Analysis of the CLEAR Protocol per the National Academies' Framework

Steven M. Bellovin, Matt Blaze, Dan Boneh, Susan Landau, Ronald L. Rivest*

CUCS-003-18
May 10, 2018

Abstract: The debate over "exceptional access"—the government's ability to read encrypted data—has been going on for many years and shows no signs of resolution any time soon. On the one hand, some people came it can be accomplished safely; others dispute that. In an attempt to make progress, a National Academies study committee propounded a framework to use when analyzing proposed solutions. We apply that framework to the CLEAR protocol and show the limitations of the design.

The encryption debate is several decades old. Between the 1970s and the late1990s, the fight was over end-to-end encryption that provided confidentiality to communications; more recently the dispute has been over locked devices. To protect users against attacks that used data from lost or stolen iPhones, in 2011 Apple began securing such data; several years later, Google did the same for the Android operating system. The FBI objected, arguing that the new security systems prevented accessing evidence even when there was a court order to do so. The conflict came to a head in 2015 over the locked iPhone of the San Bernardino terrorist. That case was resolved when a third party successfully unlocked the phone. But the larger issue of Exceptional Access—mechanisms that enable law-enforcement access to unlock phones without cooperation of the device's owner—remained unresolved.

A study committee constituted by the National Academies of Sciences, Engineering, and Medicine recently examined the issue of law enforcement and intelligence access to plaintext information.[1] The committee developed a framework to apply to evaluating choices in encryption policy. The framework's purpose "is not simply to help policymakers determine whether a particular approach is optimal or desirable, but also to help ensure that any approach that policymakers might pursue is implemented in a way that maximizes its effectiveness while minimizing harmful side effects."[2]

During the course of the committee's study, several computer scientists proposed possible technologies for Exceptional Access. This included Ray Ozzie, former Chief Technology Officer and Chief Software Architect at Microsoft. The Academies study committee was not constituted to evaluate technical approaches and did not do so. But it seemed valuable to subject Ozzie's suggested approach to a technical evaluation. Ozzie graciously agreed to do so, and in May 2017, an ad hoc group of technical experts met with Ozzie to discuss his

---

* Steven M. Bellovin: Columbia University, smb@cs.columbia.edu. Matt Blaze: University of Pennsylvania, mab@crypto.com. Dan Boneh: Stanford University, dabo@cs.columbia.edu. Susan Landau, Tufts University, Susan.Landau@PrivacyInk.org. Ronald L. Rivest: MIT, rivest@mit.edu.

[1] Committee on Law Enforcement and Intelligence Access to Plaintext Information, Computer Science and Telecommunications Board, Division on Engineering and Physical Sciences, National Academies of Sciences, Engineering, and Medicine, *Decrypting the Encryption Debate: A Framework for Decision Makers*, 2018, available at https://www.nap.edu/catalog/25010/decrypting-the-encryption-debate-a-framework-for-decision-makers.

[2] Ibid, p. 2.

approach. Here we examine Ozzie's approach using the NAS study's framework.[3] We begin by briefly describing the proposed approach.

The CLEAR Approach

Ozzie's CLEAR proposal is for a device's disk-encryption key to be encrypted by the public-key of the device's "vendor" and stored on the device outside of the normal, encrypted storage. Using a court order, law enforcement could obtain the wrapped key from the device, present it to the vendor for decryption, and then access the device's contents using the vendor-supplied disk-encryption key. Vendors would presumably store their private decryption keys in Hardware Security Modules (HSMs). Importantly, the proposal does not require shipping the device to the manufacturer for decryption.

When law enforcement wishes to unlock a phone, they take some action on the phone to make it display the wrapped key. When the vendor-supplied key is returned, the target phone unlocks itself, entering a mode where no more changes to its flash memory are possible. The phone's contents are thus preserved for forensic analysis, at the cost of effectively destroying the device.

1. **To what extent will the proposed approach be effective in permitting law enforcement and/or the intelligence community to access plaintext at or near the scale, timeliness, and reliability that proponents seek?**

CLEAR is not suitable for access to encrypted communications; it applies to only to devices. The approach should be scalable, but whether it is so depends on how vendor response centers are designed and staffed.

The CLEAR mechanism may be easily rendered useless by a phone owner who downloads an app to provide an additional layer of encryption to data stored on the phone.

2. **To what extent will the proposed approach affect the security of the type of data or device to which access would be required, as well as cybersecurity more broadly?**

The CLEAR approach is not a fully worked-out proposal; in particular, it is insufficiently complete enough to fully assess its risks. Absent more details, it is impossible to assess how likely it is that improper parties will make requests for exceptional access. International access, which seems likely, will greatly magnify the risks; see in particular the discussion of localization in Point 7 below. In addition, compromise of the vendor's CLEAR keys would make all phones produced by that vendor vulnerable to compromise by third parties.

There is a known "phone in the middle" attack that can be used by criminals to trick vendors into unlocking a target phone. More precisely, the perpetrators would induce law enforcement

[3] Ibid, pp. 68-72.

to attempt to open some other, specially prepared phone; the response from the vendor would in fact provide the information necessary to open the targeted phone[4].

Such a hack would work in organized crime scenarios and the like, but less so in situations of covert access such as a border search. That is because under CLEAR an unlocked phone is permanently "bricked"; this would tend to discourage covert or border access. Whether or not all of the data from an unlocked phone could be restored to a replacement phone (to fool its owner) is unclear.

3. To what extent will the proposed approach affect the privacy, civil liberties and human rights of targeted individuals and groups?

There are insufficient procedural details to make this determination. Any mechanism for providing government access to private data stored on phones is, however, susceptible to abuse by oppressive regimes.

4. To what extent will the proposed approach affect commerce, economic competitiveness, and innovation?

CLEAR poses two major risks to innovation and competitiveness. First, any new design by an innovator would have to incorporate suitable exceptional access mechanisms and provide for and staff a suitable response facility. If the law applies only to large companies, there is a disincentive to growth. It would also seriously penalize open source innovators: a product offering would have to be accompanied by an ongoing service.

Second, it is quite possible that certain innovative designs will be impossible to realize if an exceptional access requirement applies. Consider, for example, the incompatibility between the requirements of CALEA and the original, peer-to-peer, design of Skype.[5]

Third, there is an opportunity cost imposed by any technical mandate. Designing a secure, scalable, reliable CLEAR system would impose this cost on the device manufacturer. The product would either be delayed getting to market by the requirements or missing other features that could have been developed in the same time frame. More generally, cybersecurity experts employed to design, implement, and maintain CLEAR would not be available to work on other pressing cybersecurity problems relevant to both economic competitiveness and national security.

5. To what extent will financial costs be imposed by the proposed approach, and who will bear them?

---

[4] Eran Tromer, "Eran Tromer's Attack on Ray Ozzie's CLEAR Protocol," SMBlog, May 2, 2018, https://www.cs.columbia.edu/~smb/blog/2018-05/2018-05-02.html

[5] Steven M. Bellovin, Matt Blaze, Sandy Clark, and Susan Landau. Lawful hacking: Using existing vulnerabilities for wiretapping on the Internet. *Northwestern Journal of Technology & Intellectual Property*, 12(1), 2014, available at https://scholarlycommons.law.northwestern.edu/njtip/vol12/iss1/1/.

There are two principle costs to the CLEAR scheme: the cost of the targeted phone—it is permanently disabled by the exceptional access procedure—and the cost to the vendor of code design and of maintaining and operating the law enforcement exceptional access facility.

Most likely, the cost of replacing the targeted phone would have to be borne by law enforcement; to do otherwise would seem to run afoul of the Fifth Amendment.[6] The cost will, of course, vary by device, but it is likely to be several hundred dollars.

The operational cost for the vendor, however, is likely to be significant. Apart from the need to create, maintain, and replace HSMs, the largest cost is likely to be the authentication and authorization infrastructure, and associated legal staff. This will be similar to other such infrastructures; however, it will be world-wide, with the concomitant difficulties. Presumably, the cost will be amortized over exceptional access request; setting the price will be difficult, especially for international requests. The cost would be billed to law enforcement, similar to what is done today for wiretaps.[7] Those costs are high: in 2006, the cost to law enforcement for each CALEA tap was an average of $2,200.[8]

It is hard to assess the development cost. For CALEA, Congress appropriated $500 million dollars; this was not sufficient to convert all phone switches.[9] Carriers report costs in the millions for equipping post-1995 switches.[10] While mobile devices are significantly simpler than phone switches, there are many more architectures, and they change much more frequently. The costs borne by industry will result in less innovation; that could have harmful effects both economically and to national security (as a result of the Clinger-Cohen Act, the Department of Defense relies on heavily on COTS devices for information technology needs).

6. To what extent is the proposed approach consistent with existing law and other government priorities?

Many government agencies have warned of the importance of protecting data, especially when traveling abroad. CLEAR exposes devices to risk of compromise by other governments. Furthermore, to the extent that CLEAR is used internationally, it may undercut American stress on the rule of law, by enabling more mischief against their own citizens by authoritarian governments.

7. To what extent will the international context affect the proposed approach, and what will be the impact of the proposed approach internationally?

---

[6] "nor shall private property be taken for public use, without just compensation".
[7] 18 U.S.C. §2518(4)(e) ("Any provider of wire or electronic communication service, landlord, custodian or other person furnishing such facilities or technical assistance shall be compensated therefor by the applicant for reasonable expenses incurred in providing such facilities or assistance.")
[8] *The Implementation of the Communications Assistance for Law Enforcement Act,* U.S. Department of Justice, Office of the Inspector General, Audit Division, Audit Report 06-13 March 2006, p. 56, available at https://oig.justice.gov/reports/FBI/a0613/final.pdf.
[9] Susan Landau, *Surveillance or Security*, MIT Press, 2010, p. 84.
[10] *The Implementation of the Communications Assistance for Law Enforcement Act,* pp. 54-56.

If exceptional access is legislated into US law, it is all but certain that most other developed countries will insist on similar access. This, of course, includes countries that do not respect the rule of law in any way even vaguely similar to American standards. While the basic CLEAR scheme could easily be used for all countries' access, it seems likely that many countries will demand that unlocking facilities be located within their borders, similar to what they demand for personal data storage.[11] This will complicate the operational issues and greatly magnify the security risks.

A complete analysis of the internationalization implications would be quite lengthy. Some obvious issues are protection of the vendor's private CLEAR keys, which keys would be stored in which countries, who would operate the centers in assorted countries, verifying the authenticity and authorization of unlock requests from other countries, and securing cooperation from another country's unlocking centers when one of the phones for which they have access needs to be unlocked within the U.S.

The CLEAR scheme is not applicable to any data communications.

Conclusions:

It is clear from this evaluation that Ozzie's approach is a sketch of an idea, not a fully fledged proposal. In that sense, it is impossible to answer the framework's questions; most of the answers are "It is impossible to determine." Given that level of uncertainty, we conclude that it would be foolish to proceed with a legislative solution based on the Ozzie approach. It is of course possible—though to us, not plausible—that a solution based on the approach could be achieved without too great a risk to security of devices that are not legitimately targeted. But more study, and far more details, would be needed before the tradeoffs on risks could be determined. Right now, there is simply no there there.

[11] See, e.g., Sophia Yan, "China's new cybersecurity law takes effect today, and many are confused", *CNBC*, May 31, 2017, available at https://www.cnbc.com/2017/05/31/chinas-new-cybersecurity-law-takes-effect-today.html, or Ben Knight, "German data storage laws 'threaten free trade'", *Deutsche Welle*, December 1, 2017, available at http://www.dw.com/en/german-data-storage-laws-threaten-free-trade/a-37110699.