Analysis of Arguments For and Against Lawful Access of Data

Tyler Bontrager

December 2021

1 Table Of Contents

2 Abstract

In this work, we read extensively into the perspectives of Lawful Access, which is the idea that law enforcement agents ought to have access to data when a court order is issued. The issue that law enforcement agencies face nowadays is the common, yet very strong, encryption protocols featured in many popular communication apps. While this kind of encryption offers privacy that guarantees total confidentiality and minimal intrusion, it severely hinders law enforcement efforts to keep people safe as digital evidence becomes harder and harder to acquire.

We have designed a questionnaire to survey students on campus. This offered us valuable insights into the perspectives of a small subset of the student body with respect to privacy through curious questions about the nature and general usage of common communications apps, and the concept of Lawful Access via questions that gauged respondents' reactions to various hypothetical scenarios involving others having access to their private data.

Though the reach of our survey was limited, we were still surprised by the fact that privacy concerns were not as prevalent as the tension of the Lawful Access debate had suggested. Furthermore, the results of the survey revealed that the secure end-to-end encryption technology was quite unfamiliar to most respondents, which implies a general lack of awareness of modern day privacy-enhancing technologies.

3 Background

Lawful Access has become a hot topic in recent times, and was catalyzed by recent developments in data encryption technologies that are so secure that not even a court order can grant access to certain evidence. Some examples of this kind of encryption are end-to-end encryption and other OS-level encryption defaults found on iOS and Android devices. End-to-end encryption is technology that allows two devices to become the lock and key for all data transmitted between the two "ends," and Android and iOS operating systems encrypt all data on the device by default. Similar technology is available for hard drives on personal computers.

The Lawful Access debate boils down to the extent to which privacy is valued over public safety and vice versa. On one hand, everyone has the right to a standard of privacy in digital cyberspace such that it would be impossible for any unauthorized third-party to intrude on private affairs. On the other hand, this level of privacy may be applied to bad actors such that the third-party they are trying to avoid is law enforcement. In the present work, we will examine the different views of Lawful Access, its pros, and its cons.

3.1 History

The Lawful Access efforts started back before modern encryption technologies were invented.

The Clipper Chip and Key Escrow

The Clipper Chip[Mack, 2020, 21] was a device that was developed by the NSA and was encouraged to become the standard chipset in telecommunications. The Clipper Chip had a backdoor that the NSA could use to intercept encrypted transmissions if they had the lawful authority to do so. However, a researcher at AT&T found a serious vulnerability in the chip that discredited the integrity of the device and discouraged its further use[Blaze, 1994].

CALEA

The Communications Assistance for Law Enforcement Act is a law that allows law enforcement to eavesdrop on communications when it has the lawful authority to do so. When this law was introduced in 1994, it only applied to telecommunication companies. However, in 2004, it broadened its scope to apply to voice over IP (VoIP) communications provided by broadband internet service providers as well[Mack, 2020, 23]. With technologies like end-to-end encryption, this kind of surveillance would be impossible to perform, which is part of the reason why there is a push to grant the government more access to citizen's data.

3.2 Pros for Lawful Access

Exclusivity of Cybercrimes -

Cybercrimes are notoriously difficult in terms of the approach required to solve them: they all occur almost entirely in cyberspace, which means they will not tend to leave any physical evidence behind. Several examples include crimes like all kinds of fraud (identity theft, scams, counterfeiting, etc.), illegal hacking (unauthorized intrusions into systems), and child pornography production and distribution[FBI, 2001]. All of these crimes victimize people and cannot be solved easily by traditional investigative tactics. Thus, there should be a solution for this problem.

If the Lawful Access bill were to become public policy, then it would require all companies to implement some kind of mechanism by which law enforcement could access user data with lawful authority. This kind of access could immediately provide law enforcement with a trove of evidence against perpetrators of particularly heinous cyber crimes, and quickly put an end to further victimization. The Canadian government boasts a 90% conviction rate when evidence seized by "lawful interception" is presented in court[Government of Canada, 2021].

Justice for Victims -

A long thesis titled "The Key To Lawful Access"[Mack, 2020] brings up various case studies that support the proposal of Lawful Access. Mack discusses cases including child pornography and sexual exploitation in Florida and Manhattan, a 2015 homicide case in Baton Rouge, and mass shootings in Ohio (2019) and Texas (2017). He presents the argument that there are valid reasons to pursue information on encrypted devices, as they might contain information with "significant implications for an investigation, including bringing any co-conspirators to justice"[Mack, 2020, 59]. He argues that the debate of Lawful Access does not give adequate consideration to victims of crimes that the of which justice might be expedited because of law enforcement's ability to quickly gather evidence against perpetrators.

Access to Evidence -

In one case study offered by Mack, he talks about the benefit of having evidence extracted from encrypted devices. In 2019, a U.S. naval air station in Pensacola, Florida was attacked, and yet again the authorities managed to recover an encrypted device from the shooter. In May of 2020, the FBI successfully gained access to the device, and gathered enough intel to launch an operation against a co-conspirator, "weakening that member's cell"[Mack, 2020, 51].

It should be noted that this information was only learned because the authorities managed to gain access to the device. It would be fair to assume that without that information, the operation

would have not been possible. Data encrypted on personal devices will not be found anywhere besides the storage of the device, and it could be said that the data on one's encrypted device is harder to access than the evidence lying around in somebody's room.

Public Safety Concerns -

Perhaps the most important consideration in this debate is the value we place on public safety and national security. Should it be the case that crucial evidence be inaccessible to law enforcement even if there is a lawful authorization signed by a judge to obtain said evidence? Attorney General William P. Barr has said that "encryption should keep us safe and secure, not provide an impenetrable safe haven for predators, terrorists, and criminals"[Barr, 2020]. Unfortunately, thanks to the strong encryption technologies offered to us nowadays, bad actors can use it to undermine the efforts of law enforcement to keep the public safe.

Attorney General Barr acknowledges the American citizen's Fourth Amendment right to privacy, and made an analogy of advances in technologies to a scale tipping[Barr, 2019]: "When these advances tip the scales too far in favor of the Government, the response is to expand privacy protections. And when these advances threaten public safety by thwarting effective law enforcement, the response should be to preserve lawful access." He went on to say that data should be as secure as the safety of American citizens, and that solutions should be found that seek to prioritize both of these[Barr, 2020].

3.3 Cons against Lawful Access

Importance of Encryption -

Encryption has its benefits in the cyber-world as a means to ensure confidentiality of information sent over a network. The Internet is a vast network of networks which can easily leak information to unauthorized third-parties if websites are not carefully ensuring that their data stays secured. Encryption is a good way to secure said data.

Encryption becomes less significant and meaningful when we allow third-parties access to data that is supposed to be inaccessible to them. If there exists a way to break the encryption, then it does not matter whether permission must be gained in order to use the key from a cybersecurity perspective. For instance, we can see a commonly cited example of data being accessed without permission when we look at the Facebook–Cambridge Analytica scandal in 2018[Wagner, 2018]; political consultants gained access to millions of Facebook users because of a feature that allowed app developers to collect and use information with the consent of a subset of those users. Despite it being against Facebook's terms of service, the consultant gave a third party company access to the data without the consent of all of the users involved in the leak. Now, whether or not the law is in possession of such a key to be able to access all the data they want, the point of concern is not *who is in possession of such a key*, but rather *the fact that the key exists*. Regardless of whether the intruding entities are held accountable, the damages that leaks cause will be irreparable.

Importance of Privacy -

For the reason listed above, it is beneficial to consider means such as end-to-end encryption. This kind of encryption is completely secure by virtue of the fact that the encryption is managed

by the device itself. The sending device encrypts all data being transmitted while the recipient device is the only device allowed to decrypt the data to read it. While this poses a problem for law enforcement and their ability to access data on a device using end-to-end encryption, it is important to remember that this technology can prevent leaks of sensitive data that can threaten the safety of ordinary people. For example, there was an incident in Israel where hackers had illegally gained access to the database of an Israeli LGBTQ+ dating site, Atraf[staff et al., 2021], which contained very private data on individuals who were very concerned about being outed by the leak. This shows that this attack on Israeli LGBTQ+ people would have been easily avoided if Atraf simply had no access to the data itself given it would be encrypted.

Importance of Constitutional Rights -

There exists a clear power disparity between police and citizens, and we see too many instances of abuse of police power to carry out what authorities may call "enforcement of the law," but this is always ever one-sided and usually does not have the suspect's rights in mind. Despite having potentially incriminating evidence, there is no obligation for the owner of the locked device to unlock it for the police, nor should it be up to any tech companies to breach an individual's right to due process by the law and the right to decline to self-incriminate.

False arrests can occur where law enforcement decides that an arrest is necessary when it is not based on any probable cause, then proceed to find evidence of some violation of the penal code. The discovery of such evidence, and any arrest made on such grounds, would be based on an illegal search and seizure which would be a violation of the victim's constitutional rights.

Consider the case of Revat Vara of Houston in 2006: Vara was stopped for missing his car's front license plate, and arrested based on false testimony[Reilly and Nichols, 2019]. This prominent case demonstrates that abuse of law enforcement authority is a problem in the United States, as a USA Today investigation in 2019 found hundreds of false arrest incidents. Allowing police access to people's devices unhindered by encryption and other protective measures would only harm ordinary citizens.

Therefore, to protect individuals from illegal searches, it is necessary to guard their devices with an encryption that cannot be broken without the consent of the accused. There is no guarantee that officers of the law will find only the evidence that they are looking for during their search assuming they have a legitimate reason.

Existence of Other Evidence -

In the case of the San Bernardino shooting in 2015, the FBI had a legal battle with Apple to try to break through the lock that secured one of the shooters' device[Nakashima and Albergotti, 2021]. This effort proved futile as Apple had believed that creating a backdoor into its system would leave a vulnerability for unauthorized individuals to exploit. However, the FBI's investigation uncovered other evidence that were not discovered via the secured iPhone. For instance, the FBI knew of online private communications[Baker and Santora, 2015] months before the FBI director, James Comey, made the announcement that they have yet to gain access to the encrypted phoneVolz and Hosenball [2016]. This shows that if there is any evidence on a phone, it is very likely that other evidence will show up somewhere else in a suspect's life: for instance, their room, where a dozen IEDs were found[Erik Ortiz and Bruton, 2015], or through other means like internet traffic easily accessible by Internet Service Providers.

It will never be the case that the only evidence that would aid law enforcement investigation would exist on an encrypted device because it is not possible to only leave a trail behind that exists only on devices that can be encrypted. Therefore, advocating for a bill like lawful access would come at the expense of ordinary consumers, as mentioned before, for edge cases that require law enforcement to closely investigate a person's life, and all because of the fallacious claim that the only evidence that would aid investigators would only exist on encrypted devices.

4 Methods

We made a survey to gain insight into student perspectives of their use of communications apps on their devices, the nature of their communications, their comfort level with allowing third-parties access to their devices, and so forth. The survey was designed to allow open answers whenever feasible to learn the most about each student's perspective.

4.1 Survey Audience

We reached out to students at Willamette University for their input, and we got a total of 28 responses at the time of writing (12/17/2021). The survey distribution locations involved the cafe on campus and the library. The survey was designed to take approximately 5–10 minutes to complete.

4.2 Questions

The nature of the questions in the survey was all-encompassing. Below are paraphrased versions of the questions we had asked:

1. Which end-to-end encryption-secured apps have you ever used for the purposes of communication?
2. How often do you use such apps?
3. "What is the nature of your communications using such apps?"
4. How would you feel about some random person (not law enforcement) accessing the data on your phone?
5. How would you feel if law enforcement and tech companies started to cooperate and give law enforcement access to your data?
6. How would you feel if you learned that there was an unauthorized way for some random person to access your data and they were not law enforcement?
7. To what extent do you agree with the following statement: I have nothing to hide
8. With whom would you be least comfortable having access to your data?
9. Which app would you never give anybody access?

10. To what extent have you thought about end-to-end encryption or made other privacy considerations before taking this survey?

5 Results

We received 28 responses, and the input was insightful to start thinking about the general campus opinion of Lawful Access and the privacy offered by modern communication apps.

5.1 Overview

To begin, it turns out that iMessage, Instagram Messages, and Snapchat were the most popular communication apps used among respondents (89.3%), and apps like WhatsApp (67.9%), Facebook Messenger (57.1%), and Skype (46.4%) came next in popularity. One surprising element is that the app Signal was not widely used (10.7%), yet Signal's encryption protocol is both secure and largely flawless[Cohn-Gordon et al., 2016, 24]. It might be assumed that the 3 students who have Signal are aware of the extent of privacy the app truly offers. The most common response to the question pertaining to the nature of communications on these apps and others was related to some permutation of "personal use" or "casual conversation." In fact, this response was present in some way for all responses to this prompt.

There are interesting observations to be made for the responses to the hypothetical situations the survey posed. Perhaps unsurprisingly, the majority of respondents (64.4%) were uncomfortable with a random non-law enforcement entity having access to their phone (answered a "5" or lower), yet 3 students responded that they would be completely undisturbed by such a scenario. Everybody who responded showed some concern when prompted with the possibility of collaboration between tech companies and law enforcement: "distrustful", "uncertain", "uncomfortable", "conflicted," and "invasive" were all common words in the responses. When prompted with the possibility of unauthorized individuals having access to their private data, there was a more concerned tone to each response with some respondents even going as far as to say "pissed off" and "angry." There were 4 or 5 responses that showed some concern, but no immediately obvious signs of discomfort.

The most interesting question was the prompt with such a varied response, which was question number 7 as labeled above:

- Strongly agree: 1
- Agree: 8
- Neutral: 10
- Disagree: 6
- Strongly disagree: 3

Of course, it should not be considered too suspicious that people would have something to hide. After all, the most common responses to the question pertaining to who would be least welcome to access their data involved parents specifically (46.4%) with only two responses indicating specifically

law enforcement officers and another 2 responses indicating work-related concerns (employer or coworker).

The app most specified in response to the question posed by question 9 was Snapchat with (32.1%) of respondents agreeing. A comparable number of respondents (28.5%) did not specify any app, or explicitly said that they did not care.

Finally, 71.4% of respondents said that they didn't think too much about privacy-related concerns or end-to-end encryption when using communication apps.

5.2 Highlights

The takeaway from this survey is that privacy is not as much of a concern as the "tense Lawful Access debate" might suggest, insofar as the small subset of the Willamette campus surveyed has indicated. It does not seem to be the case that the idea of end-to-end encryption is well known or understood despite the fact that most modern apps with communication capabilities have such security enabled by default.

6 Discussion

This project added various insights into the Lawful Access debate in terms of how the conversation applies to people in the local area. The current, and rather obvious, limitations to this work include the small sample size, and the fact that this survey was conducted in only two locations on campus and being actively distributed for only 5 hours for one day while being passively advertised for several days afterward. Demographic information was not collected, so we cannot say for sure how diverse these perspectives are.

Privacy is clearly an important value to a significant number of people; both who have been surveyed and in general. The vigilance of the American public with respect to the government's observation of constitutional rights is impressive, yet perhaps too confrontational and skeptical. Attorney General Barr properly surmised that encryption technologies these days act as an "impenetrable digital shield," and that crimes could have been prevented with early intervention[Barr, 2019], but his same statements imply that the only way to prevent crimes before they happen is to be able to monitor real-time data traffic as the government becomes suspicious of some individual's activities. This is, unfortunately, not a convincing enough sentiment to justify allowing strong encryption protocols to be broken by a key that people outside of law enforcement may or may not have access to. There were also concerns discussed in this work that law enforcement may not always act in the best interest of its citizens or in the most legitimate of ways, and is usually not held to a good standard of accountability when things are not totally lawful.

7 Further Study

An extension to this work would be to expand the reach of the survey to a much larger sample. This was not feasible given the time constraints of this project. Instead of being an extremely localized questionnaire, the prompts could be refined and the survey could be distributed to people across the city, state, or even nationwide. It is impossible to conclude whether these particular perspectives are held at a similar proportion at a broader scope of the region, or in different areas of the country. The general theme, as presented by the findings of our survey, is that privacy is not quite at the forefront of the mind when it comes to casual use of communication apps that happen to feature end-to-end encryption.

8 Conclusion

The present work has examined several perspectives of Lawful Access as presented in various literature, and analysis of various case studies has revealed when government agents have succeeded when access was granted to encrypted data. However, the dangers of allowing vulnerabilities capable of personal and private data leakage must also be factored into consideration when proposing solutions to this complex problem.

We designed a study to gauge the views of students on campus to better inform our knowledge of public opinion with respect to privacy and the idea of Lawful Access presented by various hypothetical scenarios on an open-ended questionnaire. The responses we have received thus far surprisingly indicated that privacy is not the concern of everybody using online communication apps, and that end-to-end encryption was a seldom understood technology.

9 Works Cited

References

William R Mack. *THE KEY TO LAWFUL ACCESS: AN ANALYSIS OF THE ALTERNATIVES OFFERED IN THE ENCRYPTION DEBATE*. PhD thesis, Calhoun, 2020.

Matt Blaze. Protocol failure in the escrowed encryption standard. In *Proceedings of the 2nd ACM Conference on Computer and Communications Security*, CCS '94, page 59–67, New York, NY, USA, 1994. Association for Computing Machinery. ISBN 0897917324. doi: 10.1145/191177.191193. URL https://doi.org/10.1145/191177.191193.

FBI. The fbi's perspective on the cybercrime problem, Jun 2001. URL https://archives.fbi.gov/archives/news/testimony/the-fbis-perspective-on-the-cybercrime-problem.

Department of Justice Government of Canada. Summary of submissions to the lawful access consultation, Sep 2021. URL https://www.justice.gc.ca/eng/cons/la-al/sum-res/faq.html.

William P Barr. Statement from attorney general william p. barr on introduction of lawful access bill in senate, Jun 2020. URL https://www.justice.gov/opa/pr/statement-attorney-general-william-p-barr-introduction-lawful-access-bill-senate.

William P Barr.
Attorney general william p. barr delivers keynote address at the international conference on cyber security, Jul 2019. URL https://www.justice.gov/opa/speech/attorney-general-william-p-barr-delivers-keynote-address-international-conference-cyber.

Kurt Wagner. Here's how facebook allowed cambridge analytica to get data for 50 million users, Mar 2018. URL https://www.vox.com/2018/3/17/17134072/facebook-cambridge-analytica-trump-explained-user-data.

TOI staff, Shira Hanau, Afp, Jacob Magid, Jacob Magid, Stuart Winer staff, TOI, Luke Tress, Marcia Dunn, Nathan Jeffay, Andrew Meldrum, and et al. Hackers claim to leak details of lgbtq dating site after ransom not paid, Nov 2021. URL https://www.timesofisrael.com/hackers-claim-to-leak-details-of-lgbtq-dating-site-after-ransom-not-paid/.

Steve Reilly and Mark Nichols. Hundreds of police officers have been labeled liars. some still help send people to prison., Dec 2019. URL https://www.usatoday.com/in-depth/news/investigations/2019/10/14/brady-lists-police-officers-dishonest-corrupt-still-testify-investigation-database/2233386001/.

Ellen Nakashima and Reed Albergotti. The fbi wanted to unlock the san bernardino shooter's iphone. it turned to a little-known australian firm., Apr 2021. URL https://www.washingtonpost.com/technology/2021/04/14/azimuth-san-bernardino-apple-iphone-fbi/.

Al Baker and Marc Santora. San bernardino attackers discussed jihad in private messages, f.b.i. says, Dec 2015. URL https://www.nytimes.com/2015/12/17/us/san-bernardino-attackers-discussed-jihad-in-private-messages-fbi-says.html.

Dustin Volz and Mark Hosenball. Fbi director says investigators unable to unlock san bernardino shooter's phone content, Feb 2016. URL https://www.reuters.com/article/us-california-shooting-encryption-idUSKCN0VI22A.

Karen Lucht Erik Ortiz and F. Brinley Bruton. San bernardino massacre suspects appear to have been radicalized, Dec 2015. URL https://www.nbcnews.com/storyline/san-bernardino-shooting/san-bernadino-shooting-suspects-left-baby-daughter-grandma-n473261.

Katriel Cohn-Gordon, Cas Cremers, Benjamin Dowling, Luke Garratt, and Douglas Stebila. A formal security analysis of the signal messaging protocol. Cryptology ePrint Archive, Report 2016/1013, 2016. https://ia.cr/2016/1013.