BRIEF

Privacy vs. Transparency: **The Tightrope of Modern Government Communications**

marsh®

No industry can hide from technology — and that includes the public sector. The technology revolution continues to thrive with new communication channels, and the data they create, growing exponentially. Pandora's box has been opened and the way government employees communicate has changed for good. Emails have fallen down the communications food chain, which is now ruled by 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 the reality. But what are the implications?

Watch the full webinar:

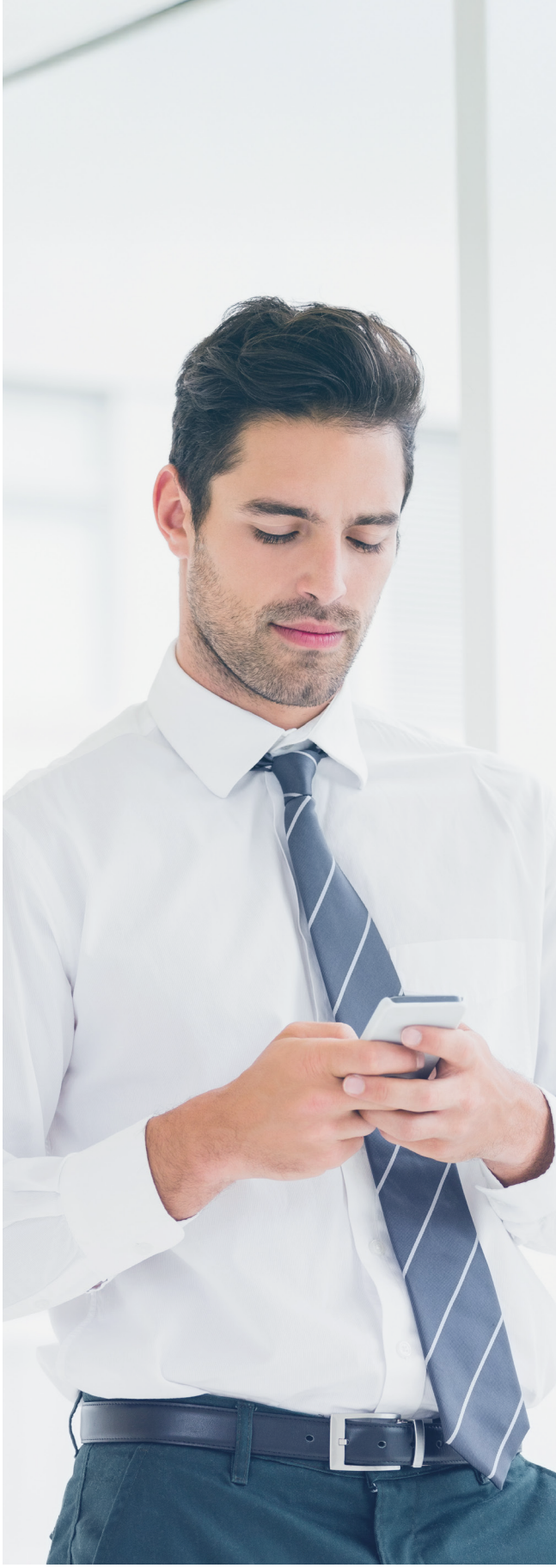
As collaborative technology and apps become more powerful and accessible, governments need to examine how those communications are being captured and archived to ensure they meet their recordkeeping obligations.

The great digital transformation

Some may point to a not-so-fondly remembered time — the 2020 pandemic — as the start of the digital transformation. But that's not true.

The transformation was already well underway as older workers retired and younger and increasingly tech-savvy employees entered the workforce.

This shift in the workforce isn't unique to the public sector. We're seeing this similar movement in every white-collar industry. The world continues to spin, technology advances, and the way we conduct business changes.



Digital transformation or digital minefield?

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.

Communications can be considered records, even if they're on personal devices. Some agencies are concerned with how to search those records and come up with evidence and respond to things like FOIA requests.

Adapting to the Digital Age: 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 requests if it's 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 particularly crucial for organizations with BYOD policies. The goal is to create a policy that aligns with your organization's technology use trends while staying compliant with current laws and case precedents. It's essential to ensure your policy doesn't unintentionally conflict with legal requirements.

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.

It's becoming increasingly clear that even if a device is personal, it can be subject to e-discovery or public records requests if it's 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 particularly crucial for organizations with BYOD policies. The goal is to create a policy that aligns with your organization's technology use trends while staying compliant with current laws and case precedents. It's essential to ensure your policy doesn't unintentionally conflict with legal requirements.

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.”

The urgent need for vigilance: 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.

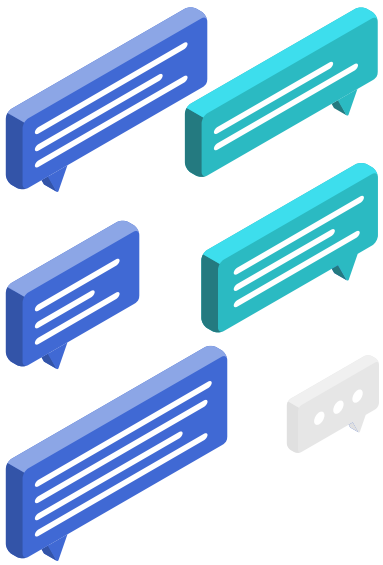
For example, government officials may be collaborating via a Zoom video call to discuss government business. That video is a government record and is subject to discovery. However, if an employee’s child happens to walk into frame, that’s a different story. While the child’s presence doesn’t need to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

This is also evident with police body cameras. There are instances where these cameras may record private family situations, putting someone’s privacy at risk. In addition to storing, recording, and tracking all this information, agencies must be mindful of privacy concerns arising from the overlap between private and public data.

Don’t swim against the current: Recognize how employees work

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

One key principle in technology and security is that convenience always takes precedence, for better or worse. While it’s important to accommodate convenience, you can’t simply give up and walk away from the necessary security measures.



This sentiment highlights a significant challenge faced by government agencies in the modern workplace: the disconnect between policy and practice. Simply implementing a ban on specific communication channels, such as personal messaging apps or social media, does not guarantee adherence to records management obligations.

Employees will often gravitate toward the tools that facilitate their work most effectively, regardless of the official policies in place. This is especially true in environments where collaboration is key, and quick communication is essential to meeting project deadlines. The need for monitoring becomes paramount.

Without ongoing oversight, agencies may have little insight into employee communications, leaving them vulnerable to risks. If a prohibited channel is used for work-related discussions, the absence of a monitoring system means potential breaches in policy go unnoticed. This lack of accountability not only undermines the agency's goals but also exposes it legally if unmonitored communications are called into question.

If any records are unaccounted for, the ramifications can be severe, including violations of transparency laws or loss of public trust. Agencies must not only enforce rules but also create a culture of responsible communication, where employees understand the importance of utilizing approved channels and the implications of failing to meet recordkeeping requirements.

Break free from inefficiency: Improving records management

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.

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.

smarsh®

Smarsh® enables companies to transform oversight into foresight by surfacing business-critical signals from the most in-demand communications channels. Regulated agencies 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 advisers and U.S. state and local government agencies. To discover more about the future of communications capture, archiving and oversight, visit www.smarsh.com

Brief - 03/25

+1 (866) 762-7741 www.smarsh.com @SmarshInc SmarshInc Company/smarsh