

TECH

Facebook Plans New Emphasis on Private Communications

Chief Executive Mark Zuckerberg sees Facebook's future focused more on private sharing than public content



Facebook Chief Mark Zuckerberg said the social network will make a major shift to encrypted messaging as it puts new emphasis on privately shared conversations. PHOTO: BERTRAND GUAY/AGENCE FRANCE-PRESSE/GETTY IMAGES

By Jeff Horwitz

Updated March 6, 2019 7:24 p.m. ET

Facebook Inc., which became the world's biggest social network by encouraging people to share photos and messages publicly, said it is now betting on the opposite: that the future of social media lies in private messaging and small-group chats.

In a major shift in strategy, Facebook plans to offer encrypted messaging across all of its major products and allow people to make private conversations ephemeral, Chief Executive Mark Zuckerberg wrote in a blog post. It also will develop products within those messaging services—such as payments and e-commerce—that eventually could allow it to diversify from the ad-supported business model that led to a number of privacy missteps, he said.

In an interview, Mr. Zuckerberg couched the shift as a response to user demand, saying people increasingly prefer to communicate in small groups or one-to-one in the style of its WhatsApp messaging platform, rather than blasting their thoughts to a public audience, as most users do on its Instagram and the company's flagship Facebook platform.

“I don’t view this as replacing the public platform. Facebook and Instagram will continue to get more important,” Mr. Zuckerberg said. But “there is as rich of a platform to develop around the intimate and private communications as there is around the more public one.”

Facebook’s plans could intensify the battle among tech giants to score user loyalty through messaging. Apple Inc. has leaned on its encrypted iMessage service to retain iPhone users over the years, and Alphabet Inc. has pushed to keep pace by beefing up the text-messaging service on its Android operating system, though it isn’t automatically encrypted.

Snap Inc.’s disappearing-messages app Snapchat developed a following particularly among young people in part because it offered the type of intimate communications Mr. Zuckerberg is now embracing.

Equally notable is the model in China, where WeChat exploded in popularity primarily as a messaging app and gradually added other services, including mobile payments, ride hailing and more. The Tencent Holdings Ltd. product—though not encrypted and open to government surveillance—today is one of that country’s dominant technology services.

Mr. Zuckerberg likened one-to-one and small-group communications to conversations in someone’s living room that deserve absolute privacy, as opposed to discussions in the town square. Facebook wouldn’t be able to read messages that are end-to-end encrypted, nor could advertisers mine their contents to target users.

By building an impregnable wall around large swaths of user conversations, Facebook also would in effect be limiting its own responsibility for policing content—an area where it has been investing billions of dollars in recent years in response to widespread abuse and misinformation on the platforms.

Mr. Zuckerberg in a blog post acknowledged that many will be skeptical that Facebook is the right champion for people’s right to control who can peer into their digital lives.

“I understand that many people don’t think Facebook can or would even want to build this kind of privacy-focused platform—because frankly we don’t currently have a strong reputation for building privacy protective services, and we’ve historically focused on tools for more open sharing,” he wrote. “But we’ve repeatedly shown that we can evolve to build the services that people really want, including in private messaging and stories.”

If Facebook's efforts are well-received by users focused on privacy, they likely won't be praised by governments, which would also be blocked from accessing encrypted messages.

Facebook is already defending its existing practices from numerous governments' demands for access.

In Australia and the U.K., Facebook and other tech companies are pushing back on legislation that would make it easier to compel communications platforms to turn over data. In the U.S. last year, it beat back an effort by federal investigators to allow wiretaps of Facebook Messenger's private communications. And in India, WhatsApp is refusing government demands to gain oversight of discussions on that platform.

Mr. Zuckerberg acknowledged "big trade-offs" between safety and privacy, because encrypted communications couldn't readily be monitored for those engaged in political misinformation or illegal acts such as child pornography. He said Facebook could still use "patterns of activity and other signals to identify and stop bad actors."

He said the company would pursue its encryption plans even if it led some countries to block access to Facebook entirely.

In a tweet, former Facebook chief security officer Alex Stamos, now a cybersecurity researcher at Stanford University's Center for International Security and Cooperation, said Mr. Zuckerberg's move is a plus for user privacy.

"Turning a ship that large is difficult," Mr. Stamos wrote. Mr. Zuckerberg, he added, "is coming down pretty hard on putting data outside of Facebook's reach for advertising, content moderation, investigation and government requests."

The changes aren't imminent, Mr. Zuckerberg told the Journal, with the encryption currently standard on WhatsApp not planned to roll out on Facebook's other messaging products until at least next year. The delay will give Facebook time to talk with privacy experts, regulators and law enforcement entities around the world about how best to implement its technology and privacy goals to strike a balance with user safety.

That also would give Facebook time to develop more ways to make money through messaging, which is no small task. The company currently makes 98% of its revenue through advertising. By contrast, WhatsApp— which Facebook bought for \$19 billion in 2014 and is hugely popular around the world—doesn't generate significant revenue.

As part of its encryption push, Facebook also will focus on bringing interoperability to its three central platforms: Facebook, WhatsApp and Instagram. Mr. Zuckerberg said the goal would be to let users interact securely regardless of what platform they used, but not to unify their underlying architecture.

"I think a lot of people thought we were going in the direction of combining all the apps in some way. That's not the plan," he said, saying the goal was to erase the "artificial" boundaries

preventing someone on one Facebook platform from having private conversations with a person on another.

The move is unlikely to placate Facebook critics concerned with the company's dominant position in social media. Ashkan Soltani, an independent researcher and former chief technology officer at the Federal Trade Commission, noted that Mr. Zuckerberg's announcement came amid a sustained focus by members of the Democratic-controlled House of Representatives on privacy and antitrust concerns surrounding the company.

"They're very good at knowing how to leverage privacy for competitive needs," he said of Facebook, arguing that interoperability between Facebook's three platforms would only entrench the company's dominance in messaging and make future antitrust remedies harder to pursue.

Mr. Soltani also speculated that, as with Apple, Facebook's embrace of encryption would let it capitalize on the sheer size of its 2.3 billion user base by steering them toward internal Facebook resources like chatbots and payments.

—*Tripp Mickle contributed to this article.*

Copyright © 2019 Dow Jones & Company, Inc. All Rights Reserved

This copy is for your personal, non-commercial use only. To order presentation-ready copies for distribution to your colleagues, clients or customers visit <https://www.djreprints.com>.