

Retain, search, review and produce government mobile text messages



Employees are now using mobile phones for business communications just as much, if not more than, their desk phones. At the same time, government entities of all types and sizes must make sure they have processes in place to respond quickly and thoroughly to public open records requests (e.g. FOIA, Sunshine Law) for mobile messages.

Many government organizations have already transitioned key business processes to leverage the productivity benefits of text messaging (e.g. responding to citizens and technicians, emergency and crisis management, reaching key stakeholders throughout the organization when an immediate response or

approval is needed) and are now facing the related challenges of staying compliant and meeting record retention and production requirements for this form of electronic communication.

Smarsh's Archiving Platform can help agencies meet these requirements and respond

Potential Benefits

- An enterprise-class, text message archiving solution with AWS Gov Cloud storage options
- Available to agencies purchasing under the NASPO Value Point agreement
- Quick and simple activation: Network-based service, device agnostic with no need to install or manage mobile applications
- Helps meet government compliance and records management requirements where retention and review of text messages is needed
- No change in subscriber behavior needed for message archiving: no mobile app installation
- Authorized users automatically have their messages archived, with retention parameters set by the enterprise
- Helps implement internal agency compliance policies regarding use of mobile communications in the workplace with options for active supervision and review of messages
- Archiving of additional digital message types such as email, IM, web and social media is available from Smarsh

The Archiving Platform™ from Smarsh®



quickly and effectively should they need to produce specific messages to respond to public records requests. It enables government organizations to actively manage, archive, audit, supervise and review business use of text messaging.

Network-based solution

This solution automatically captures text messages and retains them in a “search-ready” state to help meet record retention and production needs. All text messages sent from or terminating to an agency-subscribed mobile phone are temporarily stored by the network and then automatically forwarded to The Archiving Platform from Smarsh, where they are ingested, indexed and retained, enabling on-demand retrieval when needed and pro-active message review capabilities. The solution currently supports AT&T and Verizon corporate mobile phones, with additional US carriers planned for 2H 2017.

No Changes to User Behavior

Gaining user acceptance for any new solution can be a challenge. In fact, recording applications that reside on a device are more likely to be bypassed if they require users to make extra logins that could interrupt calls or disrupt their normal, familiar workflow with additional tasks.

With The Archiving Platform from Smarsh mobile message archiving solution:

- Agency device users send and receive messages in the usual way, using their own mobile phone number and the covered wireless network
- Automated storage, retention rules and policy-driven processes require minimal user intervention
- Message capture, storage and forwarding takes place within the carrier network and helps avoid re-routing and connection time delays that can frustrate users and customers



Archiving Features

- Automatically captures text messages and attachments on provisioned agency-subscribed mobile phones
- Messages are captured and retained even when roaming
- Messages are indexed and stored in a “search-ready” state in the Smarsh platform where they can be quickly and easily produced when needed
- **Lightning-fast search:**
The Smarsh platform supports universal, saved and proximity searches across people, dates, files and message content
- **Advanced Admin & Reporting:**
Use features built for enterprises to manage users, identifiers and profiles, groups, roles and enhanced security
- **User-centric UX and UI design**
- **Also available from Smarsh:**
 - **Effective Policy Engine:**
Purpose-built for automated message classification and integrations with advanced supervision and discovery workflows. The policy engine will route messages to specifically defined queues based on the nature of the potential issue.
 - **Available Add-on Modules:**
Add specialized Supervision and Discovery workflows to extend the capabilities of The Archiving Platform to meet advanced compliance-driven message review requirements and to leverage archived data for legal purposes with extended case management and faceted search functionality.

Helps meet agency compliance requirements

The truth is, you can't always depend upon your personnel to conduct business in a way that fully supports your compliance needs. For example, if an archiving application resides on users' devices, they may either forget to turn the function on, or they may opt to turn it off, possibly violating your agency's compliance policies and applicable records retention requirements.

To implement a program that helps you meet requirements for the capture, storage and timely retrieval of messages, this solution:

- Automatically captures originating and terminating SMS and MMS messages for provisioned users who are on the networks of AT&T and other participating carriers
- Allows you, and not the corporate device user, to maintain control over what is captured
- Sends message files and related metadata to your instance of The Archiving Platform from Smarsh
- Allows you to supervise the content of messages as they are ingested and indexed in the Smarsh platform
- Enables you to centralize archiving of stored text message data to quickly retrieve, select and produce messages when needed
- Complements AT&T's Mobile Call Recording (MCR) solution
- Features flexible storage options including AWS Gov Cloud.

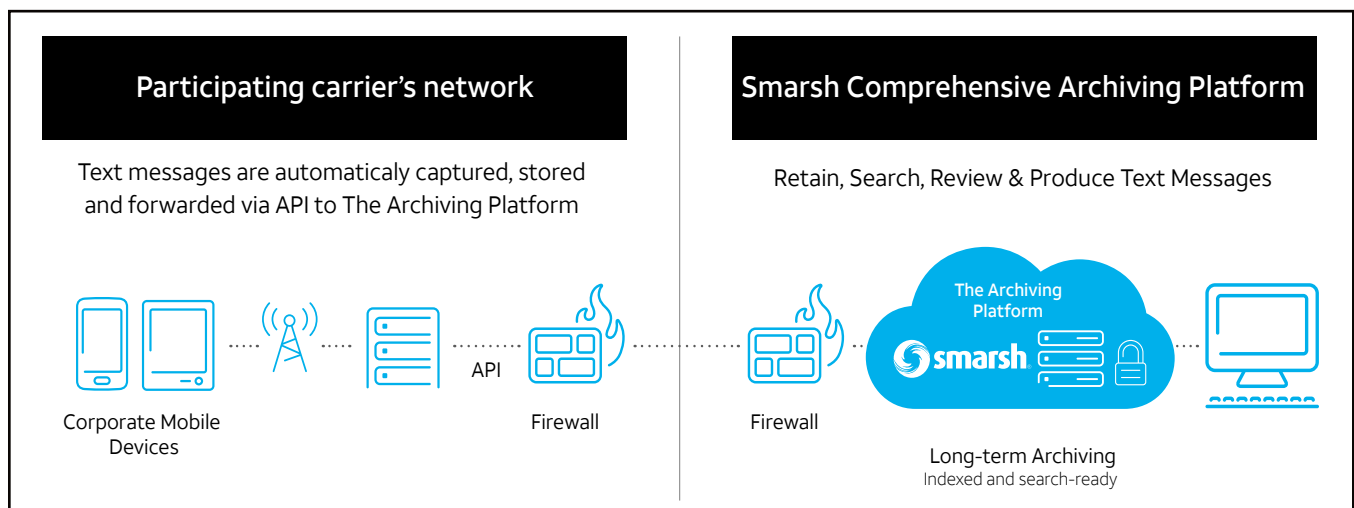
Depend on enterprise-class services

Why rely on a device, application or users for message storage? With AT&T and The Archiving Platform from Smarsh, we can help you extend and expand message archiving services to employees across your enterprise.

From the built-in wireless connections that enable message storage, to the highly secure and reliable technology infrastructure that support them, AT&T can be your single provider for enterprise-class mobile message storage solutions you can depend on.

How it works

The company admin provides consent to use the service and AT&T enables the solution to be applied on the selected AT&T corporate mobile phones. Then, all corporate text messages that originate from or terminate to these phones are automatically stored on the AT&T Mobility network before being forwarded to the Smarsh platform, where they are retained in a "search-ready" state alongside all other archived electronic communications (e.g. email, social media, web, IM, etc.). Similarly, the other participating US carriers enable archiving on their respective networks. The Smarsh archiving platform then aggregates all messages on a single corporate web portal view, enabling a multi-carrier solution.



Pricing

- \$8 per device per month
- No storage limit
- No upfront costs

The Archiving Platform from Smarsh at Work

- **Comply** - Use this solution as part of a program to help your organization comply with agency-specific mobile communications usage and retention policies.
- **Respond** - Satisfy open records requests for text messages in a timely manner by proactively archiving them in a system that enables granular search, rapid retrieval and flexible production options
- **Verify** - Reconstruct and verify appropriate communications between employees and the public they serve.
- **Train** - Use examples of archived messages from seasoned and successful personnel to guide new workers in creating positive interactions that support your public service initiatives and agency compliance policies.
- **Mobilize** - Enable personnel to take full advantage of mobile communications outside the confines of your offices, while still maintaining proper governance and retention of the content they send and receive.
- **Resolve** - Get to the bottom of complaints or flagged potential text messaging compliance violations with a complete record of messages to help resolve issues more quickly and create an audit trail of discussions about disputes and remedial actions taken to address non-compliant usage and content.
- **Supervise** - Enable on-going monitoring and review of agency messaging traffic and evaluation of individual and team performance. Quickly identify and escalate messages that may pose compliance issues for proactive internal review ahead of public open records requests and be prepared.

Important Information

General - The Archiving Platform from Smarsh, as described in this product brief (the "Solution") is available only to eligible customers with a qualified AT&T agreement ("Qualified Agreement"). The Solution is subject to (a) the terms and conditions found at: www.smarsh.com/legal ("Additional Product Terms"), (b) the Qualified Agreement; and (c) applicable Sales Information. For government customers, any Additional Product Terms not allowable under applicable law will not apply, and the Qualified Agreement will control in the event of any material conflict between the Qualified Agreement and the Additional Product Terms. Any service discounts, equipment discounts, and/or other discounts set forth in the Qualified Agreement do not apply to the Solution. The Solution is only available to customer's corporate responsibility users. The Solution may not be available for purchase in all sales channels or in all areas and may not be accessible at all times. Additional hardware, software, service and/or network connections may be required to access the Solution. Availability, accessibility, security, delivery, speed, timeliness, accuracy, and reliability are not guaranteed by AT&T.

Emergency Notification/Personal Health Information - The Solution must not be used as the primary or sole method of storing messages sent over the AT&T mobility network ("AT&T Messages") that contain information that is essential to the protection of life or property. First responders should not rely on the Solution for such situations. Customer may not use the Solution to store Protected Health Information ("PHI").

Requirements - The Solution requires Internet access. Wireless service is subject to transmission limitations and terrain, system, capacity and other limitations. AT&T wireless coverage maps are available at www.wireless.att.com/coverageviewer. Not all device types are supported. Check with your Sales representative for excluded device types. Additional fees, charges, taxes and other restrictions may apply. Offer subject to change.

AT&T Messages - Customer is solely responsible for the content of all AT&T Messages Customer stores using the Solution. AT&T has no responsibility for the accuracy, completeness, safety, reliability, timeliness, innocuousness, legality or applicability of any Content. AT&T Messages may not be successfully downloaded for reasons such as the device not working properly, being switched off or out of range, or the storage medium having insufficient message storage space. AT&T Messages are deemed to have been delivered when they are delivered to the immediate destination, including mobile telephone networks, or any other intermediary server /API that is designated as the point of delivery for the AT&T Message. Delivery on behalf of mobile carriers is not guaranteed. AT&T Messages stored using the Solution will be retained for a period of up to seven (7) years and as long as Customer remains an AT&T customer and a customer of the Solution. The actual retention period (up to 7 years) will be set by Customer, and

Customer may also download and store the AT&T Messages for as long as it wishes. As between AT&T and Customer, all AT&T Messages are Customer's information, to which AT&T makes no claim of ownership. Each Carrier is individually and solely responsible for the handling of its own Content. AT&T disclaims all responsibility and liability with regard to the transmission, storage, access to or use of other Content sent over other carriers' networks.

Other Carriers' Messages - The terms and conditions relating to Customer's use of the Solution with Content sent using other carriers' networks are subject to such other carriers' terms and conditions. AT&T has no access to other carriers' Content that is stored as part of the Solution. Support for Content sent over other carriers' networks is provided solely by the applicable carrier.

Reservations - Rich Communications Services ("RCS") messages between RCS-enabled devices are not archived. AT&T and its suppliers disclaim all service level agreements and/or guarantees with respect to the Solution. The delivery time of Messages to the Service Portal is dependent upon the conditions prevailing at the time of submission, and the actual delivery and/or delivery of Messages within a specific period of time is not guaranteed. AT&T reserves the right to perform work at a remote location or use, in AT&T's sole discretion, employees, contractors or suppliers located outside the United States to perform work in connection with or in support of the Solution. AT&T reserves the right to modify, suspend and/or terminate Customer's use of the Solution for any reason at any time without cause. All fees paid for the Solution are non-refundable.

Customer Responsibilities - Customer is responsible for managing, maintaining and securing information about consents of individual recipients and group distribution lists used in connection with the Solution. Customer is also responsible for ensuring the accuracy of phone numbers entered into the Solution's address book and group distribution lists, and Customer is responsible for removing any unwanted phone numbers from the Solution's address book and group distribution lists. Customer must inform users that messages may be retained regardless of whether they have been deleted by individual Users and the period of time that Customer will retain the messages. Customer may only access the Solution via the interface purchased and by no other means. Customer is solely responsible for safeguarding its access to the Solution. Customer must take all reasonable steps to ensure that Customer's passwords, and username(s) are not disclosed to unauthorized third parties or compromised in any way. Further, Customer is solely responsible for all activities that occur in connection with its account. If Customer becomes aware of any unauthorized use of its password(s) or of its account, Customer must immediately notify AT&T Customer Care at 866-563-4703 or via use of the Support link on the Service Portal.

Data Privacy - Customer Personal Data may be transferred to or accessible by (i) AT&T personnel around the world (ii) third-parties who act on AT&T's or AT&T's supplier's behalf as subcontractors; and (iii) third parties (such as courts, law enforcement or regulatory authorities) where required by law. Customer will only provide or make Customer Personal Data accessible when Customer has the legal authority to do so and for which it has obtained the necessary consents from its end users, and will camouflage or securely encrypt Customer Personal Data in a manner compatible with the service. As used herein, the term Customer Personal Data includes, without limitation, name, phone number, email address, wireless location information or any other information that identifies or could reasonably be used to identify Customer or its Users. Customer is responsible for providing Users with clear notice of AT&T's and Customer's collection and use of Customer Personal Data obtained via the Solution and for obtaining Users' consent to that collection and use. Customer may satisfy its notification requirements as to AT&T by advising Users in writing that AT&T and its suppliers may collect and use Customer Personal Data by providing for User review the relevant links to the Product Brief or other sales information that describes the Solution and to AT&T's Privacy Policy at www.att.com/privacy.

AT&T Wireless Terms and Conditions for Access to Archived Messages - AT&T values its Customers' privacy, and AT&T will not release a Customer's Messages or Content to a third-party without the Customer's consent. Customer authorizes AT&T to make its AT&T Messages available to Smarsh for use solely in connection with the Solution. Customer acknowledges that AT&T will have no further control for the archived AT&T Messages after they

are provided to Smarsh and agrees that AT&T will have no responsibility or liability to Customer with respect to the archived AT&T Messages after they are provided to Smarsh. Customer may access archived AT&T Messages only with the express knowledge and consent of the individuals who sent such messages; if such persons revoke their consent at any time, Customer must immediately cease initiating requests for those individuals' archived AT&T Messages.

Messages, Privacy and SPAM - AT&T is a strong supporter of a SPAM-free communication environment. Any account found to be using the Solution for SPAM may be suspended without notice, and Message volume will be throttled on accounts deemed to be sending SPAM messages. If customers knows of or suspect any violators, please notify AT&T immediately at mobilityabuse@att.com or deliver an SMS message to 7726. Notwithstanding AT&T's anti-SPAM commitment and procedures, it is customer's responsibility to comply with all applicable SPAM and privacy regulations and guidelines in each jurisdiction where messages are transmitted, distributed or received. Customer may not use the Solution to store any communication that would violate any applicable federal, state or local law, court order or regulation, including but not limited to the Telephone Consumer Protection Act, 47 U.S.C. § 227 ("TCPA"), the rules governing the DoNotCall Registry, currently found at www.donotcall.gov, and the CAN-SPAM Act. Use of the Solution is subject to the AT&T Acceptable Use Policy, which can be found at <http://www.att.com/aup>. Customer and its users must cooperate with AT&T and/or governmental authorities in investigations alleging a violation or prohibited use of the Solution.