Privacy and Security
Encryption and Surveillance
Why the law-enforcement access question will not just go away.

Encryption and Surveillance as a Policy Question
Many cryptographers, computer-security researchers, and LE officials have chimed in on the LEA controversy. On
one side is the LE view that the technology industry’s post-Snowden embrace of default encryption is willfully thwarting the lawful exercise of properly authorized warrants. The FBI’s motion to compel Apple to develop software to unlock the iPhone of a dead terrorist perfectly exemplifies this side of the debate. Under this view, the salient fact is that individuals and organizations are obligated, under the All Writs Act in the U.S. and similar laws in other democratic countries, to assist the government in the execution of warrants.

On the other side is the view, embraced by many technologists and civil-liberties advocates, that, since the 9/11 terrorist attacks, governments have conducted far too much mass surveillance and that the appropriate grassroots response is mass encryption. Moreover, widespread use of sound encryption is our strongest weapon in the fight against intellectual-property theft, identity theft, and many other online crimes—something that LE should applaud. As in the 1990s crypto war, customers of U.S. technology firms might be driven into the arms of foreign competitors in search of promises that their data will not be decrypted by third parties, even when those third parties are pursuing legitimate goals. This view is explicated and endorsed by, for example, Landau and Schneier in their individual statements in Zittran et al.

Encryption and Surveillance as a Technical Question

That LEA is at best technically difficult and perhaps technically infeasible has been argued eloquently by numerous experts. While acknowledging that criminals can use encryption to avoid detection and prosecution and that increasing use of encryption hampers LE, these authors point out that the LE community has not quantified the extent of the problem. They explain that LE often has at its disposal other means of obtaining the information it needs, for example, vulnerability-based unlocking toolkits or back-up copies that can be decrypted by cloud-service providers. Indeed, the FBI withdrew its motion to compel Apple to assist it in unlocking the dead San Bernardino terrorist’s iPhone when it discovered a “gray-hat” hacking toolkit that could unlock the device. As reported in Bellovin et al., the firm Grayshift “will sell law enforcement a $15,000 tool that opens 300 locked phones or online access for $30,000 to open as many phones as law enforcement has warrants for.”

If LE wants something more general, more powerful, or more rigorously analyzed by the research community, it will need to specify precisely what its LEA requirements are. What range of surveillance tasks does it expect to accomplish in the presence of default encryption? How does it expect LEA technology to interact with legal processes and, in particular, would the technology be available to the more than 15,000 police departments in the U.S.? Would technology vendors be expected to cooperate on LEA not only with the U.S. government but with the governments of all countries in which their products are sold, including authoritarian governments (and, if not, what is to stop criminals from buying their devices in countries with which vendors do not cooperate)?

Notwithstanding the absence of fully fleshed-out requirements, several computer scientists have proposed

Widespread use of sound encryption is our strongest weapon in the fight against intellectual-property theft, identity theft, and many other online crimes.

---

b See https://www.clearinghouse.net/detail.php?id=15497.

c 28 USC 1651(a), 1789: “The Supreme Court and all courts established by Act of Congress may issue all writs necessary or appropriate in aid of their respective jurisdictions and agreeable to the usages and principles of law.”
Unlike purely technical problems, compelling policy problems are rarely definitively “solved” and no longer discussed.

inconvenience and expense on the LE community is not a good enough reason to mandate LEA features that might render immensely popular products and services less secure, more expensive, or unsellable on world markets.

However, I also believe LEA deserves further study. The desire of many in computer security and related communities for the LEA question to be declared “asked and answered” and simply go away is unrealistic. Unlike purely technical problems, compelling policy problems are rarely definitively “solved” and no longer discussed. The losing position in the 1990s crypto war is still appealing to many people, some of whom were not yet born when that war was won by the opponents of key escrow. If LEA is to be rejected, the argument must continue, and a new generation must be convinced.

My experience with Yale students has revealed two loci of resistance to the ideas that the tech community should not or cannot assist LE. The first is perceived arrogance of the technology industry. Government regulates many consumer products: why not smartphones or computers? The second is technical in nature: Many strong students do not see intuitively why it is infeasible to build personal devices that, in typical circumstances, can only be unlocked by their owners but, in atypical circumstances, and with proper judicial authorization, can also be unlocked by a designated third party. If smartphone owners trust cloud-service providers to decrypt back-up copies only under appropriate circumstances, why is there no organization that can be similarly trusted with the ability to unlock devices? Until clear answers to such questions are more widely disseminated, intuitive resistance to the claim that LEA is technically infeasible will continue.

Indeed, it has not actually been shown that no useful form of LEA can be implemented without creating unacceptable risk. We have heard convincing arguments that mandated LEA capabilities might be ineffective, extremely costly, or hijacked by the very criminals they were built to thwart. However, we have also heard that LE has not precisely specified its requirements. A cryptographic goal that cannot be met in its most general form is sometimes achievable in a weaker but still useful form. Perhaps the final verdict on LEA will be that it cannot be done securely at reasonable cost, but, in order to prove that, we will have to know exactly what the meaning of “it” is.

References
4. Hermessey, S. and Wittes, B. Apple is selling you a phone, not civil liberties. Lawfare (Feb. 18, 2016); https://lawfareblog.com/apple-selling-you-phone-not-civil-liberties

Joan Feigenbaum (joan.feigenbaum@yale.edu) is the Grace Murray Hopper Professor of Computer Science at Yale University. New Haven, CT, USA.

This work was supported in part by U.S. National Science Foundation grants CNS-1407454 and CNS-1409599 and U.S. Office of Naval Research grant N00014-18-1-2743.

Copyright held by author.

A Compromise Position

Although neither side in this debate can simply be dismissed, I find the call to implement LEA unpersuasive at this time. There has indeed been too much surveillance since 9/11, and it is entirely reasonable for the technology industry to react by enabling its customers to keep data truly confidential. Rather than causing LE to “go dark,” locked devices and default-encrypted communications appear to be causing it, in some cases, to use less convenient or more expensive methods than it would prefer to use. Imposition of as-yet-unquantified "solutions" to one version of the LEA problem, namely building devices that, in the absence of the device owner’s passcode, can still be unlocked, usually with the manufacturer’s cooperation, by LE agents who present valid warrants. I have put “solutions” in quotes, because these are often high-level ideas rather than completely specified proposals. The one that has received the most attention is that of Ray Ozzie, who is the inventor of Lotus Notes and a former Microsoft VP. In Ozzie’s scheme, the device’s encryption key is stored on the device itself, encrypted under a manufacturer’s key. An LE agent who has physical possession of the device and a warrant to unlock it extracts the encrypted device key from the phone and sends it to the manufacturer. The manufacturer decrypts the device key and sends it back to LE, which can then unlock the device. A notable feature of Ozzie’s approach is that, when the target device is unlocked, it also “bricks” itself, preventing any further changes to its contents. Bricking both preserves evidence for use in court and informs the owner that someone has unlocked his device so that he can power it down and put it in a safe place, thus preventing subsequent access.

My experience with Yale students has revealed two loci of resistance to the ideas that the tech community should not or cannot assist LE. The first is perceived arrogance of the technology industry. Government regulates many consumer products: why not smartphones or computers? The second is technical in nature: Many strong students do not see intuitively why it is infeasible to build personal devices that, in typical circumstances, can only be unlocked by their owners but, in atypical circumstances, and with proper judicial authorization, can also be unlocked by a designated third party. If smartphone owners trust cloud-service providers to decrypt back-up copies only under appropriate circumstances, why is there no organization that can be trusted with the ability to unlock devices? Until clear answers to such questions are more widely disseminated, intuitive resistance to the claim that LEA is technically infeasible will continue.

Indeed, it has not actually been shown that no useful form of LEA can be implemented without creating unacceptable risk. We have heard convincing arguments that mandated LEA capabilities might be ineffective, extremely costly, or hijacked by the very criminals they were built to thwart. However, we have also heard that LE has not precisely specified its requirements. A cryptographic goal that cannot be met in its most general form is sometimes achievable in a weaker but still useful form. Perhaps the final verdict on LEA will be that it cannot be done securely at reasonable cost, but, in order to prove that, we will have to know exactly what the meaning of “it” is.