# FBI Warns iPhone, Android Users—Change WhatsApp, Facebook Messenger, Signal Apps

FBI warns all users to stop texting—but secure messaging apps must also be changed. Here's what you need to know.

By Zak Doffman

Dec 19, 2024 07:15 AM · 11 min. read · View original


Stop texting—but these apps need to change as well.

Anadolu Agency via Getty Images

*Republished on December 11 with proposed new legislation to enforce cybersecurity rules on U.S. networks, this follows proposals to mandate interoperability between the end-to-end encrypted platforms.*

Last week, the FBI warned iPhone and Android users to stop texting and to use an encrypted messaging platform instead. The news made global headlines, with cyber experts urging smartphone users to switch to fully secured platforms—WhatsApp, Signal, Facebook Messenger. But the FBI also has a serious security warning for U.S. citizens using encrypted platforms—those apps, it says, need to change.

While China has denied any involvement in the ongoing cyberattacks on U.S. telco networks, describing this as "a pretext to smear China," government agencies are clear that Salt Typhoon hackers linked to China's Ministry of State Security, have infiltrated multiple networks, putting both metadata and actual content at risk.

ForbesApple's Surprising iPhone Update —Green Bubbles End Next WeekBy Zak Doffman

Encrypting content is certainly the answer, and the FBI's advice to citizens seemed clear-cut, "use a cell phone that automatically receives timely operating system updates, responsibly managed encryption and phishing resistant MFA for email, social media and collaboration tool accounts."

What was missed in almost all the reports covering Salt Typhoon was the FBI's precise warning. "Responsibly managed" encryption is a game-changer. None of the messaging platforms which cyber experts and the media urged SMS/RCS users to switch to are "responsibly managed" under this definition.

suggestions from Forbes and its affiliates.

The FBI has now expanded on its warning last week, telling me that “law enforcement supports strong, responsibly managed encryption. This encryption should be designed to protect people’s privacy and also managed so U.S. tech companies can provide readable content in response to a lawful court order.”

There are just three providers of end-to-end encrypted messaging that matter. Apple, Google and Meta—albeit Signal provides a smaller platform favored by security experts. These are the “U.S. tech companies” the FBI says should change platforms and policy to “provide readable content in response to a lawful court order.”

This doesn’t mean giving the FBI or other agencies a direct line into content, it means Meta, Apple and Google should have the means, the keys to provide content when warranted to do so by a court. Right now they cannot, Police chiefs and other agencies describe this

situation as “going dark” and they want it to change.

The onus for forcing this change will fall to public opinion, to users. FBI Director Christopher Wray warns that “the public should not have to choose between safe data and safe communities. We should be able to have both—and we can have both… Collecting the stuff—the evidence—is getting harder, because so much of that evidence now lives in the digital realm. Terrorists, hackers, child predators, and more are taking advantage of end-to-end encryption to conceal their communications and illegal activities from us.”

This is a dilemma. Apple, Google and Meta all make a virtue of their own lack of access to user content. Apple, by way of example, assures that “end-to-end encrypted data can be decrypted only on your trusted devices where you're signed in to your Apple Account. No one else can access your end-to-end encrypted data—not even Apple—and this data remains secure even in the case of a data breach in the cloud.”

"Unfortunately," Wray said, "this means that even when we have rock-solid legal process—a warrant issued by a judge, based on probable cause—the FBI and our partners often can't obtain digital evidence, which makes it even harder for us to stop the bad guys... the reality is we have an entirely unfettered space that's completely beyond fully lawful access—a place where child predators, terrorists, and spies can conceal their communications and operate with impunity—and we've got to find a way to deal with that problem."

The dilemma is that if Google or Meta or even Apple *does* have the keys, as used to be the case, then the end-to-end encryption enclave falls away. How would users feel if Google could access their currently encrypted content if required/wanted. This is as much about distrust of big tech as trust or otherwise of law enforcement. And, as ever, while the argument runs one way in the U.S. and Europe, the same technical back doors would exist in the Middle East, Africa, China, Russia, South East Asia, countries with a different view on privacy and state monitoring activities.

The FBI has essentially already warned users away from messaging on Google's and Apple's own platforms—full encryption doesn't work cross-platform. That leaves Meta as the world's leading provider of cross-platform, encrypted messaging, with WhatsApp and Facebook Messenger each counting their user bases in the billions.

In response to last week's FBI's warning and its push for "responsibly managed" encryption, Meta told me that "the level best way to protect and secure people's communications is end-to-end encryption. This recent attack makes that point incredibly clear and we will continue to provide this technology to people who rely on WhatsApp." Signal hasn't yet provided a response. What is clear, though, is there is still no appetite across big tech to make any such changes. And they've proven willing to fight to protect encryption even if it means exiting countries or even regions.

But the U.S. is different—and for this tech the U.S. is home. This debate will change if—and only if public attitudes change. The politics are fraught with risk without

a shift in public sentiment, and there is no sign yet of that change. Users want security and privacy. End-to-end encryption has become table stakes for iPhone and Android, it is expanding—as we saw with Facebook Messenger's recent update—not retracting.

Deputy U.S Attorney General Rod Rosenstein first pushed "responsible encryption" in 2017, under the first Trump presidency. "Encryption is a foundational element of data security and authentication," he said. "Essential to the growth and flourishing of the digital economy, and we in law enforcement have no desire to undermine it."

But Rosenstein warned that "the advent of 'warrant-proof' encryption is a serious problem... The law recognizes that legitimate law enforcement needs can outweigh personal privacy concerns. Our society has never had a system where evidence of criminal wrongdoing was totally impervious to detection... But that is the world that technology companies are creating."

In response, EFF said Rosenstein's "'Responsible Encryption' demand is bad and he should feel bad... DOJ has said that they want to have an 'adult conversation' about encryption. This is not it. The DOJ needs to understand that secure end-to-end encryption is a responsible security measure that helps protect people."

The argument against "responsible encryption" is simple. Content is either secure or it's not. "A backdoor for anybody is a backdoor for everybody." If someone else has a key to your content, regardless of the policies protecting its use, your content is at risk. That's why the security community feels so strongly about this—it's seen as black and white, as binary. Seven years later and the debate has not changed. And in the U.S. and Europe and elsewhere, 2025 looks like the year it ignites all over again.

ForbesNew Android Spyware Alert—Delete All These Apps NowBy Zak Doffman

While the FBI has urged citizens to use encrypted messaging, not all encrypted messaging is the same. That's the other twist we have seen this year, the reality

versus the optics when it comes to user security and privacy. Now that twist is making headlines all over again—with just perfect timing.

*The Korea Times* has just reported that "Telegram installation [has] surged in Korea on fears of state censorship under martial law... New installations of global messaging app Telegram have spiked in Korea, data showed Tuesday, as concerns brewed over possible media censorship following the martial law fiasco."

Telegram is the oddity amongst the world's leading "secure" messengers, in that it's not actually as secure as it has always made out. Unlike WhatsApp or Signal or Facebook Messenger—or iMessage and Google Messages within their respective walled gardens, Telegram does not end-to-end encrypt content by default.

But Telegram has always come across as a secure alternative to those other mainstream platforms, which is a neat example of the power of marketing. "The number of new Telegram installations came to 40,576 cases last Tuesday," *The Korea Times* said, citing IGAWorksthe

data from “the day President Yoon Suk Yeol declared martial law, only to have it reversed by the National Assembly within hours. The tally was more than fourfold of 9,016 new installations posted the previous day.”

Telegram’s security vulnerabilities came to a head this year, when its billionaire CEO Pavel Durov was arrested in France and then u-turned on collaboration with the authorities, something Telegram had said it would never do. The platform started to hand over user data and introduce content monitoring. Ironically, it’s only Telegram’s security weaknesses and lack of end-to-end encryption that enables such monitoring.

“Over the last few weeks,” Durov posted to his own channel at the time, “a dedicated team of moderators, leveraging AI, has made Telegram Search much safer. All the problematic content we identified in Search is no longer accessible… To further deter criminals from abusing Telegram Search, we have updated our Terms of Service and Privacy Policy, ensuring they are consistent across the world. We’ve made

it clear that the IP addresses and phone numbers of those who violate our rules can be disclosed to relevant authorities in response to valid legal requests."

This is a far cry from *The Financial Times* description of the platform before Durov's arrest. "Durov has sought to cast the platform as a privacy-orientated alternative to Big Tech platforms, one that is unassailable from government interference. It is, he insists, a censorship-resistant safe haven for citizens living in repressive regimes, such as Belarus, Iran and Hong Kong."

Notwithstanding that change in policy, "Telegram was the most downloaded mobile messenger in [Korea] from Tuesday to Friday last week," according to *The Korea Times,* suggesting its reputation has survived. "Last month, Telegram ranked fourth on the list of newly downloaded mobile messengers here, while Line, a messenger developed by Korean internet portal operator Naver was at the top spot. Many internet users had expressed concerns over the possible shutdown of domestic messaging apps, such as KakaoTalk, or

censorship on such platforms under martial law, saying they have downloaded Telegram as an alternative."

While Telegram is not fully encrypted by default, the other irony is that it's actually now more in line with the FBI's push for "responsibly managed encryption" than its bête noire reputation might suggest. Unlike its blue chip competitors—WhatsApp, iMessage, Signal, Telegram *can* provide data to law enforcement when required, there is no technical impediment that would stop it doing to.

That said, a platform that *The FT* described as "social media giant or the new dark web" is probably not one the FBI or any other law enforcement agency will ever hold up as an example of what good looks like.

ForbesNew Google Play Store Warning—Do Not Update These AppsBy Zak Doffman

On Tuesday, U.S. Senator Ron Wyden, (D-Ore) proposed draft legislation "following the massive breach of the American telecommunications system by Chinese-government hackers," urging the Senate to "pass three bills to finally protect U.S.

communications against foreign hackers and spies."

In response to the proposals, Consumer Reports' Justin Brookman said that "when the FBI and CISA warn consumers that they should use encrypted messaging apps to prevent hackers from accessing the content of their texts because of a massive incursion by Chinese hackers into U.S. telecommunications networks, it is past time to ensure that those networks are secure. Consumer Reports supports the Secure American Communications Act and believes it is a good first step in securing the communications networks that American consumers rely upon every day."

The new legislation would mandate telcos to conduct annual assessments of their networks, documenting the results of those assessments and the detail of any changes that come about as a result. The mandate will also include formal, independent audits, the results of which will be shared with FCC.

Wyden warned that "it was inevitable that foreign hackers would burrow deep into

the American communications system the moment the FCC decided to let phone companies write their own cybersecurity rules. Telecom companies and federal regulators were asleep on the job and as a result, Americans' calls, messages, and phone records have been accessed by foreign spies intent on undermining our national security. Congress needs to step up and pass mandatory security rules to finally secure our telecom system against an infestation of hackers and spies."

Some of the detail of these "binding cybersecurity rules for telecommunications systems" was set out in a press release shared with the media"

- "Implement specific cybersecurity requirements as designed by the FCC, in consultation with the Director of CISA and the Director of National Intelligence, to prevent unauthorized interceptions by any person or entity, including by an advanced persistent threat (APT).
- Conduct annual testing to evaluate whether their systems are susceptible to unauthorized interceptions by any person or entity, including by an advanced persistent threat; take such corrective measures as indicated by

the test; and document the findings and all corrective measures taken in response.
- Contract with an independent auditor to conduct an annual assessment of compliance with FCC cybersecurity rules; and document the audit findings, including areas of noncompliance.
- Submit annually to the FCC:
- the documentation from annual tests and audits.
- a written statement signed by the CEO and CISO (or equivalent) stating that the telecom carrier is in compliance with FCC cybersecurity rules."

It is unsurprising that Wyden has put this together. Earlier this year he also proposed new legislation "requiring the government to adopt secure communications software," which he now says "would have shielded officials' texts and calls despite the [Salt Typhoon] phone network breach."

At that time, Wyden warned that "multiple disastrous hacks of U.S. government systems have been enabled by poor cybersecurity practices by Big Tech companies providing services to the government. Most recently, the Department of Homeland Security Cyber Safety Review Board cited a 'cascade' of

errors by Microsoft, allowing Chinese hackers to breach federal email systems. The Secure and Interoperable Government Collaboration Technology Act would require the government to set new secure, open standards for collaboration software, which would also promote competition and save taxpayer dollars."

The secure communications bill was directed at the platforms providing the secure, end-to-end communications rather than the networks carrying the traffic. As such it's the encryption solution to the open networks problem. Wyden highlighted Zoom, Teams and Slack as examples of platforms that would need to meet the newly proposed "Security and Interoperability Standards."

Just last month, Zoom was criticized for overstating its security. As *Mashable* reported, "the company cut some corners when it came to privacy of its users. Despite Zoom's claims that its video meetings are end-to-end encrypted, it came to light that this was not true, resulting in a class action lawsuit that

Zoom settled for $85 million. In 2021, Zoom also settled with the Federal Trade Commission over misleading its users about the privacy and security of its core product."

Not only would the new proposals ensure solutions are secure, they would also interoperability which would stop government users being committed to one platform or another, with little option to change.

As the PR at the time explained, "while phone calls and email messages allow users to communicate no matter which mobile network or email provider they use, collaboration software is frustratingly walled off. Although video conferencing software like Zoom, Webex, and Microsoft Teams offer similar functionality, users cannot communicate across platforms. Similar barriers exist for chat services like Slack and document editors like Google Docs and Microsoft Office. As a result, agencies often become locked into expensive, insecure walled gardens that result in wasted time and taxpayer dollars as government employees switch constantly

between different collaboration software products."

Parallels here with the push in Europe under DMA to mandate the largest end-to-end encrypted messaging platforms to open access to competitors to enable third-party chats. Meta has led the way in this development and has proven that it's possible to provide end-to-end encrypted messaging without controlling both ends.

That's critical because it undermines the texting issue that caused this furor in the first place. RCS, the SMS update to carrier messaging, is essentially controlled by Google through its Google Messages platform. Apple has famously jumped on board—to an extent—with its latest iOS 18 iPhone firmware. But this doesn't include or participate in the full encryption that Google has wrapped around its own platform.

That is why texting remains insecure, driving the FBI/CISA warning to use other solutions. Put simply, if Apple and Google collaborated on an encryption bridge between their platforms, this wouldn't have happened in this way, and

user messaging communications would not have been exposed.