The State of Electronic Communications in Government

RESEARCH BRIEF

smarsh®

govloop

Introduction

Not too long ago, nuclear families across the country practiced common customs when sitting around their dinner tables: no phones, no TV, no business talk. But in most cases nowadays, personal and professional cultures have merged, and business conversations are creeping more into every setting of life – traveling from the office to the bus to the dinner table.

The digital revolution has transformed the way government functions too – but policies and practices aren't always up to date with the reality of how employees work in the 21st century.

Public sector work is unique in that security, transparency and archival laws govern the way agencies interact. While private sector organizations might not have reason to track every employee communication, tax dollars are on the line for every email that government workers send.

The thing is, government employees aren't only corresponding through emails anymore, no matter what official organizational policy may say about other forms of communication. Texts, private messaging apps and Facebook chats are all ways that employees discuss government business, and these forms of communication are equally subject to federal and state Freedom of Information Act (FOIA) laws.

All electronic messages sent from government-issued devices, as well as government communications sent from privately owned devices, by law must be treated as public records and thus need to be archived. Agencies at all levels must be able to produce these files to satisfy public records requests or support e-discovery events and investigations.

Most public sector organizations, however, have not ironed out use and retention policies for this new wave of nonstop and cross-platform communication. And the consequences of not being prepared for FOIA requests and so-called "sunshine" transparency laws across various levels of government can result in extreme reputational damage, litigation and financial penalties.

Choosing the right technology solutions and policies to manage electronic communications is vital for agencies today, especially as new communication applications and platforms emerge and records requests continue to flood government inboxes.

To discover how governments are capturing, monitoring and managing their electronic communication records, **GovLoop surveyed more than 300 qualified government officials across local, state and federal levels who deal with records management.** GovLoop also spoke with Robert Cruz, Senior Director of Information Governance at Smarsh, a leader in the capture and retention of electronic communications, to break down the results of the survey and discuss how federal and state agencies can close the gaps between electronic communications archiving and FOIA responses.

In the following pages, you'll learn about the results of the survey, the dangers faced by governments that are unprepared for open records requests and the advantages for governments that develop a strategy for modern records management. To save time and costs, ensure compliance and enable maximum productivity in the future, agencies need to reconsider their approach to the retention and management of the mass of texts, emails, social content and collaborative messages in the present.

Who We Talked to

Communication is a crucial component of every government organization's operation. While separate agencies might serve unique missions as they span levels and locations of government, communication is a constant.

In the survey, 30% of respondents worked at the federal level; 31% represented city, town and county governments; and 28% were employed in state governments. Another 11% were from other entities, including police, school boards and parks (see Figure 1).

The size of constituencies these governments serve varies significantly as well, from large states, cities and national agencies to populations below 5,000 people. Both small and large departments face challenges in records management. Smaller offices may not have defined roles or systems for records management, while larger organizations can be inundated by a massive volume of communication data to capture, search and review in the face of numerous requests (see Figure 2).

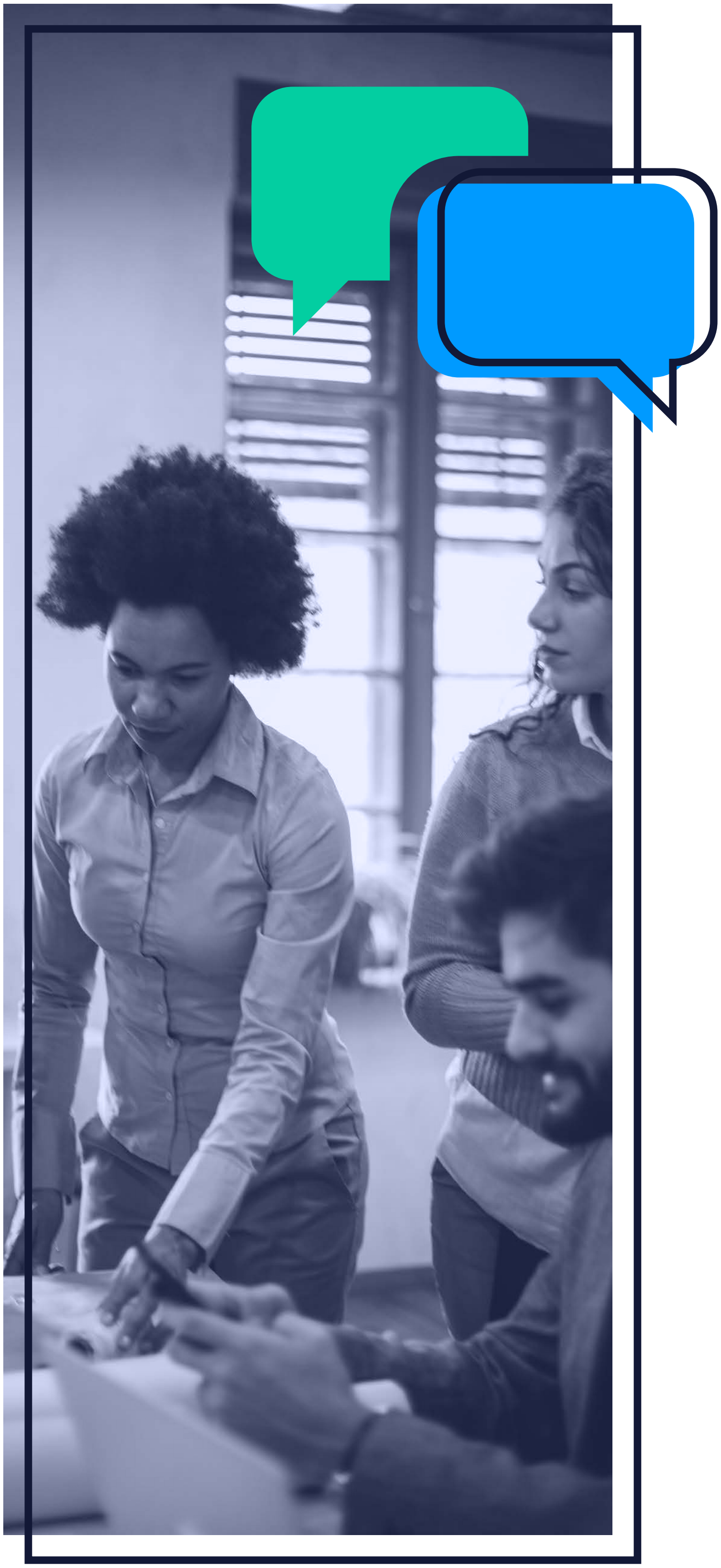


FIGURE **1**

What type of government do you work for?

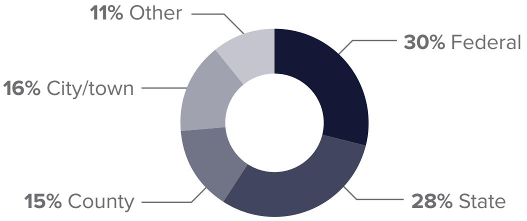
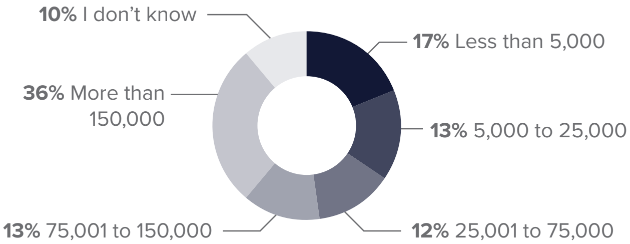


FIGURE **2**

What is the size of the population your organization supports?

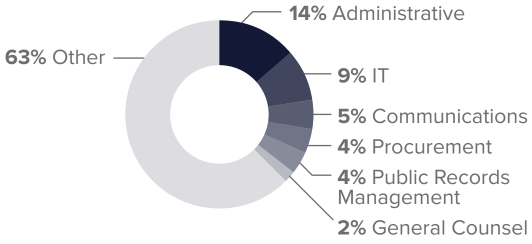


While job roles may share communication oversight, records management does not fall cleanly into one vocational bucket. Many governments lack a public records officer or someone with the specific duties of compiling and administration of records. Instead, the responsibility can fall on anyone – from clerks and communication directors to human resources, and most certainly IT.

With the exception of "Other," the second-largest department, selected by 14% of survey participants, was the "Administrative" category, with jobs such as clerks and project managers. In GovLoop's survey, the lion's share of respondents, 63%, marked themselves in the category of "Other," with a wide variety of titles such as teacher, senior volunteer, park ranger and clinical social worker. The results of this survey demonstrate how the responsibility of records management can fall to a wide variety of operational roles (see Figure 3).

FIGURE **3**

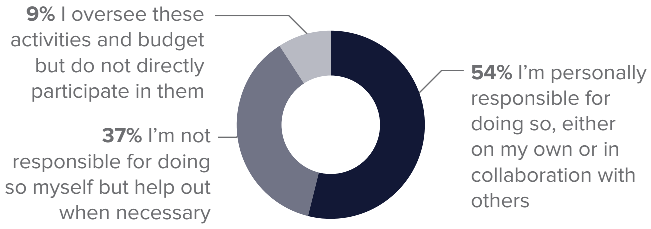
In which department do you work?



Responding to open information requests often isn't a single-track project. Still, a majority of respondents – 54% – marked themselves as "personally responsible" for responding to and managing records requests within their organizations, either with other employees or alone. And 37% said they do not have records management responsibilities but "help out when necessary" (see Figure 4).

FIGURE **4**

What is your role when it comes to responding to and managing records requests for the department or organization in which you serve?



Those with roles in records management were asked several questions later in the survey about their agencies' capture and retention policies for electronic communication content. Types of electronic communication content include emails, text messages, collaboration platform activity, instant messaging, social media channels and more.

If managing records in government seems somewhat nebulous, that's because it is. Responsibilities can fall on anyone's shoulders, and maximizing resources to easily capture, store and organize records so that they can be shared or used is an indefinite science. So why should records management matter to public sector employees, if most may never have to respond to a request or track down a file? See the next section to find out.

Introducing You to the Technology

Throughout this guide, we'll reference very specific categories of communication technologies. For your ease of reading, here are some recognizable brands and products that belong to each category.

- **EMAIL - ORGANIZATIONAL**
  Microsoft Outlook
- **EMAIL - OTHER**
  Gmail, Yahoo! Mail
- **INSTANT MESSAGING (IM) & COLLABORATION**
  Slack, Microsoft Teams, Yammer, WebEx Teams, IBM Sametime, IBM Connections, Workplace by Facebook
- **PUBLIC INSTANT MESSAGING**
  Skype, Facebook Messenger, Google Chat, Slack
- **SOCIAL MEDIA**
  LinkedIn, Facebook, Twitter, Instagram
- **ENCRYPTED CHANNELS**
  WhatsApp, WeChat, iMessage, Telegram, Signal

The Changing Nature of Work in Government

As technology greets new forms of interpersonal and mass communication, government has had to adjust. Employees demand the same tools they use to communicate in their personal lives be available at work. That means social media, instant messaging and collaboration channels, and text messaging are now all necessary for public work. And just like emails and other forms of public record communications, they're subject to government retention and FOIA laws.

FOIA laws are expansive. By sending a FOIA request to a public communications officer or through an online portal, a citizen can find out what bonuses a state college football coach is eligible for or receive emails concerning sanctuary city discussions between a mayor and city council members.

This information is open to the public, and it's crucial that it is. FOIA and sunshine laws help reporters expose fraud and waste and keep citizens informed about the inner workings of their governments. Today, transparency is more valued than ever, and government business and decisions are widely discussed in the always-on realm of social media. FOIA requests cover these modern forms of electronic communications as well.

"More government agencies are recognizing the benefit of operating in that way, just from a government transparency perspective. A good way to establish and build the trust of your constituents is to always respond with thorough electronic records requests and not get caught up in missing or incomplete data," Cruz said.

*A 2019 U.S. Justice Department (DOJ) report found that the federal government received a record-high **863,729 FOIA requests** in fiscal year 2018. That was a 5.6% jump from the previous high set in 2017, and there were 150,000 more requests in fiscal year 2019 than in fiscal year 2015.*

Governments also need to manage information from more internal sources than ever. A common trope in recent years has been "data overload," and those in charge of records are experiencing it firsthand. Enabling employees to use modern communication channels to discuss official business and interact with citizens is an important first step to capturing and managing content.

While most government agencies have well-documented practices for recording and retaining emails, the same can't be said for text and collaborative messaging, which are becoming increasingly common channels as the public sector environment tilts to welcome modern workforces. Under law, all messaging types of electronic communications, including video and voice, must be retained for records requests.

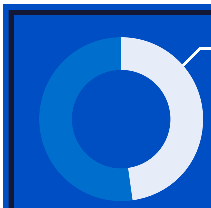
Modern communication apps allowed for government:

30%
of respondants allow or are considering SMS/text for government use

53%
of governements that use IM & collaboration tools are using Microsoft Teams

27%
allow or are considering IM & collaboration platforms

"Just the idea of engaging in a chat, that's what younger workers expect," Cruz said. "That's the way they prefer to interact – with text messages, social media and different forms of instant messaging or collaboration channels."



48% of organizations surveyed lacked confidence they could respond to a records request that included messages sent via SMS/ text or IM & collaboration.

Responding to records requests with "We don't have it" is not good enough, and that's not only when it comes to fostering a transparent and trustworthy connection for the public sector. Government agencies that struggle to respond to requests can drain resources, time and money, and if the request is part of an e-discovery event or litigation, organizations that delay or provide incomplete responses may encounter lawsuits and court-ordered fines.

"Changing demographics are going to force organizations into making a choice of either supporting modern communication tools or potentially losing that employee or losing the interest of that constituent as they request service."

- Robert Cruz, Senior Director of Information Governance at Smarsh

The Electronic Communication Tools of Today's Government

While they modernize, governments are facing a transformation – not just in the change in demographics, but also in the unique preferences that each generation of employees brings to the workplace.

As one might guess, the ways that millennials and Generation Zers prefer to work and engage coworkers or citizens look very different from Generation X and baby boomers' preferences for email, voicemail and face-to-face meetings. In fact, younger employees' preferences for chat and text messaging reflect more than a need for immediacy in communications; they're also a function of the tools they've grown up with and become accustomed to. These seismic societal trends have a grand implication for government: The great amount of data generated from all communications channels must be captured and made available for public records requests.

In asking which communication types were allowed in offices, the clear standard was organizational email accounts, such as Microsoft Office. It's no surprise that agencies have been using and retaining email for years, but it is noteworthy that close behind are SMS/text and social media platforms.

These forms of communication are hardly novel, however. By comparison, the private sector has blazed the path to newer instant messaging and collaboration platforms for chatting, and the public sector has begun making the pivot as well. Text is now more likely than not to be accepted as a form of communication, according to respondents, and many governments are widely considering or adopting other communication technologies like Microsoft Teams, WebEx Teams and Google Chat – all popular instant messaging platforms (see Figure 5).

Even though encrypted channels, such as WhatsApp and iMessage, remain prohibited in most respondents' departments, a surprising number of respondents are hearing employees want to use encrypted apps for work – which is contrary to best practices for electronic records retention.

The worry specifically with encrypted messaging apps is retention. Encrypted channels automatically delete messages after a period of time – a practice that defies government records regulations. News stories of national significance have centered on the deletion of important messages from government employees, and therefore organizations must prohibit technologies that cannot be archived.

"There's a basic premise that if you're going to allow communications through a specific channel, you have to be able to reliably capture it," Cruz said.

FIGURE **5**

✓

THE TOP 3 CHANNELS
ALLOWED
IN GOVERNMENT

1. Organizational email
2. SMS/text messaging
3. Social media

?

THE TOP 3 CHANNELS
UNDER CONSIDERATION*
IN GOVERNMENT

1. IM & collaboration
2. Public instant messaging
3. SMS/text messaging

✗

THE TOP 3 CHANNELS
PROHIBITED
IN GOVERNMENT

1. Public instant messaging
2. Encrypted channels
3. Other types of email

**Channels listed exclude 'Encrypted Messaging Channels' which cannot be archived and therefore must be prohibited*

While Slack, Google Chat, WebEx and Microsoft Teams are the most popular messaging and collaboration tools in use in government, Microsoft Teams seems to be far and away the favorite. More than half of respondents who have instant messaging and collaboration tools use Microsoft Teams. Both WebEx and Google Chat are used by over 20% of those who rely on collaboration tools (see Figure 6).

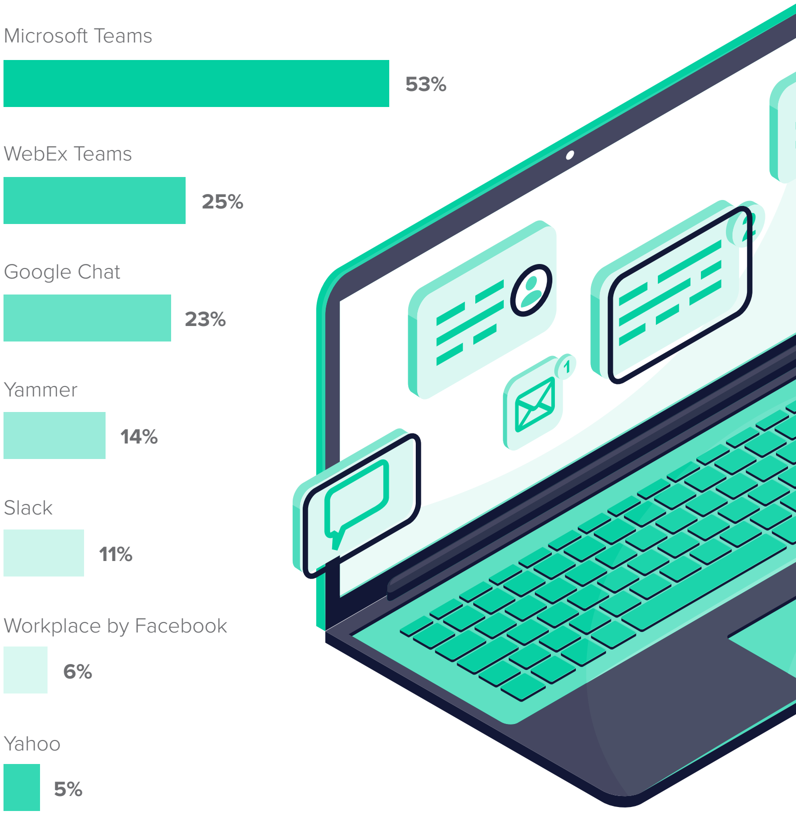
There's a push-pull to adopt these direct messaging and collaboration applications, said Cruz. The push can come from IT departments, which want to maximize what they can add to off-premise stacks easily with popular and user-friendly tools that minimize their burden on-premise. Microsoft Teams is likely the most popular collaboration tool because it can integrate with Microsoft Outlook and Office 365, which are also carried on the cloud, and users are familiar with its interface.

The pull comes from recruits – a younger generation that covets the same choices they currently use for personal communications, which are also more widely adopted in the private sector. Many public sector organizations are trying to attract these newer members of the workforce as baby boomers are retiring, but government employers often struggle to match private industry tools and policies. By adopting text, collaboration and instant messaging applications, the public sector can work to shorten the gap of workplace allure for the younger generation.

"If you don't provide support for these interactive tools, the chances are other employers will," Cruz said. "And they're going to be a more attractive location for the people that you're trying to attract."

FIGURE 6

Which of these IM/Collaboration platforms does your organization use? (Select all that apply)



The two most important factors respondents identified for managing electronic communications as they relate to records requests were:

#1 Modernizing public record management for a transparent government – community relationship

#2 Implementing a tech solution to search electronically within all data vs. a collection of scanned (flattened) or printed content for further manual search

Importantly, social media has increasingly necessitated a new forum for government electronic records storage as well. Government agencies have their own social media presence though official profile pages – a new paradigm for public-facing information. From these channels, employees can respond to questions, post updates and interact with constituents under the shield of one entity. These social media communications are part of the government record as well.

All of the above communication sources carry immense potential for productivity in the public sector. Unfortunately, they create challenges as well. Governments are responsible for archiving and accessing records from these sources to ensure that they are transparent and in a good position to respond to FOIA and e-discovery requests.

The Potential and Risk of Electronic Communication in Government

Agencies are making proactive and progressive strides to attract new workers by permitting modern channels of communication. Before jumping in headfirst to the next big technological trend, however, the right controls need to be put into place – both in technology and employee use policies, as well as with electronic records retention and management solutions.

Take text messaging, for instance. Although studies consistently show that about two-thirds of public sector organizations permit text messaging for business purposes, 100% of public sector organizations need to be ready to capture and archive employee text messages for public record responses.

Official policy might prohibit employees from using text for work communications, but as ubiquitous as cell phones are, official business conversations will naturally take place via text. From a "running five minutes late" text to a quick debrief of a committee meeting to an important planning decision, governments are responsible for recording the business communications of employees – and use policies need to account for such. Governments that haven't strategically planned for modern messaging can still be held responsible in court if the private communications of an employee prove to contain sensitive information.

"They need to be realistic, and sometimes that new reality arrives when you get a request for historical information from a mobile device," Cruz said.

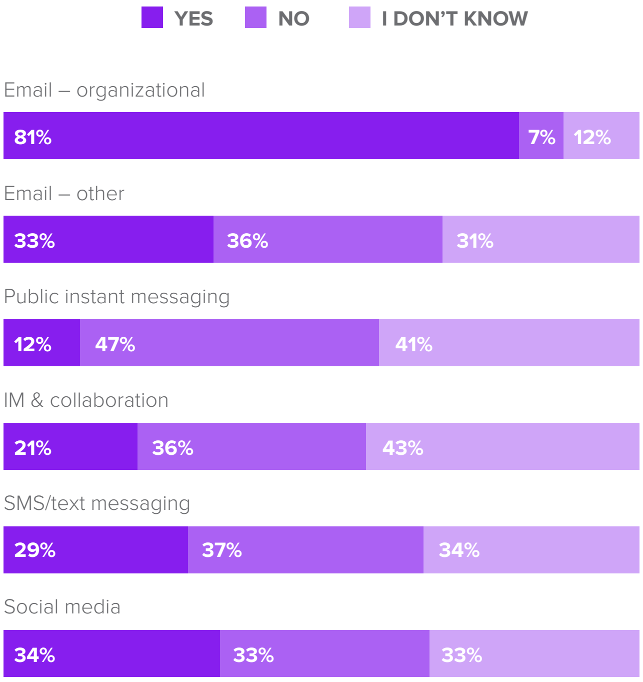
Without official retention strategies and use policies in place, organizations must go to extreme lengths to obtain information sent through SMS. Dealing with many parties – from carriers to IT, HR and employees – they have to extract what's available, which is time-consuming and expensive, and likely inexact or incomplete.

Too often, agencies fail to capture and store SMS data, or even consider that they need to have a plan in place. With text, 29% of respondents said they are archiving text message content, 37% said they were not archiving text and 34% didn't know. The vast majority did not have their texts recorded or didn't know their agency's policy (see Figure 7).

When no solution exists to capture and archive employees' text communications, public sector organizations are at risk of fines and litigation due to incomplete records and, on occasion, inability to respond to requests. Some organizations put the onus on employees to save and store their texts, but individuals can fail to remember to do so or fail to understand the importance of the policy. And when employees are unaware of what their responsibilities are, that risk jumps higher.

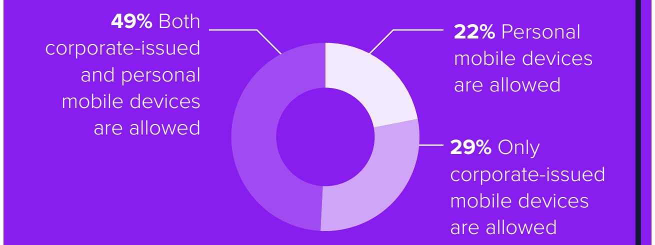
FIGURE 7

Does your organization capture and retain the following channels* for public records requests, litigation events or internal reviews related to business conduct?



*Encrypted channels data excluded. Encrypted messaging cannot be archived.

What is your organization's mobile device scenario and use policy?



The most common carriers used in government were **Verizon and AT&T.** Also popular were U.S. Cellular, T-Mobile and Blackberry.

“What agencies should be saying to their employees is that, ‘I want to allow you to use the technology of your choice, the technologies that you’re familiar with,’” Cruz said. “‘But as soon as I allow you to use that tool, you need to understand that we have obligations to capture and preserve those communications.’”

The survey asked why government organizations don’t retain more types of electronic communications, and the responses were highly varied. The most common response was that “It isn’t required to be captured/retained by law,” with 20% of responses. Other common answers included lack of resources (see Figure 8).

While some public sector organizations might not think electronic messages are required to be captured by law, courts and legislative bodies often beg to differ. The Illinois attorney general’s office recently reinforced that all records “pertaining to public business” are included under FOIA requests, regardless of their physical form. The issuance was in response to an Illinois city withholding texts because it did not believe they constituted a public record. Texas also amended its government code to add a set of new rules requiring the retention of text messages, including heavy penalties for noncompliance.

At the federal level, there is specific guidance requiring federal electronic communications to be preserved. A National Archives Bulletin (Guidance on Managing Electronic Messages) published to the heads of all federal agencies officially delineates texts, instant messaging, chats, voicemails and other messaging apps as forms of electronic communication per the **Federal Records Act**, which was updated in 2014 to include electronic communications. It reads: **“Electronic messages created or received in the course of agency business are Federal records.”**

State and local laws can be looser than national regulations. Still, archiving messages can be thought of under a more holistic interpretation of the law, as it is critical for public records requests and litigation, and leveraging this data can also be beneficial for training and internal investigations. Compliant oversight of electronic communications also leads the way for public bodies to detect fraud and malfeasance from officials as well as proactively address such occurrences before they become public.

“There may not be an explicit objective that it has to be captured, but you may just want to be looking at these electronic records from a governance perspective,” Cruz said. “Do they have risk or value? Is there a possibility that something that is an asset of the entity might be exposed through the use of this network?”

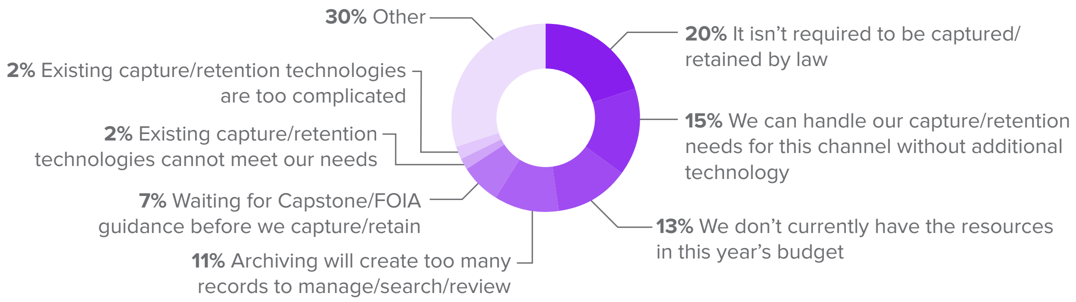
When agencies fail to have the right technologies or procedures in place, data loss can go undetected. That can lead to devastating outcomes.

Insider threats often “channel hop,” finding unmonitored networks so that they can easily extract and send out information, Cruz said. It’s a technique, he said, similar to what teenagers engage in to avoid the overwatch of parents.

Insider threats, however, are far more pernicious than average teenagers, and government agencies are expected to be more hands-on than the average parent. Formal use and retention policies that cover all channels are a way to ensure that insider threats cannot share information coming from within networks without the government knowing about it. Therefore, valuable information is more likely to remain within agency doors, preventing governments from needing to pick up the pieces after a leak.

FIGURE **8**

What is the main reason your organization does NOT capture/retain channels?



Where Government Falls Short in Electronic Records Management

Governments are confident that they'll be able to answer requests for public records that include text messages, the data shows. Unfortunately, survey results show that confidence might be misplaced, with a lack of practices and techniques in place to accurately capture SMS/text communications.

From the survey, 30% of respondents don't expect their government to ever capture SMS or text data, and yet 43% view SMS and text as the highest compliance risk (see Figure 9). Only social channels, at 53%, were perceived as a higher compliance risk (see Figure 10).

FIGURE 9

When do you expect your organization to begin archiving/retaining SMS/text content?

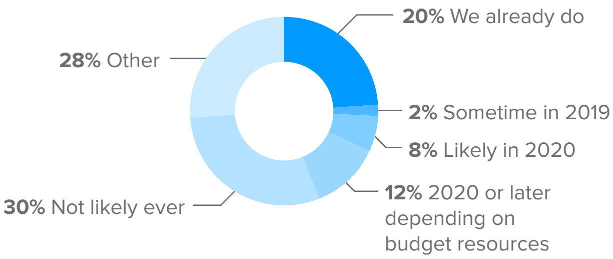


FIGURE 10

Besides email, which types of content do you perceive as the top sources of the most compliance risk?

#1	#2	#3
Social channels	SMS or text message	Encrypted channels

The most common worry with these records generally is cybersecurity – which 55% of respondents selected as a major concern. Other common concerns were the inability to produce complete records on request, at 44%, and inadequate processes or finances for taking on new forms of communication, at 47% (see Figure 11).

Moreover, these stats suggest that government organizations are most concerned about their ability to comply with records requests involving social content and SMS/text content.

FIGURE 11

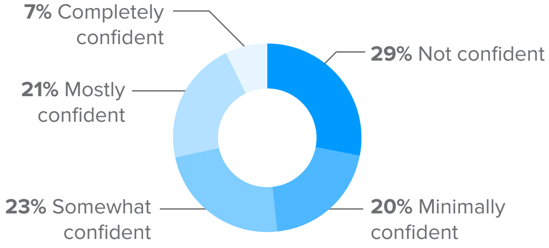
Top concerns government organizations have related to the systems and process of archiving electronic communications:

1. Cybersecurity threats posed by the use of electronic messaging platforms
2. Security/capabilities of third-party vendors being used to manage data
3. Inadequate process to take on new devices and applications insufficient financial resources (e.g. budget or capital)
4. Inability to produce complete records for all electronic communications channels upon request
5. Managing/maintaining multiple archiving providers or review platforms
6. Variety/volume of both content from multiple channels and devices

Yet despite these concerns, respondents felt relatively confident in their agencies' ability to produce text records for employees. The survey asked participants whether their agency could retrieve all electronic communications around the subject of "CONTRACTS" "promptly for a litigation request." Over half of respondents – 51% – were somewhat confident or more that their agency could complete the order (see Figure 12). Furthermore, 49% of respondents said their agency could complete the request in four weeks. And, 20% of respondents claimed their agencies would need quite a bit more time to complete the request estimating between one to three months.

FIGURE 12

SCENARIO: Your organization receives a request to produce all electronic communications for your organizational leader that contain a specific keyword. How confident are you that you could produce a completed response with all required message types, promptly for a litigation request?



And yet, this confidence seems overly optimistic considering the low retention rates of instant messaging, social media, collaboration tools and SMS communications – none of which was being captured more than 35% of the time in surveyed agencies. Based on this, it seems unlikely that these organizations would be able to quickly gather, process and and deliver a complete response to the sample request. In fact, said Cruz, agencies often aren't able to respond quickly except for when processes are in place.

Nearly half – 49% of respondents had ***little or no confidence*** *they could respond to a request for text records.*

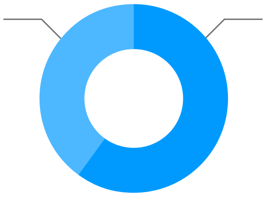
A cautionary point for agencies: Even if the response could be answered anytime between four weeks and three months, they would be operating on borrowed time. While many electronic communications requests may take months to process, some requests, such as records pertaining to time-sensitive court cases, must be produced in as little as 15 days. In addition, FOIA requests have terms attached: In the federal government, agencies have 20 days to respond to a FOIA request, although they might be able to gain an extra 10-day extension.

States and local governments have different laws, but they often offer even less of a window. For example, government organizations in Michigan have five days to respond and 10 days for a potential extension.

Extracting these requests without a well-defined capture and archiving strategy and solution can be time-consuming and costly – even more so if litigation arises due to failure to answer a FOIA request in a timely manner or because of an incomplete response. In 2018, federal agencies spent over $500 million processing FOIA costs and another $40 million in litigation charges, both record highs. Litigation cases also increased in number to new highs. About 40% of respondents said their organization had been involved in litigation over a FOIA or public records request over the past three years (see Figure 13).

FIGURE **13**

Based on the answers of those who knew their organization's involvement with litigation related to public records requests:



40% of organizations had **not** been involved in litigation regarding FOIA/ public records requests in the last three years.

60% of organizations had been involved in litigation regarding FOIA/public records requests in the last three years.

Agencies can file for extra time in the case of extremely laborious FOIA requests and recoup some processing costs by asking for expenses from requesters.

However, there's a way around all of that. In the next section you'll learn how to manage electronic communication records.

The Top Three Survey Results to Remember

#1

Besides email, the next three channels ALLOWED are: SMS/text (18%), social media (15%) and IM & collaboration (11%).

- For governments using IM & collaboration platforms, the survey says 53% of organizations are using Microsoft Teams.
- The top three channels in consideration are encrypted channels (20%), IM & collaboration (16%) and SMS/text messaging (12%).

#2

The channels with most perceived risk are: social (53%), SMS/text (43%), encrypted channels (24%) and IM & collaboration (20%).

#3

The top concerns related to archiving solutions and processes are:

- Cybersecurity threats (55%),
- Security/capabilities of third-party vendors being used to manage data (48%),
- Inadequate processes to take on new devices/insufficient financial resources (47%), inability to produce complete records for all electronic comms channels (44%).

How Agencies Should Handle Electronic Communication

As gleaned from the survey, governments are exerting great effort to manage their electronic communications, but obsolete methods of archival and retention have left them underprepared to manage the data generated by new channels. New communications channels, such as text and IM, are deluging governments with data that existing public records systems cannot handle.

But the problem can't be solved by just banning devices and apps. In fact, trying to do so only increases the risk of compliance breaches and security loopholes, which can leave governments vulnerable to penalties and fines. Therefore, it's important that agencies take a strategic and balanced approach.

Using a central solution, an agency can monitor all of its channels of communication in one seamless archive. Electronic records management can be efficient when all content is captured in native context and rapidly searchable by user, channel or keyword, versus disparate searches of a variety of archives or hard drives that would have required effort from different departments (such as IT, records, HR or users themselves).

Agencies should select an archiving partner to capture all electronic communications in a comprehensive archive including text, social and instant messaging, email and collaboration content. For all electronic communication records, a single view that integrates different channels is necessary for accuracy and completeness of record retrieval, as well as ensuring expediency.

Even if agencies have policies for archiving content from a variety of sources, without a single searchable platform, they end up spending an inordinate amount of time searching through content from different archives. And often, that content is flattened into an email and stored, stripping important context and metadata. These problems are a significant drain on resources and impact many departments within the organization.

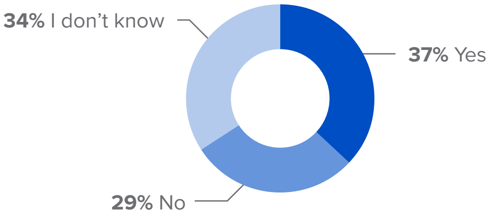
More so, governments can give power back to their constituents while reducing work for themselves. A good place to start is by building an online portal, something that more than a third of respondents did not know if their organization uses (see Figure 14).

Online portals are especially useful in government because they can immediately answer questions that would usually have to be processed as a regular FOIA request. For example, if a FOIA request came in for communication about the 2019 Memorial Day parade from the city planning office, with a portal, that request would be formally sent to a designated person capable of handling it. Once the project management component was completed and the request was answered, the portal would log related emails and documents. From then on, requestors could see and search those requests before submitting a new one, thus eliminating time and cost associated with duplication of requests.

Whether an agency has a portal or is just beginning to comprehensively track electronic communications, it must employ tried and true practices and policies to mange all organizational channels of electronic communication.

FIGURE **14**

Does your organization use a public facing portal application to receive and deliver records requests?



Best Practices for Evolving Electronic Communication Management

Determine which platforms and specific applications are allowed for employees to use for both internal and external communications.

PRO TIP:

- Take employee preferences into consideration when it comes to channels. The majority of employees prefer to text and chat with coworkers and outside contacts. Enable them to communicate on platforms you will capture and archive.

Create specific mobile policies to define which types of devices are allowed, for example corporate-issued devices only or personal devices including phones and tablets.

PRO TIPS:

- Users should be specifically informed on what the organization is collecting, how it will be used, and why it needs to be captured and archived. Apps, documents and other departmental materials must be protected and controlled by IT if the employee decides to leave the organization.
- If you allow personal devices, consider mobile device management (MDM) and enterprise mobility management (EMM) solutions, as they restrict collection of content such as personal emails, contacts, calendars, location, photos, text messages, call history and voicemail.

Create use policies for employees that are specific about which applications they are allowed to use. Define both allowed and prohibited channels and clearly outline how content will be captured and archived for public records management.

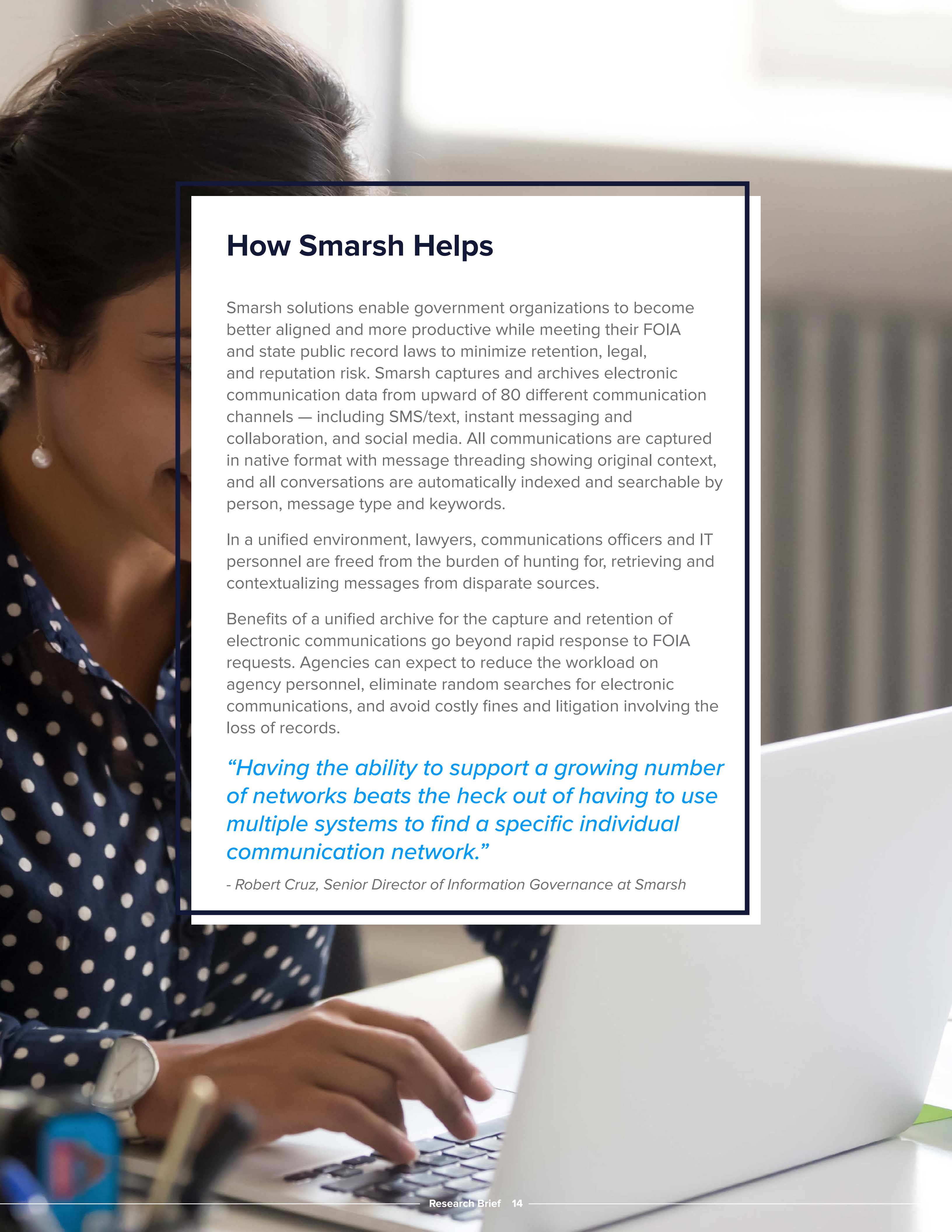
PRO TIPS:

- Enable your workforce to use text messaging by implementing an archiving solution for the direct carrier capture of organization-issued devices, or a containerized mobile device solution for employees using their own devices.
- Prohibit applications where content cannot be reliably captured and archived, such as iMessage, WeChat and WhatsApp.

Determine how security assessments will be carried out, and what will happen if prohibition or use policies are violated. It's important to be transparent about protocols regarding the capture and handling of electronic communications.

PRO TIP:

- Clear policies and procedures should deter employees from downloading and using prohibited apps and devices, as well as deleting content.



How Smarsh Helps

Smarsh solutions enable government organizations to become better aligned and more productive while meeting their FOIA and state public record laws to minimize retention, legal, and reputation risk. Smarsh captures and archives electronic communication data from upward of 80 different communication channels — including SMS/text, instant messaging and collaboration, and social media. All communications are captured in native format with message threading showing original context, and all conversations are automatically indexed and searchable by person, message type and keywords.

In a unified environment, lawyers, communications officers and IT personnel are freed from the burden of hunting for, retrieving and contextualizing messages from disparate sources.

Benefits of a unified archive for the capture and retention of electronic communications go beyond rapid response to FOIA requests. Agencies can expect to reduce the workload on agency personnel, eliminate random searches for electronic communications, and avoid costly fines and litigation involving the loss of records.

“Having the ability to support a growing number of networks beats the heck out of having to use multiple systems to find a specific individual communication network.”

- Robert Cruz, Senior Director of Information Governance at Smarsh

Conclusion

In government, leadership and employees don't always agree. But conquering the hassle of records and electronic communications management involves everybody in the public sector. As organizations devote time to antiquated platforms or delve into the annals of long-ago public records to answer FOIA requests, management can see costs – of overtime, retrieval, storage or fines – skyrocket.

Going forward, agencies can own their time and future. The management of electronic communications doesn't have to be a ball and chain to employees, lawyers or IT departments, and then, they can be mission-enablers. By implementing electronic communications use, capture and archiving strategies, the government becomes less paper-pushing and record-digging and even more dedicated to serving the public and doing business in a transparent and efficient manner.

About Smarsh

Smarsh helps government organizations get ahead – and stay ahead – of the risk within their electronic communications. Utilizing the Smarsh Connected Suite, agencies can reduce the burden and time required when responding to records requests and consolidate from multiple systems into a modernized, comprehensive retention and production solution. Capture, archiving and monitoring solutions extend across the industry's widest breadth of channels, including email, social media, mobile/text messaging, instant messaging/collaboration, websites and voice. Government agencies in 40 of the 50 U.S. states rely on Smarsh to help meet their recordkeeping and e-discovery requirements. Founded in 2001, the company is headquartered in Portland, Ore. with nine offices worldwide, including locations in Silicon Valley, New York, London and Bangalore, India.

For more information, visit www.smarsh.com.

About GovLoop

GovLoop's mission is to "connect government to improve government." We aim to inspire public-sector professionals by serving as the knowledge network for government. GovLoop connects more than 300,000 members, fostering cross-government collaboration, solving common problems and advancing government careers. GovLoop is headquartered in Washington, D.C., with a team of dedicated professionals who share a commitment to connect and improve government.

For more information about this report, please reach out to info@govloop.com.

govloop

1152 15th St. NW Suite 800
Washington, DC 20005

P (202) 407-7421 | F (202) 407-7501

www.govloop.com

@GovLoop