available to the public upon request like any other public record.

---

[239] *See, e.g., id.* ("The people, in delegating authority, do not give their public servants the right to decide what is good for the people to know and what is not good for them to know.").
[240] *See, e.g.*, WASH. REV. CODE ANN. § 42.56.010 (West 2018) (writing means, inter alia, "magnetic or punched cards, discs, drums, [and] diskettes . . . .").
[241] Vera, *supra* note 6, at 25.
[242] *See supra* Part I.A.
[243] *See, e.g.*, Vera, *supra* note 6, at 24; *see generally* Senat, *supra* note 17.
[244] *See* Petition, Sansone v. Greitens, No. 17AC-CC0065 (Cir. Ct. of Cole Cty., Mo. filed Dec. 29, 2017).
[245] Vera, *supra* note 6, at 31.

If it is not possible to retain and retrieve ephemeral messages, state legislatures should consider restricting the use of ephemeral messaging apps by state and local government officials. There is no compelling reason for a public official to utilize an ephemeral messaging app to conduct the public's business. Other tools such as traditional email may be used to accomplish the same purpose as ephemeral communications. The difference, of course, is that the use of email creates a record that can be easily retained. Those records can then be retrieved when necessary to respond to a records request. If it is not possible to retain and retrieve ephemeral messages, a public official or agency could easily circumvent the intent of that state's public records statute to provide open access to government records. This would contravene public policy.

CONCLUSION

Sunshine laws are designed to ensure open access to public documents, albeit with some limitations.[246] Public access to government documents promotes democracy and fosters trust in state and local government.[247] People have the right to know how, when, and why government agencies make decisions that impact their state or community.[248] Transparency is paramount in a free society.[249] The public must have access to public records to remain informed and hold state and local governments accountable.[250]

It is not clear if ephemeral messages generated or received on a personal electronic device are public records under existing state statutes. The court decisions from California and Washington described above provide some guidance.[251] However, it is possible to argue that the holdings in *City of San Jose* and *Nissen* do not encompass ephemeral messages. If that is the case, ephemeral messages may not be covered by public records statutes. The public would have no effective means to access and review these government-related messages.

---

[246] *See supra* Part I.A.
[247] *See supra* Part I.A.
[248] *See supra* Part I.A.
[249] *See supra* Part I.A.
[250] *See supra* Part I.A.
[251] *See* City of San Jose v. Super. Ct. of Santa Clara Cty., 389 P.3d 848 (Cal. 2017); Nissen v. Pierce Cty., 357 P.3d 45 (2015).

Public policy considerations strongly suggest that ephemeral messages should be categorized as public records.[252] To avoid ambiguity and litigation, state legislatures should revise state statutes to make it clear that ephemeral messages that pertain to government-related actions are public records. If ephemeral messages cannot be stored and retrieved to ensure public access, state legislatures should err on the side of caution and restrict the use of ephemeral messaging apps by state and local government officials.

[252]*See generally* City of San Jose, 389 P.3d 848; Nissen, 357 P.3d 45.