

Privacy, Security and Accountability: The new imperative for digital platforms

[July 2, 2026](#) / [CIO&Leader](#)



Recent scrutiny of Telegram has reignited debate around the responsibilities of digital platforms and the limits of digital freedom. Much of the discussion has been about Telegram itself, but the larger problem is larger than any one platform.

Communication platforms are becoming a major part everyday life but are also attractive tools for cybercriminals, fraudsters, and organised criminal networks. It's no longer just a conversation about messaging apps. It relates to the response of digital platforms when their services are repeatedly associated with cybercrime, fraud, exploitation and other forms of abuse. The bigger question is how technology providers can protect privacy and build protections against misuse.

Different communication platforms have implemented different approaches to moderation, abuse prevention, and cooperation with law enforcement agencies. Although privacy remains a top user expectation, cybersecurity experts increasingly understand that platforms also need to address misuse by cybercriminals and organized threat actors.

Historically, Telegram has taken a different approach, with a focus on privacy and limited intervention. This philosophy is attractive to many users, but it has also raised some concerns as to whether sufficient safeguards are in place to prevent its misuse by criminal actors.

Between 2013 and 2024, Telegram failed to respond to 2,460 legal requests from governments worldwide. From a cybersecurity perspective, censorship is not the issue. The question is whether digital platforms provide sufficient tools to combat documented abuse and to assist legitimate investigations of serious criminal activity.

Telegram's scale, privacy-focused positioning, and repeated scrutiny from regulators worldwide have made it a prominent example in the ongoing debate around platform accountability. But the issue is no longer only about one platform. It's about the broader responsibility of digital services to stop abuse, while still protecting valid privacy rights.

What "anti-censorship" principles actually meant in practice:

Under Telegram's approach to moderation, concerns have been raised regarding the use of the digital platforms for:

- Child sexual abuse material (CSAM)
- Drug trafficking channels
- Human trafficking networks

- Examination paper leaks and fraud
- Financial scams and cybercrime operations

These examples illustrate a challenge faced by all digital platforms: balancing privacy and freedom of communication with the need to prevent harm and criminal misuse.

The challenge of balancing privacy and security

Privacy and freedom of expression remain essential principles of the internet. However, cybersecurity professionals have long argued that privacy protections must coexist with safeguards that help prevent exploitation, fraud, cybercrime, and abuse.

As communication platforms grow in influence and reach, expectations around transparency, accountability, and user safety naturally increase. The conversation is therefore not just about Telegram, but about the responsibilities of digital platforms in an increasingly connected world.

Cybersecurity risks associated with open platforms

The risks are bigger than content moderation. Cybercriminals are increasingly using digital communication platforms to coordinate illicit activity, share fraudulent content, steal credentials and evade traditional detection mechanisms.

Credential theft remains one of the biggest concerns. eScan’s threat telemetry indicates that over 20% of the identified phishing spam emails are misusing Telegram’s Bot API to exfiltrate credentials. Attackers create fake login pages that send usernames and passwords directly to Telegram bots. Credentials are sent to attacker-controlled chat rooms in seconds, no need for dedicated infrastructure.

This demonstrates how communication platforms can unintentionally become part of the cybercrime ecosystem when sufficient safeguards are not in place.

The responsibility of digital platforms

Digital platforms serving hundreds of millions of users have become critical components of the modern digital ecosystem. With that scale comes responsibility—not only to protect privacy and freedom of communication, but also to reduce opportunities for cybercriminals to exploit the platform for harmful activities.

This shows how communication platforms can unwittingly become part of the cybercrime ecosystem when adequate safeguards are not in place.

Conclusion

In the end, the discussion about Telegram is not really about one platform. It is a sign of the increasing challenge the technology industry faces in striking the balance between responsibility, security and privacy in an increasingly connected world.

The question isn’t whether, from a cybersecurity standpoint, platforms should have robust privacy protections. The question is rather whether those safeguards can be combined with safeguards that help to prevent fraud, exploitation, cybercrime and other types of abuse.

The lesson for cybersecurity professionals is clear: privacy and security are not opposing goals. Sustainable digital ecosystems require strong privacy protections and effective safeguards against misuse.

As governments, regulators and tech companies continue to wrestle with this balance, platform accountability is set to be one of the defining cybersecurity discussions of the next decade. “The future of trusted digital platforms will be about getting the right balance between privacy, security and responsibility.

