Encryption and Surveillance: Why the "Exceptional-Access" Question Won't Just Go Away

Joan Feigenbaum
Yale University
http://www.cs.yale.edu/homes/jf/

Boston University; October 10, 2018

What is the "Exceptional-Access" Question?

- 1990's "Crypto War" Redux
  - US Government: Cold-war era strong-encryption technology should only be fully deregulated if vendors provided "key escrow" features.
  - (Most) Technologists and civil-liberties advocates: Key escrow is hard to implement securely and would give an advantage to foreign competitors of US technology companies.
  - Opponents of key escrow won this war.

What is the "Exceptional-Access" Question?

- 1990's "Crypto War" Redux
  - US Government: Cold-war era strong-encryption technology should only be fully deregulated if vendors provided "key escrow" features.
  - (Most) Technologists and civil-liberties advocates: Key escrow is hard to implement securely and would give an advantage to foreign competitors of US technology companies.
  - Opponents of key escrow won this war.

- 2010's: Tech industry reacts to the Snowden revelations.
  - Broader and deeper use of E2E encryption, often by default, and often in a manner that prevents even the vendor from decrypting without the user's passcode.
  - Law enforcement (LE) claims that it is "going dark." It calls upon vendors to implement "exceptional-access" features to **enable decryption by LE with a duly authorized warrant but without the user's passcode.**
  - Vendors object, saying that EA would hurt customers' security and privacy.

What is the "Exceptional-Access" Question?

- 1990's "Crypto War" Redux
  - US Government: Cold-war era strong-encryption technology should only be fully deregulated if vendors provided "key escrow" features.
  - (Most) Technologists and civil-liberties advocates: Key escrow is hard to implement securely and would give an advantage to foreign competitors of US technology companies.
  - Opponents of key escrow won this war.

- 2010's: Tech industry reacts to the Snowden revelations.
  - Broader and deeper use of E2E encryption, often by default, and often in a manner that prevents even the vendor from decrypting without the user's passcode.
  - Law enforcement (LE) claims that it is "going dark." It calls upon vendors to implement "exceptional-access" features to **enable decryption by LE with a duly authorized warrant but without the user's passcode.**
  - Vendors object, saying that EA would hurt customers' security and privacy.

- (Perfect) example: FBI vs. Apple (2016)

James Comey (2014)

"Those charged with protecting our people aren't always able to access the evidence we need to prosecute crime and prevent terrorism even with lawful authority. We have the legal authority to intercept and access communications and information pursuant to court order, but we often lack the technical ability to do so."

Tim Cook (2016)

"The government is asking Apple to hack our own users and undermine decades of security advancements that protect our customers — including tens of millions of American citizens — from sophisticated hackers and cybercriminals. … We can find no precedent for an American company being forced to expose its customers to a greater risk of attack."

Terminological point: ~~"Exceptional Access"~~

- The term "exceptional access" makes it sound as though these access features are to be bolted on to an existing design as "exceptions."
- It was chosen "to stress that the situation is *not one that was included within the intended bounds of the original transaction* but is an unusual subsequent event" [NA+18] (emphasis mine). "Intended bounds of the original transaction" is not a standard term of art.
- If these access features are to be provided, they must be carefully designed and built in from the beginning, not bolted on at the end as exceptions.

Terminological point: ~~"Exceptional Access"~~

- The term "exceptional access" makes it sound as though these access features are to be bolted on to an existing design as "exceptions."
- It was chosen "to stress that the situation is *not one that was included within the intended bounds of the original transaction* but is an unusual subsequent event" [NA+18] (emphasis mine). "Intended bounds of the original transaction" is not a standard term of art.
- If these access features are to be provided, they must be carefully designed and built in from the beginning, not bolted on at the end as exceptions.

⇒ I use the term **law-enforcement access (LEA).**

Pro-LEA Side of the E+S *Policy* Debate

- The technology industry's post-Snowden embrace of default encryption is willfully thwarting the *lawful* exercise of properly authorized warrants and court orders.
- Individuals and organizations are obligated, under the All Writs Act in the US and similar laws in other democratic countries, to provide necessary assistance to government agencies in the execution of warrants.

> 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 of and principles of law."

- This position is fleshed out and explained well by Hennessey and Wittes [HW16].

Anti-LEA Side of the Policy Debate

- This is the argument made by many technologists and civil-liberties advocates. This side does ***not*** deny that E2E, default encryption hampers legitimate LE activity to some extent. But …

Anti-LEA Side of the Policy Debate

- This is the argument made by many technologists and civil-liberties advocates. This side does ***not*** deny that E2E, default encryption hampers legitimate LE activity to some extent. But …
- Since 9-11, there has been far too much mass surveillance. The best grass-roots response is mass encryption.

Anti-LEA Side of the Policy Debate

- This is the argument made by many technologists and civil-liberties advocates. This side does ***not*** deny that E2E, default encryption hampers legitimate LE activity to some extent. But …
- Since 9-11, there has been far too much mass surveillance. The best grass-roots response is mass encryption.
- 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.

Anti-LEA Side of the Policy Debate

- This is the argument made by many technologists and civil-liberties advocates. This side does ***not*** deny that E2E, default encryption hampers legitimate LE activity to some extent. But …
- Since 9-11, there has been far too much mass surveillance. The best grass-roots response is mass encryption.
- 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 1990's crypto war, foreign competitors could gain an advantage if US technology vendors are required to build in access capabilities for use by the ***US*** LE community.

Anti-LEA Side of the Policy Debate

- This is the argument made by many technologists and civil-liberties advocates. This side does ***not*** deny that E2E, default encryption hampers legitimate LE activity to some extent. But …
- Since 9-11, there has been far too much mass surveillance. The best grass-roots response is mass encryption.
- 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 1990's crypto war, foreign competitors could gain an advantage if US technology vendors are required to build in access capabilities for use by the ***US*** LE community.
- The ***extent*** of cooperation required by the All Writs Act is unclear.
- This is the position taken by, e.g., Schneier and Landau in their individual statements in [ZO+16].

Anti-LEA Side of the E+S *Technical* Debate (1)

- LEA features may create unacceptable cybersecurity risk. ***Once a technical capability is built into a system, there is always a risk that it will be misused*** – sometimes by the very criminals that it was designed to thwart.
- Classic example: the Vodaphone Greece scandal. The Greek government contracted with Vodaphone to build a phone system that had a wiretapping capability mandated by US Law. Hackers broke into the system and used the wiretapping feature to eavesdrop on the Greek government.

Anti-LEA Side of the E+S *Technical* Debate (2)

- LE has not quantified the extent to which default encryption hinders it.

Anti-LEA Side of the E+S *Technical* Debate (2)

- LE has not quantified the extent to which default encryption hinders it.
- LE often has other means of obtaining the information it needs, *e.g.*:
  - Back-up copies decryptable by cloud-service providers or corporate key-escrow systems
  - Sensitive data collected in plaintext form by ad-supported platform services
  - Vulnerability-based unlocking toolkits (the anti-climactic end to FBI vs. Apple) [BB+18]

Anti-LEA Side of the E+S *Technical* Debate (2)

- LE has not quantified the extent to which default encryption hinders it.
- LE often has other means of obtaining the information it needs, *e.g.*:
  - Back-up copies decryptable by cloud-service providers or corporate key-escrow systems
  - Sensitive data collected in plaintext form by ad-supported platform services
  - Vulnerability-based unlocking toolkits (the anti-climactic end to FBI vs. Apple) [BB+18]
- LE has not precisely specified the requirements that an LEA system must satisfy. For example, it has not explained:
  - Which surveillance tasks does LE expect to accomplish despite default encryption?
  - How will LEA technology interact with legal processes? There are more than 15,000 police departments in the US. Will they all have access to this technology?
  - Will US technology vendors cooperate not only with US LE agencies but with those in all countries in which their products are sold (including dictatorships)? If not, why won't criminals just buy their devices in countries with whom vendors don't cooperate?

Anti-LEA Side of the E+S *Technical* Debate (2)

- LE has not quantified the extent to which default encryption hinders it.
- LE often has other means of obtaining the information it needs, *e.g.*:
  - Back-up copies decryptable by cloud-service providers or corporate key-escrow systems
  - Sensitive data collected in plaintext form by ad-supported platform services
  - Vulnerability-based unlocking toolkits (the anti-climactic end to FBI vs. Apple) [BB+18]
- LE has not precisely specified the requirements that an LEA system must satisfy. For example, it has not explained:
  - Which surveillance tasks does LE expect to accomplish despite default encryption?
  - How will LEA technology interact with legal processes? There are more than 15,000 police departments in the US. Will they all have access to this technology?
  - Will US technology vendors cooperate not only with US LE agencies but with those in all countries in which their products are sold (including dictatorships)? If not, why won't criminals just buy their devices in countries with whom vendors don't cooperate?
- These arguments are given in, e.g., [AA+15, NA+18, ZO+16]. A framework for evaluating proposed LEA designs in given in [NA+18].

Technical Ideas for LEA Features (1)

- High-level ideas. No fully specified proposals yet.
- Most target the design of devices that can be unlocked, with manufacturer's cooperation, by LE agents who have physical possession of the device and a valid warrant (but not user's passcode).

Technical Ideas for LEA Features (1)

- High-level ideas. No fully specified proposals yet.
- Most target the design of devices that can be unlocked, with manufacturer's cooperation, by LE agents who have physical possession of the device and a valid warrant (but not user's passcode).
- Best known idea is due to Ozzie:
  - Device's encryption key is stored on the device, encrypted under a manufacturer's key.
  - An LE agent in possession of the device, with 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.
  - A device that is unlocked without the passcode "bricks" itself (tamper-evidence).

Technical Ideas for LEA Features (1)

- High-level ideas. No fully specified proposals yet.
- Most target the design of devices that can be unlocked, with manufacturer's cooperation, by LE agents who have physical possession of the device and a valid warrant (but not user's passcode).
- Best known idea is due to Ozzie:
  - Device's encryption key is stored on the device, encrypted under a manufacturer's key.
  - An LE agent in possession of the device, with 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.
  - A device that is unlocked without the passcode "bricks" itself (tamper-evidence).
- Flaws were quickly found in Ozzie's scheme [BB+18]. It's not yet clear whether the basic idea can be built into a sound, fully specified scheme.
- Related ideas due to Brickell, Savage, and Tait were presented at an Encryption and Surveillance Workshop at Crypto'18.

Technical Ideas for LEA Features (2)

- Different approach due to Wright and Varia [WV18].
- Not restricted to unlocking devices without users' passcodes. Enables the decryption of *a limited number of ciphertexts*, which can be found in any system or application.

Technical Ideas for LEA Features (2)

- Different approach due to Wright and Varia [WV18].
- Not restricted to unlocking devices without users' passcodes. Enables the decryption of *a limited number of ciphertexts*, which can be found in any system or application.
- Deploy cryptosystems in which the key space has less than maximum entropy.
  A very well resourced attacker can then:
  - Perform an extremely expensive (approx. $100M to $3B) upfront computation to narrow down the key space ("abrasion").
  - Perform a limited number of moderately expensive (approx. $1K to $1M per message) brute-force searches for the keys needed to decrypt specific, targeted messages ("crumpling").

Technical Ideas for LEA Features (2)

- Different approach due to Wright and Varia [WV18].
- Not restricted to unlocking devices without users' passcodes. Enables the decryption of *a limited number of ciphertexts*, which can be found in any system or application.
- Deploy cryptosystems in which the key space has less than maximum entropy.
  A very well resourced attacker can then:
  - Perform an extremely expensive (approx. $100M to $3B) upfront computation to narrow down the key space ("abrasion").
  - Perform a limited number of moderately expensive (approx. $1K to $1M per message) brute-force searches for the keys needed to decrypt specific, targeted messages ("crumpling").
- The "well resourced attacker" does ***not*** need to be an LE agency (much less a US LE agency). This is (intentionally) not a NOBUS approach.

Technical Ideas for LEA Features (2)

- Different approach due to Wright and Varia [WV18].
- Not restricted to unlocking devices without users' passcodes. Enables the decryption of *a limited number of ciphertexts*, which can be found in any system or application.
- Deploy cryptosystems in which the key space has less than maximum entropy.
  A very well resourced attacker can then:
  - Perform an extremely expensive (approx. $100M to $3B) upfront computation to narrow down the key space ("abrasion").
  - Perform a limited number of moderately expensive (approx. $1K to $1M per message) brute-force searches for the keys needed to decrypt specific, targeted messages ("crumpling").
- The "well resourced attacker" does ***not*** need to be an LE agency (much less a US LE agency). This is (intentionally) not a NOBUS approach.
- This approach does not require LE to cooperate with device manufacturers or secure-protocol developers in order to decrypt the targeted ciphertexts. It uses only simple, lightweight constructions that can be woven into existing protocols and applications.

My Position in the LEA "Debate"

- Don't implement LEA at this time.
- The arguments in [AA+15, NA+18, ZO+16] are persuasive, especially:
  - Lack of agreed-upon technical requirements: Until we know exactly what LE wants, we can't know whether it's technically feasible and cost-effective.
  - We don't yet have a fully specified LEA proposal to evaluate, build, and test.
  - Availability of alternatives to LEA
- [LEA might also just be a bad idea on principle.]

My Position in the LEA "Debate"

- Don't implement LEA at this time.
- The arguments in [AA+15, NA+18, ZO+16] are persuasive, especially:
  - Lack of agreed-upon technical requirements: Until we know exactly what LE wants, we can't know whether it's technically feasible and cost-effective.
  - We don't yet have a fully specified LEA proposal to evaluate, build, and test.
  - Availability of alternatives to LEA
- [LEA might also just be a bad idea on principle.]

- **But I also think that LEA deserves further study.**

The Status Quo is Unsatisfactory

Jonathan Zittrain (2016)

"I empathize with the idea that just how much government can learn about us should not depend on the cat and mouse game of technological measure and counter-measure. ... Ideally, a polity would carefully calibrate its legal authorities to permit access exactly and only where it comports with the imperatives of legitimate security."

The Status Quo is Unsatisfactory

- The Crypto research community should not be telling LE to:
  - Rely on the fact that there's lots of plaintext out there, or
  - Buy gray-hat hacking toolkits from Greyshift or Cellbrite or some other company that profits from unremediated bugs and might be selling those toolkits to bad actors.

Doing so is rank hypocrisy!

The Status Quo is Unsatisfactory

- The Crypto research community should not be telling LE to:
  - Rely on the fact that there's lots of plaintext out there, or
  - Buy gray-hat hacking toolkits from Greyshift or Cellbrite or some other company that profits from unremediated bugs and might be selling those toolkits to bad actors.

  Doing so is rank hypocrisy!

- Theory of cryptography may enable us to design a provably secure, cost-effective LEA scheme ***or to prove that no such scheme exists***.

“Just Say No” to LE Doesn’t Play Well

- The LEA question probably won’t just go away. The arguments for LEA still appeal to many people, some of whom had not even been born in the 1990’s when the crypto war was fought and won. The technological landscape has changed dramatically since the 1990’s, and it’s not clear what, if any, effect the changes have had on the feasibility and desirability of LEA.
- The tech industry’s assertion that it cannot or should not comply with LE requirements strikes many people as arrogant. Government regulates many products in the name of public safety. Why not iPhones or laptops?
- Even technically knowledgeable people do not see intuitively why LEA is infeasible.

Discussion

References (1)

[AA+15] H. Abelson, R. Anderson, S. Bellovin, J. Benaloh, M. Blaze, W. Diffie, J. Gilmore, M. Green, S. Landau, P. Neumann, R. Rivest, J. Schiller, B. Schneier, M. Specter, and D. Weitzner. "Keys under doormats: mandating insecurity by requiring government access to all data and communications," *Journal of Cybersecurity* **1:1** (2015), pp. 69-79.

[BB+18] S. Bellovin, M. Blaze, D. Boneh, S. Landua, and R. Rivest. "Op-ed: Ray Ozzie's crypto proposal—a dose of technical reality," *ars technica.* **https://arstechnica.com/information-technology/2018/05/op-ed-ray-ozzies-crypto-proposal-a-dose-of-technical-reality/**, May 7, 2018.

[FF17] J. Feigenbaum and B. Ford, "Multiple Objectives of Lawful-Surveillance Protocols," in *Proceedings of the 2017 International Workshop on Security Protocols* (Cambridge SPW).

[FP+18] J. Frankle, S. Park, D. Shaar, D. Weitzner, and S. Goldwasser, "Practical Accountability of Secret Processes," in *Proceedings of the 2018 USENIX Security Symposium*.

References (2)

[FW18] J. Feigenbaum and D. Weitzner, "On the incommensurability of law and technical mechanisms: Or, what cryptography can't do," to appear in *Proceedings of the 2018 International Workshop on Security Protocols* (Cambridge SPW), **http://www.cs.yale.edu/homes/jf/5.1-weitzner-feigenbaum3.pdf**

[HW16] S. Hennessey and B. Wittes. "Apple is selling you a phone, not civil liberties," Lawfare. **https://lawfareblog.com/apple-selling-you-phone-not-civil-liberties**, Feb. 18, 2016.

[K14] S. Kamara, "Restructuring the NSA Metadata Program," in *Proceedings of the 2014 Workshop on Applied Homomorphic Cryptography*.

[KR+16] M. Kearns, A. Roth, Z. S. Wu, and G. Yaroslavtsev, "Private algorithms for the protected in social network search," *Proceedings of the National Academy of Sciences* **113(4)**, 913–918 (2016).

[KF+14] J. A. Kroll, E. W. Felten, and D. Boneh, "Secure protocols for accountable warrant execution." **http://www.cs.princeton.edu/~felten/warrant-paper.pdf** (2014)

References (3)

[NA+18] National Academies of Sciences, Engineering, and Medicine. 2018. **Decrypting the Encryption Debate: A Framework for Decision Makers.** Washington, DC: The National Academies Press. **https://doi.org/10.17266/25010**

[SF+16] A. Segal, J. Feigenbaum, and B. Ford, "Open, privacy-preserving protocols for lawful surveillance," **https://arxiv.org/abs/1607.03659**.

[WV18] C. Wright and M. Varia, "Crypto Crumple Zones: Enabling Limited Access without Mass Surveillance," in *Proceedings of the 3rd IEEE European Symposium on Security and Privacy*, IEEE Computer Society, 2018.

[ZO+16] J. Zittrain, M. Olsen, D. O'Brien, and B. Schneier. 2016. "Don't Panic: Making Progress on the `Going Dark' Debate." Berkman Center Research Publication 2016-1. **http://nrs.harvard.edu/urn-3:HUL.InstRepos:28552576**

High Country Bandits

2010 case – string of bank robberies in Arizona, Colorado

FBI intersection attack compared 3 cell-tower dumps totaling 150,000 users

- 1 number found in all 3 cell dumps – led to arrest
- 149,999 innocent users' information acquired

Privacy-Preserving, Surveillance

- Identify an unknown target but preserve privacy of untargeted users
  - Collect a large set of encrypted data records (on both targeted and untargeted users), use a cryptographic protocol to winnow it down to just the records of the targets, and then decrypt only those records.

Privacy-Preserving, Accountable Surveillance

- Identify an unknown target but preserve privacy of untargeted users
  - Collect a large set of encrypted data records (on both targeted and untargeted users), use a cryptographic protocol to winnow it down to just the records of the targets, and then decrypt only those records.
- Distributed trust
  - No one agency can compromise privacy.
- Enforced scope limiting
  - No overly broad group of users' data are captured.
- Sealing time and notification
  - After a finite, reasonable time, surveilled users are notified.
- Accountability
  - Surveillance statistics are maintained and audited.

Segal, Ford, & F. Solution in FOCI 2014

- **Privacy-preserving set intersection**
  - Implemented protocol is a variation of Vaidya and Clifton's "secure set-intersection cardinality" protocol [J. Computer Security, 2005].
  - One key technical ingredient is the *mutual commutativity* of the **ElGamal** and **Pohlig-Hellman** encryption schemes:

$$D_2(D_3(D_1(E_3(E_2(E_1(x)))))) = x$$

$$D_3(D_2(E_3(D_1(E_2(E_1(x)))))) = x$$

- **Efficient (offline) operation:** Completes 150,000-record instances in 10 minutes.

Related Work

- Kamara (2014) and Kroll, Felten, Boneh (2014)
  - Cryptographic protocols for privacy-preserving, accountable surveillance of **known** targets
- Kearns, Roth, Wu, Yaroslavtsev (2016)
  - Differentially private, graph-search algorithms for **distinguishing targeted users from untargeted users**
- Segal, Feigenbaum, Ford (2016)
  - Privacy-preserving, accountable **contact chaining through encrypted phone records to identify unknown targets** (same privacy and accountability goals as "bandits," different algorithm)
- Frankle, Park, Shaar, Weitzner, Goldwasser (2018)
  - Cryptographic protocols for accountability in **secret government processes**.

- Support from DARPA and IARPA (since ~ 2011)

Wide Range of Objections

- "Evil": We (crypto researchers) should aim for "no surveillance."
- "Won't work"
  - LE and IC won't accept distributed trust, scope limits, etc.
  - FISA is not an "open" legal process, and FISC won't set meaningful limits or allow notification of targets or statistical reporting.
- "Exotic protocols" can't be used for these purposes.
  - People who seek warrants won't know when these techniques are applicable, won't set appropriate parameters, and won't interpret results correctly.
  - SMPC and similar protocols are too hard to implement and deploy.
- "Function drag"
- "Don't give aid and comfort to the enemy"
  - Justification for bulk collection of encrypted data might be morphed into a justification to backdoor all crypto protocols (because of malice or ignorance).

Refutations of all objections in [FF17]

- "Technological unilateralism" doesn't play well.

- People (even those who don't want to be snooped on) expect their governments to catch bad guys.
  - **There is strong support for bulk collection and mining of communications data for the purpose of identifying bad guys.**
  - **There is strong support for protection of citizens' privacy.**
  - **➔ Use privacy-preserving computational techniques to reduce the tension between these two goals.**