Keep your texts private in Trump's America (and everywhere else, too)

**1.2k**

SHARES

Share on Facebook Share on Twitter

WHAT'S THIS?



*IMAGE: BOB AL-GREENE/MASHABLE*

BY DAMON BERES AND LOUISE MATSAKIS4 HOURS AGO

So, here we are: With a new president come new [concerns](http://mashable.com/2016/11/10/twitter-worried-surveillance-state-under-trump/) over surveillance powers that could so forcefully bite us in the ass.

The public has good reason to believe that President Donald Trump would love to [expand](https://www.bloomberg.com/news/articles/2016-11-29/fbi-and-nsa-poised-to-gain-new-surveillance-powers-under-trump) data-collection programs in his administration. He's said, [repeatedly](http://www.cnn.com/2016/06/15/politics/donald-trump-muslims-mosque-surveillance/), that he'd like to surveil mosques. Rep. Mike Pompeo—Trump's pick for CIA director who's likely to be confirmed in the next few days—has also [advocated](http://www.theatlantic.com/technology/archive/2016/11/trumps-cia-director-wants-to-return-to-a-pre-snowden-world/508136/) for expanded spy efforts. All signs point to lots of little electronic eyeballs, watching us always.

**SEE ALSO:**[**This is President Trump's first tweet as @POTUS**](http://mashable.com/2017/01/20/president-trump-first-tweet-/)

To be fair, Trump didn't build this machine. It was President Barack Obama who extended the Patriot Act during his tenure, and [defended](http://www.huffingtonpost.com/2013/06/17/obama-nsa-surveillance_n_3455771.html) the National Security Agency's mass surveillance programs after Edward Snowden brought them to light.

Those powers were eventually limited by [reforms](https://www.cnet.com/news/senate-approves-sweeping-reforms-to-nsa-phone-surveillance/) in 2015. But with Trump's administration now in control, things can change. As *Foreign Policy*[pointed out](http://foreignpolicy.com/2017/01/06/donald-trump-has-the-keys-to-the-most-invasive-surveillance-state-in-history-nsa-cia/) earlier this month, "Americans have been warned for decades about the potential consequences of the U.S. surveillance state—the largest, most powerful, and most intrusive in the world—falling into a would-be tyrant’s hands."

Surveillance is a complicated, sticky issue, and to maintain complete privacy while communicating online would essentially require a lifestyle change for many of us, what with our sprawling social networks and all. That said, it's relatively easy to keep your smartphone conversations secret. That's a great first step.

Herewith, some tools to help you keep your messages between friends.

**Lock it down**

This is simple: If you want to reduce the overall likelihood that anyone could pry into your communications, use a secure messaging app.

After Trump's election, there was a [surge](http://variety.com/2016/digital/news/trump-election-encrypted-messaging-signal-app-download-1201916353/) in downloads for [Signal](https://itunes.apple.com/us/app/signal-private-messenger/id874139669?mt=8" \t "_blank), a private messenger that works on smartphones. Many security experts agree that it's one of the safest platforms you can use. It’s user-friendly and was designed to prioritize privacy.

The code that Signal runs on is completely open source, meaning that anyone can analyze it to make sure it works properly. The company that created the app, [Open Whisper Systems,](https://whispersystems.org/" \t "_blank) is a nonprofit, so it has no incentive to store data for advertisers. In fact, Signal’s [privacy policy](https://whispersystems.org/signal/privacy/" \t "_blank) states that it doesn’t store any metadata at all.



Beyond text messaging, Signal also includes security features for phone calls. It will display code words — like "waffle sandalwood," pictured here — on each person's device that they can use to confirm one another's identity.

*IMAGE: LILI SAMS/MASHABLE*

Signal, like many messaging apps today, uses an end-to-end encryption system. In layman's terms, the message you send is scrambled, and it can only be unscrambled using a special "key" on the recipient's device. Whatever you say can't be intercepted by a middle man, and your words aren't stored on some server that anyone could access via a third device.

"Good encryption relies heavily on good implementation, and that comes down to how much you trust the developers maintaining the project," said Jonathan Zdziarski, a cybersecurity and forensics exper*. "*Most people trust [the developers] to have done a good job in designing Signal, and that’s been proven by a number of people who have analyzed the software, including myself."

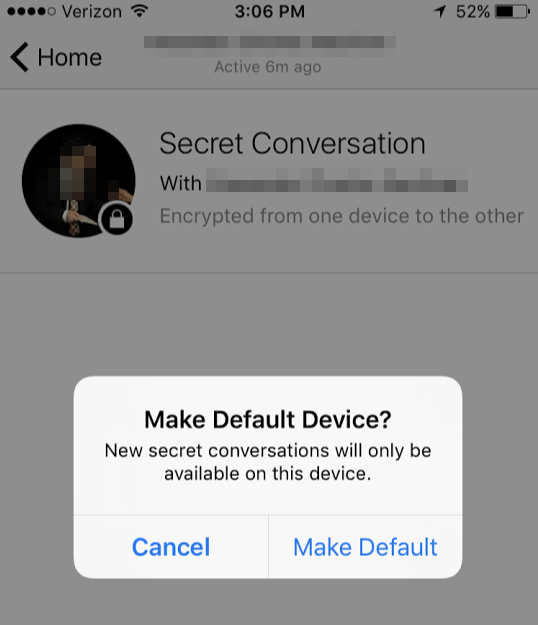
"Is there room for other solutions? Sure, but I have yet to see one as proven and accepted in the infosec community as Signal," he added.

About those other solutions: They're not always great.

**Not all encryption is created equal**

Consider Facebook's Messenger app for a moment. It recently enabled [end-to-end encryption](http://mashable.com/2016/10/05/facebook-messenger-encryption/), which would be great were it not so wonky. Most people like the app because it allows their Facebook messages to be accessed from any device—their work computer, tablet and smartphone, all at once. But messages with end-to-end encryption can't (and don't) work that way: They're sent from *one*device to another device.

To actually send a secure message to your friends on Messenger, you have to start an entirely new thread, tap "Secret" in the top-right corner, and go from there. Otherwise, the routine messages you sent via Messenger don't make use of the end-to-end encryption feature—which means they can be accessed on any device where your Facebook profile is open.



Moreover, if you do take the proper steps and send an encrypted message to your friend, they'll end up with a sketchy notification on their phone, masking your identity and the message's contents: