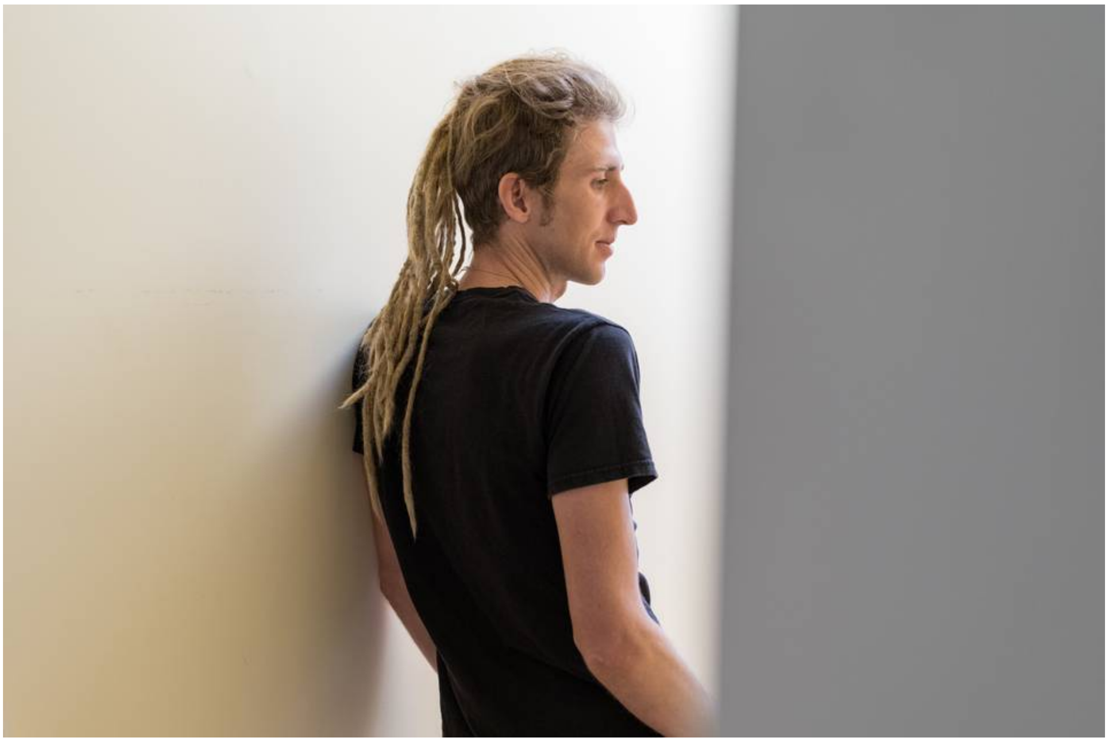
Moxie Marlinspike: The Coder Who Encrypted Your Texts

By Danny Yadron



ENLARGE

Moxie Marlinspike says he sees an opening, following Edward Snowden's revelations, to simplify encryption so more people use it. Photo: Jason Henry for The Wall Street Journal

July 9, 2015 7:57 p.m. ET

SAN FRANCISCO—In the past decade, Moxie Marlinspike has squatted on an abandoned island, toured the U.S. by hopping trains, he says, and earned the enmity of government officials for writing software.

Mr. Marlinspike created an encryption program that scrambles messages until they reach the intended reader. It's so simple that Facebook Inc.'s WhatsApp made it a standard feature for many of the app's 800 million users.

The software is effective enough to alarm governments. Earlier this year, shortly after WhatsApp adopted it, British Prime Minister David Cameron called protected-messaging apps a "safe space" for terrorists. The following week, President Barack Obama called them "a problem."

That makes the lanky, dreadlocked and intensely private coder a central figure in an escalating debate about government and commercial surveillance. In a research paper released Tuesday, 15 prominent technologists citec three programs relying on Mr. Marlinspike's code as options for shielding communications.

His encrypted texting and calling app, Signal, has come up in White House meetings, says an attendee. Speaking via video link last year as part of a panel on surveillance, former National Security Agency contractor Edward Snowden, who leaked troves of U.S. spying secrets, urged listeners to use "anything" that Mr. Marlinspike releases.

Related

That endorsement was "a little bit terrifying," Mr. Marlinspike says. But he says he sees an opening, following Mr.

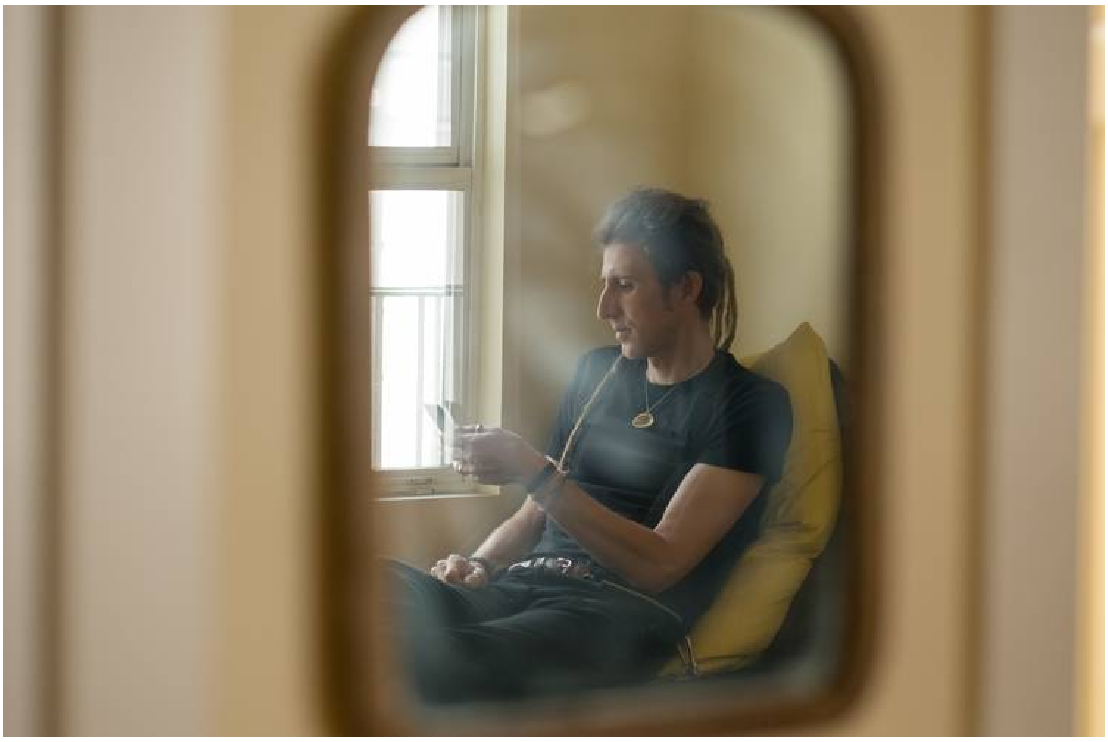
Snowden's revelations, to demystify, and simplify, encryption, so more people use it. He finds most privacy software too complicated for most users.

The former teenage hacker studies popular apps like Snapchat and Facebook Messenger, trying to understand their mass appeal. He says he wants to build simple, "frictionless" apps, adopting a Silicon Valley buzzword for "easy to use."

"I really started thinking about, 'How do I be more in touch with reality?' " he says.

Those who know him say he has both the will and the technical chops to popularize complex technology.

A few years ago, Matthew Green, a cryptographer and professor at Johns Hopkins University, unleashed his students on Mr. Marlinspike's code. To Prof. Green's surprise, they didn't find any errors. He compared the experience to working with a home contractor who made "every single corner perfectly squared."



ENLARGE

Coder Moxie Marlinspike and a government official missed meeting one another at a San Francisco burrito joint because the visitor assumed the dreadlocked Mr. Marlinspike couldn't be the person he was there to see. Photo: Jason Henry for The Wall Street Journal

During chats about surveillance and security, Mr. Marlinspike also won over Morgan Marquis-Boire, a researcher who has worked on security for Google Inc. In a fellowship recommendation for Mr. Marlinspike, Mr. Marquis-Boire wrote, "There are very few people who write privacy tools that I trust, and Moxie is one of them."

Mr. Marlinspike says it is more important that users trust his software than trust him. "It's easier to trust that I haven't made mistakes," he says.

Even by the standards of privacy activists, Mr. Marlinspike is unusually secretive about himself. He won't give his age, except to say he is "in his 30s." In an interview, he wouldn't say whether Moxie Marlinspike was his birth name. In an 2011 online interview with the website Slashdot, however, he wrote, "the name my parents put on my birth certificate is 'Matthew.' " Friends and former associates say they know him only as Moxie.

Consumer encryption tools like Mr. Marlinspike's have been around since the early 1990s, but most are so cumbersome that few people use them. A popular email-encryption program, PGP, or Pretty Good Privacy, requires users to swap a series of thousands of random letters and numbers with anyone they wish to contact. Sending a message requires several clicks, a password, and sometimes, copying and pasting.

A young Mr. Marlinspike once thought users would eventually adopt such tools. “That hasn’t really worked out,” he says now.

Phil Zimmermann, who invented PGP, says he rarely uses it because “it doesn’t seem to work well on the current version of MacIntosh.”

Such headaches have limited the use of encryption to a level law enforcement has mostly learned to live with. Big technology companies like Google, Microsoft Corp. and Yahoo Inc. usually maintain access to customer messages and provide user emails and contact information to authorities when faced with a court order, even if they oppose it. Consumer services like these typically haven’t had strong encryption.

Adding easy-to-use encryption that companies can’t unscramble to products used by millions changes that calculus. After Apple Inc. tweaked its iPhone software so that the company could no longer unlock phones for police, the director of the Federal Bureau of Investigation accused Apple of aiding criminals. Apple Chief Executive Tim Cook counters that he is defending user privacy.

The incident sparked a continuing war of words between Silicon Valley and Washington. “Encryption has moved from something that is available to something that is the default,” FBI Director James Comey told a congressional panel Wednesday. “This is a world that in some ways is wonderful and in some ways has serious public-safety ramifications.”

Technology companies, once cozy with Washington, sound increasingly like Mr. Marlinspike. Apple, Facebook, Google and others are resisting efforts to give the government access to encrypted communications.

Last fall, WhatsApp added Mr. Marlinspike’s encryption scheme to text messages between users with Android smartphones, but there is no easy way to verify that the encryption software is actually turned on. The app maker, acquired by Facebook for $22 billion last year, plans to extend encryption to images and iPhone messages, a person familiar with the project said.

Behind the clash lurks this reality: Even if the big tech companies come around, there are others like Mr. Marlinspike who will pick fights with code.

Mr. Marlinspike argues for safe spaces online. His personal Web address is thoughtcrime.org, a reference to George Orwell’s “1984.”

As a teenager, Mr. Marlinspike says, he was more interested in breaking software than creating it. He turned to protecting data as he grew more concerned about surveillance.

He moved to San Francisco in the late 1990s and worked for several technology companies before the dot-com bust, including business-software maker BEA Systems Inc. Since then, he often has lived on the edge of the Bay Area’s tech-wonk scene.

During the mid-2000s, he and three friends refurbished a derelict sailboat and spent summers being blown around the Bahamas, without a backup motor, as depicted in a home movie Mr. Marlinspike posted online.

In 2010, Mr. Marlinspike’s company, Whisper Systems, released an encryption app, TextSecure. Twitter Inc. bought Whisper Systems for an undisclosed sum in 2011 primarily so that Mr. Marlinspike could help the then-startup improve its security, two people familiar with the transaction said. He worked to bolster privacy technology for the social-media firm, leaving in 2013.

Around that time, the State Department was looking to use technology to support pro-democracy movements overseas. Mr. Marlinspike’s work caught the attention of Ian Schuler, manager of the department’s Internet freedom programs. Encrypted messaging was viewed as a way for dissidents to get around repressive regimes.

With help from Mr. Schuler, Radio Free Asia's Open Technology Fund, which is funded by the government and has a relationship with the State Department, granted Mr. Marlinspike more than $1.3 million between 2013 and 2014, according to the fund's website.

Mr. Marlinspike was hardly a conventional Washington player. He and a government official missed meeting one another at a San Francisco burrito joint because the visitor assumed the dreadlocked Mr. Marlinspike couldn't be the person he was there to see, Messrs. Schuler and Marlinspike said.

Mr. Marlinspike now runs a new firm, Open Whisper Systems, from a low-rent workspace in San Francisco's Mission District. He has received other grants but says he isn't interested in venture capital, partly because he would have to promise returns to investors.

His latest app, Signal, promises users secure text messages and voice calls. He acknowledges that it still has some kinks. Calls can drop if a user receives a traditional phone call while on an encrypted call. Mr. Marlinspike won't disclose how many people use the app.

He still has work to do if he wants typical users to adopt encrypted communications.

But its minimalist blue-and-white design looks like something that could have emerged from Facebook.

Mr. Marlinspike says the San Francisco Police Department called last year to ask whether the app was secure enough for its officers to use. A spokesman for the department said it "did look at this vendor."

Write to Danny Yadron at danny.yadron@wsj.com