CS 492
Section 70
Spring 2020
Christopher K. Schmitt Ethics Survey

The Ethics of End-To-End Cryptosystems

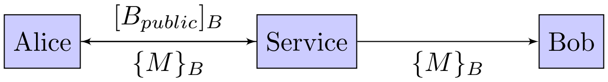
Thanks to modern mathematics, digital cryptosystems can be made functionally unbreakable. This revolutionary idea of an unbreakable lock has enabled the development of many wonders of the modern world. Everything from banking to blogging to browsing is made possible by these provably invulnerable digital locks. The whole of the internet itself depends on the secure communication which these locks provide. The unbreakable nature of these locks, however, presents several ethical and legal predicaments which require both a technical and legal understanding of the problem.

It's easy to point to situation where unbreakable cryptography is harmful. Take for example, the tragedy that took place on December 2, 2015. A domestic terrorist ended the lives of fourteen innocent bystanders, with an additional twenty-two injuries. As part of the investigation, the FBI demanded, with a legal warrant, that the phones manufacturer aid in decrypting the phones contents. The manufacturer refused, citing user privacy concerns [1]. Society in general agrees that there are certain situations where law enforcement would ideally be able to access encrypted content. The ACM code of ethics includes a provision for this with its ”for the public good” clause [2]. It is impossible, however, to to develop a cryptosystem which only the just can use and the partial cannot. Therefore, it is necessary to balance the duty to behave responsibly with private data and the duty to act ethically with respect to the law.

Lavabit provides an interesting case study. Lavabit was a webmail service launched in 2014 which advertised itself as a privacy focused alternative to Google's popular GMail service. The Lavabit platform had complied with legal warrants in the past involving a user suspected of distributing child pornography [3]. However, in July of 2013 the FBI ordered Lavabit to turn over their SSL keys, which would enable them to monitor all of Lavabit's userbase without any sort of notification. In response, Lavabit shut down its operations without turning over the data. Lavabit founder, Ladar Levison later revealed that he was under gag order not to reveal to the public that the FBI had requested the keys [4]. The government argued that The Stored Communication Act allowed the FBI to compel any third party to turn over any stored electronic communications [5]. Levison disagreed, claiming that turning over the SSL keys exposed every one of his users' data and violating their fourth amendment protections against unreasonable searches and seizures [5]. The ACM code of computer ethics has several provisions that would address a situation similar in nature to Lavabit's. Specifically, sections 1.2, 1.3, and 1.6 deal with privacy and honesty [2]. Section 1.2, “Avoid harm”, explicitly mentions: “Examples of harm include ... unjustified destruction or disclosure of information” [2]. In this case, Levison acted to protect his users from an obviously unjustified disclosure. Section 1.3, ‘Be honest and trustworthy” reads: “A computing professional should be transparent and provide full disclosure of all pertinent system capabilities, limitations, and potential problems to the appropriate parties” [2]. Because Levison was under gag order, he was unable to legally disclose that the security which he had advertised to his users had been compromised. In this case, shutting down the entire service was the *only* ethical option remaining. Section 1.6, “Respect Privacy” is the most pertinent here. It puts the responsibly of maintaining privacy on the computing professional. If the onus to defend users’ privacy was on Levison, then taking action to protect that privacy was ethically necessary.

In contrast with the Lavabit case, *CARPENTER v. UNITED STATES* offers legal arguments which protect a user’s data from unreasonable searches as per the 4’th amendment, even in cases involving third parties [6]. The facts of the case revolved around the FBI’s use of cell tower’s timestamped logs to confirm that Carpenter, the suspect, was at the scene of the crime as it was happening. Carpenter was convicted on all but one counts and sentenced to one-hundred years in prison [6]. The sixth circuit appeals court held that Carpenter lacked ”A reasonable expectation of privacy” as cell phone users voluntarily relinquish this data to cell carriers and are therefore not entitled to fourth amendment protections. Chief Justice Roberts, in writing his opinion, states: “we determined that the Government - absent a warrant - could not capitalize on such new sense-enhancing technology to explore what was happening within the home” [6], in reference to *Kyllo v. United States*, where police used sophisticated infrared imaging techniques to effectively search a home without first obtaining a legal warrant to do so. Roberts also states: “ ... police officers must generally obtain a warrant before searching the contents of a phone” [6]. Roberts held that: “A person does not surrender all Fourth Amendment protection by venturing into the public sphere. To the contrary, “what [one] seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected.” Katz, 389 U. S., at 351–352” [6]. Roberts recognized the threat to privacy that such technology posed, stating: “... cell phone tracking is remarkably easy, cheap, and efficient compared to traditional investigative tools. With just the click of a button, the Government can access each carrier’s deep repository of historical location information at practically no expense” [6], and: “In fact, historical cell-site records present even greater privacy concerns than GPS monitoring ...” [6]. This supreme court decision, held 5-4 in favor of Carpenter, established that third party doctrine cannot simply be applied mechanically. Context matters and the users privacy is of upmost importance when designing a service that utilizes user data of any kind. This applies to data that is not strictly own by the user. In this case, cell records where not supplied by the user, but created by the carrier.

Despite the ruling of the courts in Carpenter v. United States, service providers big and small can still be (and have been) approached by law enforcement and been compelled to surrender documents to investigators under gag order and without a legal warrant. In face of this, the onus is on the developers to take appropriate action to defend user privacy. In applications where the service provider does not need to view and access communications (like messaging services), techniques like end to end encryption can be used. In end to end encryption schemes, the service provider does not hold any keys, they simply act as a proxy between the senders and receivers of messages. Because the service provider does not hold any of the keys required to decrypt any message, trying to compel a service provider to aid in any surveillance actions is pointless. No government agency would be able to use a warrant, legal or otherwise, to spy on people in an illegal manner. The government can still compel an individual to hand over their private keys, but this is entirely legal. This is the closest to an ideal situation that can realistically be achieved. Law enforcement would still be able to access necessary data *sometimes*, but trying to perform any mass surveillance over the service would become impractical.



The above figure demonstrates states how an (unsecure) service might be structured to prevent the service provider from being able to know the contents of a message. If Alice wished to send a message to bob, she first retrieves his public key from the service. She then encrypts the message using bobs public key. The service then simply forwards the message onto Bob, who can decrypt the message using his private key. Because everyone maintains their own keys, it is impossible for the service provider to read any of the communications between Alice and Bob. Note that it is not impossible for their communications to be read, This model is vulnerable to a man-in-the-middle attack. But is is impossible to ask the service provider who only maintains a list of public keys to read any message sent to Bob. A model like this allows the service provider to protect users' privacy while maintaining a certain legal standard.

References

[1] Ranking Member Feinstein. Statement for the record senate judiciary committee hearing on encryption, 2019.

[2] Ronald E. Anderson. Acm code of ethics and professional conduct. *Commun. ACM*, 35(5):94–99, May 1992.

[3] In the Matter of the Search of: Lavabit LLC Email Account for Joey006@lavabit.com, 1:13-mj-00607, No. 4 (D.Md. Jun. 10, 2013).

[4] Joe Mullin. Lavabit founder, under gag order, speaks out about shutdown decision, Aug 2013.

[5] United states v. lavabit, llc., 749 f.3d 276 (4th cir. 2014).

[6] Carpenter v. United States, No. 16-402, 585 U.S. ___ (2018).