

Tech tools gain traction amid Trump war on leaks

February 19 2017, by Rob Lever



Graffiti urging people to use Signal, a highly-encrypted messaging app, is spray-painted on a wall during a protest in Berkeley, California

As President Donald Trump warns of a crackdown on US government leaks to media, interest is growing in technology tools that allow sources to share information anonymously.

One such tool called SecureDrop, being used by at least 30 US and

global media organizations, offers a way for sources to anonymously communicate via encrypted servers.

"We've seen an explosion of interest in SecureDrop in the past two months," said Trevor Timm, executive director of the Freedom of the Press Foundation, which created the tool.

Timm said "dozens" of news organizations had expressed interest in using the tool which enables sharing without leaving digital traces.

"Ever since the election there seems to be an urgency within these organizations to set up a more secure way to get information from whistleblowers," he told AFP.

While news leaks have come from a variety of sources, Trump, who took office on January 20, has denounced the release of classified information by officials as "criminal" and vowed to punish leakers.

Timm argued however that the news leaks have been important in holding elected officials accountable and helping the truth emerge.

He said the resignation of [national security](#) adviser Michael Flynn, caught lying about his contacts with Russia, was an important example.

"Not only are leaks allowing the public to put pressure on the government to pull back awful policies, but it's even informing other people within the Trump administration," Timm said in a blog post for the Columbia Journalism Review.

Though the methods for leaks are not always known, some news organizations have acknowledged using SecureDrop, including the Associated Press and First Look Media's investigative site The Intercept.

SecureDrop "is the system easiest to use for newsrooms to facilitate communication that allows a back-and-forth exchange while allowing the source to remain completely anonymous," said Intercept editor-in-chief Betsy Reed.

The system "has become an increasingly useful source of genuinely newsworthy documents for us," Reed noted.

"In the current political environment there can be tremendous risks to cooperating with a journalist and becoming a whistleblower, and it makes sense to offer this as protection."

Reed said she expects the media to rely more on these kinds of sources, with the Trump administration seeking to control the flow of information.

"We're going to have feistier independent journalism that depends on cultivating these kinds of sources," she said.

"Whistleblower journalism will have its heyday, and access journalism is on the decline."

Secure mobile apps

Meanwhile some government officials, fearful of monitoring, have taken to using encrypted mobile applications to share information.

Some newsrooms use a secure chat app called Signal. Another application called Confide, which takes a cue from Snapchat by allowing people to send messages that disappear after being read, also is gaining popularity.

The app offers "the digital equivalent of a face-to-face conversation,"

according to Confide co-founder Jon Brod.

"End-to-end encryption ensures that only the intended recipient can read the message, but ephemerality adds another layer of protection ensuring that no copies reside on any servers or devices."

Founded in 2014, Confide has seen downloads and usage spike during times of well-publicized hacks or leaks.

"Our growth has accelerated significantly since the US election and we have seen a recent surge in our business—the number of new users joining Confide this week is more than seven times higher than last week's," Brod told AFP.

Legal questions

But the use of private channels by officials raises a host of questions, such as those that surfaced over Democratic presidential candidate Hillary Clinton's private email server.

"Conducting official White House business in this way almost certainly violates the Presidential Records Act, which requires preservation of any correspondence or records" of top officials, says a Lawfare blog post by Brookings Institution fellow Susan Hennessey, with Harvard law student Helen Klein Murillo.

Analysts point out that leaking classified information may be illegal, but the degree of enforcement has varied over the years with leakers, and even journalists, facing potential prosecution under the Espionage Act.

Even without these specific tools, news organizations have gotten major stories from leaks provided through systems such as WikiLeaks and documents obtained by former national security contractor Edward

Snowden.

Hennessey and Murillo note that the Trump administration "might have a range of criminal statutes and enforceable legal obligations to use (or threaten to use) to stem the tide of leaks."

But they added that "investigations are opened only when the leaked information is accurate—that is, the mere fact of an investigation is an indirect confirmation of the accuracy of the leak."

© 2017 AFP

Citation: Tech tools gain traction amid Trump war on leaks (2017, February 19) retrieved 19 April 2024 from <https://phys.org/news/2017-02-tech-tools-gain-traction-trump.html>

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.