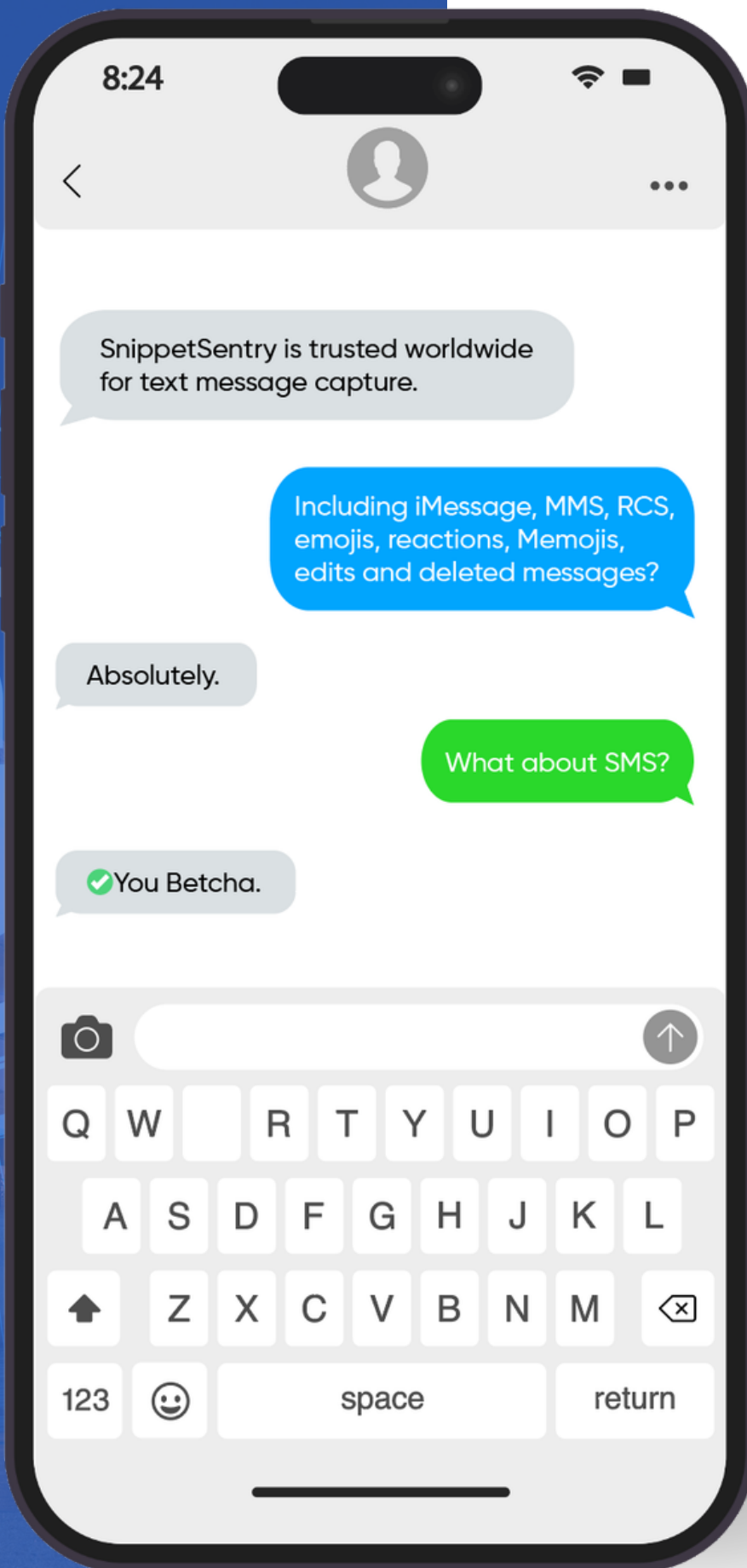




THE MESSAGING BLIND SPOT PUTTING PUBLIC SECTOR TEAMS AT RISK



Modern Messaging Has Outgrown Old Oversight.
Here's How We Fix It.

MESSAGING HAS CHANGED. **OVERSIGHT HASN'T.**

Government teams are under growing pressure to treat everyday communications as public records. With encrypted apps, BYOD policies, and hybrid work environments in the mix, it's getting harder to maintain visibility.

Without centralized message capture and automated oversight, agencies risk:

- Failing FOIA requests
- Legal discovery delays
- Audit violations
- Losing public trust

**80% of mobile
messaging apps used by
agencies are not
formally governed under
public records policy.**

– 2023 StateTech Snapshot

THE COMPLIANCE RISKS LURKING IN YOUR DEVICES



BYOD Blind Spots

When employees use their personal devices for work, those messages can still fall under public records laws.



FOIA & Discovery Failures

No records = no response = noncompliance.



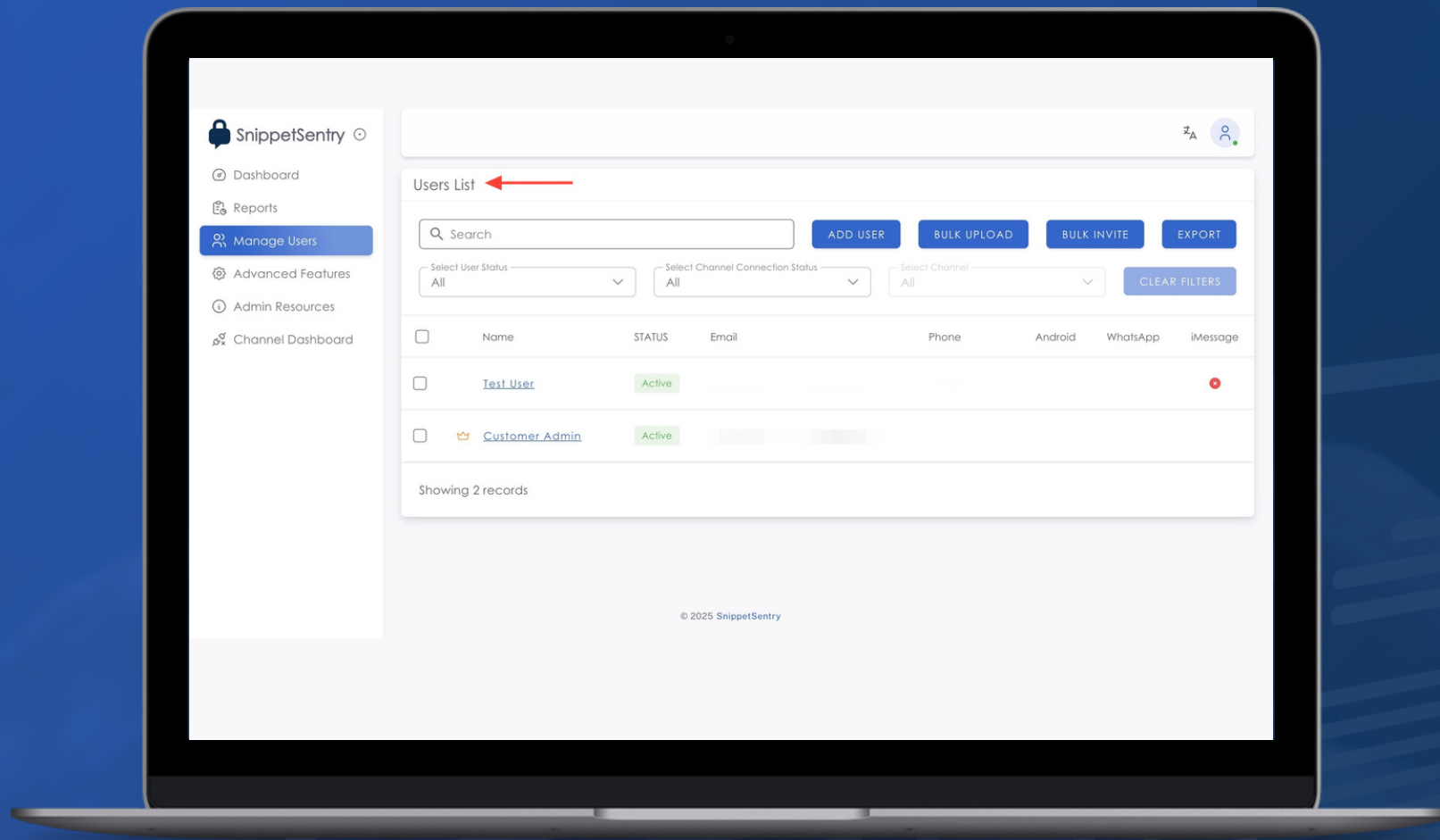
Encrypted Apps = Legal Black Holes

Tools like iMessage and WhatsApp offer no built-in archiving. Agencies are left exposed.



Manual Oversight = Burnout

Legal and IT teams can't manually enforce policy across every device.



INTRODUCING **SNIPPETSENTRY** FOR GOVERNMENT



SnippetSentry is a secure GRC tool built to capture, monitor, and archive mobile communications – natively, with no wrapped applications or new tools.

It works where government teams work (BYOD or agency devices):



WhatsApp



Android



iMessage



Signal



WeCom
coming soon!

"The tools stay the same. Oversight doesn't."
– Jeremiah Smith, CRO, SnippetSentry

BENEFITS at a Glance



**Role Based
Access
Control**



**Real-time
alerts for risky
content**



**Export-ready
archives for
audits, FOIA, or
litigation**



**End-to-end
encrypted, SOC 2
certified, hosted
on U.S. soil**

COMPLIANCE WITHOUT THE GUESSWORK

SnippetSentry aligns with key government frameworks:

REGULATION

SUPPORT PROVIDED

FOIA



Searchable, exportable message archives

FedRAMP



Aligned to NIST SP 800-53

FISMA



Security controls mapped

HIPAA



PHI-safe mobile message capture

Nara
Capstone



Role-based retention and export support



Completed



In-Progress

FEATURES

Most agencies are fully deployed within 5–10 business days.
Includes onboarding, device registration, policy configuration, and training.



US-Based Team & Infrastructure

Headquartered in San Ramon, CA
with a full stack of services,
microservices, and hosting in the US.



Message Capture

Agency-Owned and BYOD ready
across all commonly used
applications.



Connection Health Alerts

Proactive to ensure persistent
connections.



Audit-Ready Archives

Delivered data is filterable,
exportable, immutable



Secure By Design

SOC 2 Type II, ISO 27001, end-to-end
encrypted, geo-fenced hosting



IT'S TIME TO BRING MESSAGING OVERSIGHT INTO THE MODERN ERA.



Agencies are no longer asking if they need mobile message compliance. They are asking how fast they can get it.



Book a Call with Our Team