Telegram’s Security Sham

justsecurity.org/99869/telegrams-security-sham

September 9, 2024

by Michael Van Landingham and Gavin Wilde

September 9, 2024

The French government’s arrest of Telegram founder Pavel Durov on Aug. 24 and decision to charge him with crimes related to Telegram’s failure to moderate its users’ sharing of illegal content has reignited a debate over secure messaging services, content moderation, and free speech. This debate needs to take user safety—from government surveillance, in particular—as the starting point for judging the merits of platforms that present themselves as offering secure communications. Doing so would highlight the relative safety of platforms like fully encrypted-by-default Signal over cloud-based social media services with direct messaging capabilities like Telegram—a service likely compromised by governments of all stripes, Russia’s foremost.

Is Telegram User Data Safe?

Telegram, founded over a decade ago, is known for its bluster about refusing to comply with lawful subpoenas, and in the past five years it has found favor among a U.S. audience who baselessly believe Signal was developed as a U.S. government plot to undermine foreign governments. Indeed, Telegram has earned a reputation among technology policy watchdogs for failure to implement basic safety controls that would prevent users from

sharing illegal content, such as child sexual abuse material and narcotics trafficking. In early May, Durov publicly criticized Signal for its failure to be a platform “independent of government interference,” implying the app was vulnerable to government surveillance, unlike Telegram.

But there is a subtle yet crucial distinction between Telegram and a fully encrypted messenger like Signal: the former seems unwilling to conduct any content moderation on its platform; the latter is specifically designed to neither host nor access any content on its platform. For users, only one of these approaches reasonably can be deemed secure.

Durov’s routine refusal to cooperate with U.S. or French authorities does not mean Telegram user data is safe from them, or anyone else. Telegram has drawn a skeptical reception from privacy advocates about its claims to have default end-to-end encryption, in which only the sender and recipient of messages may read them. Instead, Telegram is better thought of as a social media platform with messaging capability, which may be encrypted with additional steps the user must take themselves. Otherwise, Telegram channels allow information sharing with large audiences, and most messages are stored in plain, unencrypted text on Telegram servers – to which the company has total access.

Beyond this fundamental level of data insecurity, Telegram as both a platform and organization has demonstrated that it’s much more likely to serve as a viable avenue for, rather than impediment to, intelligence collection. Matt Tait, a former information security specialist for the United Kingdom’s digital espionage agency, GCHQ, has noted the Telegram app leaks metadata that can be used to track users. Going one step further, Telegram has cooperated with Russian authorities’ requests and “may” provide authorities with “selectors” like telephone numbers that can be used to develop further information, according to an unclassified FBI chart. All this while Telegram’s encryption protocol remains a proprietary secret.

For comparison, Signal, and to a lesser extent Meta’s WhatsApp, presents a more categorically secure service offered via a notably more transparent provider. Both apps’ messages are encrypted by default. While WhatsApp messages may be stored less securely in unencrypted cloud backups, Signal’s are stored locally on user devices and the company maintains only minimal metadata on users (timestamps on account creation and most recent connection to the company servers). Signal recently made it easier for users to associate their accounts with user-generated handles rather than phone numbers—significantly reducing the platform’s viability as a source of selectors for third-party interception. And Signal’s encryption protocol is available for all to audit or, as in the case of WhatsApp, to incorporate into their own products.

Ironically, this openness is the most compelling counterpoint to baseless conspiracies involving Signal and western authorities. Signal’s code and protocol are available for all comers to test, poke, and prod. This way, says Signal president Meredith Whittaker, users and researchers are “not just trusting me to not play nice with governments” but are able to validate for themselves that “we literally don’t have the data” to provide them.

Telegram and Russian Security Services

By contrast, the outsized role Telegram plays in Russia creates a potential security threat for any users that Moscow might view as political enemies. Russia maintains an enormous lawful intercept network, known as SORM, for both telephony and internet data. Ten years ago, Russia passed a law requiring all firms to maintain data centers in-country, subjecting them to government requests for data on any individual or firm “under control,” or investigation.

Five years ago, Telegram positioned itself as an anti-surveillance advocate and was to be blocked by the Russian telecommunications regulator. However, the regulator reversed course in 2020, noting Durov’s willingness “to counter terrorism and extremism” – which Moscow defines in increasingly broad terms. This raises questions about Telegram’s safety from the Russian security services’ SORM panopticon, in which “terrorism” and “extremism” are often used to describe legitimate speech and political activity.

In early 2022, Russian Duma member Oleg Matveychev, deputy chair of the legislative body’s committee on technology policy, told Russian media that Telegram both complies with Russian Federal Security Service (FSB) demands for data on “terrorists or anyone under investigation” and installed SORM monitoring devices, essentially enabling unfettered FSB access to their networks “so that it is possible to monitor all dangerous individuals.” Also in 2022, Russian military forces used Telegram to spy on and repress Ukrainians in occupied territory, exploiting its vulnerabilities and Ukrainians’ reliance on the messenger to communicate. The harsh reaction Russian government officials have had to France’s recent arrest of Durov raises further questions as to whether Telegram content is available to Moscow’s security services.

It would be easy to view this condemnation of Telegram and endorsement of Signal with respect to the security of their users’ data with some cynicism, given our backgrounds as U.S. intelligence officers. But neither we nor Signal—a non-profit organization with which we have no relationship—stand to gain anything from correcting the inaccurate image Durov and his supporters seem to promote of Telegram as a safe harbor for free speech. Readers need not take our word for it, however. This image is openly contradicted by Russian government officials’ own statements, as well as Moscow’s own actions that exploit Telegram for surveillance and propaganda.

Users who are genuinely interested in privacy and security should forget “whataboutist” attacks on messaging services (such as those on Signal or WhatsApp). By focusing instead on the company’s track record and transparency, as well as the testimony of security researchers and privacy advocates, it is plain that Telegram’s claims of security are not to be trusted.

IMAGE: In this photo illustration, the Telegram logo is displayed on a number of screens on August 26, 2024 in London, England. (Photo illustration by Leon Neal/Getty Images)

Featured Articles