

Gone in an Instant

How Instant Messaging Threatens
the Freedom of Information Act

Executive Summary

The public's right to access information through the Freedom of Information Act ("FOIA") is critical to holding the federal government accountable. But the FOIA faces threats on numerous fronts: ever-increasing backlogs, heavy-handed political review, and pages painted with black ink. There is another threat that could undermine the FOIA and put much of the federal government in the dark—technology. The increasing integration of new electronic messaging technologies into the workplace is changing the way employees communicate, and the federal government is not keeping pace by preserving records in accordance with federal law and guidance from the National Archives and Records Administration ("NARA").

In 2014, Congress amended the Federal Records Act ("FRA") to modernize the definition of a record and cover new forms of communication. The amendments updated the definition of electronic messages to include "electronic mail and other electronic messaging systems that are used for purposes of communicating between individuals." A few months later, NARA released guidance for management of instant messaging ("IM") records.

In 2018, Cause of Action Institute ("CoA Institute") and Americans for Prosperity Foundation ("AFPF") began investigating dozens of agencies' IM records management policies and practices. Based on our experience, we suspected that federal agencies were unwilling or unable to properly address the increasing use of IM platforms for government work. We analyze records obtained through FOIA requests to determine whether agencies are using instant messaging and preserving those messages in accordance with the FRA and NARA guidance. We find that many of the forty federal agencies we investigated have inadequate records management policies that fail to properly account for instant messaging.

- Thirteen of the sixteen agencies that produced their policies for the administration of IM in response to our FOIA request do not preserve instant messages as a matter of policy—a violation of federal law and NARA guidance.
- Only three agencies produced records reflecting policies to automatically preserve instant messages using features common in IM platforms.

- Of the twenty agencies that produced their policies for employee use of IM, thirteen allow its use but prohibit employees from creating or sending a record through IM and three ban IM use altogether. Prohibiting IM use to conduct business is contrary to NARA guidance.
- Many agencies have failed to incorporate the 2014 Presidential and Federal Records Act Amendments and subsequent NARA guidance into their records management policies and practices.
- Agencies are shirking their responsibility to manage IM records by prohibiting the use of instant messaging or claiming erroneously that instant messages are insignificant and need not be saved.

While new ways of doing business can strain records management compliance, these technological advancements also provide opportunities for better records management. The tools needed to keep federal agencies compliant with the law already exist.

The IM platforms that agencies are using offer enterprise-level message retention, data loss prevention, and eDiscovery tools. Agencies should embrace IM's increasing integration and use in the workplace—providing employees with an official IM option for work that is equipped with the necessary features to comply with legal requirements. The Federal Communications Commission, for example, provides its employees with an IM platform called Jabber and keeps logs of all messages and can produce those logs upon receiving a FOIA request.

Both the FRA and FOIA are instrumental to government transparency and accountability. But for these laws to serve their purpose, agencies must implement policies and practices that track advancements in technology and effectively account for how agencies generate and transmit information.

Findings

We analyze agencies' IM policies and practices across five dimensions. Agencies receive points if they have updated their policies since the 2014 FRA amendments, allow employees to use instant messaging, preserve instant messages, and produce messages upon request.

Scores for agencies are plotted on Figure 1. Agencies with good scores are in the green area and those in the yellow area need to improve their IM practices. Agencies with poor IM policies and practices appear in the red region and those that did not respond to our FOIA requests are listed at the bottom.

Only four agencies receive passing scores: FCC, CIGIE, USDA, and NASA. These agencies all have up-to-date policies and allow IM use, though two maintain policies that IM should not be used to send non-transitory information. Two of the agencies automatically preserve instant messages and the other two enable their employees to do so, which is reflected in their archive settings. All but CIGIE provided us records of instant messages.

Nine agencies need improvement. These agencies allow IM use but fail to properly preserve and produce instant messages. About half (thirteen) of the agencies that responded to our FOIA request have very poor policies regarding IM. These agencies, for the most part, claim to not allow IM use, do not preserve instant messages, and did not produce any messages. Agencies in the red region of Figure 1 are not complying with federal records laws.

Agency Performance on Instant Message Record Management

100	
90	• FCC
80	• CIGIE • USDA
70	• NASA
60	• CFPB • DOI • VA • EPA • FERC
50	• ED • NLRB
40	• DHS • IRS
30	• GSA
20	• DOD • DOL • EXIM • FBI • FEC • FTC • NOAA • SEC • USAID
10	• DOE
0	• HHS • SBA
Did not respond to FOIA request	• CIA • DOC • HUD • DOJ • DOS • USDT • DOT • ICE • NARA • NSA • OMB • OSTP • OSC • USCIS

Figure 1: Agency scores across five measures of IM policies and practices.



About Americans for Prosperity Foundation

Americans for Prosperity Foundation is a 501(c)(3) nonprofit organization committed to educating and training Americans to be courageous advocates for the ideas, principles, and policies of a free and open society.



About Cause of Action Institute

Cause of Action Institute is a 501(c)(3) nonprofit, nonpartisan government oversight organization that uses investigative, legal, and communications tools to educate the public on how government accountability, transparency, the rule of law, and principled enforcement of the separation of powers protects liberty and economic opportunity.

About The Authors

[Thomas Kimbrell](#) is a Policy Analyst at Americans for Prosperity Foundation, who started as an Investigative Analyst at Cause of Action Institute in 2017. His work currently focuses on government transparency, trade, cronyism and corporate welfare.

[James Valvo](#) is Chief Policy Counsel at Americans for Prosperity Foundation. He is also Executive Director of Cause of Action Institute, where he has worked since 2013. Mr. Valvo's work focuses on the separation of powers, administrative law, and government oversight and transparency. He was a member of the 2016–18 Federal Freedom of Information Act Advisory Council.

[Kevin Schmidt](#) is Director of Investigations at Americans for Prosperity Foundation. His work focuses on cronyism and corporate welfare, government spending, trade, and immigration. He is also a co-founder and contributor to FOIA Advisor, a forum designed to help the public learn more about the federal Freedom of Information Act.

Table of Contents

Executive Summary	1
The Tension Between Technology and Transparency	6
The Investigation	7
Agencies are Choosing not to Preserve Instant Messages	11
Agencies Need to Adjust Their Policies to Growing IM Use	15
Ephemeral Messaging	17
Scoring Agency IM Records Management Practices	18
Technology Provides Opportunities for Better Records Administration	19
Conclusion	19
Appendix	20

List of Tables

Table 1: Agency Policies on Administration of IM	8
Table 2: Agency Policies on IM Use	9
Table 3: Agency Policies on IM Use and Retention	16
Table 4: Sample of Messaging Applications on Agency-Owned Devices	17
Table 5: Agencies Included in Investigation	001
Table 6: Summary of Agencies Policies on Use and Retention of IM	002

List of Figures

Figure 1: Agency scores across five measures of IM policies and practices	2
Figure 2: NOAA Unified Messaging Service Operational Procedures (2012)	6
Figure 3: Timeline of Agencies with Records Management Policies that predate the 2014 FRA Amendments	10
Figure 4: NOAA email re “CHAT” policy decision” (Nov. 12, 2011)	11
Figure 5: GSA email memorializing decision to turn off the History feature on Google Hangouts (Mar. 5, 2018)	12
Figure 6: Internal Revenue Service, IRM 1.15.6, Records and Information Management, Managing Electronic Records (Nov. 23, 2016)	12
Figure 7: U.S. Dept. of Veterans Affairs, FSS Bull. 345, Microsoft Skype for Business (2017)	12
Figure 8: U.S. Dept. of Veterans Affairs email re Skype IM Automatic-Save/Missed IM Email Feature Being Deactivated to Protect PII/PHI (Nov. 26, 2018)	13
Figure 9: Dept. of Homeland Security, Policy Directive 141-03, Electronic Records Management Updates for Chat, Text, and Instant Messaging (Feb. 23, 2018)	13
Figure 10: Nat’l Labor Relations Board email re Skype for Business Configuration Changes (Apr. 13, 2017)	14
Figure 11: U.S. Dept. of the Interior, OCIO Directive 2014-003, Acceptable Use of Bison Connect Electronic gChat Technology (2014)	15

The Tension Between Technology and Transparency

The FRA stipulates what information the government must preserve. Through the FOIA, the public can access agency records and see what the government is doing. Both the FRA and FOIA are instrumental to government transparency and accountability. But, for these laws to serve their purpose, agencies must maintain policies and practices that track advancements in technology and effectively account for how agencies generate and receive information.

The modern history of the FRA and FOIA is beset with tension between advances in information technology and agencies' administration of the statutes. That tension sometimes leads to legislative action to clarify the reach and application of the law. For example, as computers became dominant in the workplace, email became a prominent method of communication and agency records were increasingly stored in electronic format. In response, Congress amended the FOIA in 1996 to update the definition of a "record" to include "information that would be an agency record . . . when maintained by an agency in any format, including an electronic format."¹

The proliferation of mobile devices and communications technology has made communicating quicker and easier. Like email, these technologies have naturally been incorporated into the workplace. People now commonly conduct business with novel forms of electronic messaging, including text and instant messaging. Congress amended the FRA in 2014, expanding its coverage to include "all recorded information, regardless of form or characteristics . . . including information . . . in digital or electronic form."² The 2014 Amendments also redefined "electronic messages" to include "electronic mail and other electronic messaging systems that are used for purposes of communicating between individuals."³

A few months after the 2014 Amendments were signed into law, NARA circulated a bulletin giving agencies guidance for managing electronic messages—specifically, instant messaging and similar novel forms of communication. The guidance states that "agencies

must capture and manage these records in compliance with Federal records management laws, regulations, and policies."⁴ However, recent revelations about the federal government's misuse of and failure to preserve electronic messages suggest that agencies have been slow to comply.

In 2015, for example, the Treasury Inspector General for Tax Administration revealed that, pursuant to a memorandum of understanding between the Internal Revenue Service ("IRS") and the National Treasury Employees Union, the IRS was not preserving instant messages.⁵ Through litigation, CoA Institute secured interim guidance requiring appropriate preservation of those records.⁶ Additionally, a 2017 CoA Institute investigation showed that National Oceanic and Atmospheric Administration ("NOAA") employees were using Google Hangouts for work but did not preserve messages because agency policy treated the app as "off the record."⁷

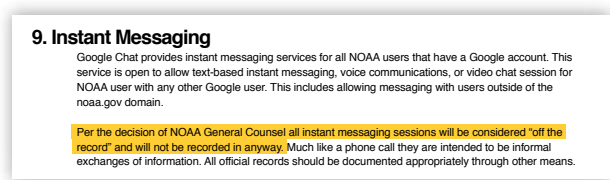


Figure 2: NOAA Unified Messaging Service Operational Procedures (2012).

News reports revealed that some employees at the Environmental Protection Agency ("EPA") were using an encrypted messaging app called Signal to communicate with one other about how to react to new management as the Trump Administration took office in 2017.⁸ Later that year, a group of employees at the Consumer Financial Protection Bureau ("CFPB"), who dubbed themselves "Dumbledore's Army," used encrypted messaging apps to resist changes being implemented by the Bureau's newly appointed director.⁹ In the White House, some staffers downloaded the app Confide, an app that erases messages as soon as they are read.¹⁰

1. Electronic Freedom of Information Act Amendments of 1996, pub. L. 104-231, § 3, 110 Stat. 3048, 3049 (Codified at 5 U.S.C. § 552(F)(2)); see s. Rep. 104-272, At 5 (1996) ("[t]he FOIA is in the midst of a new challenge. The phenomenon of Federal executive department and agency records being produced and retained in electronic formats has grown at a fast rate during the past several years as Government use of personal computers and digital storage media . . . Has become more widespread.")

2. 44 U.S.C. § 2911. The Federal Records Act refers to the collection of statutes that govern the creation, management, and disposal of the records of federal agencies. See 44 U.S.C. Chs. 21, 29, 31, 33.

3. *Id.*

4. NAT'L ARCHIVES & RECORDS ADMIN., NARA BULL. 2015-02, GUIDANCE ON MANAGING ELECTRONIC MESSAGES (2015), available at <https://www.Archives.gov/records-mgmt/bulletins/2015/2015-02.html>.

5. See TREASURY INSPECTOR GEN. FOR TAX ADMIN., REPORT OF INVESTIGATION: EXEMPT ORGANIZATIONS DATA LOSS, at 21 (June 30, 2015), available at <http://bit.ly/2nfr3aF>.

6. Mem. From Celia Doggette, Dir., Identity & Records Protection, Internal Revenue Serv., To Comm'r of Internal Revenue, *et al.*, Electronic Message Usage and Preservation (July 29, 2016), available at <http://bit.ly/2mmA4RP>.

7. NAT'L OCEANIC & ATMOSPHERIC ADMIN., NOAA UNIFIED MESSAGING SERVICE OPERATIONAL PROCEDURES (2012), available at <http://bit.ly/2utmkLI>.

8. Andrew Restuccia, *et al.*, *Federal workers turn to encryption to thwart Trump*, POLITICO, Feb. 2, 2017, <http://politi.co/2km4Qrb>.

9. Jessica Silver-Greenberg & Stacy Cowley, *Consumer Bureau's New Leader Steers a Sudden Reversal*, N.Y. TIMES, Dec. 5, 2017, <https://nyti.ms/3bGyvFI>.

10. See Ashley Parker & Phillip Rucker, *Upheaval is now standard operating procedure inside the White House*, WASH. POST, Feb. 13, 2017, <http://wapo.st/2II71cl> ("Staffers, meanwhile, are so fearful of being accused of talking to the media that some have resorted to a secret chat app—Confide—that erases messages as soon as they're read.")

Former White House Press Secretary Sean Spicer instructed staffers that use of the app violated the Presidential Records Act.¹¹

These developments prompted U.S. House Committee on Oversight and Government Reform to send a letter to fifty-five federal agencies in March 2017 seeking to better understand agencies' policies on the use of such applications.¹² The Committee asked for information about how agencies are preserving those types of records and how they comply "with FOIA requests that may require searching and production of documents stored on non-official email accounts, social networking platforms, or other messaging or communications."¹³ To date, the Committee has not publicly revealed any responses.

Spurred by these events and our experience, we initiated an investigation in 2018 into federal agency behavior pertaining to the use, retention, and reproduction of instant messages transmitted to conduct agency business. At the time, it was clear agency employees' exploitation of IM and agencies' apparent failure to govern that technology imperiled government transparency and accountability.

The Investigation

In 2018, we sent FOIA requests¹⁴ to 39 agencies (listed in Table 5)¹⁵ that included cabinet departments, major independent agencies, important sub-cabinet agencies, and White House offices subject to the FOIA. The requests sought agency records reflecting:

1. Policies on the retention and management of instant messages
2. Policies on the use of instant messaging
3. Implementation of guidance given in NARA Bulletin 2015-02
4. A list of instant messaging applications installed on agency devices
5. Settings for archiving, indexing, and eDiscovery features on instant messaging apps
6. Actual instant messages

Request Items 1 and 2 sought agency policies on the use and administration of instant messaging to answer basic questions such as: Are agency employees allowed to use instant messaging and, if so, for what purpose? Are messages supposed to be retained for records scheduling? We included Request Item 3 to determine if agencies

have updated their policies pursuant to the legislative amendments and NARA guidance.

We included Request Items 4, 5, and 6 to uncover revealed practices around agency use and retention of instant messages. That is, regardless of policy, are employees using instant messaging? Are those messages being archived? And can agencies produce records created by employees on instant messaging platforms upon receipt of a FOIA request?

Because of the size and scope of the study, we decided at the outset that we would appeal adverse FOIA determinations when appropriate but would not pursue litigation against agencies that failed to respond or denied our appeals. Agency responses have been largely disappointing. Fourteen agencies (denoted in Table 5) have yet to produce any records. Of those that did, many ignored one or more of the request items or returned a "no records" response even though other records they provided suggest the records should exist.

At the time of this report, we have received final responses to our FOIA request from twenty agencies, five of which are under administrative appeal. We received interim productions from five agencies, while fourteen failed to respond. Our analysis below includes the twenty-five agencies that produced records with the addition of NOAA, from which we received records relevant to this investigation through a previous FOIA request.

We reviewed the records and grouped the responses into common categories for each of the six items in the FOIA request. The categories reflect whether records were produced and, if so, information about what the records reveal. For example, Item 1—which sought records reflecting agency policies regarding the retention, management, and administration of IM—is grouped into the following categories: "IM not retained per policy," "IM should be retained manually (not automatically) when necessary," "IM retained automatically," and "no records/no response." By contrast, responses to request Item 6 are divided into two categories that show whether the agency produced instant messages.

11. Annie Karni & Alex Isenstadt, *Sean Spicer targets own staff in leak crackdown*, POLITICO, Feb. 26, 2017, <http://politi.co/2njJCHy>. And if staffers worked in a White House office subject to FOIA, it would also create problems under the FOIA and FRA.

12. Letter from Rep. Jason Chaffetz, Chairman & Rep. Elijah Cummings, Ranking Member, H. Comm. On Oversight & Gov't Reform, to Kathleen McGettigan, Acting Dir., Office of Personnel Mgmt. (Mar. 8, 2017), *available at* <http://bit.ly/2mLGuea>.

13. *Id.*

14. App. at 004.

15. App. at 001.

1. Few agencies have policies that provide for the preservation of IM

Like many business organizations, government agencies provide employees with laptops, smartphones, and other IT devices to do their work. And, like many organizations, agencies exert a degree of administrative control over the hardware and software on those devices for legal and security purposes. One would reasonably expect that in the government’s case central administration of these devices would be sophisticated given federal agencies’ unique record-keeping, legal, and security requirements. Some information cannot be lost; it must be preserved. Other information cannot be leaked as it is classified or protected under any number of statutes protecting personally identifiable information.

We designed Item 1 to illuminate the administrative capabilities of agency IT for IM and determine whether agencies’ policies required the preservation of instant messages. Unfortunately, we received little

to no information on the former. As to the latter, of the twenty-six agencies that responded to our FOIA request, only three have policies to automatically capture and preserve instant messages.

Ten agencies either did not produce records in response to Item 1 or returned a “no records” response. Seven agencies did not automatically retain instant messages but directed employees to preserve messages

Only three agencies have policies to automatically capture and preserve instant messages

manually as they deemed necessary. For example, several agency policies instructed employees who send non-transitory information by instant message to copy/paste or forward the message to the agencies’ official record-keeping system. Finally, six agencies had policies expressly stating that instant messages would not be preserved.

Table 1: Agency Policies on Administration of IM

IM Not Retained	IM Retained Manually	IM Retained Automatically	No Response/Unclear
Department of Energy	Department of Agriculture	Council of Inspectors General on Integrity and Efficiency	Consumer Financial Protection Bureau
Department of Labor	Department of Homeland Security	Department of Education	Department of Defense
Department of Veterans Affairs	Department of the Interior	Federal Communications Commission	Department of Health and Human Services
General Services Administration	Environmental Protection Agency		Export-Import Bank
National Labor Relations Board	Internal Revenue Service		Federal Bureau Investigation
National Oceanic and Atmospheric Administration	Federal Energy Regulatory Commission		Federal Elections Commission
	National Aeronautics and Space Administration		Federal Trade Commission
			Securities and Exchange Commission
			Small Business Administration
			U.S. Agency for Foreign Development

2. Policies regarding use of IM vary across agencies

Item 2 of the request sought records regarding agencies' policies on the use of IM. Seven agencies failed to produce records relevant to this request item. Those that did reveal three common policies on

IM use: six agencies allow employees to use IM to conduct business, ten agencies allow IM use but prohibit using it to send or create a record, and three agencies forbid IM use.

Table 2: Agency Policies on IM Use

IM Use Prohibited	IM Use Permitted, But Not to Create a Record	Policy Allows IM Use	No Response/Unclear
Federal Bureau of Investigation	Consumer Financial Protection Bureau	Council of Inspectors General on Integrity and Efficiency	Department of Defense
Federal Trade Commission	Department of Education	Department of Agriculture	Department of Health and Human Services
U.S. Agency for Foreign Development	Department of Energy	Department of the Interior	Department of Labor
	Department of Homeland Security	Department of Veterans Affairs	Export-Import Bank
	Federal Communications Commission	Environmental Protection Agency	Federal Election Commission
	Federal Energy Regulator Commission	National Oceanic and Atmospheric Administration	Securities and Exchange Commission
	General Services Administration		Small Business Administration
	Internal Revenue Service		
	National Aeronautics and Space Administration		
	National Labor Relations Board		

3. Only eleven agencies could prove that they have incorporated NARA's guidance

Nearly three years after NARA Bulletin 2015-02 provided guidance for managing instant messaging records, our FOIA request asked for agencies' records related to the receipt, implementation, or compliance with the guidance. CoA Institute sought evidence that agencies are updating their policies, as appropriate, to incorporate the

2014 Amendments and NARA guidance. Five agencies searched but were unable to locate any records while nine agencies simply did not provide any response. Eleven agencies produced records indicating that the NARA guidance has been incorporated into their policies. Five agencies, four of which are using IM, produced electronic records management policies that predated the 2014 amendments.

Agencies with Outdated Records Management Policies on Electronic Messaging

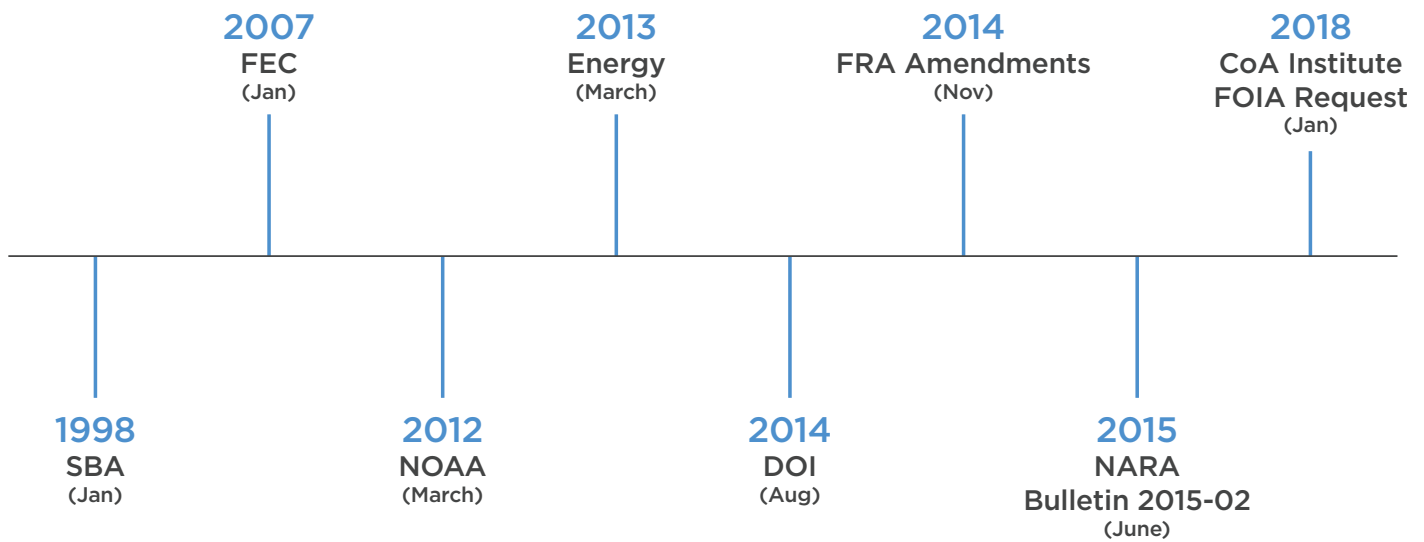


Figure 3: Timeline of Agencies with Records Management Policies that predate the 2014 FRA Amendments

4. All four agencies that produced a full list of messaging apps on agency devices show multiple IM apps

Item 4 sought records reflecting the instant messaging applications downloaded on agency devices. We are especially interested in encrypted ephemeral messaging apps—such as Signal, Snapchat, or Wickr Me—present on government devices. Common tasks of an organization’s IT administration are providing employees with a suite of enterprise applications to conduct their work (*e.g.*, Microsoft Office) and white/black-listing other applications that can be downloaded to organization-owned devices. This information is typically accessible through IT administration tools and agencies should easily produce it. But surprisingly, fifteen agencies did not produce records responsive to this request item. Six more failed to fulfill the request by providing a list of only the “officially supported” IM application(s) on agency devices (*e.g.*, Skype as part of agencies’ Microsoft Office subscription). Four agencies, however, did provide a full accounting of all the IM applications downloaded to their devices, all of which show several different IM apps.

5. Few agencies produced records that show they preserve instant messages

Many personal IM applications allow users to turn the chat history on or off. Likewise, many enterprise messaging systems include archiving features that can be enabled or disabled. Organizations commonly control these settings centrally for an entire organization through IT administration tools. Item 5 sought records reflecting whether agencies had enabled or disabled the archiving features of the IM applications they use. Despite the request being straightforward, ten agencies did not respond or returned a “no records” response. Five agencies’ records reveal they do not archive IM, and two others’ responses did not indicate that they do. Four agencies allowed users to turn their own chat histories on or off. Only four agencies produced records that confirmed they archive messages shared on their official IM systems.

6. Only ten agencies produced instant messages

Finally, regardless of whether agency policies provided for the use or retention of IM, it is important to know if the agencies could produce IM records. Ten agencies provided us with instant messages, fifteen did not.

Agencies are Choosing not to Preserve Instant Messages

Thirteen agencies produced policies reflecting that they do not automatically preserve IM. From these agencies’ policies, two common threads emerged: some simply forbid the use of IM to conduct business or create records and others claim instant messages are transient in nature and need not be preserved. Some do both.

NOAA records, for example, reveal the agency uses Google Hangouts for instant messaging. An email from an official at NOAA argues that instant messages are “transient electrons.”¹⁶ But in the same email the agency official acknowledges that if instant messages are saved, they could constitute federal records¹⁷—as if, somehow, whether information is preserved determines if it is a federal record and not the other way around. Although the email, which we received pursuant to a 2017 FOIA request, predates the FRA amendments and NARA guidance, it represents latest policy NOAA produced for IM.

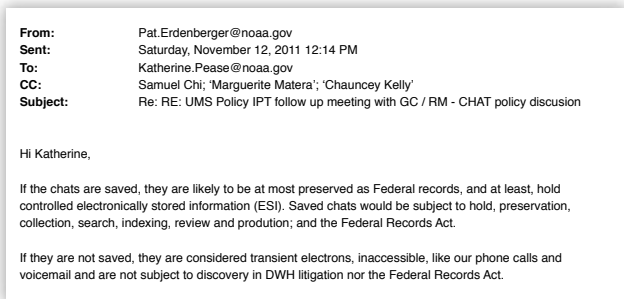


Figure 4: NOAA email re “CHAT policy decision” (Nov. 12, 2011)

Like NOAA, the General Services Administration (“GSA”) uses Google Hangouts to communicate but does not preserve messages, arguing that they are transient. Ironically, the agency chose to disable the archiving feature in Google Hangouts after an inquiry from the GSA Office of General Counsel into whether the IT department searches Slack (another IM platform GSA uses) when completing eDiscovery requests.¹⁸ Incredibly, records reveal GSA chooses not to search the IM platform that inherently archives all messages (Slack) and has disabled the message preservation functionality in the other (Hangouts).

16. App. at 010.

17. *Id.*

18. App. at 019.

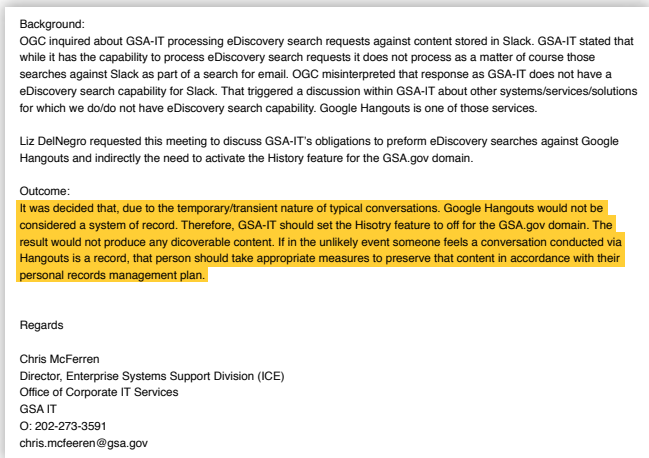


Figure 5: GSA email memorializing decision to turn off the History feature on Google Hangouts (Mar. 5, 2018)

Meanwhile, the GSA Office of Inspector General (“OIG”) policy states that “Instant Messaging shall not be used to conduct official business. Further, instant messages shall not be maintained in our official system of records. Instant messages and instant messaging histories should be deleted.”¹⁹ Despite this prohibition, GSA OIG makes clear that work-related messages on these platforms “should be permanently saved to the case file.”²⁰ Ambiguous and contradictory policies like GSA OIG’s and other agencies not only violate the law, but create confusion and create unnecessary work for federal employees who have to comply.

IRS records management policies also maintain that IM is for “transitory” communications only and prohibit employees from using it to create records.²¹ At the same time, IRS policy allows employees to use IM to share Personally Identifiable Information (“PII”) and sensitive but unclassified information—the type of information usually linked to more substantive messages.²² IRS’s records management policy for IM seems to contradict its policy on the appropriate uses of IM.

Further, messages in IRS’s system apparently do not live beyond the chat session in which they are sent. That is, records reflect that once the chat window is closed, the messages are permanently lost. The only way to preserve the messages is for employees to save them manually before closing the chat.²³ Such a system presents a high risk for unlawful destruction of records, intentional or not.

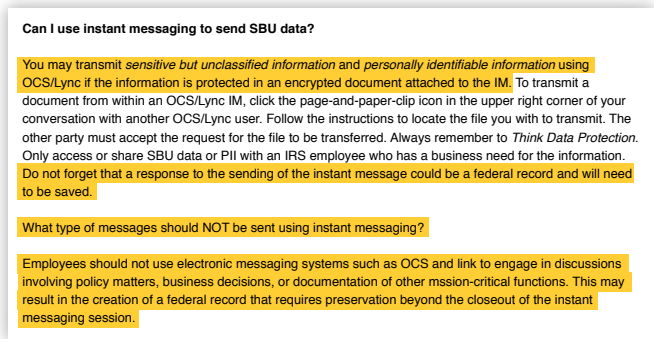


Figure 6: Internal Revenue Service, IRM 1.15.6, Records and Information Management, Managing Electronic Records (Nov. 23, 2016)

Similarly, the Department of Veterans Affairs (“VA”), which “does not currently have a specific policy regarding IM communications,”²⁴ allows employees to conduct business and send sensitive information via instant messaging,²⁵ but does not archive instant messages and maintains they “are not resourced or directed to archive any Skype for Business relevant data.”²⁶

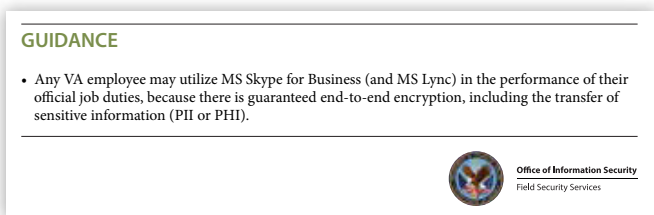


Figure 7: U.S. Dept. of Veterans Affairs, FSS Bull. 345, Microsoft Skype for Business (2017)

19. App. At 021.

20. *Id.*

21. INTERNAL REVENUE SERV., IRM 1.15.6, RECORDS AND INFORMATION MANAGEMENT, MANAGING ELECTRONIC RECORDS (Nov. 23, 2016)

22. *Id.*

23. *Id.*

24. Letter from U.S. Dept. Of Veterans Affairs to Cause of Action Institute (June 13, 2018).

25. U.S. DEPT. OF VETERANS AFFAIRS, FSS BULL. 345, MICROSOFT SKYPE FOR BUSINESS (2017).

26. *Supra* note 24.



Permitting employees to send sensitive information through IM, it turns out, precludes the VA from preserving instant messages. A November 2018 email we obtained describes how the auto-save feature in Skype for Business could potentially expose PII/PHI included in a missed/unread instant message by sending the intended recipient the same message in an unencrypted email. To remedy this security flaw, the VA disabled the archiving feature on Skype for Business. This specific scenario presents an intriguing dilemma, pitting information security directly against transparency obligations.

Like the IRS and GSA, other agencies that prohibit creating records on IM include the Department of Energy, Department of Homeland Security (“DHS”), Federal Trade Commission, and National Aeronautics and Space Administration (“NASA”). NASA acknowledges that its enterprise IM system, Skype for Business, has archiving functionality, but go on to say that “it is a user selected option and is not turned on by default.”²⁷ DHS policy at least requires that IM apps on agency devices display a banner reminding users that the app is not to be used to conduct official business.²⁸

From: US. Department of Veterans Affairs <US.VA@va.gov>
 Sent: Monday, November 26, 2018 12:40 PM
 To: VAAIEXOMailBoxes <VAAIEXOMailboxes@va.gov>
 Subject: Skype IM Automatic-Save/Missed IM Email Feature Being Deactivated to Protect PII/PHI

Skype IM Automatic-Save/Missed IM Email Feature Being Deactivated to Protect PII/PHI

Veterans trust the Department of Veterans Affairs (VA) to protect their personally identifiable information (PII), protected health information (PHI), and all sensitive data. The Office of Information and Technology (OIT) and all VA organizations take this responsibility seriously. An optional feature of the Microsoft Skype application, the Skype Instant Message (IM) Automatic-Save feature, could potentially put that information at risk, and therefore must be disabled immediately.

The Skype IM Automatic-Save feature saves information from the missed IM and automatically sends the message as an unencrypted email to the intended recipient. While this feature conveniently allows users to save and view Skype conversations at a later time, it could potentially compromise protected data.

To ensure that we remain wholly compliant with VA policy, the deactivation of the Automatic-Save functionality will apply to all VA network Skype users, even those who do not routinely deal with sensitive information. Although the Automatic-Save feature will be disabled, healthcare providers and all other users across VA will still be able to rely on Skype’s guaranteed, automated end-to-end encryption to aid them in IM communication of Veteran PII, PHI, and other sensitive information as allowed in Field Security Service Bulletin 345. If at any time in the future Microsoft makes a change that prompts automatic encryption of saved IMs, the Automatic-Save feature may be reconsidered for activation.

As a general reminder, VA personnel should remain vigilant to protect against the inadvertent or unauthorized display of PII, PHI, and other sensitive information. It is everyone’s responsibility and obligation to protect Veteran information. For Skype service issues, please contact the Enterprise Service Desk at 855-673-4357.

- All DHS business transactions by electronic means are required to comply with the Department’s records management policies. DHS employees should take steps to establish and maintain federal records when conducting business using chat, text, or instant messaging.
- All internal DHS chat/messaging systems (i.e., Lync, Skype, or other tools) must display a banner/disclaimer prohibiting the system to be used to formally transact agency business or to document the activities of the organization.

Figure 9: Dept. of Homeland Security, Policy Directive 141-03, Electronic Records Management Updates for Chat, Text, and Instant Messaging (Feb. 23, 2018).

Some agencies do not provide any policy justification for not preserving instant messages. The Department of Labor’s records management program, dated 2017, contains a single sentence regarding IM policy: “NOTE: At this time DOL has determined Instant Messaging will not be used to create records.”²⁹ The National Labor Relations Board (“NLRB”) did not provide any policy regarding IM but produced an email from April 2017 instructing an employee to configure NLRB’s Skype for Business to disable the auto-save feature and to remove the option for users to save messages manually.

Figure 8: U.S. Dept. of Veterans Affairs email re Skype IM Automatic-Save/Missed IM Email Feature Being Deactivated to Protect PII/PHI (Nov. 26, 2018)

27. Letter from Nat’l Aeronautics & Space Agency to Cause of Action Institute (August 21, 2018), *see app.* At 030.

28. DEPT. OF HOMELAND SECURITY, POLICY DIRECTIVE 141-03, ELECTRONIC RECORDS MANAGEMENT UPDATES FOR CHAT, TEXT, AND INSTANT MESSAGING (Feb. 23, 2018).

29. Dep’t of Labor, DLMS 1 – RECORDS MANAGEMENT (2017).

From: Sanders, Laurie
To: Marks, Eric
CC: Aburvasamy, Prem
Subject: RE: Skype for Business Configuration Changes
Date: Thursday, April 13, 2017 10:54:19 AM

Eric,
 I will have Robert submit it for CAB and proceed with the changes. Are we going to inform the users that we are making this change. Some people like having the transcript of VMs in outlook. Thanks.
 Laurie J. Sanders
 Associate Chief Information Officer, Infrastructure Section
 National Labor Relations Board
 1015 Half Stree, SE., Suite 3068 | Washington, DC 20570
Laurie.sanders@nlrb.gov
 Office - 202-273-4095
 Cell - 202-375-0624

From: Marks, Eric
Sent: Thursday, April 13, 2017 10:51 AM
To: Sanders, Laurie
CC: Aburvasamy, Prem
Subject: Skype for Business Configuration Changes

Laurie,
 Time permitting, can Robert proceed with the following Skype for Business configuration changes per Prems's request.
Set-CcClientPolicy Changes
<https://technet.microsoft.com/en-us/library/gg398300.aspx>

Settings	NLRB Requirement	Value	Discription
DisableSavingIM	Prevent the saving of IM messages within	True	When set to true, the options for saving an instant message session are removed from the menu bar in the Skype for Business Conversation window. When set to false, these options are available in the Conversation window. Note that setting this value to true removes the menu options that make it easy for users to save instant message transcripts. However, it does not prevent users from copying all the text in a transcript to the clipboard, pasting that text into another application, and then saving the transcript that way
EnableIMAutoArchiving	Prevent the saving of IM messages within Outlook Conversation History older	False	When set to true, a transcript of every instant message session that a user takes part in will be saved to the Conversation History folder in Outlook. When set to false, these transcripts will not be saved automatically. (However, users will have the option to manually save instant message transcripts.)

Set-UMMailboxPolicy Changes

Figure 10: Nat'l Labor Relations Board email re Skype for Business Configuration Changes (Apr. 13, 2017)

Finally, the Department of Agriculture (“USDA”) and Department of the Interior (“Interior”) policies allow for IM use but leave message preservation settings to end users. At USDA, employees can toggle the auto-save function in Skype for Business, though the records do not make clear whether the auto-save function is on or off by default.³⁰ Interior’s current IM policy predates the 2014 FRA amendments so it includes the wrong definition of a federal record and incorrectly states that “in general, there are no record retention requirements associated with gChat conversations other than when a given conversation meets the Federal record definition provided by NARA.”³¹

Directive Requirements

DOI employees must appropriately determine when to take the necessary individual action to preserve gChat conversations as a Federal record when those conversations meet the NARA definition of a Federal record (see definitions). For purposes of records management, many gChat conversations may not be Federal records. Consequently, in general, there are no record retention requirements associated with gChat conversations other than when a given conversation meets the Federal records definition provided by NARA. If a specific gChat conversation is determined to be a Federal record, it would be managed in accordance with the appropriate records schedule.

Figure 11: U.S. Dept. of the Interior, OCIO Directive 2014-003, *Acceptable Use of Bison Connect Electronic gChat Technology* (2014)

Agencies Need to Adjust Their Policies to Growing IM Use

Agency policies that claim instant messages are transient in nature and therefore need not be preserved fall short of statutory obligations under the FRA and FOIA. In fact, the justification of “temporary/transient nature of typical conversations” is not a sound distinction. Moreover, these policies blatantly contradict the guidance provided in NARA Bulletin 2015-02, which instructs agencies that while “current business practices make it more likely” that instant messages “contain transitory information,” nevertheless “agencies must capture and manage these records in compliance with Federal records management laws, regulations, and policies.”³²

Likewise, agencies are shortsighted and unrealistic when they prohibit IM use for official agency business. In fiscal year 2016, NARA conducted a year-long study of federal agencies’ use and management of electronic messaging technology and concluded that

“prohibiting the use of electronic messaging is not a viable approach. Agencies should provide employees both the tools they need for their work and mechanisms to manage the records created using those tools.”³³ Instant messaging is becoming an integral part of doing work. **Dismissing IM as insignificant or prohibiting its use to shirk records management responsibilities should no longer be acceptable options for compliance.**

The integration of IM into business applications provides new ways for employees to communicate and collaborate that are becoming increasingly popular. Prohibiting the use of IM for work today would be akin to forbidding email twenty years ago. Indeed, the use of IM for business communications has become so common that most enterprise software suites include IM functionality (e.g., Google Hangouts and Skype for Business as components of Google’s G Suite and Microsoft Office 365, respectively). One of the most popular messaging platforms, Slack, was built to virtually replace email in the workplace.

NARA’s initial guidance on managing IM, disseminated in 2015, instructs agencies to review and update their policies for managing IM as its use changes over time. At the time, Microsoft Teams didn’t even exist, and Slack had only a million daily users.³⁴ Now, Slack has around twelve million daily users³⁵ and Microsoft Teams has about thirteen million daily users.³⁶ IM apps are especially popular among younger workers who prefer IM/text to email. Younger workers—millennials and post-millennials—are a growing demographic that already make up more than forty percent of the workforce,³⁷ meaning the public can only expect to see IM’s integration and use in the workplace continue to increase.

Of the twenty agencies that produced their policies for use of IM, thirteen allow employees to use IM but prohibit them from creating or sending a record through IM, and three ban IM use altogether. Despite barring IM for official business, these agencies’ policies usually include a boilerplate statement about preserving instant messages that constitute federal records. Perhaps the inadequacy of these policies is highlighted by their prohibition of creating records through a practice they paradoxically acknowledge is being employed to conduct business.

30. Letter from U.S. Dep’t of Agric. To Cause of Action Institute (July 27, 2018), see app. At 036.

31. U.S. DEPT OF THE INTERIOR, OCIO DIRECTIVE 2014-003, ACCEPTABLE USE OF BISON CONNECT ELECTRONIC GCHAT TECHNOLOGY (2014).

32. *Supra* note 4.

33. NAT’L ARCHIVES & RECORDS ADMIN., ELECTRONIC MESSAGES WHITE PAPER (2016), available at <http://bit.ly/2qjtR7Y>.

34. Eugene Kim, *Slack hits another big milestone, proving its massive \$2.8 Billion valuation*, BUSINESS INSIDER, June 24, 2015, <http://bit.ly/37F5S8P>.

35. Rosalie Chan, *Slack says that while its user numbers still lag Microsoft’s, what really matters is that users love its app a lot*, BUSINESS INSIDER, Oct. 10, 2019, <http://bit.ly/3bKRz5H>.

36. Rosalie Chan, *With 13 million daily active users, Microsoft says its teams chat app is now growing faster than Slack*, BUSINESS INSIDER, July 11, 2019, <http://bit.ly/324z1sV>.

37. Richard Fry, *Millennials are the largest generation in the U.S. Labor force*, PEW RESEARCH CENTER: FACT TANK (Apr. 11, 2019), <https://pewrsf.ch/2P818Ce>.

Table 3: Agency Policies on IM Use and Retention

Agency	Policy Allows for Use of IM	Policy to Auto Retain IM
Consumer Financial Protection Bureau	✓	✗
Council of Inspectors General on Integrity and Efficiency	✓	✓
Department of Agriculture	✓	✗
Department of Education	✓	✓
Department of Energy	✓	✗
Department of Homeland Security	✓	✗
Department of the Interior	✓	✗
Department of Veterans Affairs	✓	✗
Environmental Protection Agency	✓	✗
Federal Communications Commission	✓	✓
Federal Energy Regulatory Commission	✓	✗
General Services Administration	✓	✗
General Services Administration Office of Inspector General	✗	✗
Internal Revenue Service	✓	✗
National Aeronautics and Space Administration	✓	✗
National Labor Relations Board	✓	✗
National Oceanic and Atmospheric Administration	✗	✗
Federal Bureau of Investigation	✗	✗
Federal Trade Commission	✗	✗
U.S. Agency for Foreign Development	✗	✗

Ephemeral Messaging

Only four of the thirty-nine agencies to which we sent a FOIA request produced a list of all messaging apps installed on agency-owned devices. We could have forced more agencies to produce this information through litigation but chose to forgo seeking judicial review. Three of the four agencies had instances of encrypted and ephemeral messaging apps.

Ephemeral messaging apps inherently present a higher risk of unlawful records destruction. This class of apps work like other IM apps with the added feature that messages are automatically deleted, or “disappear,” after being read. Thus, agencies should carefully consider whether allowing these apps to be installed on government-furnished devices unnecessarily facilitates employees using them to conduct government business.

Table 4: Sample of Messaging Applications on Agency-Owned Devices

Consumer Financial Protection Bureau	General Services Administration	National Aeronautics and Space Administration
Facebook	Cisco Jabber	Allo
GroupMe	Facebook	Blackberry Messenger
Hangouts	GroupMe	Conversations
KeeperChat	Hangouts	CoverMe
Skype	IM+	Facebook Messenger
Snapchat	InstaMessage	GroupMe
WeChat	Kik	Jabber
WhatsApp	Messenger	LINE
	Microsoft Chat	Signal
	Pidgin	Skype and Skype for Business
	Skype	Slack
	Slack	Snapchat
	Social Messenger	Viber
	TeamSnap	WeChat
	WeChat	WhatsApp
	WhatsApp	Wickr Me
	Windows Messenger	
	Yahoo! Messenger	

Scoring Agency IM Records Management Practices

To better understand agency performance regarding their policies and practices on IM, we mapped each agency across five aspects, including whether agencies:

1. Updated their records management policies since the 2014 FRA amendments
2. Allow IM use
3. Have policies to preserve instant messages
4. Archive instant messages
5. Produced instant messages pursuant to our request.

Each measure has a max of twenty points, making one hundred the maximum possible score for an agency. For the first measure, agencies that have updated their policies since the 2014 FRA amendments to incorporate the new definition of an electronic record receive twenty points and those that have not receive zero points. Next, agencies that allow IM use receive twenty points. Agencies that, in practice, allow IM use but have policies that forbid employees to from creating or sending a federal record via IM receive ten points. Agencies that claim to prohibit IM use receive zero points. This is because, as discussed above, NARA maintains that agencies should provide employees with the tools necessary to do their jobs and the mechanisms to maintain records created with those tools.³⁸ And because, in all reality, employees will do so anyway.

The third and fourth measures also have three possible point allocations. For the former, agencies with policies to automatically preserve instant messages are given twenty points. Those that have a functional IM archiving feature but which the end user (*i.e.*, employee) enables/disables receives ten points, and agencies that do not preserve instant messages per policy garner zero points. The fourth measure is closely related to the third but grades agencies on their practices, rather than their policies. That is, do agencies' records reflect they are preserving instant messages? Agencies with records showing they employ enterprise-level IM preservation tools gain twenty points. Agencies that give employees the ability to turn on/off their chat histories receive ten points and those that don't preserve messages get zero points. Finally, agencies that provided us with instant messages gain twenty points and those that did not receive no points.

Scores for each agency are detailed in Table 6³⁹ and plotted on Figure 1. From the data, three tranches appear. Agencies with scores that fall

within the green area are categorized as “satisfactory” and those in the yellow “need improvement.” Agencies with poor IM policies and practices appear in the red region of Figure 1.

Only four agencies receive passing scores: FCC, CIGIE, USDA, and NASA. These agencies all have up-to-date policies and allow IM use, though two maintain policies that IM should not be used to send non-transitory information. Two of the agencies have policies to automatically preserve instant messages and the other two enable their employees to do so, which is reflected in their archive settings as well. All but CIGIE provided us records of instant messages.

In the next tranche, nine agencies need to improve their policies for IM records management. While all these agencies allow IM use, six do not allow employees to send or create records via instant message. None of these agencies policies provide for central archiving of instant messages (except maybe ED, though it is unclear from the records), though three give end users the option to save their chat histories.

Thirteen agencies, half that responded to our FOIA request, have very poor policies regarding IM. These agencies, for the most part, claim to not allow IM use, do not preserve instant messages, and did not produce any messages. Agencies in the red region of Figure 1 are not complying with federal records laws.

Overall, as Figure 1 illustrates, federal agencies have so far largely failed to adequately account for IM in their policies and practices. IM is inevitably integrating into agency business, but agencies are not properly managing records to comply with federal law and NARA guidance.

Agency Performance on Instant Message Record Management

100	
90	• FCC
80	• CIGIE • USDA
70	• NASA
60	• CFPB • DOI • VA • EPA • FERC
50	• ED • NLRB
40	• DHS • IRS
30	• GSA
20	• DOD • DOL • EXIM • FBI • FEC • FTC • NOAA • SEC • USAID
10	• DOE
0	• HHS • SBA
Did not respond to FOIA request	• CIA • DOC • HUD • DOJ • DOS • USDT • DOT • ICE • NARA • NSA • OMB • OSTP • OSC • USCIS

38. *Supra* note 33 at 5.

39. App. At 002.

Technology Provides Opportunities for Better Records Administration

While changes in technology can pressure agencies to adapt their records management policies and procedures to keep pace with new business practices, technological advancements also provide an opportunity for better records management. In this case, besides a new way to communicate and get work done, popular enterprise IM applications also offer robust information management tools. The name Slack, in fact, is a “backronym” for “Searchable Log of All Conversation and Knowledge.”⁴⁰ The platform was designed specifically to retain and make searchable all information shared within it. Unsurprisingly, Slack’s competitors followed suit.

Slack, Hangouts Chat, Microsoft Teams, and Skype for Business—applications records show agencies are using—offer enterprise-level message retention, data loss prevention, eDiscovery, legal holds, and so on. These tools are highly automatable, flexible, and customizable, thus enabling organizations to efficiently configure sophisticated information management protocols in line with federal records laws.

NARA even suggests that the provision of official IM capabilities for work would reduce employee use of personal accounts to conduct agency business.⁴¹ Secretary of State Hillary Clinton’s use of a personal email server to conduct official government business drew much attention to this problem. This has not been an isolated incident. Secretary of State Colin Powell,⁴² Secretary of Defense Ash Carter,⁴³ Secretary of Homeland Security Jeh Johnson and some of his staff,⁴⁴ White House Office of Science and Technology Policy Director John Holdren,⁴⁵ White House Council on Environmental Quality Managing Director Christy Goldfuss,⁴⁶ Department of Justice Director of Public Affairs Sarah Isgur,⁴⁷ United States Trade Representative (“USTR”) Ambassador Robert Lighthizer,⁴⁸ General Counsel to the USTR Stephen Vaughn,⁴⁹ and potentially others also have used personal email accounts to conduct government business.

The 2014 FRA amendments prohibit agency employees from creating or sending federal records through non-official electronic messaging

accounts unless they forward the record to their official account within twenty days of the record’s creation or transmission. Unlike IM, for which agencies can provide an official platform integrated with information management mechanisms, agencies cannot do much more than educate employees about their obligations when they go outside the system.

While there are many reasons agency employees may use personal accounts to conduct official business, convenience of communication is certainly among them. Modern technology has fundamentally changed the way people communicate. People expect to send or receive information quickly from nearly anywhere at any time. Providing employees with an official messaging system that allows them to do so, such as IM, could mitigate risk of record loss from the use of non-official accounts.

Conclusion

The retention of government records in a searchable system is fundamental to transparency. The mechanisms that capture and preserve records must keep pace with technology for the system to be an effective tool to enforce executive branch integrity. Instant messaging is the latest technological phenomenon to strain federal records management. Like email, IM’s integration into the workplace has changed how information is transmitted and transformed the way work is being done. Congress accounted for these changes legislatively, but in the years since the 2014 FRA amendments, agencies have been slow to bring their records management policies and practices regarding IM into compliance. No longer should agencies dismiss IM as inherently transient and insignificant. Prohibiting IM use is not a realistic policy either.

Records management policies must reflect how agencies generate and transmit information. Agencies should embrace IM’s increasing integration and utilization in the workplace and provide employees with an official instant messaging option for work that is equipped with the necessary features to comply with the law and NARA guidance. This report should serve as a wakeup call for federal agencies to take decisive action to ensure they are complying with federal law.

40. Stewart Butterfield (@stewart), TWITTER (Sept 27, 2016 7:07 pm), <http://bit.ly/3bIkVSp>.

41. *Supra* note 33 at 5.

42. Josh Gerstein, *Colin Powell defends personal email use*, POLITICO, Sept. 8, 2016, <http://politi.co/2lZsdpy>.

43. CBS NEWS & ASSOCIATED PRESS, *Defense Secretary used personal email account for nearly a year*, MAR. 26, 2016, <http://cbsn.ws/2mmwve8>.

44. Josh Gerstein, *Judge orders 4 HomelandSecurity officials to preserve private-account emails*, POLITICO, Jan. 18, 2017, <http://politi.co/2lZnFj9>.

45. Stephen Dinan, *Obama science chief’s email fiasco mirrors Hillary Clinton case*, WASH. TIMES, Nov. 3, 2016, <http://bit.ly/2lEGWuX>.

46. Robin Bravender, *Watchdogs want CEQ director’s personal emails*, GREENWIRE, Oct. 27, 2016 (“A government watchdog group is seeking personal emails from the head of the White House council on environmental quality after recently hacked emails indicate she may have used her personal account to conduct government business.”).

47. Jacob Brogan, *The DOJ’s Director of Public Affairs Used Gmail to Send a Work Email. Is That Legal?*, SLATE, Mar. 2, 2017, <http://slate.me/2mCx83L>.

48. Thomas Kimbrell, *USTR Records Show Ambassador Lighthizer Used Personal Email for Government Business*, CAUSE OF ACTION INSTITUTE (June 6, 2019), <https://coainst.org/38H2P15>.

49. *Id.*

Appendix

Table 5: Agencies Included in Investigation












Produced Records in Response to FOIA		Did Not Respond to FOIA
Consumer Financial Protection Bureau	Federal Bureau of Investigation	Central Intelligence Agency
Council of Inspectors General on Integrity and Efficiency	Federal Communications Commission	Department of Commerce
Department of Agriculture	Federal Election Commission	Department of Housing and Urban Development
Department of Defense	Federal Energy Regulatory Commission	Department of Justice
Department of Education	Federal Trade Commission	Department of State
Department of Energy	General Services Administration	Department of the Treasury
Department of Health and Human Services	Internal Revenue Service	Department of Transportation
Department of Homeland Security	National Aeronautics and Space Administration	Immigration and Customs Enforcement
Department of Labor	National Labor Relations Board	National Archives and Records Administration
Department of the Interior	National Oceanic and Atmospheric Administration*	National Security Agency
Department of Veterans Affairs	Securities and Exchange Commission	Office of Management and Budget
Environmental Protection Agency	Small Business Administration	Office of Science and Technology Policy
Export-Import Bank	U.S. Agency for International Development	Office of Special Counsel
		U.S. Citizenship and Immigration Services

* NOAA records were obtained through separate FOIA requests submitted prior to the FOIA request sent to the other agencies included in the study

Table 6: Summary of Agency Policies on Use and Retention of IM

Agency	Official IM Application	Latest Policy Update	Policy to Allow IM Use	Policy to Preserve IM	IM Archive Enabled	Produced IM on Request	Grade
Federal Communications Commission	Jabber	Mar-18 (20)	10	20	20	20	90
Council for Inspectors General on Integrity and Efficiency	Skype for Business	Jun-19 (20)	20	20	20	0	80
Department of Agriculture	Skype for Business	Aug-16 (20)	20	10	10	20	80
National Aeronautics and Space Administration	Skype, Jabber	Jan-15 (20)	10	10	10	20	70
Consumer Financial Protection Bureau	Unknown	Jul-15 (20)	10	-	10	20	60
Department of the Interior	Google Hangouts	Aug-14 (0)	20	10	10	20	60
Department of Veterans Affairs	Skype for Business, Slack	Nov-18 (20)	20	0	0	20	60
Environmental Protection Agency	Skype for Business	Feb-15 (20)	20	10	10	0	60
Federal Energy Regulatory Commission	Skype for Business	Dec-16 (20)	10	10	0	20	60
Department of Education	Skype for Business	Apr-17 (20)	10	20	-	0	50
National Labor Relations Board	Skype for Business	Apr-17 (20)	10	0	0	20	50
Department of Homeland Security	Unknown	Feb-18 (20)	10	10	0	0	40
Internal Revenue Service	Lync	Nov-16 (20)	10	10	0	0	40
General Services Administration	Slack, Google Hangouts	Jun-15 (20)	10	0	0	0	30
Department of Defense	Defense Collaboration Services	Aug-17 (20)	-	-	-	0	20
Department of Labor	Unknown	May-17 (20)	-	0	0	0	20
Export-Import Bank of the U.S.	Skype for Business	Nov-17 (20)	-	-	-	0	20

Agency	Official IM Application	Latest Policy Update	Policy to Allow IM Use	Policy to Preserve IM	IM Archive Enabled	Produced IM on Request	Grade
Federal Bureau of Investigation	Unknown	Dec-17 (20)	0	-	-	0	20
Federal Election Commission	Skype for Business	Jan-07 (0)	-	-	-	20	20
Federal Trade Commission	Unknown	Mar-15 (0)	0	-	0	0	20
National Oceanic and Atmospheric Administration	Google Hangouts	Mar-12 (0)	20	0	0	0	20
Securities and Exchange Commission	Unknown	Unknown (0)	-	-	-	20	20
U.S. Agency for Foreign Development	Unknown	Jul-16 (20)	0	-	-	0	20
Department of Energy	Skype for Business	Mar-13 (0)	10	0	0	0	10
Department of Health and Human Services	Unknown	Unknown (0)	-	-	-	0	0
Small Business Administration	Skype for Business	Dec-98 (0)	-	-	-	0	0

Policy to Allow IM Use		Policy allows IM Use
		IM use permitted but not to create a record
		IM use prohibited
Policy to Preserve IM		IM retained automatically
		IM retained manually
		IM not retained
IM Archive Enabled		Central IM archiving
		IM records to be saved by end users
		IM not saved
Produced IM on Request		Produced IM
		Did not produce IM

