Hold the Phone: How State & Local Governments Manage Mobile Records

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 messaging and mobile texts. What happens in meetings are 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.

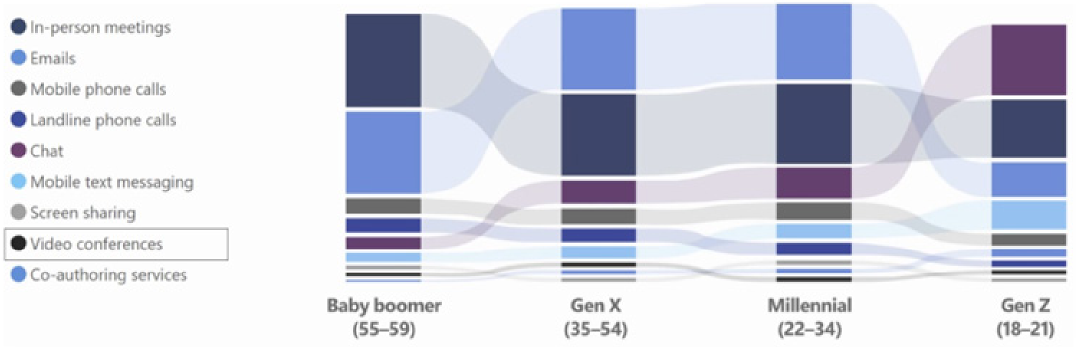
Government organizations know this is happening. But what are the implications?

As collaborative technology and apps become more powerful and accessible, government agencies need to examine how those communications are being captured and archived to ensure they meet their recordkeeping obligations. Failing to do so could lead to fines and legal or reputational risks.

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.

Pre-Pandemic: Digital Transformation Underway



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 gets 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 DLT Solutions. “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.

It’s becoming increasingly clear that even if a device is personal, it can be subject to e-discovery or a 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, as it still relies on users to follow procedures. (For example, a user can simply forward a work-related email with sensitive information to their personal email account.)

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.

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.

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."

What Agencies Can Do

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.

For many agencies, responding to a records 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," says MacLean. "Without that, the process will become unwieldy and almost impossible to truly respond in a way that's compliant with the laws."