WEBINAR BRIEF

Hold the Phone:

How State & Local Governments Manage Mobile Records

smarsh®

TD SYNNEX
Public Sector

The way government workers communicate has evolved with technology and the office culture. Emails are no longer the primary way messages are exchanged; it's now instant and text messaging. What happens in meetings is no longer found only in meeting notes; they're now complete recordings of the virtual meeting itself. The majority of work is no longer completed at the office; work is now done anywhere.

Government organizations know this is happening. But what are the implications?

Watch the full webinar:

WEBINAR

Hold the Phone:

How State & Local Governments Manage Mobile Records

As collaborative technology and apps become more powerful and accessible, governments need to examine how those communications are being captured and archived to ensure they meet their recordkeeping obligations.

The great digital transformation

The start of the digital transformation wasn't the result of sending people home during the early moments of the pandemic. The transformation was already well underway as older workers retired and younger and increasingly tech-savvy employees entered the workforce. This isn't unique to the public sector — we're seeing it in every white-collar industry.

Panelists

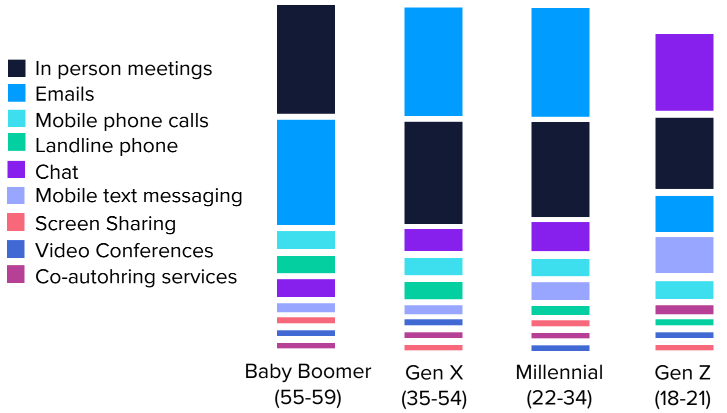
Don MacLean
Cybersecurity Technologist
TD SYNNEX Public Sector

Mark Carlin
Head of the Americas
TeleMessage

Robert Cruz
Vice President for
Information Governance
Smarsh

Pre Pandemic: Digital Transformation

Workers are gravitating toward interactive, multimodal and engaging platforms that have powerful collaborative features — chat, screen share, live annotations and editing — to get work done. While many government agencies are embracing this digital transformation, they need to be aware of their recordkeeping obligations as communications data get larger, richer, and more complex.



“There’s a lot of concern with how to search those records and come up with evidence and respond to things like FOIA requests,” says Don MacLean, Cybersecurity Technologist at TD SYNNEX Public Sector. “Add to that the difficulty of gaining access to many of these platforms. Communications can be considered records, even if they’re on personal devices.”

The benefits of forward-facing policies

At the legislative level, states realize that there are different ways for employees to communicate with one another or with subcontractors. So, while many state FOIA laws don’t specifically mention text, SMS messaging or messaging apps, they are worded so that they should be treated the same as all other forms of public record, according to the Reporters Committee for Freedom of the Press.

Examples of state recordkeeping laws that don’t mention text:

State	Why Texts Can Still Be Considered Public Records
Alabama	There is legal precedent requiring access to emails, which may also apply to texts. See Tenn. Valley Printing Co. v. Health Care Auth. of Lauderdale Cnty., 61 So. 3d 1027 (Ala. 2010)
California	Government-related writings fall under the state’s definition of a public record. See Cal. Gov’t Code § 6252(g) and Cal. Gov’t Code § 6252(e)
Delaware	Text messages and other electronic messages are likely to be considered public records since they fit the definition of a public record under the Delaware Freedom of Information Act.

California	There is legal precedent requiring a third-party service provider to produce the text messages that eventually caused the resignation and conviction of Detroit Mayor Kwame Kilpatrick. See Detroit Free Press, Inc. v. City of Detroit, No. 08-100214-CZ (June 26, 2008)
Iowa	Texts would still be considered public records as they are “records, documents, tape, or other information, stored or preserved in any medium.” See Iowa Code § 22.1(3)

It’s becoming increasingly clear that even if a device is personal, it can be subject to e-discovery or public records request if it was used for government work. If a worker adds business accounts (e.g., email, phone, social media) to their personal devices, the agency must be able to capture and archive those communications.

This is especially important for organizations that have BYOD policies.

“The key is to draft a policy that addresses the technology use trends in your organization while being aware of, in compliance with, or in accord with whatever case law is out there,” says Mark Carlin, Head of the Americas, TeleMessage. “You don’t want to draft a policy that’s going to somehow violate or be at odds with the law.”

Key things to consider

The digital transformation isn’t slowing down, and business-related communications will continue to cross paths with personal messages on both personal and work devices.

Mobile device management or containerization

Mobile device management systems can be installed to give agencies greater visibility and control of what’s being used at the device level.

Containerization technologies allow for a greater separation of work and personal accounts. However, this isn’t foolproof.

Understand policy and open record act trends. All states have different laws. Some may already have clearly worded recordkeeping laws in place that specifically include text messages and digital communications, while others don’t. But that may be changing.

“I think there’s a pretty significant trend of states creating clearer language,” says MacLean. “I don’t see a lot of these states rescinding their laws. I think it’s going to go the other way.”

> ***“My own phone has one that I use for business. “I can’t cut and paste from an email that I get on my business account into another email. That said, it’s still possible to get around it. If I want to get an email onto my personal device, I just forward it to a personal email address, and then I can cut and paste it. These are guardrails — not actual preventative mechanisms.”***
>
> — Don MacLean

Recognize what needs redaction or anonymization

While states trend toward capturing a broader variety of communication channels, agencies still need to be able to redact or anonymize data.

For example, government officials may be collaborating via a Zoom video call to discuss government business. That video is a government record and is subject to discovery. However, if an employee's child happens to walk into frame, that's a different story. While the child's presence doesn't need to be deleted from the video, the child's face should be obscured.

"We see this also just in the instance of police cameras, their body cams," says MacLean. "There are cases where they may film a family situation where someone's privacy is at risk as well. So in addition to being able to store and record and track all of this information and to know what's in it and what's relevant, agencies also have to be aware of the privacy concerns due to the intersection of private and public data."

Recognize how employees work

It's easy to mandate which communication technologies or behaviors are allowed, but executing on those orders isn't. Public agencies need to be able to meet their employees where they collaborate.

"One of my mantras in technology and security is that convenience always wins over everything else, for better or worse," says MacLean. "So you have to accommodate convenience, but at the same time, you can't just throw up your hands and walk away."

"There's no reason not to start with simpler initiatives, With technologies that are able to capture text message content, agencies can start with that on corporate devices. The employee does nothing. The employee can use his mobile phone for texting, and all that texting can be captured all behind the scenes. Start small, and then look at other things that need to be captured on mobile devices."

– Mark Carlin

Next steps

For many agencies, responding to a record request is a time-consuming and manual process. If a system is fundamentally designed for email or records within a Word document, Zoom video meetings or digital communications data from a mobile app can be harder to store or find. This means records managers will be tasked to manually find and retrieve this hard-to-find data.

Having a system in place that can capture and archive rich, multimedia data is crucial. Agencies need to look at what's in place and whether their systems are enabling the kind of response time they need to search and retrieve from this greater volume and variety of data.

"Automation is the key here. Without that, the process will become unwieldy and almost impossible to truly respond in a way that's compliant with the laws. Another part is that some laws have age requirements. In other words, you can delete or archive or get rid of data after a certain period. That cuts down on the volume you're searching through when responding to requests."

– Don MacLean

That's not to say government agencies should build a completely new repository from scratch. Implementation and migrations should be done in manageable chunks.

How Smarsh can help

U.S. public sector organizations are required by state law to capture and store all of their electronic communications records, including email, instant messages, social media and text messages. This has become more complex and time consuming as modern communications have evolved. Failing to do so could lead to fines and legal or reputational risks.

Smarsh simplifies the capture and search of more than 100 channels of communications data, including from text messages and mobile apps. This means organizations can meet recordkeeping obligations, manage risk and reduce the time and cost of responding to public records requests from a single, comprehensive solution.

> *"There's no reason not to start with simpler initiatives," says Carlin. "With technologies that are able to capture text message content, agencies can start with that on corporate devices. The employee does nothing. The employee can use his mobile phone for texting, and all that texting can be captured all behind the scenes. Start small, and then look at other things that need to be captured on mobile devices."*
>
> – Mark Carlin

smarsh®

Smarsh enables companies to transform oversight into foresight by surfacing business-critical signals from more than 100 digital communications channels. Regulated organizations of all sizes rely upon the Smarsh portfolio of cloud-native digital communications capture, retention and oversight solutions to help them identify regulatory and reputational risks within their communications data before those risks become fines or headlines.

Smarsh serves a global client base spanning the top banks in North America, Europe and Asia, along with leading brokerage firms, insurers, and registered investment advisors and U.S. state and local government agencies. To discover more about the future of communications capture, archiving and oversight, visit www.smarsh.com.

Smarsh provides marketing materials for informational purposes only. Smarsh does not provide legal advice or opinions. You must consult your attorney regarding your compliance with applicable laws and regulations.

Webinar Brief - 08/22

☎ 1-866-762-7741 www.smarsh.com @SmarshInc SmarshInc Company/smarsh