CAUSE of ACTION
INSTITUTE

Pursuing Freedom & Opportunity through Justice & Accountability℠

March 12, 2019

VIA CERTIFIED & ELECTRONIC MAIL

The Honorable Elijah E. Cummings, Chairman
Committee on Oversight and Reform
U.S. House of Representatives
2157 Rayburn House Office Building
Washington, D.C. 20515

Re: Unauthorized Mobile Applications at the Environmental Protection Agency

Dear Chairman Cummings:

I write on behalf of Cause of Action Institute ("CoA Institute"), a nonprofit strategic oversight group committed to ensuring that government decision-making is open, honest, and fair.[1] In carrying out its mission, CoA Institute uses investigative and legal tools—including the Freedom of Information Act ("FOIA")—to educate the public about the importance of government transparency.

Over the past few years, we have examined the possible violation of the Federal Records Act ("FRA") and the FOIA at the Environmental Protection Agency ("EPA"). CoA Institute's interest in the EPA was prompted by agency employees reportedly using alternative methods of communication, including encrypted messaging applications, to conduct official business, despite agency rules to the contrary.[2] The use of those unauthorized applications raises the question of whether EPA employees sought to circumvent record preservation laws and frustrate the public's ability, and Congress's, to conduct oversight.

CoA Institute twice advised the EPA Administrator of the obligations imposed by the FRA with respect to the recovery of records created or received on unauthorized mobile applications,[3] and we also requested that the EPA Office of Inspector General ("OIG") investigate the matter.[4] The National Archives and Records Administration ("NARA") opened its own inquiry into the same.[5]

---

[1] *See* CAUSE OF ACTION INST., *About*, www.causeofaction.org/about (last accessed Mar. 12, 2019).

[2] Andrew Restuccia, Marianne Levine, & Nahal Toosi, *Federal workers turn to encryption to thwart Trump*, POLITICO (Feb. 2, 2017), http://politi.co/2km4Qrb. The use of encrypted messaging applications at the EPA mirrored reports about the use of similar platforms across the federal government. *See, e.g.*, Hamza Shaban, *After Trump's Win, Secure Messaging App Signal's Downloads Increase 400%*, BUZZFEED (Dec. 1, 2016), https://bzfd.it/2IuoZWZ.

[3] Letter from CoA Inst. to Hon. Scott Pruitt, Adm'r, Envtl. Prot. Agency (Apr. 10, 2018) (on file with CoA Inst.); Letter from CoA Inst. to Catherine McCabe, Acting Adm'r, & Ann Dunkin, Chief Info. Officer, Envtl. Prot. Agency (Feb. 2, 2017) (on file with CoA Inst.).

[4] Letter from CoA Inst. to Hon. Arthur A. Elkins, Jr., Inspector Gen., Envtl. Prot. Agency (Apr. 11, 2018), *available at* https://coainst.org/2TslmL3; *see also CoA Institute Calls for EPA Watchdog Investigation into the Use of Unauthorized Electronic Messaging and Web-Based Email Apps on Agency Devices*, COA INST. (Apr. 12, 2018), https://coainst.org/2G8UJz4.

[5] Letter from Laurence Brewer, Chief Records Officer, Nat'l Archives & Records Admin., to John Ellis, Envtl. Prot. Agency (Feb. 22, 2017), *available at* https://coainst.org/2H9LtNu.

One of the more alarming facts discovered during our investigation was the widespread use of instant messaging applications and personal web-based email accounts by EPA employees on agency-furnished and taxpayer-funded iPhones and iPads. According to EPA records, at least eighteen different mobile applications with electronic messaging capabilities, none of which were authorized, were downloaded and operating on EPA hardware.[6] In addition, several web-based email programs had been installed by EPA employees, including AOL, Gmail, and Yahoo Mail.[7] These applications raise FRA and FOIA concerns because they can be used by agency employees to communicate about work-related business on a personal account and thereby bypass official record-keeping systems. EPA records also revealed that hundreds of other non-work-related applications were installed on agency-furnished mobile devices without authorization and in violation of official EPA policy; these applications included social media platforms, dating programs, personal banking and finance tools, entertainment and sports betting applications, and much more.[8]

In a February 2018 report, the EPA OIG stated that the EPA had disabled the "Apple Store" on most agency-furnished devices.[9] Although that report left unanswered the question of whether any agency employees still had the ability to download unapproved applications, or whether already-installed unauthorized applications had been deleted, the EPA's subsequent report to NARA clarified the matter. By letter, dated October 10, 2018, the EPA reported that, as of June 2018, it had "completed its process" of disabling downloads of unauthorized applications, subject to two minor exceptions, and *removed* applications previously installed without permission.[10]

But a record released to CoA Institute last week suggests that the EPA may have misinformed NARA.[11] The record—a Microsoft Excel spreadsheet that appears to have been created on October 17, 2018, a week after the agency's final report to NARA—contains a list of mobile applications installed on employee devices, including 24,717 "non-managed," or unapproved, applications. That number represents 62.16% of all installations on EPA-furnished devices, and the various applications listed in the chart include many of the same non-work-related or encrypted messaging applications previously identified by the EPA.

As we embark on Sunshine Week—a national celebration of government transparency and accountability—we are concerned that the EPA may have misinformed NARA and that employees within the agency continue to conduct government business on non-government platforms. We respectfully request that you and the House Oversight and Reform Committee seek clarification from the EPA during the Committee's upcoming FOIA hearing about the foregoing matter. If the EPA

---

[6] Ryan P. Mulvey *Investigation Update: EPA Employees Used a Range of Messaging Apps and Other Non-Work-Related Programs on Agency-Issued Mobile Devices*, COA INST. (Apr. 4, 2018), https://coainst.org/2qcAMBQ.

[7] *See id.*

[8] *See generally* MDM App Summary (Feb. 6, 2017), *available at* https://coainst.org/2O0vfK8.

[9] *See, e.g.*, Envtl. Protection Agency, Office of Inspector Gen., Final Summary Report at 2 n.1 (Feb. 28, 2018), *available at* https://coainst.org/2IvYAYC ("In support of [the EPA policy that prohibits the installation of unauthorized applications], on or about June 13, 2017, the agency disabled the ability of iPhone 6 and iPad users to download the Apple Store app. Exceptions were made for On-Scene Coordinators and other emergency responder staff; moreover, the agency is still in the process of removing the Apple Store app on older iPhone 5 models.").

[10] *See* Letter from John B. Ellis, Envtl. Prot. Agency, to Laurence Brewer, Chief Records Officer, Nat'l Archives & Records Admin. (Oct. 10, 2018), *available at* https://coainst.org/2XO3ngA.

[11] *See generally* "EPA Installed Apps 10-17-18v2," *available at* https://coainst.org/2SX4wPh.

has failed to implement its own prohibitions on the downloading of unauthorized mobile devices, or if it has failed to undertake the steps necessary to ensure compliance with its record-keeping obligations under the FRA and the FOIA, Congress should take the opportunity to expose those failures and hold the agency to account.

I welcome the opportunity to discuss the issues raised in this letter. If you have any questions, please contact me by telephone at (202) 499-4232 or by e-mail at john.vecchione@causeofaction.org. Thank you again for your attention to this matter.

Sincerely,

JOHN J. VECCHIONE
PRESIDENT & CEO

CC: The Honorable Jim Jordan, Ranking Member
U.S. House of Representatives Committee on Oversight and Reform

Mr. Charles J. Sheehan, Acting Inspector General
Environmental Protection Agency Office of Inspector General

Mr. Laurence Brewer, Chief Records Officer for the U.S. Government
National Archives and Records Administration