BOARD OF ETHICS AND GOVERNMENT ACCOUNTABILITY
GOVERNMENT OF THE DISTRICT OF COLUMBIA

March 16, 2022

VIA ELECTRONIC MAIL
The Honorable Muriel E. Bowser
Mayor, District of Columbia
1350 Pennsylvania Ave., NW
Washington, DC 20004

RE: Applicability of D.C. FOIA to Text Messaging (including Ephemeral-Content Applications, such as WhatsApp)
(#OOG 2022-001)

Dear Mayor Bowser:

This advisory opinion construes the applicability of the District of Columbia's Freedom of Information Act of 1976[1] ("D.C. FOIA") to District of Columbia government (the "District") officials' and employees' use of text messages to conduct the District's business. It clarifies that all texting protocols potentially generate public records that are subject to D.C. FOIA.

Because of the intangible and electronic character of text messages, it may be intuitive to regard them as not being "public records" subject to D.C. FOIA. But the breadth of the statute, and the interpretations given by federal FOIA and sister jurisdictions to comparable statutes, support the conclusion that text messages, to the extent that their contents are government business, are public records. This is true if they are executed through the use of personal or third-party devices. Therefore, the District's record-retention policies require modernization to specifically cover text messages and ensure their preservation and availability in response to D.C. FOIA requests.

Currently, there is no government-wide guidance on the retention of text records or the use of personal devices to conduct government business through text messages. Therefore, I urge you to issue a Mayor's Order to: (1) recognize that text messages concerning government business are public records, even if they are stored on a private device; (2) retain these texts for purposes of D.C. FOIA; (3) strongly discourage employees from texting using personal devices to transact public business and doing so only in rare instances where access to their District provided device is, for practical reasons, not available; (4) require an employee in instances where personal devices are used to transact public business, to separate and retain such records; (5) require employees to execute an affidavit attesting to search efforts conducted for responsive records on personal

[1]Freedom of Information Act of 1976, effective March. 29, 1977 (D.C. Law 1-96; D.C. Official Code § 2-531 *et seq.*).

devices; and (6) prohibit the use of ephemeral text messaging applications to conduct government business.

As Director of Open Government, I am authorized to issue advisory opinions on the implementation of D.C. FOIA pursuant to section 205c(d) of the Board of Ethics and Government Accountability Establishment and Comprehensive Ethics Reform Amendment Act of 2011, effective October 30, 2018 (D.C. Law 19-124; D.C. Official Code § 1-1162.05c(d)). I am issuing this advisory opinion *sua sponte* to provide advice and guidance on the interpretation and application of D.C. FOIA to District government officials and employees using text messages to conduct government business electronically.

I. BACKGROUND

The Office of Open Government ("OOG") receives many inquiries about whether text messages that concern government business are public records under D.C. FOIA. Moreover, the recent proliferation of ephemeral-text applications (those that are designed and marketed to obliterate the messages and the identity of their senders and other metadata after a short time)[2] has raised novel transparency concerns. The D.C. Open Government Coalition raised those concerns with you in a November 6, 2019, letter requesting that you prohibit the use of ephemeral text applications. Its President, Thomas Susman, also stated that "[f]or executive officials to use WhatsApp [(which now includes an ephemeral feature)] is such a flagrant effort to avoid public disclosure … [T]he public's business should be done in a medium that's available for public access."[3]

D.C. FOIA case law, Mayor's FOIA appeals, and D.C. FOIA regulations have not yet expressly construed text messages as "public records" under D.C. FOIA;[2] nor do the Office of the Chief Technology Officer ("OCTO") and the Office of the Secretary ("OS") expressly include text messages in their published information technology or record retention policies.[4] However, the District's policy concerning its records and affairs is that they be open to the public: "The public policy of the District of Columbia is that all persons are entitled to full and complete information regarding the affairs of government and the official acts of those who represent them as public officials and employees. To that end, provisions of [D.C. FOIA] shall be construed . . . toward expansion of public access . . . ."[5]

Therefore, I am issuing this advisory opinion that supports the interpretation and conclusion that text messages are public records under D.C. FOIA and address the need to standardize a text-messaging policy District-wide. I recommend that you adopt this interpretation and issue a Mayor's Order requiring District officials and employees to only use new technology, including text messages, in a manner that does not evade their record-keeping obligations under D.C. FOIA.

---

[2] *See generally, e.g.*, Comment, Kurt J. Starman, "Now You See It, Now You Don't: The Emerging Use of Ephemeral Messaging Apps by State and Local Government Officials," 4 CONCORDIA L. REV. 213 (Apr. 2019).

[3] Martin Austermuhle, American University Radio (WAMU 88.5 FM), "D.C. Officials Using WhatsApp for City Business May Skirt Open Records Laws" (Oct. 9, 2019), https://wamu.org/story/19/10/09/d-c-officials-using-WhatsApp-for-city-business-may-skirt-open-records-laws/.

[4] https://octo.dc.gov/page/it-policies (OCTO); Gen. Records Scheds., https://os.dc.gov/service/public-records-center (Pub. Records Ctr.).

[5] Section 201 of D.C. FOIA (D.C. Official Code § 2-531).

A. Definition and Hierarchy of Terms

I begin with a brief discussion of the technical vocabulary of text messages because several concepts and terms overlap.

Text messages can be broadly divided among:

- **SMS**—short-message service. This is the most traditional protocol for texting, using only the most common characters such as A–Z, 0–9, spaces, and basic punctuation; and

- **MMS**—multimedia messaging service. This is the now-common format with enhanced features like hyperlinks and emoji.

The default messaging applications ("**apps**") used by modern handheld devices tend to support both SMS and MMS, including enhanced media content such as photos and video.

- **OTT**—"over-the-top"—apps transmit via the internet as opposed to a cellular connection. The term "OTT" covers many common apps such as WhatsApp, Snapchat, Signal, LINE, Facebook Messenger, and Kik.[6]

Among OTT developers, many have begun to include (and promote) **ephemeral messaging**, whereby messages self-destruct soon after the reception. Ephemeral apps circumvent retention by either the sending or receiving party, reduce the risk of embarrassment, and otherwise increase secrecy. Ephemeral apps are designed to delete or obliterate content through features such as locking the recipient's phone's screen-shot capability and revealing only one line of text at a time as the user scrolls.[7] "Ephemeral messaging applications enable senders of a message to control its deletion, ranging from immediately upon reading the message . . . to . . . weeks afterwards. Different applications offer . . . the ability to control distribution of messages (to a small group versus a community . . .), . . . encryption, . . . , prevention of screenshots, . . . and removal of messages from others' devices."[8]

B. Local and International Examples that Highlight the Problem of Using Ephemeral Apps To Conduct Official Government Business

Unfortunately, the use of ephemeral applications for official business invites practices that run counter to record-retention and transparency. "Undergirding the discussion of text messages . . . as public records is the suspicion, in some cases, that these communication formats are not used accident[al]ly, but in fact in a purposeful effort to avoid . . . open records laws."[9]

---

[6]The Sedona Conference Primer on Social Media," 20 SEDONA CONF. J. 1 (2d ed. 2019).
[7]*E.g.*, https://getconfide.com.
[8] Sedona Conference, *supra* note 7 (citations omitted).
[9]Helen Vera, "Regardless of Physical Form," 32 COMM. LAW. 24, 31 (Spring 2017).

In response to concerns about Maryland Governor Larry Hogan using the ephemeral-messaging "app Wickr to communicate about a range of public issues with top aides and other state employees,"[10] Maryland House and Senate members have introduced companion bills that would amend the definition of "[p]ublic record" for purposes of both the public-information law and the records-management law to "include . . . any written, electronic, or recorded audio or video communication made in connection with the transaction of public business"; and define "unit" for purposes of records-management to "include[] the Office of the Governor."[11] The Governor stated at a January 2022 press conference, "[W]e certainly have the ability to communicate in an informal way in person, on the phone and through messaging chats . . . I think it's a pretty common practice and there's absolutely nothing wrong with it."[12]

The Senate Education, Health, and Environmental Affairs Committee and the House Health and Government Operations Committee each held a hearing on February 15, 2022. Both measures remain pending.

Additionally, a CBS affiliate in San Francisco reported that members of the Board of Supervisors (the local legislature) "us[ed] an encrypted messaging app," called Telegram, "that allows the text to self-destruct so [it] cannot be retrieved even with a court order."[13] A member of the Board confirmed that he used the app, though he appeared to believe that, if he was not communicating with a *quorum* of the Board, or of a committee, they were not in danger of creating (and thus allowing the dissipation/non-retention of) public records.[14]

Similarly, in the United Kingdom, a transparency group named Foxglove recently challenged—in an open letter—its government ministers on using the self-destructing–message features in WhatsApp and Signal, "arguing that politicians and staff could avoid accountability."[15]

In July 2021, Foxglove proceeded into court against certain government ministers, alleging violations of one of the United Kingdom's Public Records Acts.[16] Foxglove explained, "evidence of critical government decisions . . . may be lost . . . . Unlike automatic deletion of emails, where there is a period that a deleted email can be recovered, for example, to answer a FOIA request,

---

[10] Steve Thompson, "Maryland Lawmakers Target Gov. Hogan's Self-Destructing Messages," WASH. POST (Feb. 11, 2022), https://washingtonpost.com/dc-md-va/2022/02/11/hogan-wickr-deleting-messages.

[11] Transparency in Public Records Act of 2022, Md. H. Bill 395 (introduced Jan. 19, 2022); Md. Sen. Bill 307 (introduced Jan. 20, 2022).

[12] *Id.*

[13] https://sanfrancisco.cbslocal.com/2016/03/17/report-san-francisco-officials-using-secret-messaging-app.

[14] *See id.* In the District, whether a communication is a "public record," *see infra* part II, does not turn on its being communicated among any particular number of people. While quorum is necessary to enable a body to take dispositive action, and factors into whether a gathering of members constitutes a *meeting* for purposes of the Open Meetings Act, a *public record* can be created by even one District employee acting alone.

[15] *Legal Challenge over the Government using Whats*[*A*]*pp*, https://bbc.com/news/technology-56570650(Mar. 29, 2021) (citing *WhatsApp Lets Messages Vanish After Seven Days*, bbc.com/news/technology-54825021 (Nov. 5, 2020)). For its part, the Cabinet Office responded that "records of official communications are 'retained in line with guidance' " and that "this is kept under periodic review." *See id.*

[16] https://crowdjustice.com/case/stop-disappearing-gov-messages/#case_campaign_update (citing 6 & 7 Eliz. 2, chap. 51 (July 23, 1958) (compiled at legislation.gov.uk/ukpga/Eliz2/6-7/51)).

when WhatsApp or Signal messages are deleted they are gone for good. That's why we are going to court!"[17]

I echo the local and international concern about ensuring that text messages are recognized as public records and that government personnel lawfully retain these records so that they are available to fulfill D.C. FOIA requests.

C. Record Retention and Third-Party Non-Government Hosting

A particular concern about record-retention arises under ephemeral messaging or where the content is saved only by a third party (on an application like Facebook Messenger or WhatsApp) and not downloaded onto the hardware of the District official, employee, or public-body–member.

On March 1, 2022, the Council of the District of Columbia unanimously passed Bill 24-0692, the "Fidelity in Access to Government Communications Clarification Emergency Amendment Act of 2022," on an emergency basis. The title of the measure and its accompanying emergency declaration resolution[18] emphasize "that communications created or received electronically in the course of official business are subject to existing record retention obligations." The Council found that the "[u]se of applications[] such as WhatsApp, with their ability to destroy or delete communications or keep them hidden or obscured, is contrary to the District's emphasis on governmental transparency, and makes public access to these records significantly more difficult, if not impossible (in cases where certain communications are deleted)."[19] Accordingly, the Council's emergency measure would amend the PRMA[20] to clarify that (1) "public record[s]"—as defined for PRMA purposes[21]—include not just "electronic mail" but also "other communications transmitted electronically, including through any electronic messaging service"; and (2) electronic records "created or received by the District in the course of official business" must not be "destroyed, sold, transferred, or disposed of" by "enabling settings on electronic devices that allow for . . . non-retention or automatic deletion."[22]

Developers of ephemeral apps *promote* the impermanency of the content as the advantage of their software. "These ephemeral messaging apps are designed to intentionally avoid creating a record that can be accessed at a later date."[23] For example, the developer of the app "Confide" touts its product, described as "Your Confidential Messenger," as follows:

---

[17] Press Release, *We've Brought the First-Ever Lawsuit over Government Use of WhatsApp and Signal To Make Key Decisions* (July 16, 2021), https://foxglove.org.uk/2021/07/16/weve-brought-the-first-ever-lawsuit-over-government-use-of-whatsapp-and-signal-to-make-key-decisions.

[18] Fidelity in Access to Government Communications Clarification Emergency Declaration Resolution of 2022, D.C. Council Res. 24-0404 (adopted Mar. 1, 2022) (13–0 vote).

[19] *Id.* § 2(d).

[20] District of Columbia Public Records Management Act of 1985, effective Sept. 5, 1985 (D.C. Law 6-19; D.C. Official Code § 2-1701 *et seq.*).

[21] The legislation amends the PRMA but does not amend or directly refer to D.C. FOIA or to its separate (though similar) definition of "public record" (incorporated from Title I of the District of Columbia Administrative Procedure Act ("D.C. APA")). See full comparison *infra*, pt. II.A.

[22] Bill 24-0692, § 2 (amending provisions codified at D.C. Official Code §§ 2-1701(13), 2-1706(a)(1)).

[23] Starman, *supra* note 3, at 224.

> Communicate digitally with the same level of privacy and security as the spoken word.
>
> With encrypted, self-destructing, and screenshot-proof messages, Confide gives you the comfort of knowing that your private communication will now truly stay that way.
>
> . . . .
>
> Confide messages self-destruct. After they are read once, they are gone. We delete them from our servers and wipe them from the device. No forwarding, no printing, no saving . . . no nothing.[24]

I continue my discussion below with an analysis of the particular definition of "public record" that applies to D.C. FOIA.

II. TEXT MESSAGES GENERALLY MEET THE DEFINITION OF "PUBLIC RECORD"

As a threshold matter, I will discuss whether text messages, which are electronic, intangible, and frequently casual, when used to conduct government business, are "public records" under D.C. FOIA. While this question does not yet have a bright-line answer, the breadth of the definitions and public policy statements concerning public records in District statutes, and the Council's recent adoption of the amendment, discussed above, to the "public record" definition in the PRMA strongly implies that text messages are public records under D.C. FOIA.

A. District law implicitly defines "public record" to include texts.

D.C. FOIA is title II of the District of Columbia Administrative Procedure Act ("D.C. APA"),[25] but incorporates certain global definitions from Title I of the D.C. APA, including that of "public record."[26] So, for purposes of D.C. FOIA, "[t]he term 'public record' includes all . . . documentary materials, *regardless of physical form or characteristics*[,] prepared, owned, used, in the possession of, or retained by a public body. *Public records include information stored in an electronic format.*"[27]

Also, even before its recent amendment, section 2(13) of the PRMA covered intangible records generally and regardless of medium:

> "Public record" means any document, . . . photographic image, electronic data recording, electronic mail,[28] . . . video recording, sound recording, . . . or other material, *regardless of physical form or characteristic*, that documents a transaction or activity made, received, or retained pursuant to

[24] https://getconfide.com/ (one ellipsis in original).
[25] Pub. L. 90–614, effective Oct. 21, 1968 (D.C. Official Code § 2-501 et seq.).
[26] Section 209(a) of D.C. FOIA (D.C. Official Code § 2-539(a)) provides that, for "purposes of [D.C. FOIA]," the term "public record" has "the same meaning[] as provided in section 102" (*i.e.*, section 102 of the D.C. APA (D.C. Official Code § 2-502)).
[27] Section 102(18) of the D.C. APA (D.C. Official Code § 2-502(18)).
[28] The new amendment inserts before this comma the language "or other communications transmitted electronically, including through any electronic messaging service."

> law or in connection with the transaction of public business by or with any officer or employee of the District. *The medium upon which such information is recorded shall have no bearing on the determination of whether the record is a public record.*[29]

A comparison of D.C. Official Code § 2-1701(13) with D.C. Official Code §§ 2-502(18), 2-539(a)(10) shows that both statutory definitions of "public record" contemplate that public records can be intangible.

Furthermore, ever since their promulgation in 1987, the Public Records Administrator's rules have required that agencies' retention schedules account for computerized content.[30]

While District law strongly implies that texts fall among the broad range of D.C. FOIA media, texts are not yet *expressly* enumerated. The District is not alone in that regard: as of 2019, only three states' open-records laws specifically enumerated texts as potential public records, and *no* state had handed down a policy about *ephemeral*-messaging apps, either legislatively or administratively,[31] although as mentioned above, a bill is currently before Maryland's General Assembly.

Next, I review the construction of the federal Freedom of Information Act[32] and other jurisdictions' open-records law. Though not binding precedent, extra-jurisdictional authority is persuasive as guidance.

[29] *Id.* (emphasis added). The last sentence ("The medium . . . shall have no bearing . . . .") has appeared in this definition since June 13, 2008.

[30] *See* 1 D.C.M.R. § 1508.6(e) (requiring all records retention schedules to "[d]escribe permanent records adequately to show the types of records, arrangement, content, and purpose of the series, finding aids and indexes, restrictions on access, and physical form if the records are non-textual items such as maps, photographs, microforms, sound recordings, [or] computer tapes . . . .") (emphasis added).

[31] Vera, *supra* note 10, at 27; *see also* Annotation, DISCLOSURE OF ELECTRONIC DATA UNDER STATE PUBLIC RECORDS AND FREEDOM OF INFORMATION ACTS § 20, 54 A.L.R.6th 653 (2010 & Supp. 2021).

On November 9, 2021, the Michigan Legislature passed a measure directing the state's Department of Technology, Management, and Budget to "issue directives that all state departments and all state agencies must not use any app, software, or other technology that prevents it from maintaining or preserving a public record as required by law on an electronic device that is used to create a public record." MICH. ACT NO. 114. Governor Whitmer signed the bill into effect on November 22, 2021.

[32] 5 U.S.C. § 552. Section 552 was enacted into positive law as one section of Title 5 of the United States Code by Public Law 89–554. The "Freedom of Information 'Act' " is section 552's common, though unenacted, short title.

B. Federal and extra-jurisdictional authorities support the conclusion that "public records" under D.C. FOIA include text messages.

1. *Under the federal Freedom of Information Act, "Physical Form" Is Also Immaterial.*

The District of Columbia Court of Appeals has held that D.C. FOIA may be interpreted according to like provisions of the federal Freedom of Information Act, upon which D.C. FOIA was based.[33]

Federal FOIA, 5 U.S.C. § 552(f)(2)(A), expressly defines "record" to include information "maintained by an agency in any format, including an electronic format." Moreover, even before that language took effect on March 31, 1997, federal courts relied on the comparable language of 44 U.S.C. § 3301, which defined "records" to include "documentary materials, regardless of *physical* form or characteristics."[34]

In *Citizens for Responsibility & Ethics in Washington v. United States Department of Justice*,[35] the United States District Court for the District of Columbia implicitly regarded texts as "records" under 5 U.S.C. § 552, further holding that, "if the record is a text conversation with some responsive text messages, the agency must disclose the *whole* conversation" rather than only the responsive texts (removed from their context).[36] Neither party appeared to question, and the court implicitly accepted, the premise that texts are no less public records than a tangible writing (assuming their substantive contents otherwise "qualify").[37]

Based on the similarity of language in both statutes, I opine that a court will likely find the current definitions of record in District law to include text messages.

2. *Several State Courts Have Concluded that Public Records Include Texts. Some State Statutes Have Specifically Enumerated Texts as Potential Public Records.*

Several state courts have held that text messages are potentially public records (if related to government business), and that status persists even where a record is saved onto individual employees' devices or stored on a third-party server (as is often the case with commercial texting apps—texts do not necessarily download to persistent storage (such as an SD card)). Below is an analysis of these cases and statutes.

---

[33] *E.g., Dist. of Columbia v. Fraternal Order of Police Metro. Police Labor Comm.*, 33 A.3d 332, 335 n.8 (D.C. 2011).
[34] *E.g., Forsham v. Harris*, 445 U.S. 169, 183 (1980); *Save the Dolphins v. U.S. Dept. of Commerce*, 404 F. Supp. 407, 411 (N.D. Cal. 1975); *accord, e.g.*, Atl. City Conv. Ctr. Auth. v. S. Jersey Publ. Co., 637 A.2d 1261, 1266, 1267 (N.J. 1994) (citing federal case law and, *inter alia*, Colorado statute).
[35] 2020 U.S. Dist. LEXIS 92400, 2020 WL 2735570 (Case No. 1:18-cv-00007-TSC) (mem. op.) (D.D.C. May 26, 2020).
[36] *Id.* at *8 (emphasis added).
[37] *See, e.g., id.* ("The issue here is that[,] rather than considering . . . a whole text chain as 'a record,' [the defendant] defined . . . each single text as 'a record.' "). The Department of Justice's motion for summary judgment (Oct. 26, 2018) did not assert, even in the alternative, that the requested texts ought to fall outside of the definition of "records.")

a. *Michigan: Texts Used in "an Official Function" Are Public Records.*

In *Flagg v. City of Detroit*,[38] a United States District Court (applying state law) held that the defendant city government "is a 'public body' under [Michigan's freedom of information act] and that at least some of the [requested] text messages satisf[ied] the statutory definition of 'public records,' insofar as they capture communications among City officials or employees" (including then-Mayor Kwame Kilpatrick and his chief of staff) " 'in the performance of an official function.' "[39]

b. *Washington State: Texts Are Public Records if Saved on a Personal Phone or Third-Party Server.*

In *Nissen v. Pierce County*,[40] the Washington Supreme Court considered whether under the state's public records act ("PRA"),[41] text messages sent and received by a public employee in the employee's official capacity are public records. Further, the court confronted another nuance not at issue in *Flagg*: whether texts remain subject to PRA requests even if the employee used a *private* cellular phone.[42]

First, the court held that work-related text messages sent or received by the county prosecutor (where otherwise work-related) were public records. The PRA's language resembles D.C. FOIA, covering "[1] any writing [2] containing information relating to the conduct of government or the performance of any governmental or proprietary function [3] *prepared*, *owned*, *used*, or *retained* by any state or local agency."[43] The court reasoned that "when acting within the scope of his employment, [the prosecutor] 'prepare[d]' 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 . . . ."[44]

Finally, the court recognized that the prosecutor's merely conducting these government functions on his personal telephone did not undo the applicability of the PRA; the court emphasized that "employees can use their own property and still be within the scope of their employment."[45] Below I review state laws that have codified texts as public records.

[38]252 F.R.D. 346 (E.D. Mich. 2008).
[39] *Id.* at 355 (citation omitted).
[40] 357 P.3d 45 (Wash. 2015).
[41]WASH. REV. CODE chap. 42.56.
[42] The records in *Flagg* were stored on "employer-provided equipment." *See* 252 F.R.D. at 351.
[43]WASH. REV. CODE § 42.56.010(3) (emphasis added); *see also S.E.I.U. Local 925 v. Univ. of Wash.*, 447 P.3d 534, 538 (Wash. 2019) ("This definition is very broad, encompassing virtually any record related to the conduct of government."). Recall that D.C. FOIA comparably covers "all . . . documentary materials, regardless of physical form or characteristics[,] *prepared*, *owned*, *used*, in the possession of, or *retained* by a public body" (emphasis added). Part II.A, *supra*.
[44]357 P.3d at 55, 56.
[45]*Id.* at 53.

3. *States that Have Codified that Texts Are Public Records.*

Other states have *codified* the status of texts as potential public records (even where privately warehoused):

a. *Georgia*

According to Georgia law, "[p]ublic record[s]" include, *inter alia*, "computer based or generated information . . . or similar material prepared and maintained or received . . . by a private person or entity in the performance of a service or function for or on behalf of an agency or when such documents have been transferred to a *private person or entity* by an agency *for storage* or future governmental use."[46]

b. *Texas*

Section 552.002(a-2) of Texas's Government Code was amended in 2013 to modernize its references to electronic media; it provides that "*any electronic communication* created, transmitted, received, or maintained on *any* device" and "in connection with . . . official business" is included in the definition of "public information."[47] Subsection (c) adds that "[t]he general forms in which the media containing public information exist include," *inter alia*, a "*text message*, *instant message*, other electronic communication[], and a voice, data, or video representation held in computer memory."[48]

4. *Norfolk, Virginia Adopted an Express Policy that Public Records Include Text Messages.*

On January 9, 2014, People for the Ethical Treatment of Animals, Inc. (PETA), sued the City of Norfolk, Virginia, alleging, *inter alia*, that the city government had violated The Virginia Freedom of Information Act[49] by not making available certain requested text messages.[50] The parties settled and, as a term of the consent decree, the city government adopted a new policy acknowledging that "[a]ny mobile device that is used to conduct city business may be subject to [The Virginia] Freedom of Information Act" and "that text messages . . . sent or received in the conduct of public business are 'public records' as that term is defined in [The Virginia Freedom of Information Act.]"[51]

C. Summary

Based on the aforementioned, I conclude that a public body (or its agent) that creates or uses a text or similar electronic record, under the scope of employment, has thereby created a public record under D.C. FOIA. Such texts meet the definition of "public record[s]" even if the storage device

[46] GA. OFFICIAL CODE ANN. § 50-18-70(b)(2).
[47] (Emphasis added.)
[48] (Emphasis added.)
[49] CODE OF VA. title 2.2, subtitle II, pt. B, chap. 37.
[50] *PETA v. City of Norfolk*, Case No. CL14-175, consent decree at 1 (Va. Cir. Ct. Norfolk Jan. 8, 2015).
[51] *Id.* at 1, 2.

is privately owned. The term "public record" applies where the content is merely "prepared" or "used" by a public body; the *means* of storage is immaterial. Government personnel cannot evade D.C. FOIA simply by preparing records on media they happen to own. Under such an interpretation, "[i]t would matter only that the [official] paid for [a] yellow notepad, not that she is conducting the public's business on it . . . . Adopting that rationale would . . . put an increasing amount of information beyond the public's grasp" and incentivize "government officials to conduct the public's business in private."[52]

III. STATES CURRENTLY REQUIRE EMPLOYEES TO SEARCH FOR RESPONSIVE TEXT RECORDS ON PERSONAL DEVICES

Nissen, the Supreme Court of Vermont, and the Attorney General of Arizona demonstrate, it is possible to construct a procedure where employees conduct searches e for text messages concerning public business on their personal devices.

A. Arizona

In 2017 Arizona's Attorney General opined that: (1) text messages "sent or received by a government-issued electronic device or through a social media account provided by a government agency for conducting government business are public records;" and, (2) if the messages are sent or received by a personal device, "public officials have an affirmative duty to reasonably account for official activity."[53]

B. Washington State: another look at *Nissen*

The Washington Supreme Court in *Nissen* concluded that employees' "good-faith search for public records on [their] personal device[s] can satisfy an agency's obligation under" the PRA.[54]

I agree with the Washington Supreme Court that a response to a D.C. FOIA request has no choice but to rely on employees to fulfill the request. For example, even where no privately-owned storage device is involved, a FOIA officer, may submit an affidavit attesting to the search efforts for responsive records. The agency ultimately has to rely on an employee with demonstrated institutional knowledge and proper exercise of skill in identifying responsive records. Were the employee to misrepresent their efforts, or obscure or hide responsive records, they would be subject to typical personnel procedures, including discipline or termination; or prosecution, if they testified or made an affidavit or declaration. This would be the case whether the records were on personal equipment or District-owned equipment. Similarly, the District should adopt a good faith search standard requiring execution of an affidavit when an employee must search for text messages concerning government business on their personal devices. As discussed below, Vermont has adopted this process.

---

[52] Joey Senat, "Whose Business Is It . . . ?" 19 COMM. L. & POL'Y 293, 322 (Summer 2014).
[53] Nat'l Conf. of State Legislatures, PRIVACY PROTECTIONS IN STATE CONSTITUTIONS, ncsl.org/research/telecommunications-and-information-technology/privacy-protections-in-state-constitutions.aspx (Nov. 6, 2020)
[54] 357 P.3d at 56, 57, *quoted in Toensing v. Att'y Gen. of Vt.*, 178 A.3d 1000, 1011 (Vt. 2017).

C. Vermont

Toensing v. Attorney General of Vermont further emphasizes that agencies "routinely" depend on "employees' representations . . . in the context of searches of agency records," and broaches the particular procedures by which employees can be held accountable for any public records that they maintain on personal devices.[55]

Vermont's Supreme Court held that: (1) "the [Public Records Act's] definition of 'public record' includes digital documents," including text messages, even if "stored in private accounts"; and (2) the attorney general's office (AGO) was obliged, in responding to the plaintiff-appellant's underlying request, to ask the relevant staff "to provide any public records stored in their private accounts that [we]re responsive to [the] request."[56]

The court reasoned that, at least under the particular records request at issue, any "search" of private devices would be done by the individuals themselves, and that it was sufficient to rely on employees' *representations* that they searched their devices comprehensively, just as governments have no choice but to rely on the representations of the custodians of *government*-issued devices:

> . . . [T]he AGO's search will be adequate if the specified officials and employees are trained to properly distinguish public and nonpublic records, the [AGO] asks them to in good faith provide any responsive public records from their personal accounts, and they respond in a manner that provides reasonable assurance of an adequate search. This might be as simple as an *affirmation that the employee . . . has not produced or acquired any records in personal accounts in the course of agency business, or that the employee has identified all potentially responsive records through a specified word search*, and has segregated and disclosed all records produced or acquired in the course of agency business as opposed to communications of an exclusively personal nature.
>
> . . . In the absence of any evidence suggesting that an employee is conducting agency business through personal accounts, an agency may reasonably rely on the representations of its employees. In fact, agencies likely rely on their employees' representations routinely in the context of searches of agency records. That is, an agency's search of its own records may take the form of individual employees or officials searching their paper or digital files in their agency account or office, providing responsive records to the custodian of records, and representing that their search is complete. . . . [W]e decline to impose a higher burden on them when searching their personal files than applies to their search of records accessed through agency accounts or hard copies located in agency files.[57]

[55] 178 A.3d at 1013.
[56] *Id.* at 1004, 1009 (emphasis added).
[57] *Id.* at 1011–13.

The *Toensing* opinion strongly implies that, where there *is* good reason to believe work-related content is stored on private devices, employees might be subject to sworn testimony or affidavit to "ratify" their assertion that (1) their search was comprehensive, and (2) any public records were either produced or their exemptions properly justified and logged.[58]

Similarly, you should issue a Mayor's Order requiring that government officials, or employees[59] who produce potential public records on personal devices must: (1) separate and retain such content; (2) conduct a search of their personal device for public records and retrieve those records if subject to a D.C. FOIA request; and (3) provide the District with a written declaration, under oath/affirmation, that their search and retrieval of any records was conducted in good faith and whether or not the search yielded records responsive to the D.C. FOIA request.

IV. RETENTION OF RECORDS

Under District law, record-retention requirements are mandatory and broad, and any eventual disposition of records is centralized and governed by pre-established schedules. D.C. FOIA does not address the *retention* of public records *per se*, but retention is governed by other provisions, chiefly the District of Columbia Public Records Management Act of 1985.[60] Section 7(a)(1) provides: "*Any* record created or received by the District in the course of official business is the property of the District and, except as provided in paragraph (2) [concerning records retention schedules or other authorization approved by the Records Disposition Committee], shall not be destroyed, sold, transferred, or disposed of in any manner."[61] However, there is currently an inadequate retention policy specific to text messages—for example, the General Records Schedules do not expressly mention texts at all.[62]

A. Federal policy illustrates the feasibility of retaining text messages.

Despite, the intangible nature of text messages, it is practicable and inexpensive to retain them as public records. Federal guidance illustrates methods of capturing and retaining texts.

[58] *Cf. id*. at 1012 ("We do not adopt this requirement in cases like this in which there is *no* evidence that an employee has public records in personal accounts." (emphasis added)).
[59] Public bodies act constructively through their agents. *Accord Competitive Enter. Inst. v. Office of Sci. & Tech. Policy*, 827 F.3d 145, 149 (D.C. Cir. 2016) ("[A]n agency always acts through its employees and officials. If one of them possesses what would otherwise be agency records, the records do not lose their agency character just because the official who possesses them takes them out the door . . . .").
[60] Effective Sept. 5, 1985 (D.C. Law 6-19; D.C. Official Code § 2-1701 *et seq.*).
[61] D.C. Official Code § 2-1706(a)(1) (emphasis added).
[62] General Records Schedule Index. General Schedule 20 does list guidance for *electronic records* but has not been updated since 2012 and does not patently address texting.

1. *Current Interior Department Policy*

The federal Department of the Interior ("DOI") has issued a FOIA Bulletin, applicable to all department employees, that endorses several methods of retrieving and producing text messages that are responsive to federal FOIA requests.[63]

DOI supports either: (1) screenshotting, where the record custodian identifies the responsive text messages, take direct screenshots using the mobile device itself, and transmits those screenshots to the substantive office for review and delivery; (2) the "full data back-up approach," where the record custodian uploads all data from the relevant device, isolates potentially responsive texts and sends a collective document of those texts to the substantive office for processing; and (3) "print-to-file," where the record custodian reduces texts to physical form for review and response.[64]

However, it bears mentioning that DOI disfavors the official use of text messaging. While employees and officers *may* use texting, DOI recommends that employees use texting "only for brief notifications or non-substantive communications. When engaging in more comprehensive and substantive communications it is strongly recommended that employees rely on email since all email sent and received from DOI.GOV email addresses is automatically archived, ensuring both retention and accessibility to meet [DOI]'s legal and operational requirements."[65] Moreover, while DOI acknowledges that "[r]are" emergencies may demand that employees use their personal devices to conduct government business, "[a]ny business conducted on a personal device must be forwarded back to [a] government account."[66]

2. *Revision of the District's Record Retention Policy*

Similarly, OCTO should revise its Data and Records Retention Policy[67] to discuss text messages, and work with public bodies to procure, program, implement and maintain the requisite technology. Concurrently, the OS should modernize the District-wide retention policy, including the General Records Schedules, to expressly recognize that a text concerning District business is a public record that must be systematically maintained and producible.

B. Ephemeral Applications Thwart Records-Retention and Undermine D.C. FOIA.

OCTO and the OS may likely find that it is impracticable to retain public records from ephemeral-texting applications. This provides additional rationale for issuing a Mayor's Order stating that

[63] *See* DOI, FOIA BULLETIN NO. 21-01 at 1 (effective Oct. 2, 2020).
[64] *Id.* at 1, 2.
[65] *Id.* attach. at 1 (emphasis in original). *But see* NAT'L ARCHIVES & RECORDS. ADMIN., BULLETIN NO. 2015-02, § 8 (July 29, 2015) ("Simply prohibiting the use of electronic messaging accounts to conduct agency business is difficult to enforce and does not acknowledge the ways employees communicate.").
[66] DOI, *supra* note 70, attach. at 4.
[67] View these policies here: Social Media Policy (eff. Jan. 31, 2010) and Data and Records Retention Policy (rev. May 25, 2021). OCTO's policy-setting authority does not reach the D.C. Council, Office of the Auditor, or Office of the Attorney General. *See* section 1816a of the Office of the Chief Technology Officer Establishment Act of 1998 (D.C. Official Code § 1-1406).

ephemeral-texting should not be allowed on government devices or as a vehicle for government business.

Disclosure later depends on retention now. Since public bodies cannot deliver what they do not retain, the use of *ephemeral* texting indirectly circumvents D.C. FOIA by effectively treating a written conversation as a phone call. It eradicates the writing as soon as the parties "disconnect." Just as text messages, in general, are subject to the definition of "public record," it follows that ephemeral-text exchanges are as well.

Even traditional (non-ephemeral) OTT applications that retain content indefinitely, only store public records for as long as the developer remains solvent and continues to maintain the software. In the absence of a contract with the District, reliance on third parties to maintain public records invites gaps in retention and threatens public bodies' ability to fulfill D.C. FOIA requests.

Accordingly, I recommend that you issue a Mayor's Order to prohibit District government officers and employees from using OTT text message platforms[68] to circumvent D.C. FOIA or retention law. The Mayor's Order should expressly foreclose even the *appearance* of a violation.

V. RECOMMENDATIONS

A. The District Should Consider Prohibiting Ephemeral Applications.

I recommend that the District government consider prohibiting the use of ephemeral messaging applications to conduct District government business. Modernization and innovation in technology should be used to create and retain *more*, not less, transparency in the spaces where public officials and employees exercise public trust.

B. Government Personnel Must Participate in Search and Retrieval of Public Records, even if Stored on Their Personal Devices.

Where a telephone or other communication device is privately owned, it is a best practice to avoid using it to transact government business. Where a District employee disregards this best-practice and commingles work-related public records with their personal content, the government must continue to advise them that any privacy interest in a personally owned device does not extend to any public records created or maintained on that device. With the advent of new technology, the District should discourage the use of personal devices for public business under any circumstances. However, if a personal device is used for public business those District employees may be responsible to account for,[69] search for, and deliver any responsive records in their custody, in response to a D.C. FOIA request. The same principle applies to any cloud-based or third-party accounts through which texts are stored.

[68] These recommended policy changes would not derogate the means of communication that inherently do *not* produce "public records," such as non-transcribed customer-service chats or traditional telephone calls (including telephone calls that use teletypewriting (TTY) for accessibility).

[69] *See generally West v. City of Puyallup*, 410 P.3d 1197, 1201 (Wash. Ct. App. 2018) ("If an employee claims that information in personal accounts [is] not public record[, the employee] must submit an affidavit or declaration stating facts sufficient to support that claim.").

C. Public Bodies Should Consider Commercial Archiving.

To any extent that a public body continues to use text messaging, the public body should consider a commercial electronic-archiving service. These services provide automatic storage and accurate history of communications or conversations. Archiving electronic records also allows for the capture of metadata to (1) verify authenticity and integrity if needed in a court proceeding, and (2) serve the public's need for the context of a record, such as authorship and the destinations of hyperlinks.

D. The Division of Responsibility Between OCTO and the Substantive Public Body Should Extend to Texts as It Does to E-Mail.

Finally, I note the 2008 Mayor's Order that, concerning requests for *e-mail* records, OCTO is required to perform only a technical "screening" function—delivering a broad first-level batch to the *substantive* public body (i.e. agency), which, in turn, performs the detailed search and review and makes decisions about any exemption or redaction.[70] I believe that the same policy should apply to text messages by analogy. Regardless of whether a D.C. FOIA request is tendered to OCTO or the substantive public body, the public body ought to be the party responsible for timely communication with the requestor and timely delivery of any responsive, non-exempt, records.[71]

VI. CONCLUSION

Text messages used to conduct government business are public records to be preserved and produced under D.C. FOIA. Therefore, I urge you to issue a Mayor's Order to: (1) recognize that text messages concerning government business are public records, even if they are stored on a private device; (2) retain these texts for purposes of D.C. FOIA; (3) strongly discourage employees from texting using personal devices to transact public business and doing so only in rare instances where access to their District provided device is, for practical reasons, not available; (4) require an employee in instances where personal devices are used to transact public business, to separate and retain such records; (5) require employees to execute an affidavit attesting to search efforts conducted for responsive records on personal devices; and (6) prohibit the use of ephemeral text messaging applications.

[70]*See* Mayor's Order 2008-88, §§ V, VI, 55 DCR 9365, 9366, 9367 (effective June 18, 2008) ("Upon receipt of any . . . D.C. FOIA request[] initiated by any person[] other than a District of Columbia official, department or agency, the I[nspector]G[eneral], or the Auditor, OCTO will refer the request . . . to the FOIA officer(s)) of the agency([ie]s) that is[/are] the subject of the request. OCTO will produce emails in response to any request from outside the government only to the general counsel(s) or FOIA officer(s) of the agency([ie]s) that is[/are] the subject of the request . . . OCTO will not conduct a substantive review of any collected email traffic to determine whether retrieved items are responsive to the incoming request or are subject to withholding . . . . OCTO will forward the collected email traffic for substantive review . . . to the general counsel(s) or FOIA officer(s) of the subject agency([ie]s) . . . .").

[71]*See id.* § VI, 55 DCR at 9367 ("The substantive review should address whether the retrieved email traffic is responsive to the request, whether statutory restrictions limit or prohibit disclosure, whether the email traffic is subject to applicable privileges or immunities, and whether other exceptions to disclosure apply.").

Sincerely,

Niquelle M. Allen, Esq.
Director of Open Government
Board of Ethics and Government Accountability

cc:

The Honorable Eugene A. Adams
Director, Mayor's Office of Legal Counsel

Kimberly A. Bassett
Secretary of the District of Columbia

Betsy Cavendish
General Counsel to the Mayor

Lindsey Parker
Chief Technology Officer