Why should Governance care? Four everyday scenarios.

SCENARIO	**Consumer E2E Encrypted Messenger** (e.g. iMessage, Signal, WhatsApp, etc)	ARMORTEXT
Hacker attempts to intercept messages / files over the internet	Messages are end-to-end encrypted prior to leaving the device and attempts to intercept messages fail. Even Whatsapp can't see them.	Messages are end-to-end encrypted prior to leaving the device and attempts to intercept messages fail. Even ArmorText can't see them.
Employee loses device containing sensitive internal communications	**No remote message expiration, wipe, etc to address this scenario.**	Admin logs in to ArmorText management console, finds employee and wipes the lost device's ArmorText keys & data only. Employee continues to message securely from their other devices as keys for these devices are distinct from the lost device.
Legal needs to review a previous exchange of messages	**No archives to address this scenario.** **Legal could call in employee and ask to see their phone if they're still employed…**	Reviewer logs in to ArmorText review console, finds employee (if within their scope of review), decrypts messages, and finds the exchange in question, exporting as needed.
Employee or contractor is being let go and messages must be wiped from their devices and must be removed from conversations	**No remote wipe, etc to address this scenario.** **Conversation admins must remove user from each conversation one at a time…**	Admin logs in to ArmorText management console, suspends the user's account so no messages can be sent or received by this user and wipes all of the user's devices of ArmorText keys & data.