Lawful Access: A Survey of Proposed Protocols

Ramla Ijaz
CPSC 610: Topics in Computer Science and Law
May 14, 2021

Introduction

Lawful Access (LA) is the ability of law enforcement to gain access to select decrypted communications. Other works have referred to this ability as exceptional access, but the word choice clarifies the circumstances under which such a mechanism should be used, as well as its limitations. Lawful access implies that access to decrypted information should only be done through legal means, with a court-approved warrant. Implicit in this term is the idea that any request to access information will go through the legal system, and thus prevent abuse. Replacing the term exceptional access also makes clear that such a mechanism, if it exists, does not ensure rare and isolated access, since a backdoor mechanism once created will be there for anyone to use. Rather, it's the safeguards put in place by the law that will prevent abuse.

Balancing personal privacy with national security is long sought-after goal. The debate between encryption advocates and law enforcement has been ongoing for decades. This paper aims to add clarity to that debate by surveying LA proposals from the nineties till now. We believe that informing policy makers of *(i)* what is cryptographically possible and *(ii)* what specific policy decisions need to be explored will help to create a more productive conversation.

Background

Relevant history of LA goes back to the 90's, when the transition to digital communication was starting and the US government was worried about their ability to wiretap a digital switched network. They passed the Communications Assistance for Law Enforcement Act (CALEA) which required telecommunication companies to assist the federal government in wiretapping. In the same decade, concerns about cryptography on these networks rose, and the U.S. government tried to enforce the use of key escrow, a LA mechanism in which encryption keys are stored by a third-party that is receptive to government warrants. This effort culminated in Clipper, an NSA-developed encryption chip which would encode each session key in a Law Enforcement Access Field (LEAF) that was transmitted along with regular communications. Researchers discovered weaknesses within Clipper and the effort failed [1].

During this time, there was a very active debate occurring about the role of cryptography in digital communications concerning key escrow as well as the export of strong encryption on American technologies. The research community was active in proposing multiple LA protocols related to the idea of key escrow, though there was eventually consensus on the difficulty of implementing such a protocol [2]. Many of the groups against the Clipper chip also lobbied against encryption export controls, and eventually US policy changed to allow companies to export products with strong encryption [3]. The effect of these decisions in nineties has led to the prevalent use of strong encryption we see today.

Strong End-to-End Encryption (E2EE) has allowed the digital world to grow; many services and businesses have an online presence. Such standard use of the digital web for communication and transactions has been made possible through E2EE. While this should be celebrated, there are valid concerns related to illegal content that can no longer be monitored by law enforcement. In 2008, the FBI director labelled this lack of law enforcement access to plaintext messages as the “going dark” problem [4]. It was later though that the use of E2EE was brought into the public consciousness when the Snowden NSA leaks revealed extensive government wiretapping of US citizens. Tech companies began to advertise E2EE as a feature of their products while law enforcement doubled down on their right to access plaintext with the “nothing to hide, nothing to lose argument” [5].

This is where we are today, with the debate on LA ongoing. Many in the research community understand the possible harmful effects of LA, but also that doing nothing may be worse. There is an idea that something should be done to inform the wider public and legislators about technical solutions before any law is made with seen and unforeseen side effects. This viewpoint is validated by proposal of the EARN IT act, which many people have framed as an attack on encryption. There have been new LA proposals being put forward. This project is a way to analyze them and make recommendations about the questions that still need to be answered.

Concerns Related to Lawful Access

Supporters of LA make valid arguments that E2EE is exploited by bad actors to hide illegal communication. These can include child exploitation, terrorism, and fraud. There is no disagreement that law enforcement should expend resources, and companies should help, in capturing these criminals. The debate comes when people must start paying for increased security with their personal privacy and civil liberties. There must be a tradeoff between the two, the question is where the right balance lies. Opponents of LA, as well as proponents, realize there are multiple areas of concern if we are to implement a LA policy. They include:

1. Mass surveillance: How do we trust law enforcement to not abuse its power and use the LA mechanism to spy on a large amount of people?
2. Individual abuse: How do we prevent rogue individuals from taking advantage of LA?
3. Institutional abuse: How do we ensure that a government institution or manufacturer doesn’t start using LA for their own purposes?
4. Introducing vulnerabilities in systems: Once a backdoor is added to a system, then it is available for all attackers to use, not just law enforcement. This has happened

multiple times already with hackers installing illegal software in Vodafone Greece's switches, and the wiretapping of thousands of Italians through Telecom Italia [6] [7].

5. Cost of adding LA: Adding a backdoor could increase the manufacturing cost of communication devices and become economically infeasible.
6. Security of encryption keys: In the case of key escrow, can we be sure that keys can't be stolen or hacked?
7. Global effect of a LA system: Creating an ethical LA mechanism may give less democratic countries an excuse to create their own abusive LA mechanism.
8. Effect of LA on other parts of the law: The existence of LA may affect other parts of the law such as compelled decryption [8].

As we review multiple LA proposals, we will see how each proposal tries to address some concerns, but no proposal manages to address all.

Dimensions of Comparison for Lawful Access Proposals

Each LA proposal can be compared along multiple dimensions. One of the main differentiations between proposals is where the data is physically located that needs to be decrypted. Usually, it can be in one of three places: *(i)* a personal device, *(ii)* real-time communications, and *(iii)* third-party records like those stored in a data center or with telecommunication providers. Another dimension along which we compare LA proposals is the Trusted Entity Base (TEB), which we define as the set of entities that are vested with different amounts of trust to ensure the LA mechanism is used only in the specified way. The TEB could include just law enforcement or many different entities where none is trusted in isolation. The third dimension is how effective the protocol is in preventing mass surveillance. LA mechanisms sometimes use one or a combination of different techniques to ensure the high cost of decrypting a single message. The last dimension that we look at is practicality. In other words, how easy would it be to put the proposal into practice. In the next section we survey multiple LA proposals and discuss them along these dimensions.

Classification and Examples of Lawful Access Proposals

LA proposals fall into the following categories: key escrow, breakable encryption, client-side computation, lawful hacking, and self-escrow. We discuss these categories and give examples of works that fall in each.

The first category of LA proposals is key escrow. *Full key escrow* schemes store the user's encryption key with the government or a government-trusted third party. Different variations are *split key escrow* where a key can be divided into *n* parts and stored with *n* different entities and *partial key escrow* where part of the key is recovered from an escrow agent and part must be computed. Both variations attempt to impart an increased cost to key recovery. Most other proposals build on these three variations.

Oblivious key escrow is a type of split key escrow where the key is split across multiple computers on the internet. Key retrieval occurs as a broadcast request, so a LA request can never be hidden [9]. This type of key escrow adds a social cost to key retrieval and expects that the random computers that become escrow agents will follow the policy for key retrieval. *Privategrity* is a messaging application recently proposed by David Chaum, a pioneer in anonymous online communication, that is also a type of split key escrow [10]. Chaum proposes splitting the key between nine servers located in nine different democratic countries, though he gives no justification for why this number was chosen.

Another type of key escrow is *encapsulated key escrow*. This is a type of partial key escrow where the portion of the key that has to be computed is placed in a verifiable cryptographic time capsule, thus preventing early recovery attacks where law enforcement computes the missing key before the warrant is issued [11] [12]. Recent work on *crypto crumple zones* also presents a way to introduce computational cost into key recovery [13]. The authors presented two cryptographic puzzles that can be embedded into the generation of every session key in any encryption system, e.g. messaging apps or filesystem encryption. These puzzles can be tuned to ensure that a significant amount of cost will be incurred for every key recovered.

Other proposals in the real-time communication context are client-side computation and lawful hacking. Client-side computation performs hash matching of user message contents with a database of illegal material on the client's device. This contrasts with hash matching techniques currently in use by industry where the image scanning is done after client data is uploaded to a server, e.g. PhotoDNA [14]. There is precedent for moving image classification to a personal device to preserve user privacy [15]. For LA we also want to protect server privacy so that criminals cannot access the database contents and manipulate the system. There have been proposals like *privacy-preserving perceptual hash-matching* that ensure both client and server privacy using cryptographic primitives like homomorphic encryption and privacy-preserving comparison, but these proposals require a user to have a high level of trust in the service provider and can be computationally expensive [16] [17].

Lawful hacking is already in use by governments around the world to exploit existing vulnerabilities to hack into devices. The hacks can be used to unlock a personal device or to install software that can obtain copies of real-time communication. A prominent case was in 2016 when the FBI requested that Apple unlock the iPhone of a suspected shooter. Apple objected and the case went to court [18]. Before it could be resolved the FBI unlocked the iPhone using an OS vulnerability. Proponents of lawful hacking make the case that complex software systems will inherently have some vulnerabilities that will take time to discover and patch; the average time to public disclosure of a vulnerability is 312 days [19]. Rather than deliberately introducing weaknesses, governments should just take advantage of ones that are already present. Opponents question the appropriateness of governments taking part in this market and if it leads to fewer bugs being reported. System researchers are also continuously trying to build more systems with verified, bug-free software. Common vulnerabilities like buffer overflows and read-after-free will soon be eliminated using performant, memory-safe programming languages [20]. So, while lawful hacking is a short-term solution, there is evidence to suggest it might become more difficult to use.

The last category of LA proposals is self-escrow. Unlike key escrow, the encryption key is not stored with a third party, rather within the device itself. Self-escrow LA always takes place in the context of a personal device that law enforcement has within its possession. A group of self-escrow proposals rely on device manufactures as a trusted third-party. *CLEAR* is a proposal which requires all phones to encrypt a copy of their passcode with a manufacturer public key that law enforcement can later provide to the manufacturers with a warrant [21]. Manufacturers can then decrypt the passcode with their private key. The argument here is that manufacturers like Apple already have a secret key which they use to sign software updates. Another work also proposes a self-escrow scheme but puts in other safeguards to prevent mass surveillance like a time-vaulting requirement (the device must be in the physical possession of law enforcement for a certain amount of time) and per-device authorization keys [22].

Critiques of putting too much trust in one entity like the government or device manufacturer has led to the proposal of *cryptographic envelopes*; a session key can be encrypted in multiple layers of encryption using the public keys of different entities like the branches of government, device manufacturers and civil rights organizations [23]. All entities must agree to decrypt the key before it can be recovered. Another proposal, *Judge, Jury and Encryptioner*, adds a social cost to LA by requiring law enforcement to physically access a set of peer devices that are chosen by the locked device, in addition to obtaining approval for a warrant from a set of custodians [24]. Like oblivious key escrow, this scheme assumes that when normal citizens' devices are involved, it becomes hard for law enforcement to hide the frequency of its LA requests. Too many requests could lead to a backlash from the public.

Practical Limitations of Lawful Access Proposals

The LA proposals we've discussed have put forward many ways to add a procedural, computational, monetary, or social cost to limit mass surveillance. Unfortunately, besides for lawful hacking which is already in use, the proposals have many practical limitations. Some of those limitations are technical and some are due to lack of clear policy.

A prominent technical limitation for both key escrow and self-escrow is the safety of the session keys or the device manufacturer keys. Manufacturer keys leak and datacenters are not necessarily secure [25]. Setting a random number of datacenters where parts of a key will be stored may make them harder to steal but not impossible. Many works also rely on a secure enclave processor; a truly secure processor does not exist, yet [25].

Then we have the policy related questions that have not been answered. The first is how do we get cooperation from the device manufacturers (for self-escrow) or from users. The proposals that have a social cost involve ordinary citizens as a check against government abuse. Many citizens find the rare jury duty a hefty task, would they really be comfortable being involved in law enforcement’s requests for access? In addition, what would be the incentive for users to join a messaging service where they know LA can occur when there are other options? A government could mandate that all applications provide that backdoor, but how realistic is that? And what would be the effect on innovation and new application development?

A prominent suggestion to prevent mass surveillance is to include multiple entities in the LA protocol whether through split key escrow or cryptographic envelopes. On paper this seems like a great idea but when we get into the details there are many issues. Which and how many entities? If there are too many then no request will be accepted. If there are too few and too cooperative, then mass surveillance could occur. How can we be sure there that each entity is truly independent? I don’t have these answers and to be fair, we cannot expect systems researchers or cryptographers to answer these questions. These are questions for a policy debate that must take place before any LA proposal is seriously considered.

Relevant Areas Related to Lawful Access

The policy debate on LA access can be enriched by information on other areas of research. One such area is secure warrant execution. Researchers have put forward ways in which cryptographic primitives can be used to ensure that warrants for private data are only executed in a secure and accountable manner so that private data is not compromised, and the system cannot be abused by any party [26]. There have also been proposals to ensure government only accesses relevant data when it requests records from third parties, rather than gaining access to a huge data dump [27]. Perhaps a place to start in the LA debate is to bring cryptographic primitives to our legal system, to the warrants and law enforcement access that already take place. If these can be incorporated into our society, people may increase trust in the government because it can be audited by civil-rights groups and there is no way for law enforcement to bypass protocols. Then the LA discussion can go forward in a less hostile environment.

The Current Policy Debate

There have been two recent pieces of legislation put forward related to the use of E2EE. The Eliminating Abusive and Rampant Neglect of Interactive Technologies (EARN IT) Act of 2020 proposes to remove section 230 protections from companies unless they comply with best practices to prevent child sexual exploitation. Many encryption advocates opposed the bill even in its revised form, since the best practices could make it compulsory for companies to use technologies like key escrow or client-side computation, which we have already discussed as being unsafe [28].

The second is the Lawful Access to Encrypted Data (LAED) Act introduced in June 2020, again by Senator Lindsey Graham. Unlike the EARN IT act, the LAED act explicitly goes after E2EE, and requires that companies provide the government with access to encrypted communications. The LAED act has been framed by opponents as a way to make the EARN IT act seem more acceptable [29].

There is reason to be suspicious of the timing of the two laws, since they were both introduced in an election year when the role of tech giants in our society was being discussed. I do not believe these two proposals indicate that any LA proposal is seriously being considered, just that we are approaching a more nuanced understanding of our relationship with social media companies. I would argue that people who would like to see regulation from the government on content moderation would not necessarily want the government to ban E2EE. There is concern that these two issues will be conflated and the current debate on content moderation will be used to pressurize technology companies to reverse their stance on E2EE.

Conclusion

The biggest change in environment from the crypto-wars of the 90's is the presence of technology giants that act as surveillance intermediaries, companies that control majority of our communications and that the government relies on for access to our data [30]. New proposals have tried to take advantage of them as obvious candidates for key escrow and integrated them as part of LA protocols. Many techniques used in older key escrow schemes like computational costs, inclusion of citizens for transparency, and multiple warrant-approving entities are still being proposed today, but the questions that were raised then remain unanswered.

I believe there needs to be a good understanding of cryptographic primitives and the requirements of law enforcement, as well as answers to many policy questions. Only then can an actual prototype be implemented, evaluated, and critiqued. Without these steps the LA debate will be stuck in the same deadlock it has been in for the past two decades. The research community has, I believe, done a decent job of putting forward cryptographic primitives that can be used for LA. The weakness of their proposals lies in the policy debate which they do not have answers for. If the government is serious about LA, the next step should be to start a discussion with policy institutes and technology companies about overcoming the practical limitations of LA proposals. Only then can we reach the next step of the LA debate.

Works Cited

[1] M. Blaze, "Protocol failure in the escrowed encryption standard," in *Proceedings of the 2nd ACM Conference on Computer and Communications Security*, 1994.

[2] H. Abelson, R. Anderson, S. M. Bellovin, J. Benaloh, M. Blaze, W. Diffie, J. Gilmore, M. Green, S. Landau, P. G. Neumann and others, "Keys under doormats: mandating insecurity by requiring government access to all data and communications," *Journal of Cybersecurity,* vol. 1, no. 1, pp. 69-79, 2015.

[3] "Doomed to Repeat History? Lessons from the Crypto Wars of the 1990s," [Online]. Available: https://www.newamerica.org/cybersecurity-initiative/policy-papers/doomed-to-repeat-history-lessons-from-the-crypto-wars-of-the-1990s/.

[4] " About Issues Our Work Take Action Tools Donate SEARCH FBI "Going Dark" FOIA Documents - Release 1, Part 1," [Online]. Available: https://www.eff.org/document/fbi-going-dark-foia-documents-release-1-part-1.

[5] I. N. Cofone, "Nothing to hide, but something to lose," *University of Toronto Law Journal,* vol. 70, no. 1, pp. 64-90, 2019.

[6] V. Prevelakis and D. Spinellis, "The Athens Affair," 2007. [Online]. Available: https://spectrum.ieee.org/telecom/security/the-athens-affair.

[7] EDRi, "Telecom Italia wiretapping scandal," 2006. [Online]. Available: https://edri.org/our-work/edrigramnumber4-15italy/.

[8] S. Scheffler and M. Varia, "Protecting Cryptography Against Compelled Self-Incrimination," *Usenix Security 2021,* 2021.

[9] M. Blaze, "Oblivious key escrow," in *International Workshop on Information Hiding*, 1996.

[10] A. Greenberg, "The Father of Online Anonymity Has a Plan to End the Crypto War," 2016. [Online]. Available: https://www.wired.com/2016/01/david-chaum-father-of-online-anonymity-plan-to-end-the-crypto-wars/.

[11] M. Bellare and S. Goldwasser, "Encapsulated key escrow," 1996.

[12] M. Bellare and S. Goldwasser, "Verifiable partial key escrow," *Proceedings of the 4th ACM Conference on Computer and Communications Security,* pp. 78-91, 1997.

[13] C. Wright and M. Varia, "Crypto crumple zones: Enabling limited access without mass surveillance," in *2018 IEEE European Symposium on Security and Privacy (EuroS&P)*, 2018.

[14] H. Farid, "Reining in online abuses," *Technology & Innovation,* vol. 19, no. 3, pp. 593-599, 2018.

[15] Apple, "Photos: Private, on-device technologies to browse and edit photos and videos on iOS and iPadOS," September 2019. [Online]. Available: https://www.apple.com/ios/photos/pdf/Photos_Tech_Brief_Sept_2019.pdf.

[16] A. Kulshrestha and J. Mayer, "Identifying Harmful Media in End-to-End Encrypted Communication: Efficient Private Membership Computation," in *30th USENIX Security Symposium (USENIX Security 21)*, 2021.

[17] M. Green, "Can end-to-end encrypted systems detect child sexual abuse imagery?," [Online]. Available: https://blog.cryptographyengineering.com/2019/12/08/on-client-side-media-scanning/.

[18] "Apple v. FBI," [Online]. Available: https://epic.org/amicus/crypto/apple/.

[19] L. Bilge and T. Dumitras, "Before we knew it: an empirical study of zero-day attacks in the real world," in *Proceedings of the 2012 ACM conference on Computer and communications security*, 2012.

[20] "Rust: A language empowering everyone to build reliable and efficient software.," [Online]. Available: https://www.rust-lang.org/.

[21] R. Ozzie, "CLEAR," 2017. [Online]. Available: https://github.com/rayozzie/clear/blob/master/clear-rozzie.pdf.

[22] S. Savage, "Lawful device access without mass surveillance risk: A technical design discussion," *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security,* pp. 1761-1774, 2018.

[23] M. Tait, "An Approach to James Comey's Technical Challenge," 2016. [Online]. Available: https://www.lawfareblog.com/approach-james-comeys-technical-challenge.

[24] S. Servan-Schreiber and A. Wheeler, "Judge, Jury & Encryptioner: Exceptional Device Access with a Social Cost," *arXiv preprint arXiv:1912.05620,* 2019.

[25] Green and Mathew, "A few thoughts on Ray Ozzie's “Clear” Proposal," 2018. [Online]. Available: https://blog.cryptographyengineering.com/2018/04/26/a-few-thoughts-on-ray-ozzies-clear-proposal/.

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

[27] A. Segal, B. Ford and J. Feigenbaum, "Catching bandits and only bandits: Privacy-preserving intersection warrants for lawful surveillance," in *4th USENIX Workshop on Free and Open Communications on the Internet*, 2014.

[28] H. Quay-de la Vallee and M. Azarmi, "The New EARN IT Act Still Threatens Encryption and Child Exploitation Prosecutions," 2020. [Online]. Available: https://cdt.org/insights/the-new-earn-it-act-still-threatens-encryption-and-child-exploitation-prosecutions/.

[29] R. Pfefferkorn, "THERE'S NOW AN EVEN WORSE ANTI-ENCRYPTION BILL THAN EARN IT. THAT DOESN'T MAKE THE EARN IT BILL OK.," 2020. [Online]. Available: https://cyberlaw.stanford.edu/blog/2020/06/there%E2%80%99s-now-even-worse-anti-encryption-bill-earn-it-doesn%E2%80%99t-make-earn-it-bill-ok.

[30] A. Z. Rozenshtein, "Surveillance intermediaries," *Stanford Law Review,* 2018.

[31] S. M. Bellovin, M. Blaze, S. Clark and S. Landau, "Going bright: Wiretapping without weakening communications infrastructure," *IEEE Security & Privacy,* vol. 11, no. 1, pp. 62-72, 2012.

[32] N. Tyagi, M. H. Mughees, T. Ristenpart and I. Miers, "Burnbox: Self-revocable encryption in a world of compelled access," in *27th USENIX Security Symposium (USENIX Security 18)*, 2018.