Federal workers say they increasingly distrust platforms like Facebook

Federal workers say platforms they once used to communicate with their coworkers and friends increasingly feel insecure.

As Elon Musk and President Donald Trump have sought to gut and remake the federal government to their liking, federal workers have changed how they communicate with one another and with friends. They have locked down communication channels, migrated to new platforms, and what was once skepticism has grown into deep distrust — not just of their boss's boss's boss, but of the very services they use to communicate with one another, worried that their messages will be leaked to the government.

Multiple federal workers who spoke to *The Verge* on the condition of anonymity said they've moved sensitive conversations from text messages and Facebook Messenger to the encrypted messaging app Signal. Many are downloading and using Signal for the first time to communicate with each other — away from the eyes of Trump and Musk loyalists but also from mainstream tech companies. For some, everything but the most innocuous conversations have been moved. Photos of pets might stay on typical channels; almost everything else is on Signal.

"I have to have two separate conversations with someone over two different platforms," says a person who works for the US Agency for International Development (USAID). "But that's how wary people are of trusting their messages."

Another federal employee told *The Verge* that peers have asked them not to contact them on platforms like Facebook Messenger and to move any conversations about work or the federal government to Signal. Civil servants said they fear that technology companies aligned with the Trump administration, like Meta, could turn over user information to the government. One worker said they feared their data across platforms could be fed into artificial intelligence tools that would then be used to identify people who disagree with the administration.

"I know that's such an extreme take, and the sane part of me is saying that would never happen — but a lot of the stuff we said would never happen, did," they said.

Another person said day-to-day communication in work channels has also gotten more guarded.

"Normally we'll chitchat and maybe make snarky comments about leadership and general complaining stuff," they say. "But for the past three weeks, no more. I'm more circumspect, and I've noticed my colleagues are also more circumspect."

Do you work for the federal government? I'd love to hear from you. Contact me on Signal (@miasato.11) using a non-work device. You can be anonymous.

At the heart of some of the distrust is how technology companies have cozied up to the Trump administration: companies including Meta, Google, and Apple's Tim Cook all donated $1 million to

Trump's inauguration fund. For months, Mark Zuckerberg has laid it on thick in an attempt to curry favor with the administration, flattering Trump publicly and preaching the right-wing gospel on podcasts. One worker also pointed to a recent change made by Google to its calendar of holidays that removed celebrations like Pride Month and Black History Month. (A Google spokesperson told *The Verge* the calendar was switched to display only default entries for public holidays and national observances.)

Privacy experts have long raised concerns about how data held by technology companies could be used against users on the platform. In 2022, in response to a police search warrant, Meta turned over unencrypted chat logs in which two women discussed abortion pills in a state in which abortion access was restricted.

The Verge asked Meta if the company would hand over user data requested without a court order by Musk's pseudo-agency, "The Department of Government Efficiency," or DOGE. Meta spokesperson Thomas Richards said the company's policies had not changed and noted that the "vast majority" of personal messages on Messenger are end-to-end encrypted.

Meta says it follows "applicable law and [its] terms of service" when the company receives government requests for data, and publishes top-level reports on requests it receives. From January to June 2024, for example, Meta reported it received more than 14,000 requests via subpoena in the US, and some amount of data was produced in 85 percent of cases. Data requests to companies like Meta are governed by the Fourth Amendment as well as the Electronic Communications Privacy Act (ECPA), including the Stored Communications Act (SCA), says Andrew Crocker, surveillance litigation director at the Electronic Frontier Foundation.

"To my knowledge DOGE itself does not have access to any of these types of legal requests — it would have to have the assistance of a law enforcement agency like the FBI," Crocker told *The Verge* in an email.

Privacy advocates have pointed to ways law enforcement have tried to get around having a court order, like Immigration and Customs Enforcement using administrative subpoenas that aren't signed off by a judge to attempt to obtain user data from tech companies. In fact, Twitter (pre-Musk) fought a request by the Department of Homeland Security in 2017 that attempted to unmask an anonymous "alt-gov" account that was critical of policies during the first Trump administration.

"When you have companies that are functioning as large data dragnets, they could be an incredibly rich target for agencies trying to investigate or retaliate against federal employees," said Darío Maestro, senior legal fellow at the Surveillance Technology Oversight Project. "Law enforcement already has an alarming number of ways to seize digital communications, whether through subpoenas, court orders under the Electronic Communications Privacy Act, national security letters, or warrants, often with little transparency and no notification to those affected."

Both Crocker and Maestro stressed the importance of strong privacy and security measures like default end-to-end encryption.

On forums like r/fednews, users share security tips and warnings about how workers' activities could be monitored. The Signal app offers end-to-end encrypted messages, meaning the company doesn't

retain or have access to messages. But that means a user's security settings on their device are all the more important: users can set messages to disappear after a set amount of time and set up a username rather than connect with other people using a phone number.

Even on Signal, there's heightened vigilance. Some federal employees have taken extra steps to shield their identities, like changing their display names to be anonymous, fearing someone could screenshot their messages. Signal did not immediately respond to a request for comment about whether it has seen an increase in new users over the past several weeks. But according to data from Pew Research Center, as of November the federal government employed over 3 million people, or 1.87 percent of the entire US workforce.