Text Message and Social Media Compliance **Best Practices for Law Enforcement Agencies**

Public Records Policies & Best Practices

The popularity of SMS/text messaging and social media has exploded in recent years, both in our personal lives and in the workplace. Because of this, law enforcement agencies need to be aware of certain guidelines and considerations when allowing officers and agency employees to use these popular communication tools. One such consideration is the role text messages and social media play in open records requests, e-discovery and litigation events.

In this guide, we examine how law enforcement agencies can create policies that allow for compliant use of text messaging and social media, and how to retain and archive those communications for a more efficient response to open records requests.

Benefits of Social Media & Text Messaging in Law Enforcement

More than 70% of American adults are using social media platforms to communicate with one another, engage with brands, catch up on news, and share content.[1] Text messaging is often the preferred way for people to communicate with each other. While the popularity of these communications channels is undeniable, the important question is this:

> *How do the unique benefits of social media and text messaging help law enforcement agencies?*

For law enforcement agencies, social media is a useful tool for community engagement. It provides a platform to relay critical information to the public and hear concerns from members of the community. Social media offers a face to the department, which can strengthen the bond between the agency and the community they serve. It's an additional way for officers to quickly engage when they're in the field.

Many law enforcement agencies are becoming aware that the desire to use social media and texting to conduct business is driven in large part by a youthful, tech-savvy workforce. Millennials make up the largest demographic of workers, and the impact this burgeoning generation has on workplace policies is already being felt. Law enforcement agencies recognize the importance of keeping up with communication trends to better collaborate across departments, with other agencies, and most importantly, with the public.

Text Messaging

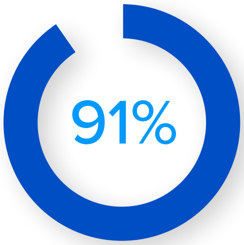
If crucial information needs to be communicated in a timely manner, a text message is often the channel of choice. According to the Pew Research Center, 98% of text messages are read within two minutes — a time savings that can literally mean the difference between life and death in an emergency. Forward-thinking agencies are already expanding dispatch services to include texting.

The police department in Flagstaff, Arizona is implementing a program that will enable its Coconino County residents to text local police rather than calling them. The program is focused on benefiting people who are deaf, hard of hearing, or unable to speak, and is designed to be a safe option for people who are in dangerous situations that may require discretion.[2]

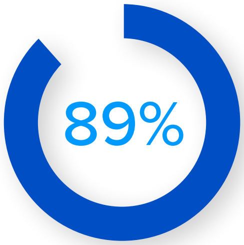
[1] https://www.pewresearch.org/internet/fact-sheet/social-media/
[2] Flagstaff Police dispatchers to expand services and include texting for hearing impaired - https://bit.ly/2YHvBL6

Social Media

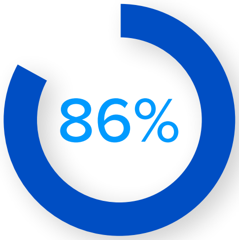
According to a Law Enforcement Use of Social Media Survey,[3] social media platforms are used for:



notifying the public of safety concerns



community outreach and citizen engagement



public relations and reputation management

Meanwhile, social media is a straightforward way to communicate with citizens or groups. It can help spread information rapidly to a wide swath of the community, which can be very useful in the event of public safety hazards or natural disasters. Social media can also reduce the time it takes for first responders to get important information they need, such as emergency coordinates to help someone in danger.

It is important to keep in mind though, that any communication sent or received by government organizations — including law enforcement departments and their employees — is subject to open records requests and must be accessible to the public. Law enforcement agencies should have a plan for collecting and archiving every message, tweet, like or share, as a means of transparency guaranteed by open-records ("sunshine") laws.

[3] 2016 Law Enforcement Use of Social Media Survey - https://urbn.is/2UWfDMc

Should Law Enforcement Allow Social Media and Text Messaging?

Archiving communications

Despite the convenience of social media and text messaging, many law enforcement agencies attempt to prohibit the use of these communication channels because of recordkeeping requirements. This method isn't practical if officers are using social media or texting in a professional capacity. Allowing the use of these communication channels can be done safely with the ability to capture and store those messages in a secure archive.

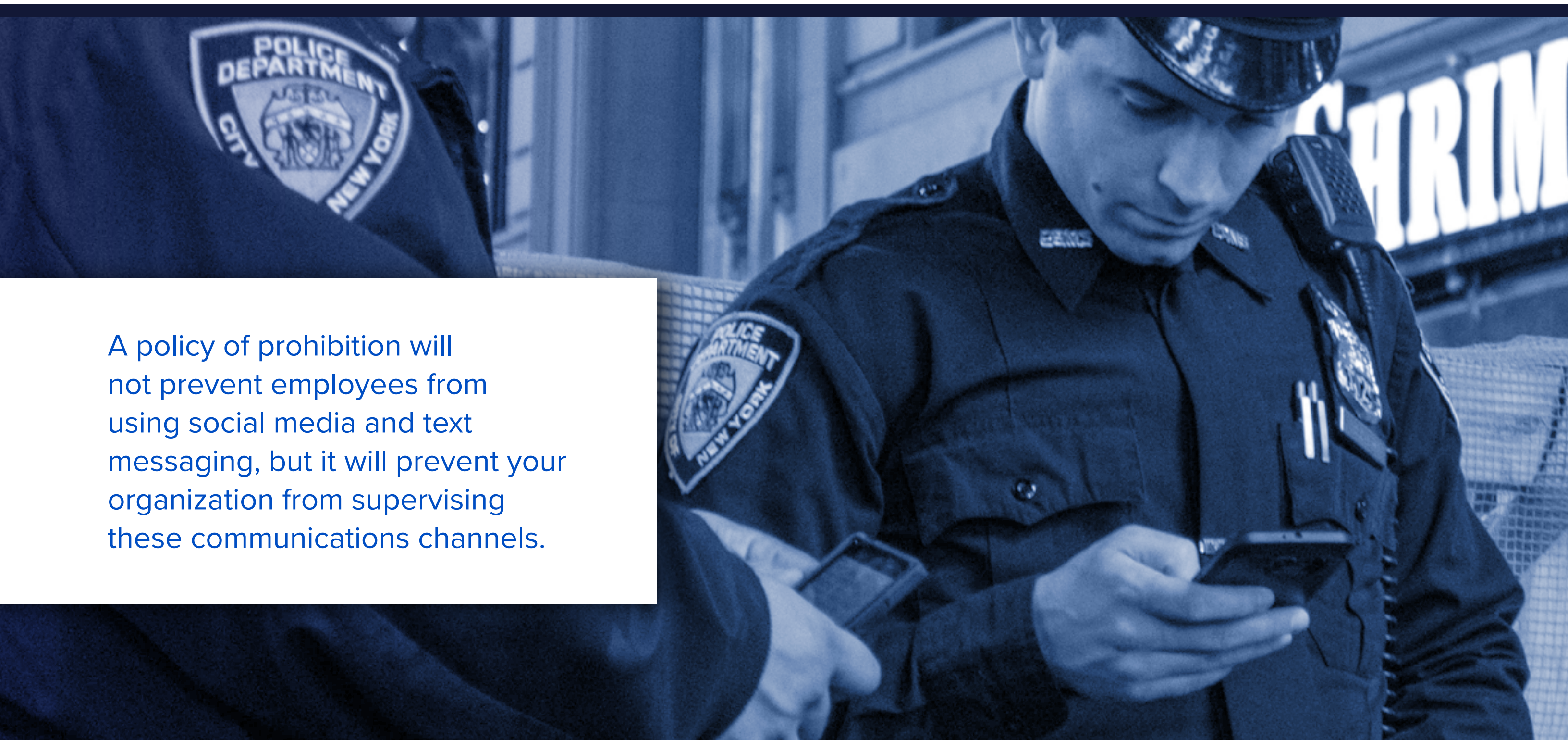
As mentioned before, all communications — including text messages and social media posts and activity — must be considered public records if they contain work-related conversations or context. This is crucial, because that information can include critical details like photos from an emergency scene or discussions between employees regarding incident response. When conversations happen without oversight or archiving, valuable records could be lost or deleted.

Producing communications

To comply with state open-records laws, government organizations must then be able to produce any business-related records requested by the public. These records are also needed for internal investigations, case logs and potential litigation.

When requested, public records must be produced quickly, accurately and in their entirety. But agencies have historically had to perform laborious forensics to acquire them. They must coordinate for officers to turn over their personal phones so text messages can be extracted. The process itself is inconvenient. It can take weeks to accomplish and keeps law enforcement officers from communicating efficiently.

If records cannot be produced comprehensively or within required time limits, the organization may be subject to heavy fines, in addition to a damaged reputation and a lack of trust. The consequences of broken trust between law enforcement agencies and the communities they serve can create challenges for employees when responding to an emergency or trying to build community support.



A policy of prohibition will not prevent employees from using social media and text messaging, but it will prevent your organization from supervising these communications channels.

We Recommend: Allow — With Documented Policies

Whether text messages and social media are prohibited or not, departments should create and implement written policies. A solid policy includes clear rules of text messaging and social media interaction, and how those communications will be retained. These rules will help meet public records requests and permit public safety employees to use mobile devices to communicate.

Written policies should describe:

- Who is permitted to use text messages and social media
- What types of information can be sent using social media and text messages
- An overview of the organizational device ownership scenario, including which carriers can be used
- Which channels and applications will be allowed for devices

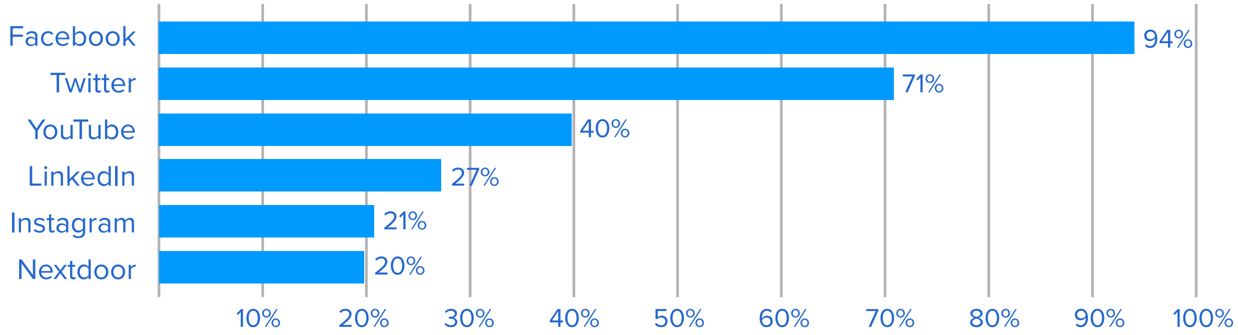
Before finalizing the policy, get feedback from key stakeholder departments who might have a role in determining the do's and don'ts and the consequences of non-compliance with the text message and social media policy. This creates top-down buy-in and makes sure the policies align with organizational needs and guidelines.

Common stakeholder departments may include:

- Human resources
- Legal counsel
- Records retention
- Administration

After the policy is finalized, employees need to be trained on the permitted use of text messaging and social media. Review and update the policy on a regular basis, especially when new technologies are adopted into the agency's communications strategies.

Social media platforms used by law enforcement agencies:[4]



Personal Social Media Accounts and Professional Conduct

An employee's personal social media pages and comments can be seen by the community as an extension of the law enforcement agency. When it comes to personal social media pages, make sure the written policy:

- Provides rules for professional online conduct, including whether employees can identify themselves as members of the agency
- Clearly states if employees are required to provide the agency with access to their personal pages
- Outlines what types of content are off-limits, including certain types of videos, photos, third-party links, or commentary about hot-button topics

[4] Social Media Guidebook for Law Enforcement Agencies - https://urbn.is/2V2wfBU

Communication Archiving Solution for Law Enforcement Agencies

As communications technologies evolve, it is important to be proactive in archiving conversations generated by employees. Proactive archiving, where all relevant communications are automatically captured and stored in a search-ready repository, makes all the difference when responding to an open records request in a timely manner.

The alternative, which requires employees to store and submit their own communications data, is both a tremendous burden on IT and increases risk of missing or deleted information. The best and most efficient way to manage and monitor social media posts and text messages — and ensure compliance with existing laws — is to have a comprehensive capture and retention system in place.

To find a best-fit solution, take these features into consideration:

- **Automated process:** An automated system provides the secure capture of records with a minimal number of people involved to ensure the communications are properly retained and archived. This can also reduce the amount of time it takes to respond to a records request.
- **Supervision:** An archiving solution with built-in supervision capabilities can help law enforcement agencies proactively flag behavior violations like inappropriate language or harassment. It can prevent these situations from escalating and put controls in place to check this type of communication before it starts.
- **Single source of truth:** Rather than performing inconvenient forensics practices like gathering phones, the ability to search for records within one secure database makes the process quicker and reduces the chances of error. It also allows for officers to continue doing their job with the tools they need to stay connected.
- **Robust search function:** Look for search capabilities (by name, keywords or content channel) that will return all possible archived messages across all communications platforms. This allows for easy retrieval of a conversation that may begin in one type of communication and concludes in another. This will also greatly reduce the time spent looking for records to satisfy requests.
- **Growth potential:** Think long term. Rather than investing in multiple standalone solutions for different content types that are limited in scope and may not work together as a unit, invest in a platform that will grow with the agency's needs and as new communication types (such as text messaging and social media) become available.
- **Direct-carrier capture:** If your agency issues mobile devices, direct-carrier capture allows for communications data to be automatically pulled from mobile networks (i.e. AT&T, Verizon, T-Mobile), making ingestion easier, faster and more effective. An archiving provider that has developed partnerships with carriers is ideal.
- **Data integrity and security:** By law, records must be produced in their original context. Find a solution that not only retains social media and text message communications, but keeps them in their original context and has secure controls that prevent records from being altered or tampered with once collected. The solution should have the capability to identify any deletions of the original record, who deleted it, and when. Also, avoid archiving systems that flatten communications into an email-like format, which negates the authenticity of the record.

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. They can also 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, Oregon with nine offices worldwide, including locations in Silicon Valley, New York, London and Bangalore, India. For more information, 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.

☎ US: 1-866-762-7742 | UK: +44 (0) 20 3608 1209 www.smarsh.com @SmarshInc SmarshInc Company/Smarsh