CENTER FOR DEMOCRACY & TECHNOLOGY

3/3/16

Issue brief: A "backdoor" to encryption for government surveillance

Encrypting smartphones and other devices helps protect against malicious hacking, identity theft, phone theft, and other crimes. However, a government mandate requiring companies to build a "backdoor" into encryption for surveillance would put consumers at grave risk and impose heavy costs on US businesses. The government can obtain information for investigations from other sources, and may be able to compel an individual to decrypt information with a search warrant.

What companies have done recently: Apple and Google recently announced that their smartphones will be "encrypted by default."[1] All the data stored on the phone itself will be unreadable to anyone who accesses the phone without knowing the device passcode, in order to unlock the encryption. Weak encryption (or obvious passwords) can be broken, but Apple and Google will apply strong encryption to their devices.[2] Many other companies and nonprofits have long offered products and services secured by strong encryption to the public.[3]

> **The primary impact:** Mobile devices increasingly mediate the most sensitive of our online transactions, from health to finance to authenticating to secure systems. Encrypting mobile devices by default will increase security from cybercriminals for regular smartphone users. Encryption by default ensures that if criminals steal or attempt to hack into a phone, they will be unable to access the owner's sensitive data on the device, such as credit card information, photos, emails, medical records, social media accounts, and authentication credentials.[4] The principle objective of securing smartphones with strong encryption is to protect against cybersecurity threats faced by millions of American smartphone users – identity theft, phone theft, and cybercrime.[5]

What the FBI wants: The FBI wants a "backdoor" into encrypted products – not just phones, but other communications services as well. FBI Director Comey has called for companies to build security flaws into their encrypted products so that the government can break through and wiretap consumers or seize data stored on their devices.[6] In the case of the San Bernardino shooting, the FBI has sought to force Apple, Inc. to produce an insecure version of its mobile operating system, which would vastly increase the security and privacy risks to hundreds of millions mobile devices.

> **A backdoor for government surveillance:** Director Comey has stated the FBI is not seeking a backdoor because he is proposing that companies intentionally build into their products a means of breaking encryption for the purpose of government access. However, this conflates a legal backdoor with a technical one: as a technical matter, creating a path through encryption to provide access that the user does not authorize is, by definition, a "backdoor" security vulnerability. It is impossible to build encryption that can be circumvented without creating a technical backdoor.

Backdoors create major problems: Backdoors severely weaken cybersecurity, leaving users exposed to malicious hacking and crime. A government-mandated security vulnerability in tech products would also be a huge burden on businesses and an obstacle to innovation.

> **User security undermined:** A fundamental problem with a backdoor is that there is no way to control who goes through it.[7] If the US government can exploit a backdoor security vulnerability to access a consumer's device, so will malicious hackers, identity thieves, and foreign governments.[8] This will devastate the security of not just individual consumers around the world, but also the many businesses that use American commercial tech products day-to-day. Ultimately, this mandate would have the effect of actually enabling cybercrime and undermining national security.

---

[1] Joe Miller, Google and Apple to introduce default encryption, BBC News, Sep. 19, 2014, http://www.bbc.com/news/technology-29276955.
[2] Dan Goodin, Why passwords have never been weaker – and crackers have never been stronger, Aug. 20, 2012, http://arstechnica.com/security/2012/08/passwords-under-assault.
[3] See, e.g., Heidi Hoopes, Apps to easily encrypt your text messaging and mobile calls, Gizmag, Sep. 27, 2014, http://www.gizmag.com/secure-text-messaging-phone-clients-comparison-ios-and-android/34000/. See also Services, Silent Circle, https://silentcircle.com/services (last accessed Oct. 31, 2014).
[4] See, e.g., Google Wallet, Google, https://www.google.com/wallet (last accessed Oct. 31, 2014). See also iOS8 Health, Apple, https://www.apple.com/ios/whats-new/health (last accessed Oct. 31, 2014).
[5] Sid Kirchheimer, How to Cyberproof Your Phone, AARP, May 2014, http://www.aarp.org/home-family/personal-technology/info-2014/cyberproof-stolen-phone-kirchheimer.html.
[6] James Comey, Remarks before the Brookings Institution, Federal Bureau of Investigation, Oct. 16, 2014, http://www.fbi.gov/news/speeches/going-dark-are-technology-privacy-and-public-safety-on-a-collision-course.
[7] Center for Democracy, CALEA II: Risks of Wiretap Modifications to Endpoints, May 17, 2013, pgs. 4-6, https://www.cdt.org/files/pdfs/CALEAII-techreport.pdf.
[8] For example: In 2010, Chinese hackers breached the internal systems that companies like Google and Microsoft use to comply with government search warrants on their users, including the email accounts of suspected terrorists and spies. Ellen Nakashima, Chinese hackers who breached Google gained access to sensitive data, U.S. officials say, Washington Post, May 20, 2013, http://www.washingtonpost.com/world/national-security/chinese-hackers-who-breached-google-gained-access-to-sensitive-data-us-officials-say/2013/05/20/51330428-be34-11e2-89c9-3be8095fe767_story.html.

US businesses harmed: Consumers outside of the US may be much less inclined to purchase American tech products that facilitate government surveillance. Consider, for example, the difficulty US companies would have selling smartphones or network servers in the EU that are built to enable easy access for the NSA. As a technical matter, it is difficult and expensive to both build a backdoor security vulnerability and then defend that vulnerability against unauthorized use. This burden would be heaviest on small businesses and innovators of new communications services, which may be create a disincentive to encrypt their products and services, which would reduce the overall security of users.

Government is not "going dark": There is no doubt that some communications are more difficult to intercept than others, and that the FBI has a legitimate concern that criminals and terrorists will gravitate to communications technologies that are more difficult to surveil. However, taken as a whole, the digital revolution has made more data about us available than ever before, and the government has more tools to obtain and analyze that data than ever before. The volume of government surveillance increases almost every year.[9] The claim that companies' increasing adoption of strong encryption by default will suddenly lead to government "going dark" and unable to access critical information is not accurate.[10]

Encryption is not new: Products and software with strong encryption have been freely available to the public – including criminals – for many years, and have not rendered law enforcement helpless to investigate crimes.[11] By recently choosing to encrypt popular smartphones by default, companies are making this security feature easier to use and more accessible to regular smartphone users who do not seek out increased security protection. This change will *reduce* overall crime by protecting all smartphone users, rather than just those who are already security-conscious.

Government has multiple options: If information is encrypted in one place, it is often available from another source. For example, emails or text messages on an encrypted phone can be retrieved from the email service provider or the phone company. Many smartphones are backed up to the cloud, where the data can be obtained from the service provider through legal process. In addition, law enforcement may be able to compel a suspect to decrypt information or devices with a search warrant.[12]

Compelled decryption: The Department of Justice takes the stance that the government can compel the owner of encrypted devices or account, such as a phone or an email account, to decrypt the information it seeks. The government has successfully argued in a number of cases that a warrant permits it to compel decryption.[13] Whether compelled decryption is permissible or is barred by the Fifth Amendment hinges on a range of issues, including whether decryption is "testimonial," whether the existence of the information sought by the government is a "foregone conclusion," and whether immunity for the act of decryption is provided.[14]

Contempt: If an individual refuses an order to decrypt an electronic device, she could be held in contempt of court. When suspects refuse to testify or answer questions, courts can impose coercive and punitive punishments for contempt, including fines and imprisonment. Imprisonment for civil contempt can last for years,[15] or until the order is obeyed. For example, the Third Circuit approved a contempt sentence that lasted 14 years, maintaining that individuals can be confined as long as they refuse a court order they are capable of obeying.[16]

END

For more information, please contact Joseph Lorenzo Hall, Chief Technologist, at joe@cdt.org.

---

[9] US Courts, Authorized Intercepts Granted Pursuant to 18 U.S.C. § 2519 as Reported in Wiretap Reports for Calendar Years 2003 – 2013, http://www.uscourts.gov/uscourts/Statistics/WiretapReports/2013/Table7.pdf (last accessed Nov. 7, 2014).

[10] The Berkman Center for Internet & Society at Harvard University, "Don't Panic. Making Progress on the 'Going Dark' Debate," (January 2016), https://cyber.law.harvard.edu/pubrelease/dont-panic/Dont_Panic_Making_Progress_on_Going_Dark_Debate.pdf.

[11] For example, the powerful and popular encryption standard "PGP" was created in 1991. PGP is available free to the public and can be used to encrypt emails, text, images, hard drives, and more. See OpenPGP Alliance, http://www.openpgp.org/index.shtml (last accessed Oct. 31, 2014).

[12] The government must generally obtain a warrant to search a smartphone. See *Riley v. California*, *134* S.Ct. 2473 (2014).

[13] See, e.g., *United States v. Fricosu*, No. 10-CR-00509 (D. Colo. Jan. 23, 2012), http://www.wired.com/images_blogs/threatlevel/2012/01/decrypt.pdf.

[14] Orin Kerr, Encryption and the Fifth Amendment Right Against Self-Incrimination, The Volokh Conspiracy, Jan. 24, 2012, http://volokh.com/2012/01/24/encrytion-and-the-fifth-amendment-right-against-self-incrimination.

[15] See, e.g., *Shillitani v. United States*, 384 U.S. 364 (1966), https://supreme.justia.com/cases/federal/us/384/364/case.html.

[16] *Chadwick v. Janecka*, 302 F.3d 107 (2002), http://law.justia.com/cases/federal/appellate-courts/F3/302/107/560004.