JOURNAL OF LAW, TECHNOLOGY & THE INTERNET • VOLUME 10 • ISSUE 1 • 2019

KILLER APPS: VANISHING MESSAGES, ENCRYPTED COMMUNICATIONS, AND CHALLENGES TO FREEDOM OF INFORMATION LAWS WHEN PUBLIC OFFICIALS "GO DARK"

Dr. Daxton R. Stewart[1]

ABSTRACT

Government officials such as White House staffers and the Missouri governor have been communicating among themselves and leaking to journalists using apps such as Signal and Confide, which allow users to encrypt messages or to make them vanish after they are received. By using these apps, government officials are "going dark" by avoiding detection of their communications in a way that undercuts freedom of information laws. This article explores the challenges presented by government employee use of encrypted and ephemeral messaging apps by examining three policy approaches: (1) banning use of the apps, (2) enhancing existing archiving and record-keeping practices, or (3) legislatively expanding quasi-government body definitions. Each of these approaches will be analyzed as potential ways to manage the threat presented by "killer apps" to open records laws.

Keywords: government, encryption, messaging, freedom of information, record-keeping, communication, privacy

[1] Ph.D., J.D., LL.M., Professor at Texas Christian University.

CONTENTS

INTRODUCTION

In Donald J. Trump's first month in the White House, staffers concerned about accusations of leaking information to the press "resorted to a secret chat app – Confide – that erases messages as soon as they're read."[2] After the email hacks that haunted Hillary Clinton's presidential campaign in 2016, the Confide app became "the tool of choice for Republicans in Washington" fearing a similar fate.[3] White House press secretary Sean Spicer, who began random phone checks shortly after the *Washington Post* revelation, reportedly told staffers that using Confide and the encrypted messaging app Signal were potential violations of the Presidential Records Act.[4] In response to these reports, the House Oversight Committee issued a letter to fifty-five federal agencies expressing concerns that the use of Signal, Confide, and WhatsApp by federal employees "could result in the creation of federal records that would be unlikely or impossible to preserve" and may allow

[2] Ashley Parker & Philip Rucker, *Upheaval is Now Standard Operating Procedure Inside the White House*, WASH. POST (Feb. 13, 2017), https://www.washingtonpost.com/politics/upheaval-is-now-standard-operating-procedure-inside-the-white-house/2017/02/13/d65dee58-f213-11e6-a9b0-ecee7ce475fc_story.html?utm_term=.b1940d392beb.
[3] David McCabe & Jonathan Swan, *Confide: The App for Paranoid Republicans*, AXIOS, (Feb. 8, 2017), https://www.axios.com/confide-the-new-app-for-paranoid-republicans-2246297664.html.
[4] Annie Karni & Alex Isenstadt, *Sean Spicer Targets Own Staff in Leak Crackdown*, POLITICO (Feb. 26, 2017, 5:25 PM), http://www.politico.com/story/2017/02/sean-spicer-targets-own-staff-in-leak-crackdown-235413.

"circumventing requirements established by federal recordkeeping and transparency laws."[5] Citizens for Responsibility and Ethics in Washington (CREW) filed suit against Trump, alleging violation of the Presidential Records Act by using encrypted disappearing-messaging apps.[6] During ethics training in 2018, White House lawyers advised personnel not to use encrypted messaging apps such as WhatsApp while conducting government business.[7]

Similar issues have trickled down to the states as well. In Missouri, two attorneys sued then-Governor Eric Greitens, arguing that his use of Confide violated the state's public records law.[8] A county judge denied their request for a temporary restraining order to halt Greitens's use of Confide, in part, because of a lack of evidence that he had been using it to conduct government business, but noted that there were "a whole bunch of open questions here," including whether the governor has a First Amendment right to use the app to communicate, as his attorneys contended.[9]

State open records laws, the federal Freedom of Information Act, and the Presidential Records Act are intended to protect the public's right to know about government officials' conduct. However, the development of privacy-protecting mobile applications that deliberately make archiving and retrieval difficult creates a unique challenge for these transparency laws.

Vanishing message apps, such as Snapchat and Confide, allow public officials, using these apps as intended, to have messages disappear automatically without a way to keep a record for public inspection. Bob Freeman, the long-time executive director of New York state's Committee on Open Government, described

[5] Letter from Jason Chaffetz, Chairman, and Elijah E. Cummings, Ranking Member, House of Representatives Committee on Oversight and Government Reform, to Kathleen McGettigan, Acting Director, Office of Personnel Management (Mar. 8, 2017), https://oversight.house.gov/wp-content/uploads/2017/03/2017-03-08-JEC-EEC-to-McGettigan-OPM-Federal-Records-Act-due-3-22.pdf

[6] Josh Gerstein, *Judge Hears Suit on Trump White House Use of Encrypted Apps*, POLITICO (Jan. 17, 2018, 1:12 PM), https://www.politico.com/story/2018/01/17/white-house-encrypted-apps-hearing-343774.

[7] Carol D. Leonnig, Josh Dawsey & Ashley Parker, *Ethics Training Reminds White House Staff Not to Use Encrypted Messages for Government Business*, WASH. POST (Feb. 5, 2018), https://www.washingtonpost.com/politics/ethics-training-reminds-white-house-staff-not-to-use-encrypted-messages-for-government-business/2018/02/04/7636265c-05eb-11e8-94e8-e8b8600ade23_story.html?utm_term=.0d04a080becd.

[8] Cyrus Farivar, *Judge Should Order Governor to Stop Using Ephemeral App, Lawyers Say*, ARSTECHNICA (Feb. 1, 2018, 6:03 AM), https://arstechnica.com/tech-policy/2018/02/lawyers-governors-secret-messaging-app-use-violates-public-records-laws/.

[9] Jason Hancock, *No Immediate Ban on Greitens' Use of Secret Text App, but Judge Has More Questions*, KAN. CITY STAR (Feb. 2, 2018), http://www.kansascity.com/news/politics-government/article198113764.html.

the dangers: "If an individual, including a government official, wants to cover his tracks, tell the world, 'I never said that,' or that he never communicated with a certain person…Snapchat, for better or worse, can be used to make it seem true. And there may be nothing we can do about it."[10]

Encrypted messaging apps, such as WhatsApp and Signal, offer a similar challenge, one that former FBI Director James Comey has called "Going Dark." Comey, speaking about the challenges of investigating and preventing crime when people have the ability to use technology to obscure themselves and their activities, largely through encryption, has said, "We have the legal authority to intercept and access communications pursuant to a court order, but we often lack the technical ability to do so."[11]

The same legal communication tools that citizens can use to avoid detection and surveillance are also available to government employees, who now appear to be "going dark" in their communications as part of their official jobs. This is not the first time a new digital communication technology has created a challenge for government record-keeping and accessibility under open records laws. But, in the past, such new technologies – email, private online chat rooms, text messaging, and private messaging through social networks, to name a few – merely offered obscurity as a secondary effect of the messaging system. Ultimately, the messages could be found and subjected to public scrutiny, though doing so may be difficult and time-consuming, and new rules have had to be put in place to account for archiving and providing a means of access to the public.

However, apps such as Snapchat and Confide provide automatic deletion of messages after they are read as a core benefit. Similarly, encrypted messaging systems make transparency difficult because people seeking access to those records would need the key to be able to read them. These features have the potential to be deadly to public records laws, providing an easy way for government officials to dodge public scrutiny without any trace of their subversion.

The purpose of this article is to examine the implications of vanishing messaging and encrypted messaging apps for freedom of information laws and to propose potential policy revisions to handle the challenges these apps present. After briefly reviewing how the apps work, three potential policy approaches are examined, using legal research methodology to consider the possible remedies that may be available to legislators and regulators to prevent "killer apps" from

[10] Robert J. Freeman, *In a "Poof," Snapchat Puts Public Records Laws to Test*, KNOXVILLE NEWS SENTINEL (Mar. 15, 2016), http://www.knoxnews.com/story/opinion/valley-views/2016/03/15/poof-snapchat-puts-public-records-laws-test/81656774/.
[11] Brookings Institution, *Are Technology, Privacy, and Public Safety on a Collision Course?*, YOUTUBE (Oct. 16, 2014), https://www.youtube.com/watch?v=A8BSr3XqVwE.

undermining the goals of freedom of information laws. Finally, these policy approaches are reviewed for their potential application to the Public Information Act, the open records law in Texas.

I. PRIVACY-PROMISING TECHNOLOGIES

At issue are two distinct kinds of communication technology, encryption and ephemeral messaging, that allow users to make records of their discussions harder to observe or retain. Jasmine McNealy and Heather Schoenberger have conceptualized these as "privacy-promising technologies," a definition that includes "technology, such as apps, software, and online tools, in which the maker or creator uses the promise of privacy, or data control, to induce users to use their digital tool."[12] While the authors were writing primarily about apps that either promised anonymity (such as YikYak or Whisper) or provided automatic message deletion (such as Snapchat), it makes sense as a concept to extend the definition to apps that protect user communications from outside scrutiny through encryption as well.

Government use of impermanent messaging apps is becoming commonplace. Presidential contenders Jeb Bush, Hillary Clinton, and Bernie Sanders had Snapchat accounts, and the app has become popular among members of Congress, including "Snapchat King of Congress" Eric Swalwell, a representative from California.[13]

Snapchat users include Washington, D.C. Mayor Muriel Bowser and Los Angeles Mayor Eric Garcetti,[14] as well as Chicago Police Superintendent Eddie Johnson.[15] And government use has not been without controversy. The New York Police Department, for instance, had to investigate an officer who posted images on Snapchat during a Brooklyn apartment raid. The posted Snapchats depicted a family in handcuffs with captions such as "Merry Christmas it's NYPD!" and "Warrant Sweeps it's still a part smh."[16] Beyond the White House examples

[12] Jasmine McNealy & Heather Schoenberger, *Reconsidering Privacy-Promising Technologies*, 19 TUL. J. TECH. & INTELL. PROP. 1, 2-3 (2016).
[13] Taylor Lorenz, *How Rep. Eric Swalwell Became the Snapchat King of Congress*, THE HILL (Apr. 27, 2016), http://thehill.com/homenews/news/277737-swalwell-snapchat.
[14] Eric Hal Schwartz, *Why DC's Mayor Joined Snapchat*, DC INNO (Apr. 11, 2016), http://dcinno.streetwise.co/2016/04/11/dc-mayor-muriel-bowser-joins-snapchat-social-media/.
[15] Kim Janssen, *Snapchat Is No Snap for Chicago's Old School Top Cop*, CHI. TRIB. (June 21, 2016), http://www.chicagotribune.com/news/chicagoinc/ct-eddie-johnson-snapchat-20160621-story.html.
[16] Shachar Peled, *NYPD Suspends Cop who Allegedly Posted Snapchat of Handcuffed Family*, CNN (Dec. 26, 2016, 9:31 PM), http://www.cnn.com/2016/12/26/us/snapchat-arrest-trnd/.

mentioned above, public officials have also been using encryption apps in other contexts. The mayor and city attorney of Chattanooga, Tennessee, for instance, both admitted using WhatsApp to communicate for government business purposes, drawing the attention of transparency advocates.[17]

However, legal research on these privacy-promising technologies has not yet extended into their implications for transparency laws such as the federal Freedom of Information Act and state open records laws. Below, encryption and ephemeral messaging are briefly described in terms of function and legal analysis to date.

A. Encryption Tools

For centuries, cryptography has existed as a way to transmit messages that are only decipherable to the intended receiver, and are indecipherable to an interceptor. Modern encryption technology intends to keep electronic data and communications safe from interception and surveillance by third parties.[18] Simply put, encryption allows its users to restrict who can read a message to those who have the key. Encryption tools, such as PGP (Pretty Good Privacy) and GPG (Gnu Privacy Guard), allow users to create encryption keys for email platforms. This allows users to communicate without fear that someone without a key can intercept and read their communications. Edward Snowden used GPG to contact Micah Lee, a technologist for the Electronic Frontier Foundation, who helped Snowden connect with documentary journalist Laura Poitras. They used GPG encryption to protect their communications and ultimately to facilitate the leak of National Security Agency documents that revealed illegal spying practices.[19]

In the past few years, encryption tools have become simpler to use through the development of smartphone apps. Signal, launched in 2013 by Open Whisper Systems, allows encrypted communications via text messages through an "idiot-proof interface, which . . . is just as straightforward as normal calling and texting."[20]

---

[17] Paul Leach, *Chattanooga Mayor Admits Using Encrypted Messaging App to Converse with Staff*, CHATTANOOGA TIMES FREE PRESS (Sept. 27, 2016), http://www.timesfreepress.com/news/local/story/2016/sep/27/mayor-andy-berke-admits-using-encrypted-messa/388807/.

[18] Orin S. Kerr & Bruce Schneier, *Encryption Workarounds*, 106 GEO. L. J. 989, 993 (2018).

[19] Micah Lee, *Ed Snowden Taught Me to Smuggle Secrets Past Incredible Danger. Now I Teach You*, INTERCEPT (Oct. 28, 2014, 1:36 PM), https://theintercept.com/2014/10/28/smuggling-snowden-secrets/.

[20] Andy Greenberg, *Signal, the Snowden-approved Crypto App, Comes to Android*, WIRED (Nov. 2, 2015, 8:06 PM), https://www.wired.com/2015/11/signals-snowden-approved-phone-crypto-app-comes-to-android/.

Instead of the key exchange in PGP and GPG, all Signal requires is that users accept invitations from other users through their phone numbers, and the app encrypts their messages. By password-protecting their phones, users provide the first layer of protection; somebody hoping to access the conversations on Signal must guess or hack the phone passcode to access the app. Signal itself keeps no records of the communications that could be demanded by government or other third parties. The chat app WhatsApp, the most popular chat app worldwide with more than 1 billion users, adopted Open Whisper Systems's Signal technology to provide encryption by default for its users starting in 2014 on Apple devices, and extended to all users by 2016.[21]

By default, Signal and WhatsApp provide end-to-end encryption, placing keys "solely in the hands of device holders" in a way that "significantly disrupts traditional forms of surveillance that have relied on third parties' (telecommunication providers and ISPs) having access to communications content, at least in most circumstances."[22] The main way for the government to access the information on these devices is by getting a "backdoor" from the tech company that develops the encryption software. The companies are reluctant to provide "backdoor[s]" in the name of protecting their users' privacy.[23] Most famously, in 2016, Apple resisted a Justice Department request to decrypt the iPhone belonging to a terrorist attack suspect in San Bernardino, California. The government's move drew the opposition of "[a]lmost every major technology company…including Facebook, Amazon, Google, Microsoft, Yahoo, AT&T, and Twitter."[24] Nearly every Justice Department effort to compel Apple to decrypt its devices, including obtaining a court order requiring decryption, failed to achieve Apple's compliance.

[21] Ellen Nakashima, *WhatsApp, the Messaging Service, Announces Full Encryption on all Platforms*, WASH. POST (Apr. 5, 2016), https://www.washingtonpost.com/world/national-security/whatsapp-the-messaging-service-announces-full-encryption-on-all-platforms/2016/04/05/80f071f6-fb3e-11e5-9140-e61d062438bb_story.html?utm_term=.11e0fdac6186.

[22] Stephanie K. Pell, *You Can't Always Get What You Want: How Will Law Enforcement Get What It Needs in a Post-CALEA, Cybersecurity-Centric Encryption Era?*, 17 N.C. J. OF L. & TECH. 599, 625 (2016).

[23] Kerr and Schneier detail six different ways of the government breaking encryption for law enforcement purposes: "find the key, guess the key, compel the key, exploit a flaw in the encryption scheme, access plaintext when the device is in use, and locate a plaintext copy." *See* Kerr & Schneier, *supra* note 17 at 22 (suggesting that a backdoor is a way of exploiting a flaw in encryption).

[24] *Id*. at 38.

Ultimately, the Justice Department turned to paying private hackers about $1 million to access the information.[25]

Encryption tools can be described as "dual use" technologies with both positive and negative functions.[26] Kerr and Schneier discuss how criminals may use encryption technology to conceal evidence, but the government often uses the same technology to "maintain the privacy of valuable government data," and thwart criminal efforts to break the encryption.[27] Similarly, these tools can be and have been used to enable encrypted communications involving government officials, which triggers potential issues under open government laws.

B. Ephemeral Messaging Apps

The innovation of disappearing messaging launched Snapchat from a startup in 2011 to one of the most popular social media apps today, with an average of 158 million daily users by the end of 2016.[28] Snapchat's key feature is that a user can send images and captions that vanish after viewing, challenging the notion that whatever is posted online is permanent.[29] Snapchat users frown upon subverting the disappearing nature of photos through taking screenshots or otherwise capturing photos before they vanish, one of the "unwritten rules" of the platform.[30] Snapchat notifies users when someone has taken a screenshot of a photo or video. Snapchat's community guidelines note, "it's okay with us if someone takes a screenshot, but we can't speak for you or your friends."[31] The disappearing message feature has

[25] Ellen Nakashima, *FBI Paid Professional Hackers One-Time Fee to Crack San Bernardino iPhone*, WASH. POST (Apr. 12, 2016), https://www.washingtonpost.com/world/national-security/fbi-paid-professional-hackers-one-time-fee-to-crack-san-bernardino-iphone/2016/04/12/5397814a-00de-11e6-9d36-33d198ea26c5_story.html?utm_term=.806637c69a3d.
[26] Kerr & Schneier, *supra* note 17, at 995.
[27] *Id.*
[28] Michael J. de la Merced & Katie Benner, *Snapchat Parent Showcases Its Strength in Preparation for I.P.O.*, N.Y. TIMES (Feb. 2, 2017), https://www.nytimes.com/2017/02/02/business/dealbook/snapchat-ipo-nyse.html.
[29] Haley Tsukayama, *Snapchat Processes 150 Million Images Per Day*, WASH. POST (Apr. 16, 2013), https://www.washingtonpost.com/business/technology/snapchat-handles-150-million-images-per-day/2013/04/16/6732c3f0-a69f-11e2-8302-3c7e0ea97057_story.html?utm_term=.436f15e5c542.
[30] Kevin Smith, *These Are The 17 Most Annoying Things On Snapchat*, BUZZFEED (Dec. 1, 2016), https://www.buzzfeed.com/kevinsmith/17-unwritten-rules-of-snapchat?utm_term=.luY4X0AYD#.jizDkgmYV.
[31] *Community Guidelines*, SNAPCHAT, https://support.snapchat.com/en-US/a/guidelines (last visited Mar. 28, 2017).

become so popular that other platforms are introducing similar features, such as Instagram's direct messaging system.[32]

The Confide app, which became popular among White House staffers in the early days of the Trump administration,[33] combines both encryption and ephemeral messaging features. As the developers note, Confide "uses military-grade end-to-end encryption to keep your messages safe and ensure they can only be read by the intended recipients" and is "ephemeral" by making messages "disappear forever after they are read once" and protecting them against screenshots.[34] As the attorneys trying to prevent Missouri Gov. Greitens from using Confide argued, "Confide has a singular purpose. To shred. To destroy. To destroy communications sent and received."[35]

One benefit of an "ephemeral conduit" like Snapchat is that it provides online obscurity to users that is not otherwise available through social networking tools.[36] Jonathan Moore referred to Snapchat and similar apps as "ephemeral" or "impermanent social media." Because the messages are ephemeral, using them as evidence in litigation presents a challenge to the courts.[37]

While legal research on ephemeral messaging has touched on privacy implications and evidence, research has not yet analyzed the ramifications on government record-keeping and freedom of information laws. The next section presents law and policy considerations of ephemeral and encrypted messaging apps in the context of freedom of information laws.

II. FREEDOM OF INFORMATION LAW AND POLICY APPROACHES

The core purpose of freedom of information laws is to provide citizens access to government records, including communications between public employees, as a means of ensuring transparency. The core purpose of encryption

[32] Natalie Jervey, *Snapchat vs. Instagram: Who's Copying Whom Most?*, HOLLYWOOD REP. (Dec. 1, 2016, 7:00 AM PST), http://www.hollywoodreporter.com/news/snapchat-instagram-whos-copying-951224.
[33] Lily Hay Newman, *Encryption Apps Help White House Staffers Leak – And Maybe Break the Law*, WIRED (Feb. 15, 2017, 12:43 PM), https://www.wired.com/2017/02/white-house-encryption-confide-app/.
[34] *Features*, CONFIDE, https://getconfide.com (last visited Mar. 27, 2017).
[35] Hancock, *supra* note 8.
[36] Woodrow Hartzog & Evan Selinger, *Surveillance as Loss of Obscurity*, 72 WASH. & LEE L. REV. 1343, 1358 (2015).
[37] Moore suggests an approach that recognizes parties' privacy expectations and limits the scope of discovery ordered by courts through a proportionality test, which would consider privacy effects, the breadth of such requests, any potential chilling effect on potential litigants, and the burden that producing such content would cause the parties. Jonathan E. Moore, *Social Media Discovery: It's a Matter of Proportion*, 31 T.M. COOLEY L. REV. 403, 418-19 (2014).

and impermanent messaging apps is to shield communications between people from outside scrutiny by making them impossible to read or by making them vanish. These core principles are in conflict, and current laws and policies regarding government record-keeping and archiving are struggling to keep up with communication technology that is growing in popularity among citizens and government officials.

Here, three potential approaches policy makers could take are addressed, each with its own legal and practical challenges: (1) Ban use of these apps by public officials; (2) Enhance and adapt archiving demands already in place to address the new technologies; and/or (3) Treat the companies that offer the technologies as quasi-governmental agencies to make it possible to access the archives they maintain.

A. Ban on Use of Encryption and Ephemeral Messaging Apps

One response could be a ban on use of encrypted and ephemeral messaging apps, either through legislation or judicial action. Reports suggest the White House cracked down on staffers using Signal and Confide to talk amongst themselves and to journalists. Reports also noted that former White House press secretary Sean Spicer considered the use of these apps for official communications a violation of the Federal Records Act, though he did not publicly comment on whether using the apps had been forbidden by the administration.[38] The attorneys seeking an injunction against Greitens similarly argued in favor of a ban on government officials using apps that operate in direct conflict with the Missouri's open records law.

Greitens's lawyers argued that such a ban on government employee speech would trigger First Amendment scrutiny. Several courts recognize a First Amendment right to use the Internet and social networks to communicate. This recognition is particularly relevant for sex offenders who have challenged bars on their access to social media. The Eighth Circuit Court of Appeals recognized a convicted sex offender's First Amendment right to access the Internet in 2005, striking down a provision of his release that would "completely bar his access to computers and the Internet" as overly broad.[39] Likewise, a federal district court in Louisiana struck down Louisiana's law barring sex offenders from "unlawful use or access of social media" because it essentially served as "a near total ban on

[38] Dylan Byers, *Spicer Cracks Down on White House Leaks*, CNN (last updated Feb. 27, 2017, 4:30 PM), http://www.cnn.com/2017/02/26/politics/spicer-leaks-crackdown/.
[39] U.S. v. Crume, 422 F.3d 728, 733 (8th Cir. 2005).

Internet access" that "unreasonably restricts many ordinary activities that have become important to everyday life in today's world."[40] The U.S. Supreme Court in 2017 struck down a North Carolina state law restricting access to "a commercial social networking Web site where the sex offender knows that the site permits minor children to become members" in a case in which the defendant, a sex offender, used Facebook.[41] Recognizing the broad free speech interests in Internet communications within the "fabric of our modern society and culture," the Supreme Court noted that "foreclos[ing] access to social media altogether prevents a citizen from engaging in the legitimate exercise of First Amendment rights."[42] The North Carolina law was significantly narrower than provisions struck down by federal courts in Louisiana[43] and Nebraska,[44] not covering social networking services that provide only one service, such as photo sharing, e-mail, or instant messaging.[45]

One might expect that public officials would have no fewer rights under the First Amendment than sex offenders to access social networks. An outright ban on using a certain tool to communicate could operate as a prior restraint and may face challenges by public officials asserting their free speech rights to use the communication tools in an unofficial capacity. In *Republican Party of Minnesota v. White*, the Supreme Court struck down the Minnesota Supreme Court's canon of conduct that limited speech about political or legal disputes of candidates for judicial election, stating that the state could not overcome the strict scrutiny test in its requirement that judicial candidates could not comment on legal or political matters in the interest of maintaining judicial impartiality.[46] Elected public officials have relied on this ruling to argue that they have stronger First Amendment rights than government employees making statements pursuant to their job duties. The U.S. Court of Appeals for the Fifth Circuit recognized this in *Rangra v. Brown*, finding protection for the speech of elected government officials "is robust and no less strenuous than that afforded to the speech of citizens in general."[47]

---

[40] Doe v. Jindal, 853 F. Supp. 2d 596, 607 (M.D. La. 2012).
[41] State v. Packingham, 777 S.E.2d 738, 743-44 (N.C. 2015).
[42] Packingham v. North Carolina, 137 U.S. 1730, 1737-38 (2017).
[43] *Doe v. Jindal*, 853 F. Supp. 2d 596.
[44] *See* Doe v. Nebraska, 898 F.Supp.2d 1086 (D. Neb. 2012).
[45] *Packingham*, 777 S.E.2d at 750.
[46] Republican Party of Minnesota v. White, 536 U.S. 765 (2002).
[47] Rangra v. Brown, 566 F.3d 515, 524 (5th Cir. 2009). The court found that the criminal provisions of the Texas Open Meetings Act were "content-based regulations of speech that require the state to satisfy the strict scrutiny test in order to uphold them." *Id.* at 521. However, the same court's decision in *Asgiersson v. Abbott* four years later upheld the Texas Open Meetings Act from a similar First Amendment challenge by government officials. *See* Asgeirsson v. Abbott, 696 F.3d 454 (5th Cir. 2012), *cert. denied*, 568 U.S. 1249 (2013). Scholars have argued that because open meetings laws of this kind are content-based, they should be reviewed using strict scrutiny rather

Compared to elected public officials, government employees have limited First Amendment protection for their speech while on the job. In *Garcetti v. Ceballos,* the U.S. Supreme Court rejected "the notion that the First Amendment shields from discipline the expressions employees make pursuant to their professional duties."[48] As such, communications sent in one's official capacity via encrypted or ephemeral messaging apps that would typically be covered by public records laws would receive limited First Amendment protection. These are not the acts of a government employee in his or her role as a citizen, an essential element for asserting the First Amendment right in this context. These tools would not be used in furtherance of the government employee's "opportunit[y] to contribute to public debate," but rather to his or her conduct in official duties.[49]

Courts have allowed some restriction of public official speech in another context – open meetings laws. Public officials in Texas challenged the criminal provisions of the state's Open Meetings Act[50] on First Amendment grounds, arguing that it "criminalizes all private speech among a quorum of a governing body that is about public policy, even if such speech does not lead to corruption."[51] The U.S. Court of Appeals for the Fifth Circuit rejected this argument in *Asgeirsson v. Abbott*, finding that the section criminalizing public officials' potential Open Meetings Act dodges was content-neutral, was not overbroad or vague, and adequately supported the goals of public disclosure laws "such as increasing transparency, fostering trust in government, and ensuring that all members of a governing body may take part in a discussion of public business."[52] Similarly, state legislatures have revised open meetings laws and state attorneys general have issued rulings to clarify that certain uses of technology by public officials may violate the law. Arizona, for instance, defines a meeting as a "gathering, in person or through technological devices, of a quorum of a public body,"[53] and the attorney general has clarified that circumventing the Open Meetings Law by using email to avoid a quorum or other aspects of the law "will subject the members of the public body and others to sanctions."[54] In Florida, where meetings of two or more members of a public body constitutes a meeting subject to the state's Sunshine Law,

than intermediate scrutiny to allow some room for private discussion by public officials. *See* Steven J. Mulroy, *Sunshine's Shadow: Overbroad Open Meetings Laws as Content-Based Speech Restrictions Distinct from Disclosure Requirements*, 51 WILLAMETTE L. REV. 135 (2015).

[48] Garcetti v. Ceballos, 547 U.S. 410, 426 (2006).

[49] Pickering v. Bd. of Educ., 391 U.S. 563, 573 (1968).

[50] Tex. Gov't Code Ann. § 551.144 (West 2017).

[51] *Asgeirsson v. Abbott*, 696 F.3d at 464.

[52] *Id.*

[53] Ariz. Rev. Stat. Ann. § 38-431(4)(a) (effective Aug. 3, 2018).

[54] Ariz. Att'y Gen. Op. 105-004, 1-2 (2005).

the attorney general opined that the use of computer-based technology by county commissioners "to communicate among themselves on issues pending before the board" would violate state law.[55] A 2009 revision to the Massachusetts Open Meeting Law limited remote participation in meetings by public officials, which the attorney general advised included bans on participation via "text messaging, instant messaging, email, and web chat without audio."[56]

The logic of these limits on public official use of technology from attorney general opinions and in the *Asgeirsson* case – that public officials' free speech rights may be suborned to serve the interest in transparent governance in statutes that require disclosure – may plausibly extend to efforts to restrict government use of certain technological tools that, even when used legally by a citizen, would allow public officials to sidestep open records laws. This may be particularly true in the case of ephemeral messaging apps such as Snapchat and Confide, which by default make detection of their messages extremely difficult if not impossible. As Professor Allison Stanger noted, "Since Confide is explicitly designed to eliminate a paper trail, its use creates at least the appearance of misconduct, if not the reality."[57]

While there may be theoretical value for a ban on public official use of encrypted and ephemeral messaging apps, and even if such a ban would be permissible under the First Amendment,[58] it would have problems in practice. First, not all government officials and employees will be using government-issued devices to do work, making monitoring of device use difficult when government employees use personal devices and the apps on them for both personal and work purposes. While government agency heads may frown upon employees using their own smartphones for work purposes in general,[59] the Obama administration in 2012 acknowledged the reality of this practice, offering guidance to federal agencies to help them develop "bring your own device" (BYOD) policies, noting employees' "increased mobility and better integration of their personal and work lives" as well as "the flexibility to work in a way that optimizes their productivity."[60] Second, as

[55] Fla. Att'y Gen. Op. 89-39, 2 (1989).
[56] MASS ATT'Y GEN., OPEN MEETING LAW GUIDE, 14 (Mar. 18, 2015), http://www.mass.gov/ago/docs/government/oml/oml-guide.pdf.
[57] Newman, *supra* note 32.
[58] One could imagine, for example, government employees arguing that a ban on using legal messaging apps for government purposes would be broader than necessary to ensure the purpose of transparency laws, particularly in light of the archiving requirements mentioned in the next section, *infra*.
[59] Amrita Jayakumar, *Report: Government Agencies Don't Like 'Bring-Your-Own-Device' Policy*, WASH. POST (Apr. 28, 2015), https://www.washingtonpost.com/business/on-it/report-government-agencies-arent-thrilled-about-bring-your-own-device-policy/2015/04/28/715fc962-edc0-11e4-8abc-d6aa3bad79dd_story.html?utm_term=.223c1e25b43d.
[60] THE WHITE HOUSE, DIGITAL SERV. ADVISORY GRP., BRING YOUR OWN DEVICE

every teenager knows, hiding or quickly deleting apps on smartphones is not difficult, making it possible for government employees to either install an app or create secret folders making detection of the apps difficult.[61] Spot checks such as the one the White House spokesman conducted could be easily sidestepped for a government staffer expecting such events. And third, more about wisdom than practicality, is acknowledging that using encrypted and ephemeral messaging apps may have benefits to providing better, more transparent government by providing whistleblowers a more secure channel to contact journalists or advocates when they want to report government abuse. After *Garcetti*, some legal scholars feared a chilling effect on whistleblowers. As Drechsel noted, "[i]f government employees can be disciplined without First Amendment limits for job-related speech, government employers now have another tool to discourage, intimidate and punish whistleblowers and leakers, as well as to control employees whose primary work is public communication."[62] Drechsel considered the risk for public employees who could be punished for speaking in ways critical of their government employers, thus threatening the free flow of information. A ban on encrypted and ephemeral messaging apps, enforceable by either legislated criminal penalties or judicial contempt sanctions, would be a similar deterrent. Without GPG encryption, Edward Snowden would have been subject to higher risk for detection when he leaked records documenting government surveillance abuses; mobile apps that provide similar avenues for government employees, while possibly subverting freedom of information laws, may at the same time help with a different method of oversight.

As such, an outright ban on government employee use of encrypted and ephemeral messaging apps would likely be permissible under First Amendment limits of government employee speech, though it would present some practical and policy challenges. The National Archives Records Administration (NARA), which oversees federal records management including compliance with the Federal Records and the Freedom of Information Act, has announced as much in its record-keeping guidance, noting, "[s]imply prohibiting the use of electronic messaging accounts to conduct agency business is difficult to enforce and does not

(Aug.23, 2012), https://obamawhitehouse.archives.gov/digitalgov/bring-your-own-device.

[61] *See, e.g.*, Mike Wehner, *How to Completely Hide Any App or Folder on Your iPhone or iPad*, ENGADGET (Mar. 26, 2014), https://www.engadget.com/2014/03/26/how-to-completely-hide-any-app-or-folder-on-your-iphone-or-ipad/; Ben Woods, *How to Securely Hide Your Files and Apps on Android*, ANDROIDPIT (Mar. 26, 2017), https://www.androidpit.com/how-to-hide-your-files-and-apps-on-android.

[62] Robert E. Drechsel, *The Declining First Amendment Rights of Government News Sources: How Garcetti v. Ceballos Threatens the Flow of Newsworthy Information*, 16 COMM. L. & POL'Y 129, 139 (2011).

acknowledge the ways employees communicate."[63] A more palatable avenue to manage government use of encrypted and ephemeral apps may instead be adapting existing record-keeping and archiving plans to address these issues.

B. Adapt and Enhance Archiving Policies

In response to the widespread use of email for government purposes, state and federal government agencies have outlined requirements for archiving emails, either through modifications of freedom of information laws or agency policies. Text messaging, on the other hand, has been a bit more problematic for records management and archiving by government agencies.[64] This presents potential problems in the context of encrypted and ephemeral messaging apps, which are essentially a form of text messaging made even more difficult to manage and archive.

There is no question that text messages are covered by public records laws at both the state and federal levels as a form of electronic communication, and the use of personal devices does not alter the reach of public records laws to text messages when they are used for government purposes. As Senat explained in his examination of the application of public records laws to private ownership of devices by government employees, most courts and attorneys general "have rejected the notion that a government official's ownership of a device is more important than the substance of the information" that was being communicated on that device.[65] What matters is whether "official government business" is being transacted on the device; if so, then the messages in question, regardless of format or device ownership, are subject to public records laws.[66]

NARA detailed archiving and retention strategies for chat/instant messaging, text messaging, voicemail messaging, and other messaging platforms (including Snapchat and WhatsApp) in a bulletin sent to agency heads in 2015, with the purpose of providing guidance for compliance with the Federal Records Act

[63] NATIONAL ARCHIVES AND RECORDS ADMINISTRATION, BULLETIN 2015-02 (July 29, 2015), https://www.archives.gov/records-mgmt/bulletins/2015/2015-02.html.
[64] *See* Sandra F. Chance & Christina M. Locke, *Struggling with Sunshine: Analyzing the Impact of Technology on Compliance with Open Government Laws Using Florida as a Case Study*, 21 FORDHAM INTELL. PROP. MEDIA & ENT. L. J. 1 (2010); Cheryl Cooper, *Sending the Wrong Message: Technology, Sunshine Law, and the Public Record in Florida*, 39 STETSON L. REV. 411 (2010).
[65] 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, 322 (2014).
[66] *Id*.

and the Freedom of Information Act.[67] This mandated agencies to have a records schedule for deletion of electronic messages, with the warning that "unscheduled records must be treated as permanent." Additionally, the bulletin encouraged agencies to "determine a minimum time frame to keep electronic messages" in a "searchable and retrievable manner," with the recognition that agencies would need to do this regardless of whether the messaging system was in house or was created by a third party.[68] But the lengths of these schedules are unclear and vary based on the kind and purpose of the record. In the context of emails, for example, NARA has noted that schedules may allow for the immediate deletion of "transitory" emails, while some agencies may retain emails "for decades and then transferred to NARA for permanent preservation," while in other cases, it may be appropriate for an agency to retain emails for one year "to meet audit and access requirements."[69]

As such, records retention policies at the federal level have created some confusion. In 2016, the Environmental Protection Agency (EPA) was audited after a conservative watchdog and U.S. Representative Lamar Smith alleged that EPA employees, including the top administrator, had improperly deleted thousands of text messages about official business to avoid compliance with the Federal Records Act and the Freedom of Information Act.[70] The EPA's Office of Inspector General found that agency employees sent 3.1 million text messages over a 12-month period on government-issued devices as well as uncountable numbers more on non-agency devices that may also have been subject to federal records laws.[71] While the audit did not find intentional wrongdoing on the part of EPA employees, it found several problems with compliance, such as a lack of procedure for the agency's "FOIA personnel" or other staff to examine text messaging that may need to be retained as a record on a regular basis, with such searches ranging from every 20 days to "periodically (at least monthly)."[72] Further, employee devices included defaults for automatic text message deletion "after 30 days, one year, or forever," with

[67] NAT'L ARCHIVES AND RECORDS ADMIN., BULLETIN 2015-02 (July 29, 2015), https://www.archives.gov/records-mgmt/bulletins/2015/2015-02.html.
[68] *Id*.
[69] NAT'L ARCHIVES AND RECORDS ADMIN., BULLETIN 2014-06 (Sept. 15, 2014), https://www.archives.gov/records-mgmt/bulletins/2014/2014-06.html.
[70] *See* Timothy Cama, *GOP Chairman Subpoenas EPA on Texts*, THE HILL (Mar. 25, 2015, 4:45 PM), http://thehill.com/policy/energy-environment/236955-gop-chairman-subpoenas-epa-on-texts.
[71] ENVIRONMENTAL PROTECTION AGENCY OFFICE OF INSPECTOR GENERAL, CONGRESSIONALLY REQUESTED AUDIT: EPA NEEDS TO IMPROVE PROCESSES FOR PRESERVING TEXT MESSAGES AS FEDERAL RECORDS, Rep. No. 17-P-0062, 1-2 (Dec. 21, 2016), https://www.epa.gov/sites/production/files/2016-12/documents/_epaoig_20161221-17-p-0062.pdf.
[72] *Id*. at 9.

employees varying in their settings, including one high-level administrator who configured his government-issued phone to delete all texts after 30 days.[73]

Similar challenges are present at the state level, where records retention schedules "vary greatly."[74] A review of email schedules in 2014, for example, noted that Pennsylvania allows purging of state employee emails after five days, while New York automatically deletes after 90 days, and North Carolina keeps all executive branch emails for five years.[75] An audit by a coalition of newspapers and television stations in North Carolina revealed difficulties in receiving the text messages reporters requested under the state's Public Records Act in January 2017. While all agencies responded and several provided records, some said their top officials did not use text messaging, while others noted that they did not have retention or archiving policies, including the state auditor. The authors concluded, "it's clear that getting access to those public records depends largely on the goodwill of those department heads."[76] An audit by journalists of Florida agencies in 2016 had similar results, showing some confusion among officials, as one city attorney declared that text messages of public officials were not public records. "Depending on what county (the public officials are) in, you may wait a long time or pay a hefty fee to find out what they've typed. And even then, you have to trust some when they say they didn't send any texts," the journalists explained.[77]

The current state of open records laws, at both the state and federal level, reflects the difficulty in retaining and archiving government text messages, even without considering the practical challenges presented by encrypted and ephemeral messaging apps. In Texas, for example, the Library and Archives Commission sets the state's records retention schedules (RRS) as a guide for agencies to use in establishing their own internal schedules, with required minimums for which records must be kept before they may be destroyed or otherwise archived.[78] The default retention period is one year from the date a record is created, though the

[73] *Id*. at 16-17.
[74] Jenni Bergal, *Save or Delete? Official Email Policies Vary by State*, PEW CHARITABLE TRUSTS STATELINE (Oct. 30, 2014), http://www.pewtrusts.org/en/research-and-analysis/blogs/stateline/2014/10/30/save-or-delete-official-email-policies-vary-by-state.
[75] *Id*.
[76] Mark Binker et al., *Lawsuits, Appointments and 'a Wreck': Texts Offer Glimpses into How NC Government Works*, NEWS & OBSERVER (Mar. 13, 2017, 8:11 PM), http://www.newsobserver.com/news/politics-government/article138062978.html.
[77] Eliot Kleinberg, *Text Messages by Local Officials Muddy Public-Records Law*, MIAMI HERALD (Mar. 10, 2016, 8:00 AM), http://www.miamiherald.com/news/state/florida/article65529447.html.
[78] TEXAS STATE LIBRARY AND ARCHIVES COMMISSION, TEXAS STATE RECORDS RETENTION SCHEDULE, 4TH ED. (Aug. 31, 2016), https://www.tsl.texas.gov/sites/default/files/public/tslac/slrm/recordspubs/RRS%202016-08-31_final.pdf.

RRS are somewhat vague about this, noting that "transitory information" such as electronic communications should be retained "until the purpose of the record has been fulfilled," and mentions nothing specifically about text messages or messaging applications.[79] The level of detailed guidance that would need to be provided to a Capstone-like coordinator or records custodian in each government office would need to be greatly enhanced in order to adequately capture and retain difficult records such as ephemeral messages on Snapchat and Confide, or managing encrypted messaging services such as WhatsApp.

At the federal level, the NARA suggested following the "Capstone Approach" that it developed in 2013 to address email retention of federal agencies, which allows agencies to rely more on automation and to create schedules for retention and archiving based on the "work and/or position" of each government employee.[80] For example, an agency could designate that messages from "the accounts of officials at the top of an agency or an organizational subcomponent" be retained permanently, while messages of lower-level employees may be kept for a shorter period of time.[81] This approach potentially shifts the burden to individual account holders and their staffers to self-report and monitor their own compliance as each agency determines through its own policy. One practical approach for agencies would be to create policies in which employees must voluntarily disclose which messaging apps they use, both on their government-issued and personal devices, and that records custodians or other staffers charged with oversight set up schedules for regular backup and archiving of those texts. In the case of encrypted messaging, the policy could require that the records custodian be provided the keys, which could be used to decrypt any messaging for review and release upon a proper open records request.

However, this does not entirely get around the problems uncovered in the state audits in North Carolina and Florida – reliance on the good faith behavior of public officials to comply with records retention and release policies that are poorly defined and have little consequence for non-compliance. Actions such as the 2016 investigation into the EPA and the House Oversight Committee's requests to federal agency heads to document agency policies on retention of messaging will put pressure on agencies to comply. The emergence of encrypted and ephemeral messaging apps makes such oversight difficult, particularly if the apps are being used by public employees deliberately to hide from public scrutiny.

---

[79] *Id*. at 21.
[80] NAT'L ARCHIVES AND RECORDS ADMIN., BULLETIN 2013-02 (Aug. 29, 2013), https://www.archives.gov/records-mgmt/bulletins/2013/2013-02.html.
[81] *Id*.

As such, while enhanced electronic records management and archiving rules should certainly be encouraged to ensure that government communications are available under state and federal freedom of information laws, relying on these policies to overcome the aforementioned obstacles threatens to fall short of the laws' transparency goals. And while reasonable oversight policies may be put in place for archiving and releasing encrypted messaging, the records management policies mentioned above still do not provide a practical way to handle archiving of disappearing messages in ephemeral apps. To tackle that problem, one possible solution may be to place a greater burden on third-party service providers.

C. Treat App Developers as Quasi-Governmental Entities

Freedom of information laws generally include some provision that extends transparency principles to private entities that serve government functions, though there is a lot of variance in the extent to which such quasi-governmental entities are covered. In general, a purely private business is not subject to public records laws; instead, the laws require some nexus between the private entity and the government, usually involving a level of government funding and function performed by the entity. The growth in privatization of services often provided by government that are now assigned out to private contractors – such as bus services for public schools, security and imprisonment of inmates, and fundraising for public universities – has led to conflicts over attempts to access the records created by those entities while doing government-like work.[82]

To be clear, there is not currently a valid legal argument to be made that developers of ephemeral messaging apps are subject to state or federal open records laws as a quasi-governmental agency. However, the theory underpinning these laws – that private entities providing important services to government that would typically be performed by government may be subject to open records laws – could be adopted by legislators to provide an avenue for public oversight of government communication that is otherwise difficult, if not impossible, for reasons mentioned in the previous sections of this article. Shifting the burden of oversight to the entity with easier access to these records – the companies themselves – on the theory that they are acting in a limited quasi-governmental capacity may fill some of the gap in access laws and regulations.

[82] *See* Rani Gupta, *Privatization v. The Public's Right to Know*, REPORTERS COMMITTEE FOR FREEDOM OF THE PRESS, 1-5 (Summer 2007), https://www.rcfp.org/rcfp/orders/docs/PRIVATIZATION.pdf.

The key elements that access laws typically require to establish that an entity is serving in a quasi-governmental role are, to put it simply, *function* and *funding*. The entity must be performing some kind of government-related task, and the government must be providing financial support to the entity.[83] In a broad sense, ephemeral messaging apps may be considered to be serving a government function by enabling a certain kind of privacy-protecting communication otherwise unavailable through official government channels such as email systems. Consider public officials who use private email services. For example, when she was governor of Alaska, Sarah Palin was found to have been using two personal Yahoo email accounts to conduct government business in a way that unlawfully sidestepped the state's open records laws.[84] In this situation, the relationship between the email service user and the provider did not automatically turn the provider into a quasi-governmental agency. Rather, the government agency responding to a request processed it by receiving the emails in question from the providers and screening them before release. Regardless, the materials were in the possession of a non-government third party, which made retrieval more difficult.

That said, private email service providers are not a perfect parallel for ephemeral messaging services such as Snapchat and Confide, which do not conduct the same kind of archiving. In its guidance to law enforcement agencies that may be seeking access to Snaps, Snapchat notes that "we delete each Snap from our servers once all recipients have viewed it," and unopened messages are deleted after 30 days, unless users put the content in their "Memories" folder for preservation.[85] Even the metadata about Snapchat messages – that is, logs of messages sent and received, which do not include the actual content – are only retained for 31 days by

[83] In some cases, statutes also require the government to exert a level of control or authority over the private body. This is the case in the federal government, which restricts FOIA to certain executive branch agencies, with a narrow definition of agency. In *Dong v. Smithsonian Institution*, the U.S. Court of Appeals for the District of Columbia Circuit held that the Smithsonian, despite ties to government on its board and its federally allocated funds, was not an "agency" under the federal Privacy Act because it was neither "government-controlled" nor otherwise established in or by the executive branch. The court noted that the language and history defining "agency" in the Privacy Act was similar to the language in the Freedom of Information Act, recognizing five categories of establishments that would qualify as an "agency" ("any executive department, military department, Government corporation, or Government controlled corporation" or "other establishment in the executive branch"). Dong v. Smithsonian Institution, 125 F.3d 877, 878 (D.C. 1997), cert. denied, 524 U.S. 922 (1998).

[84] Matea Gold, *Sarah Palin Emails: Alaska Set to Release a New Trove of Documents from Palin's Governorship*, L.A. TIMES, (June 9, 2011), http://articles.latimes.com/2011/jun/09/news/la-pn-palin-emails-20110609.

[85] Snapchat Law Enforcement Guide, 9 (Oct. 11, 2016), https://storage.googleapis.com/snap-inc/privacy/lawenforcement.pdf.

Snapchat.[86] Confide merely notes that it may be required to disclose account information "in response to lawful requests by public authorities" or otherwise to "court orders and subpoenas," without any more detail about its retention policies or ability of law enforcement to obtain content or metadata from communications.[87] However, despite these attempts to guarantee users that messages and photos sent through the ephemeral services will disappear permanently, people have found ways to hack into Snapchat, leading to massive privacy breaches. Snapchat settled a dispute with the Federal Trade Commission in 2014 involving lax security that allowed people to use third-party apps to infiltrate Snapchat photos and videos, which specifically enabled people to take screenshots and store them without the sender's knowledge.[88] While that settlement was ongoing, Snapchat was hit by hackers who published nearly 100,000 photos that users expected had disappeared.[89] Snapchat said that this was not a result of hackers accessing their servers, but rather use of third-party apps that were not allowed under its Terms of Use.[90] If hackers are able to find ways to infiltrate an ephemeral messaging app to make its messages permanent, it is certainly possible that government records custodians could work with the company on a legal solution to do the same for public records purposes, or that the company could anticipate such requests and provide more thorough archiving services in certain situations.

Recognizing a limited quasi-governmental relationship when government employees use ephemeral messaging services would help enable such solutions. However, it would require legislation as, typically, these laws have been found not to extend to private bodies without substantial connections between the business and the government. In one high-profile case, Texas law deemed not-for-profit collegiate athletic associations were not "governmental bod[ies]," which include "the part, section, or portion of an organization, corporation, commission, committee, institution, or agency that spends or that is supported in whole or in part by public funds."[91] Interpreting what at the time was called the Texas Open Records Act, the U.S. Court of Appeals for the Fifth Circuit declined to extend the definition of "government body" to the NCAA or the Southwest Conference in connection

[86] *Id*. at 8.
[87] *Privacy Policy*, CONFIDE, https://getconfide.com/privacy (last visited September 22, 2018).
[88] *See* FTC, FTC Approves Final Order Settling Charges Against Snapchat (Dec. 31, 2014), https://www.ftc.gov/news-events/press-releases/2014/12/ftc-approves-final-order-settling-charges-against-snapchat.
[89] *See* Lorenzo Franceschi-Bicchierai, *98,000 Hacked Snapchat Photos and Videos Posted Online*, MASHABLE (Oct. 13, 2014), http://mashable.com/2014/10/13/the-snappening-photos-videos-posted/#PIZJ7EOMZuqu.
[90] *See id*.
[91] Tex. Gov't Code § 552.003(1)(A)(xii) (2018).

with records requests made to those institutions regarding football recruiting violations at Southern Methodist University.[92] While the court found that "gate receipts and television revenue paid" to the NCAA and the Southwest Conference were "public funds," it did not find that the funds extended beyond "specific, measurable services" typical of a normal quid-pro-quo contract.[93]

Open records laws typically also require private businesses to have a close connection to the government body, which would not be the case for encrypted and ephemeral messaging apps absent additional legislation. For instance, a "non-profit corporation that provides emergency medical transportation services" such as ambulance and helicopter flights was found not to be a "government body" under the Texas Public Information Act. Even though the company received public funds, the threshold the court applied was whether the relationship is such that the company is "so closely associated with the governmental body that the private entity falls within" the act. In this case, the court found that the relationship was an arms-length contract with sufficient quid pro quo, and as such was merely an exchange of payment for services rather than establishing the company as a "government body" for public records purposes.[94]

While establishing a private entity as doing a public function may be somewhat difficult, funding is perhaps even more so, and a problematic one for policymakers who may be interested in extending the theory of quasi-government operations to external communication services.

The funding of a quasi-government entity typically does not have to be entirely from the state. For instance, the Indiana Supreme Court found that the Indianapolis Convention and Visitors Association, a "private not-for-profit corporation that receives revenue from both public and private sources," was a public entity "subject to the Indiana Access to Public Records Act."[95] The law was drafted broadly to allow public inspection of records of an entity if it is funded in whole or in part through public funds or tax appropriations, thus making it subject to audit by the State Board of Accounts. But the court made it clear that a "fee-for-services" arrangement would not have been enough to make the association subject to the Public Records Law.[96] If an entity is merely performing a service as part of

[92] Kneeland v. Nat'l Collegiate Athletic Ass'n, 850 F.2d 224, 231 (5th Cir. 1988).
[93] *Id*. at 228-30.
[94] CareFlite v. Rural Hill Emergency Med. Serv., Inc., 418 S.W.3d 132, 139 (Tex. Ct. App. 11th Dist. 2012).
[95] Indianapolis Convention & Visitors Ass'n, Inc. v. Indianapolis Newspapers, 577 N.E.2d 208, 209 (Ind. 1991).
[96] *Id*. at 212.

an arms-length negotiated contract, it is usually not enough to establish the entity as quasi-governmental and subject to open records laws.[97]

Because the government does not fund developers of encrypted and ephemeral messaging developers, they are not subject to current public records laws. Ephemeral messaging apps are services that are free for anyone with a smartphone to download and use, at least on a small scale. Snapchat is free for users, and derives its funding from both advertising and from providing opportunities for users to engage with brands.[98] The basic services of Confide are free for individual and small group users, with limited fee-based services (such as message retraction and priority support). They also offer a "pro" version for larger groups and businesses, which costs $15 per user per month, and even a variably-priced solution for large organizations.[99] Unless government agencies took the unlikely step of paying for these kinds of services, there would not constitute the type of financial support typically required to make private entities subject to open records laws on a quasi-government theory. Even then, if the government were merely contracting out a service for payment, it would still not likely establish that the entity was acting in a quasi-governmental capability.

As such, at both the levels of function and funding, the theory of quasi-governmental activity allowing public records law access to ephemeral messaging apps is dubious, unless legislators or policymakers were to consider targeted revisions that would allow such access by necessity. Such a move would necessarily require both that the ephemeral messaging developers maintain an archive for accounts operated by government employees and would require special access, either by the records custodians or direct request from the public, to facilitate inspection and copying of those records. The approach would also have to be very narrow to avoid security lapses and risks for abuse by government investigators. One potential example in limiting the scope of access to records held by third parties is Pennsylvania's Right to Know Law, which provides a means of access to "a public record that is not in the possession of the agency but is in the possession of a party with whom the agency has contracted to perform a governmental function on behalf of the agency, and which directly relates to the function of the government

[97] *See, e.g.*, CareFlite v. Rural Hill Emergency Med. Serv., Inc., 418 S.W.3d 132, 139 (Tex. Crim. App. 11th Dist. 2012).
[98] See Alex Barinka & Sarah Frier, *Snapchat Is Justifying Its $20 Billion Valuation by Emphasizing User Engagement*, BLOOMBERG (Jan. 20, 2017, 5:19PM), https://www.bloomberg.com/news/articles/2017-01-20/snap-said-to-stress-addicted-users-to-justify-20-billion-value.
[99] *Products & Pricing*, CONFIDE, https://getconfide.com/products (last visited Sept. 22, 2018).

agency."[100] The Pennsylvania law is limited only to those records that are of a government nature, not to all records in possession of the third party.[101] Requests for records go to the agency, which if it determines if the record is open, and consequently, if it must acquire copies from the third party to pass on to the requester.[102]

Efforts by legislators to require mandatory archiving by private companies have been met with resistance. The European Union attempted to do this through the Directive on Mandatory Retention of Communications Traffic Data in 2006, which would have required member states to adopt guidelines for electronic communication companies to retain data for six months to two years "for the purpose of the investigation, detection and prosecution of serious crime."[103] In 2014, the European Court of Justice struck down the data retention directive, finding it infringed privacy rights of citizens and did not provide sufficient safeguards to prevent against abuse and unlawful access of the data.[104]

Another possibility would be legislation which requires apps to have a "government user mode" that would automatically retain such users' texts in their archives, with the app creator acting as a quasi-government operator subject to state or federal freedom of information laws. Yet another possibility, from a proactive transparency perspective, would be legislation that requires communication app developers to build in a feature that automatically synchronizes communications to or from government employees[105] to the state or federal agency records custodian or archiving service for retention, in line with the "Capstone Approach" outlined in the previous section.

CONCLUSION

When Utah was in the process of revising its Government Records Access and Management Act in 2011, one of its more controversial provisions was closing access to private text messages and instant messages of public officials. Charles Davis, at the time the director of the National Freedom of Information Coalition,

[100] 65 Pa. Stat. Ann. § 67.506(d)(1) (2016).
[101] 65 Pa. Stat. Ann. § 67.506(d)(2).
[102] 65 Pa. Stat. Ann. § 67.506(d)(3).
[103] Council Directive 2006/24/EC, art. 4, 2006 O.J. (L 105) 54, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32006L0024&from=en.
[104] Case C-293/12 and C-594/12, Digital Rights Ireland Ltd. v. Minister for Communications, Marine and Natural Resources, ECLI:EU:C:2014:238, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:62012CJ0293&qid=1539222847866&from=EN.
[105] Daxton R. Stewart & Charles N. Davis, *Bringing Back Full Disclosure: A Call for Dismantling FOIA*, 21 COMM. L. & POL'Y 515, 529-530 (2016).

called it a "lobbyist's fantasy," expecting to have a conversation such as, "give me your cell phone number, Mr. Legislator, and we can have a private text conversation 24/7, even if you're on the floor."[106] The absurdity of such a possibility was just one reason open government advocates and others rallied against the revised law, which was repealed just weeks after it was enacted.[107]

The "lobbyist's fantasy" scenario remains a possibility under any state or federal open records law, though such laws make it clear that those text messages must be archived and available for public inspection, and record-keeping policies have been adjusted to adapt to the technology with moderate success. But what options do government agencies have when dealing with messages that are encrypted and vanish by default, leaving no trace that a communication ever happened in the first place? The "lobbyist's fantasy" is a reality that open government advocates must contend with when dealing with encrypted and ephemeral messaging services.

None of the three policy approaches examined here seem to provide an easy solution. A ban on government use of encrypted and ephemeral messaging apps—even if it is deemed constitutionally viable under the First Amendment because it is necessary to ensure transparency—faces practical enforcement challenges that are common to public records and meetings laws.[108] Modifying existing archiving and record-keeping policies is a potentially viable solution, especially regarding encryption should a custodian be required to keep keys and decrypted copies of messages routinely. Successfully enacting such policies, however, relies on voluntary compliance and cooperation by the very same government employees who may be using encrypted and ephemeral messaging apps to cover their tracks or otherwise dodge oversight required by freedom of information laws. Extending a theory of quasi-governmental action to app developers—which is not currently valid as a legal argument and would thus require legislative action to shift the burden of record-keeping and archiving to the companies providing encrypted and

[106] Nate Carlisle, *Nation Criticizes Utah's Call for Records Secrecy*, SALT LAKE TRIB. (Mar. 7, 2011), http://archive.sltrib.com/story.php?ref=/sltrib/home/51374867-76/utah-government-records-law.html.csp.
[107] Dennis Romboy & Marjorie Cortez, *Utah Lawmakers Repeal Controversial Open Records Law*, DESERET NEWS (Mar. 25, 2011), http://www.deseretnews.com/article/705369372/Utah-lawmakers-repeal-controversial-open-records-law.html.
[108] *See, e.g.*, Michele Bush Kimball, *Law Enforcement Rec. Custodians' Decision-Making Behav. in Response to Fla. Pub. Rec. Law*, 8 COMM. L. & POL'Y 313 (2003); Daxton R. "Chip" Stewart, *Let the Sunshine In, or Else: An Examination of the "Teeth" of State and Fed. Open Meetings and Open Rec. Laws*, 15 COMM. L. & POL'Y 265 (2010); and Charles N. Davis, Milagros Rivera-Sanchez & Bill F. Chamberlin, *Sunshine Laws and Jud. Discretion: A Proposal for Reform of State Sunshine Law Enforcement Provisions*, 28 URB. LAW. 41 (1996).

ephemeral messaging services—also faces substantial practical hurdles, not the least of which is the fact that the companies themselves try to protect their users' privacy by rapidly deleting messages and metadata from their own servers. Ephemeral messaging solutions are, indeed, potentially the killer apps of freedom of information laws. As Confide notes in its messaging to customers, the app was created "to bring off-the-record professional communication to the digital world."[109] Undermining public records laws is a side effect of their success.

So, what's the answer? As legal scholar Orin Kerr quipped on Twitter, "Most underused answer in law: 'I don't know.'"[110] Each of the three aforementioned options may offer some guidance to legislators and policy-makers trying to uphold the spirit of public records laws. Doing nothing is, perhaps, the worst option because it allows the "lobbyist's fantasy" scenario to advance unchecked. The best solution may be educating the public, including government officials, about the underlying purpose of freedom of information laws and their role in democracy. While compliance with open records laws is historically spotty at best, what compliance there is may have less to do with fear of the largely ineffective enforcement mechanisms and more to do with the expected behavior of public officials in American democracy. We seem to be in a moment when these democratic norms that have compelled certain behaviors are being tested, if not entirely cast aside. If the law does not compel release of government records, at the serious risk of a forceful penalty, then the request for the documents in question may go ignored. The shift to a culture of consequence-free lack of compliance with open records laws, somewhat reflective of the infamous Ashcroft Memo issued in 2001 that promised Department of Justice backing for any federal agency that denied access,[111] emboldens those in government who would keep its citizens in the dark through deliberate subversion of the law through use of encryption and impermanent messaging apps.

A better approach may be adopting a strategy similar to the federal email "Capstone Approach" to management of communication apps and accounts on personal and government-issued devices, which is revised for the technology at hand. A combination of limited bans on use of ephemeral messaging apps by public officials, as well as enhanced record keeping guidelines and a legislated archiving requirement along the lines of the quasi-governmental theory offered above could

[109] *Frequently Asked Questions*, CONFIDE, https://getconfide.com/faq (last visited Sept. 22, 2018).
[110] Orin Kerr (@OrinKerr), TWITTER (Apr. 1, 2017, 11:46 AM), https://twitter.com/OrinKerr/status/848214931887534080.
[111] *See* Ellen Nakashima, *Bush View of Secrecy is Stirring Frustration*, WASH. POST (Mar. 3, 2002) https://www.washingtonpost.com/archive/politics/2002/03/03/bush-view-of-secrecy-is-stirring-frustration/d4124b14-efc2-42b2-a8f0-c6208c94eaa7/?utm_term=.502528e05e58.

work together to ensure citizen access to otherwise vanishing government records. Current federal agency approaches have already proven problematic in managing non-ephemeral text messaging, so extending this to the state and to ephemeral or encrypted messaging may present even greater challenges.

Encryption is not a bad thing in itself; neither is ephemeral messaging. Both of these tools promise privacy and provide citizens a greater ability to discuss matters with more security against government intrusion or surveillance, a value that enhances the free exchange of ideas in democratic society. While there are valuable government uses of these technologies, there are also problematic ones that will require complex law and policy discussions to resolve. In this article, the author attempted to begin some of those discussions to lead toward the creation workable solution in the future.