# Ghost Proposals

## What are they, what is their impact, and can they achieve their goals?

### What are "ghost” proposals and why should we care?

At least one government has recently proposed that in order to facilitate access to end-to-end encrypted messages, the technology should be modified so that a third-party listener can be silently added to encrypted conversations. They say this can meet law enforcement or national security requirements without weakening the encryption used to encrypt the messages. However, the ghost proposal would introduce systemic security vulnerabilities into confidential communication services and fundamentally change the trust relationship between users and service providers.

### What is a "ghost" proposal and how does it impact security and confidentiality?

“Ghost proposal” refers to a proposal that end-to-end messaging app providers have a way to add a third-party to an encrypted communications exchange without the other parties knowing. This can only be done with the cooperation of the communication service provider. Taking advantage of the group messaging capabilities of many services, a user would be added “silently” to a conversation by suppressing the customary notifications that a new user has been added to the group.

The security of an encrypted communications service relies on effective and transparent encryption key management (ensuring only the intended recipients hold the keys to unscramble the messages). For encryption to deliver the confidentiality a user expects, the whole system must ensure that only the intended recipients can access the necessary keys (which allow encryption and decryption of content).

Proponents of the ghost proposal argue that the inclusion of a secret third-party is preferable to other technical ways of achieving exceptional access because the encryption mechanism would not be touched. However, even though the cryptography used to encrypt the content of the messages may not be affected, it would introduce a security weakness in the messaging app software that is used by every user – namely, compromised encryption key management which could allow unintended users to access the contents of encrypted communications.

Further, from the perspective of trust in a service, if a messaging system promises confidentiality and can’t deliver, it makes no difference what specific element of the services has been changed. The system is not providing the protection its users expect.

## "Ghost" proposals in practice: silent listeners in group chats

In an end-to-end encrypted (E2E) group messaging system, the service provider manages the secure distribution of keys to users. This service is largely hidden from the end-users to enable a simplified user experience, but users are informed when someone is added to a group chat. E2E group messaging relies on this service to ensure that the intended users are added to a group message and no unintended or unknown users are able to decrypt the communications, including the service providers themselves.

Key distribution is complex. For example, an encrypted chat service must also securely update a user's keys when they reinstall the app, or change devices, but want to stay in the same groups.

The ghost proposal alters the key distribution process by secretly distributing keys to people not in the group chat, allowing rogue group members to eavesdrop on the conversation. The ghost proposal would also require service providers to suppress notifications to users that new, unauthorized third parties have access to their communications.

## Problems with the ghost proposal

**It undermines the purpose of E2E encryption:** "Secure" communication systems are comprised of multiple, interlocking parts – of which encryption is an essential piece but not the only important one. Managing encryption keys and the overall trustworthiness of the system are critical elements of a secure E2E communications system. Even if the ghost proposal would not modify the encryption algorithms used by end-to-end messaging apps to encrypt and decrypt the messages, they would introduce a systemic security vulnerability into those services that would adversely impact all users, including business and government users. These proposals undermine key management and trustworthiness of the system, with the result that supposedly confidential communications between the sender and receiver may no longer be confidential, and are less secure.

**It creates vulnerabilities for criminals to exploit:** In order for third parties to be silently added to communications for even a single target, a service provider would need to alter the service for all users to enable this ability. This introduces an intentional vulnerability into the system that if discovered, exploited, or replicated, could be abused by unintended third parties (such as criminals, rogue employees, or hostile governments) to eavesdrop on communications.[1] Since E2E encrypted communications are essential to all aspects of our society including national security, law enforcement, and business, this creates an unacceptable and needless risk.

**It creates new technical and process challenges:** Adding further technical complexity to an already complex process of secure key management risks creating unintentional vulnerabilities that could be exploited by malicious actors. Effectively and securely managing authorized silent access to communications is a daunting and potentially problematic task. Organizations, including governments, have had difficulty making sure sensitive data remains secure and confidential. These capabilities would need to be secured, not only from criminals who wish to exploit them, but from rogue employees and foreign adversaries.

**Criminals will move to another service:** E2E encrypted communications systems exist outside the jurisdiction of any one government. A truly determined criminal would be able to switch away from services known or suspected to be implementing the ghost proposal to avoid getting caught.

**Mission creep - it could be used for many things:** The ghost proposal is not selective by design. It introduces vulnerabilities to the key exchange and notification protocols, and could be used in ways unintended by its proponents (e.g. to monitor members of the press, political parties or others).

[1] "The Athens Affair" is just one example. https://spectrum.ieee.org/telecom/security/the-athens-affair

## Conclusions

The ghost proposal calls for systemic flaws to be designed into mass-market protocols that are used by consumers, businesses and governments. They increase the vulnerability and complexity of the resulting systems – which, in turn, also increases the risk that developers will introduce further flaws by accident. Governments should abandon the ghost proposal as a method of access to encrypted communications – the risk is too great.

## References to learn more:

- Sharon Bradford Franklin, Andi Wilson Thompson. May 2018. *Open Letter to GCHQ on the Threats Posed by the Ghost Proposal.* https://www.lawfareblog.com/open-letter-gchq-threats-posed-ghost-proposal
- Matthew Green. December 2018. *On Ghost Users and Messaging Backdoors* https://blog.cryptographyengineering.com/2018/12/17/on-ghost-users-and-messaging-backdoors/