The Argument Against a Mobile Device Backdoor for Government

By Kevin Townsend on February 07, 2018

Just as the Scope of 'Responsible Encryption' is Vague, So Too Are the Technical Requirements Necessary to Achieve It

The 'responsible encryption' demanded by law enforcement and some politicians will not prevent criminals 'going dark'; will weaken cyber security for innocent Americans; and will have a hit on the U.S. economy. At the same time, there are existing legal methods for law enforcement to gain access to devices without requiring new legislation.

These are the conclusions of **Riana Pfefferkorn**, cryptography fellow at the Center for Internet and Society at the Stanford Law School in a paper published Tuesday titled, The Risks of "Responsible Encryption" (PDF).

One of the difficulties in commenting on government proposals for responsible encryption is that there are no proposals -- merely demands that it be introduced. Pfefferkorn consequently first analyzes the various comments of two particularly vocal proponents: U.S. Deputy Attorney General, Rod Rosenstein, and the current director of the FBI, Christopher Wray to understand what they, and other proponents, might be seeking.

Wray seems to prefer a voluntary undertaking from the technology sector. Rosenstein is looking for a federal legislative approach. Rosenstein seems primarily concerned with mobile device encryption. Wray is also concerned with access to encrypted mobile devices (and possibly other devices), but sees responsible encryption also covering messaging apps (but perhaps not other forms of data in transit).

Just as the scope of 'responsible encryption' is vague, so too are the technical requirements necessary to achieve it.

"The only technical requirement that both officials clearly want," concludes Pfefferkorn, "is a key-escrow model for exceptional access, though they differ on the specifics. Rosenstein seems to prefer that the provider store its own keys; Wray appears to prefer third-party key escrow."

The basic argument is that golden keys to devices and/or messaging apps should be maintained somewhere that law enforcement can access with a court order: that is, some form of key escrow. This is a slightly lesser ambition than that sought by government in the mid-1990s in the discussions between government (then, as now, not just in the U.S.) and technologists during what became known as the First Crypto War. At that time, government sought much wider control over encryption, and access to everyone's computer at chip level. New America published a history (PDF) of that era in 2015.

Rosenstein has argued that device and application manufacturers already have and use a form of key escrow to manage and perform software updates. The argument is that if they can do this for themselves, they can do it for government to prevent criminal communications from 'going dark'. Pfefferkorn, however, offers four arguments against this.

First, the scale is completely different. The software update key is known and used by only a very small number of internal and highly trusted staff, and then used only infrequently. But, suggests Pfefferkorn, "with law enforcement agencies from around the globe sending in requests to the manufacturer or third-party escrow agent at all hours (and expecting prompt turn-around), the decryption key would likely be called into use several times a day, every day. This, in turn, means the

holder of the key would have to provide enough staff to comply expeditiously with all those demands."

Increased use of the key increases the risk of loss through human error or malfeasance (such as extortion or bribery) -- and the loss of that key could be catastrophic.

Second, attackers will seek to exploit the process through social engineering with spear-phishing attacks against the vendor's or escrow agent's employees; and it is generally only a matter of time before spear-phishing succeeds. The likelihood of spear-phishing succeeding will increase with the sheer volume of LEA demands received. The FBI has claimed that it had around 7,800 seized phones it could not unlock in the last fiscal year. These alone, not including any phones seized by the thousands of State and local law enforcement offices, would average at more than 20 key requests every day, making a spear-phishing attempt less obvious.

Third, it would harm the U.S. economy both through loss of market share at home and abroad (since security could not be guaranteed), and through the economic effect of ID and IP theft following the likely abuse of the system.

Finally, Pfefferkorn argues that access to devices through key escrow still won't necessarily provide access to communications or content if these are separately encrypted by the user. "If the user chooses a reasonable password for the app," she says, "then unlocking the phone will not do any good... In short, an exceptional-access mandate for devices will never be completely effective."

Pfefferkorn goes further by suggesting that there are already numerous ways in which LEAs can obtain information from mobile devices. If the device is locked with a biometric identifier, the police can compel its owner to unlock it (not so with a password lock). If it is synced with other devices or backed up to the cloud, then access may be easier from these other destinations. Law enforcement already claims wide-ranging powers under the Stored Communications Act to access stored communications and transactional records held by ISPs -- as seen in the long-running battle between Microsoft and the government.

Metadata is another source of legal information. This can be gleaned from message headers, while cell towers can provide location and journey tracking. Far more metadata is likely to become available through the internet of things.

Finally, there are forensics and 'government hacking' opportunities. In early 2016 the FBI asked, and then got a court order, for Apple to provide access to the locked iPhone of Syed Rizwan Farook, known as the San Bernardino Shooter. Apple declined -- but either through contract hackers or a forensics company such as Cellebrite, the FBI eventually succeeded without help from Apple. "The success of tools such as Cellebrite's in circumventing device encryption," says Pfefferkorn, "stands as a counterpoint to federal officials' asserted need to require device vendors by law to weaken their own encryption."

Pfefferkorn's opinion in the ongoing argument for law enforcement to be granted an 'exceptional-access' mandate is clear: "It would be unwise."