December 8, 2015

The Crypto Cat is Out of the Bag:
An Illustrative Inventory of Widely-Available Encryption Applications

When it comes to encryption, the genie is out of the bottle. But encryption isn't magic. It's math, and very well-known math at that. The basic principles behind modern end-to-end encryption of digital messages, where only the recipient of the message can decode it, are nearly four decades old.[1]

U.S. companies like Apple and Facebook, providers of the encrypted messaging services iMessage and WhatsApp, don't have a monopoly on strong end-to-end encryption tools. **Strong encryption tools are everywhere, and over a billion ordinary people around the world rely on them every day.**

There are countless applications that are freely available online, across the globe, with unbreakable end-to-end encryption. The vast majority of those applications are either "open source" software that anyone is free to use, review, copy or build on,[2] and/or are offered by companies, organizations or developers outside of the United States. In fact, it's so easy to create new end-to-end encryption apps, **jihadists have been coding their very own secure messaging tools since at least 2007, tools with names like *Mujahadeen Secrets* and *Security of the Mujahid*.[3] Another app that terrorists are claimed to have used, *Telegram*, is based in Berlin.[4]**

---

[1] The foundational work in this area began with Whitfield Diffie and Martin Hellman's *New Directions in Cryptography*, IEEE Transactions in Information Theory (Nov. 6, 1976), *available at* http://www-ee.stanford.edu/~hellman/publications/24.pdf.

[2] Open-source software (OSS) is computer software with its source code made available with a license in which the copyright holder provides the rights to study, change, and distribute the software to anyone and for any purpose. Open-source software may be developed in a collaborative public manner," which we refer to below as "open development". See Wikipedia, *Open-source software* (last modified December 7, 2015), available at https://en.wikipedia.org/wiki/Open-source_software. Even the encryption in *WhatsApp*, Facebook's secure messaging app, is based on the free and open source software *TextSecure*.

[3] For a recent summary of several homegrown jihadist secure apps, most or all of which are based on open source software code, see *Measuring the Impact of the Snowden Leaks on the Use of Encryption by Online Jihadists*, Flashpoint Partners (September 2014), *available at* https://fpjintel.com/portal/assets/File/Flashpoint_Jihadi_Encryption_Software_Sept2014.pdf.

[4] Laurie Segall, CNN, *An app called telegram is the 'hot new thing among jihadists'* (November 18, 2015), *available at* http://money.cnn.com/2015/11/17/technology/isis-telegram/.

When it comes to encryption, the horse is out of the barn, the ship has sailed, and the toothpaste isn't going back in the tube. The math, and the technology, is already out there. Therefore, any attempt by the U.S. government to pressure U.S. companies to redesign their end-to-end encrypted services so that they have the keys necessary to decrypt the communications—which is really just another way of saying "stop deploying end-to-end encryption"—would be futile. **There are plenty of other reasons why anti-encryption regulation would be bad for America**, which we've laid out many times over the past year in Congressional testimony, research papers, blog posts, op-eds and more.[5] **But the biggest reason is just this: anti-encryption regulation will not make us safer. It's all cost, no benefit.**

A surveillance backdoor into U.S. products will not stop terrorists from using other end-to-end encryption tools that are widely available online around the world. It will only discourage a lot of normal, law-abiding Americans from using it, while also discouraging international users from relying on U.S. products that have been rendered less secure. **Surveillance backdoors are a lose-lose proposition: they won't make the terrorists less secure, only ourselves—and former heads of the DHS, NSA, and CIA agree.[6]**

As former NSA Director and Director of National Intelligence Mike McConnell puts it, rather than trying to fight the inevitable, government investigators need to adapt to a world with widespread encryption:

> **"Don't get in the way of progress.** Don't get in the way of innovation and creativity, because this is going to happen. Somebody's going to provide this encryption." Therefore, law enforcement must "adapt," says McConnell. "If law enforcement starts to change the way they think about this, I think there are many, many ways to carry out the mission, given that you are faced with a situation where **technology is not going to be reversed.**"[7]

---

[5] The wide variety of writing on encryption done by New America's Open Technology Institute was recently collected in this single summary: New America's Open Technology Institute, *Read This Before You Rail Against Encryption* (November 19, 2015), *available at* https://www.newamerica.org/weekly/read-this-before-you-rail-against-encryption/.

[6] Mike McConnell et al, The Washington Post, *Why the fear over ubiquitous data encryption is overblown* (July 28, 2015), *available at* https://www.washingtonpost.com/opinions/the-need-for-ubiquitous-data-encryption/2015/07/28/3d145952-324e-11e5-8353-1215475949f4_story.html; Lorenzo Franceschi-Bicchierai, Motherboard, *Former NSA Chief: I 'Would Not Support Encryption Backdoors'* (October 6, 2015), *available at* http://motherboard.vice.com/read/former-nsa-chief-strongly-disagrees-with-current-nsa-chief-on-encryption.

[7] Kaveh Wadell, The National Journal, *Former Intelligence Director: Law Enforcement Must "Adapt" to Encryption* (October 1, 2015), *available at* http://www.nationaljournal.com/s/74230/former-intelligence-director-law-enforcement-must-adapt-encryption

We agree with former Director McConnell that the encryption genie is out of the bottle, as demonstrated by the following charts. **That's why the White House and Congress should sensibly reject any calls to regulate the availability of strong encryption tools, just as they did 20 years ago.**[8]

The first chart is an illustrative inventory of the many popular, easy to get, easy to use end-to-end encryption tools available right now that are either open source, developed outside of the US, or both, and would therefore be minimally affected if at all by U.S. legislation or action by U.S. companies. **In sum, it describes sixteen popular apps for fully encrypted email, chat, messaging or voice calls that are outside of U.S. regulation's reach.**

The second chart is adapted from a chart that reportedly came from an ISIS information security training manual, which identified encrypted messaging applications that were thought to be "safe" and "safest" (as opposed to "moderately safe" or "unsafe").[9] As you'll see, **all of the encryption apps considered "safest" by ISIS are open source, foreign-based, or both, as are three out of the four apps considered "safe". Therefore, of the nine apps recommended as "safe" or "safest", eight of them are outside of U.S. regulation's reach.**

For more information, contact Kevin Bankston (bankston@opentechinstitute.org), Director of New America's Open Technology Institute, or Ross Schulman (ross@opentechinstitute.org), OTI Senior Counsel.

[8] Danielle Kehl, Andi Wilson, and Kevin Bankston, *Doomed to Repeat History? Lessons From The Crypto Wars of the 1990s*, New America's Open Technology Institute, June 2015, *available at* https://static.newamerica.org/attachments/3407-doomed-to-repeat-history-lessons-from-the-crypto-wars-of-the-1990s/OTI_Crypto_Wars_History.abe6caa19cbc40de842e01c28a028418.pdf.

[9] Margaret Corker et al, The Wall Street Journal, *How Islamic State Teaches Tech Saavy to Evade Detection* (November 16, 2015), *available at* http://www.wsj.com/articles/islamic-state-teaches-tech-savvy-1447720824.

Chart 1. An Illustrative Inventory of End-to-End Encrypted Applications That Are Open Source, Foreign-Based, or Both.

Apps in ***Yellow*** are open source, apps in ***Blue*** are not maintained by a U.S.-based company/organization, and apps in ***Green*** are both open source and not maintained by a U.S.-based company.

App	Company or Organization	What does it encrypt?	What operating systems is it available on?	Is App Open Source?	Is Company or Org U.S. Based?
Adium	N/A; Adium is an open development project	Instant messaging	Mac	***Yes***	***No***; Adium is an open development project
ChatSecure	The Guardian Project (nonprofit research and development organization)	Chat	iPhone and Android	***Yes***	***Yes***
Cryptocat	N/A; Adium is an open development project	Chat	iPhone, Mac, and via a web application for Chrome, Firefox, and Safari browsers	***Yes***	***No***; Cryptocat is an open development project
GnuPG	N/A; GnuPG is an open development project	Email	Linux	***Yes***	***No***; GnuPG is an open development project
Gpg4win	Intevation GmbH and G10 Code GmbH	Email	Windows PC	***Yes***	***No***; Intevation GmbH and G10 Code GmbH are German-based companies
GPGTools	N/A; GPGTools is an open development project	Email	Mac	***Yes***	***No***; GPGTools is an open development project
Jitsi	N/A; Jitsi is an open development project	Voice calls and text messaging	Android devices, Windows PC, Mac, and Linux	***Yes***	***No***; Jitsi is an open development project
Mailvelope	Mailvelope GmbH	Email	Web application	***Yes***	***No***; Mailvelope GmbH is a German-based company
Ostel	The Guardian Project (nonprofit research and development organization)	Voice calls	iPhone, Android devices, Blackberry, Windows PC, Mac, and Linux	***Yes***	***Yes***
Pidgin	N/A; Pidgin is an open development project	Instant messaging	Windows PC and Linux	***Yes***	***No***; Pidgin is an open development project
RetroShare	N/A; RetroShare is an open development project	Text messaging and email	Mac, Windows PC, and Linux	***Yes***	***No***; RetroShare is an open development project
Signal	Open Whisper Systems	Voice calls and text messaging	iPhone and Android	***Yes***	***Yes***
Silent Phone	Silent Circle	Voice calls and text messaging	iPhone and Android	***Yes***	***No***; Silent Circle is a Swiss-based company
Surespot	Surespot, LLC	Text messaging	iPhone and Android devices	***Yes***	***Yes***
Telegram	Telegram Messenger	Text messaging	iPhone, iPad, Android devices, Windows Phone, Windows PC, Mac, Linux, and via web application	***Partially***	***No***; Telegram Messenger is a German-based company
Threema	Threema GmbH	Text messaging	iPhone and Android	***Yes***	***No***; Threema GmbH is a Swiss-based company

Chart 2. ISIS' Favorite Encryption Apps Are Open Source, Foreign-Based, or Both.[10]

Apps in ***Yellow*** are open source, apps in ***Blue*** are not maintained by a U.S.-based company/organization, and apps in ***Green*** are both open source and not maintained by a U.S.-based company.

Labeled "Safest"	Labeled "Safe"
Silent Circle[11]	Telegram
Redphone**[12]	Wickr
OSTel	Threema
ChatSecure	Surespot
Signal	

[10] This chart is adapted from one that originally appeared in the Wall Street Journal, which was reportedly found in a manual used by ISIS for security training. See Margaret Corker et al, The Wall Street Journal, *How Islamic State Teaches Tech Saavy to Evade Detection* (November 16, 2015), *available at* http://www.wsj.com/articles/islamic-state-teaches-tech-savvy-1447720824. Some reports indicate that the manual was originally developed for use by activists and journalists, not by ISIS. See Arab Crunch, *Update: How the Media Cooks News: Kuwaiti security firm writes a guide to Cyber Security for Gaza Journalists, Wired and other Media writes it up as 'ISIS OPSEC manual'* (November 23, 2015), http://arabcrunch.com/2015/11/how-the-western-media-cooks-news-isis-opsec-manual-isnt-from-isis-it-was-reproduced-from-dec-2014-guide-for-gaza-activists-journalist.html . Regardless of its origin, the point remains: the applications considered to be the most secure are also not effectively regulable by the U.S. government nor via U.S. companies' conduct.

[11] Silent Circle's app is now called "Silent Phone", as reflected in Chart 1.

[12] Redphone is now incorporated into Signal, as reflected in Chart 1.