Bloomberg

Bitmessage's NSA-Proof E-Mail

By Max Raskin – June 27th, 2013

Revelations about the National Security Agency's surveillance program of the e-mails and phone records of Americans have been a boon to makers of commercial encryption programs such as Hushmail and Silent Circle. Yet unless customers bother to read these programs' service agreements, they may not realize these companies—just like tech giants Google (GOOG) and Yahoo! (YHOO)—honor requests for customer data made by governments and courts in cases involving potential security threats.

That's one reason a new open-source encryption standard called Bitmessage, which is out of the NSA's reach and devilishly difficult to crack, is seeing a surge in users. New York-based developer Jonathan Warren says he had the NSA and its spying techniques very much in mind when creating the software. "If I wasn't reasonably sure they were tracking our metadata, I wouldn't have done it," says the 28-year-old, who worked on Bitmessage in his spare time while employed at an educational company he declined to identify.

Bitmessage isn't owned by a corporation, nor does it rely on a centralized server that can be accessed by the government. Instead, the encryption software uses peer-to-peer technology that links computers into what is known as a distributed network. To retrieve a copy of an e-mail sent using Bitmessage, the government would have to gain access to an individual's computer. "Right now, if the Iranian government wants to block Twitter or Gmail, they can. It would be much more difficult to block access to the Bitmessage network," says Adam Melton, a developer who collaborated with Warren.

Warren drew inspiration from Bitcoin, the open-source protocol that established a virtual currency. Downloads of Bitmessage, which was introduced in November 2012, have more than quintupled since news broke in early June about NSA snooping, Warren says. Before that, most of the people using the software were in China; now more than 80 percent of downloads come from the U.S.

Unlike competing products, Bitmessage also shields the identity of the parties in any online communication. Those who download the free software can create alternate e-mail addresses that are 36-character-long strings of letters and numbers. For ease of use, the new addresses can be stored and shared as a QR code, the pixelated squares that can be scanned with a smartphone. "It's the most secure messaging system that I've ever seen," says Johannes Ullrich, chief research officer of the SANS Institute, a Bethesda (Md.)-based organization that certifies computer security specialists.

While Bitmessage's creator says he was motivated by politics rather than profit—Warren says his political inclinations are "libertarian-ish"—experts say the software has commercial potential. "Now that we understand how intrusive the government is being, it will be more important for

the business sector to secure data. Not only medical records but lawyer-client communications," says Jim Harper, director of information policy studies at the Cato Institute, a Washington-based research group dedicated to libertarian principles. "I don't know that a lawyer today will feel he's meeting his ethical obligations if he talks to his client on the phone."

Jarad Carleton, a San Francisco-based principal consultant at Frost & Sullivan, thinks investment bank mergers-and-acquisition teams could put software such as Bitmessage to good use. "Economic espionage has been going on for centuries," he says. "There are executives here in Silicon Valley that refuse to use encryption technologies because they feel it's too hard. They would definitely benefit from something easy to use."

Ullrich, of the SANS Institute, believes that Bitmessage will not come into broader use until it is integrated with popular e-mail clients, such as Microsoft (MSFT) Outlook or Google's Gmail, the way the leading paid encryption services are. Cato's Harper sees another obstacle to adoption: Americans in general are not very exercised about privacy issues. In a new poll, 56 percent said they considered the NSA's accessing of phone records "acceptable." Says Harper: "The question is whether people care enough to use these things."

The bottom line: Downloads of a free encryption program are up fivefold since early June, when news of NSA spying surfaced.