Do we have a right to encryption?

Alex Ledger

1 Introduction

Over the last few years, namely since the Snowden revelations in 2013, issues concerning privacy, anonymity and surveillance on the internet have come to the forefront of our cultural discussions. Snowden surprised many people when he provided evidence that the NSA has access to our internet activity and specifically that the NSA may read our email, a mode of communication that we commonly considered to be private. Due to this new information, many persons seeking privacy from the government resorted to using *encryption* to protect their privacy. Encryption is means of obfuscating a message - if two people use encryption, they can talk to each other without worrying that an eavesdropper might be reading their messages. In response to this, the phrase "you have nothing worry about if you have nothing to hide" became a slogan for those in support of the NSA; in effect, the slogan and idea it represents paint encryption as unpatriotic act of rebellion.

Another debate has emerged over how encryption may undermine the efforts of the law-enforcement community: encryption enables criminals to communicate such that law-enforcement cannot read their messages and

hence presenting a national security risk. Law-enforcement argues in favor of restricting the power of encryption, and in particular, requiring that all encryption used within the United States have some kind of master-key. The master-key, which the company providing the encryption would hold (e.g., Apple or Google), would allow law-enforcement agencies to decrypt encrypted messages.

The goal of this paper is to take a step back from the politicized arguments surrounding encryption and ask a basic question: do we have a right to encryption? This question is difficult to answer or even approach, and as such, this paper does not answer the question, but it introduces subproblems that need to be addressed first. This paper is a good starting point for thinking about encryption and is useful for future, rigorous work.

2 Background

In order to discuss encryption from an ethical perspective, I first give background information on encryption. Encryption has been around for centuries; we have evidence from centuries ago that various armies used some form of encryption, and more recently and famously, Hitler used the engima machine in World War II to obfuscate messages between his troops. It is only recently that society questions unrestricted encryption; my suspicion is that the main reason for this is that the public now has access to encryption, as opposed to only states having access, and so encryption needs to be restricted, perhaps to support a state that uses surveillance.

It is interesting to me as a cryptographer that we believe we can *restrict*

encryption. Encryption is at its core a mathematical fact. If I want to talk to you, we can both do some math and communicate secretly, as simple as that. To restrict encryption really means to restrict the type of encryption schemes that firms who offer encryption in their products use. For example, Apple, who encrypts users' messages sent over iMessage, could be restricted to using an encryption scheme that uses a master-key. If Apple does not use an encryption scheme with a master-key, a regulatory body could fine Apple for not abiding by the encryption regulations. If encryption does become regulated, I predict that some interesting black-market app will appear that performs the same essential functionality as WhatsApp.

The government can feasibly regulate the market, but they cannot regulate individual practices. For example, it is hard to imagine that the government could successfully prevent any person from using encryption schemes with certain properties, like me using an encryption scheme that I implement myself in Python and use to communicate with my friend. The difference between this situation and Apple is that I am not selling encryption. I would imagine that regulations on individual encryption would be disallowed by freedom of speech - the freedom to write a program - but I have been surprised by laws and court decisions before.

By requiring encryption schemes to have a master-key, the government would greatly weaken the cyber-security infrastructure. As we have seen, it is not too difficult for hackers, either private or state-sponsored, to break into databases, and in theory, steal the master-key, giving them access to all *private* messages encrypted using that master-key.

3 Parallel Situations

A common place to start when thinking about the ethics of encryption is to compare encryption to more common ethical situations such as talking or sending a letter. The aim of this section is to introduce and discuss these situations. We find that the hypothetical situations are useful but are not strong parallels to the actual usage of encryption, and as such they are not conclusive.

Encryption, as I will be using it, is a method that allows two or more parties to send messages over the internet without an eavesdropper from reading, or learning any information about, the contents of the messages. Encryption is also used to obfuscate data on a laptop or iPhone, such as in the recent case between the FBI and Apple, but I believe that it will simplify our reasoning if we leave that situation to another day.

3.0.1 Private Room, Private Conversation

If we are alone in a private room with another party, do we have the right to communicate privately - that is, do we have a right to *not* be eavesdropped on? To avoid annoying criticisms, let us further assume that we are in a private residence, talking in a soundproof room, and we have received no indication that someone might be listening to our conversation. In this case, it seems reasonable to expect a private conversation. However, the internet is not a private room with only two parties; rather, it may be considered a crowded place, so this hypothetical situation lacks a strong parallel to actual usage of encryption.

3.0.2 Private Room, Crowded Conversation

We now expand the hypothetical situation to be more similar to encryption. Instead suppose that we are in a private residence in a crowded room. I stand on one side of the room, and the other conversor stands on the other side. We wish to communicate without others in the room from listening.

The question now is, do we have a right to have a private conversation in this room despite the fact that there are others in the room listening? The answer to this question is less clear to me than the private-room-private-conversation question. For instance, it seems weird that we expect to have a private conversation in such a situation: why would we not move to a different room to talk privately? On the other hand, if we assume that room is public and we don't have access to a private room, then we need to section off a portion of the room for our private use. This would inconvenience others in the room, only for the sake of our private conversation. In some situations, if our private conversation is critical for the safety of the people in the room, then it is justified for us to inconvenience the others, but in general, it does not seem justified. It does not seem that we necessarily have a right to a private conversation; the right to the private conversation is situational.

3.0.3 Mail

The internet can be thought of as a means to communicate over a large distance in a short amount of time, like an optimized form of mail. I write an email, send it to you via the internet, and you receive the email and read

it. Since the internet runs on a public system - packets get passed around from server to server - anyone who comes across my email in the process of it getting to you could read its contents. Therefore, the only way to communicate privately with you is to use some form of encryption.

The matter is complicated by the fact that we don't *own* the internet; the internet is run by private firms and the government, and they let us use it (for a price or taxes). This makes communicating over the internet similar to communicating via the United States Post Service (USPS). I give my letter to the USPS and tell them a desired destination, the USPS does internal work to get the letter to the destination, and you eventually receive the letter. In this framing, the USPS is doing the hard word and heavy lifting, and I am using their convenient service.

We naturally ask the question, do we have a right to privacy when we send a letter using the postal service? Does the postal service have the right to open up my letter and read it? I believe - but may be wrong - that most people feel that the USPS should not open my letter and read its contents. My letter is private, and I am paying them for their communication services, so they should service my letter without meddling.

If the USPS does have the right to read letters, do I have a right to encrypt the contents my letter? Probably, but if the justification for reading letters is strong (e.g., it appeals to national security), then I may not have the same right to encryption.

Another way to think about the USPS reading letters is to think about the question using business ethics. Suppose that the USPS is an organization that performs a service S. Service S takes as input x, outputs $S(x)$. In the

process of performing S, the USPS does not need to know anything about x. I could put x into an envelope or letter, call this $e(x)$. I actually give the USPS $e(x)$ and they return $S(e(x))$. The question then is if the USPS does not need to open $e(x)$ (i.e., reveal x) in order to perform S, then do they have any right to do so?

In a general business setting, I expect that a business will perform what I ask of them with minimal intrusion into the input, x: I am paying them to perform the service, not to investigate me. Perhaps it is reasonable to say that the business can learn some information about x during processing the service, but the amount that they learn about x should be upper bounded by some value. That is, they can learn some things, because it is unreasonable to hold them an absurdly high standard of respecting my privacy, but they should not go out of their way to learn about my input.

That being said, the case of the USPS and the internet is different because it's the government that is performing the service. The aim of the government is to aid the people, and this specific case, their foremost goal is deliver my letter or internet request. In this light, it seems unreasonable for the USPS or internet provider to open my envelope to read its contents, unless there is some other priority such as national security, which makes a messier issue.

3.0.4 National Security

Many arguments for regulating encryption focus on the fact that strong encryption helps criminals undermine national security efforts. This argument is difficult to address for various reasons. However, I recall hearing that

Snowden revealed that little to none of the NSA's privacy-invading efforts had contributed to preventing an attack. Snowden also revealed that many of the privacy breaches were justified under the guise of national security, but in fact had other uses and purposes. To me, this debate in part boils down to the efficacy of invading privacy towards improving national security. There is some sweet spot where the trade-off between privacy and national security is optimized, but the public does not have adequate information to truly assess this problem, as we do not details about national security efforts or privacy invasion.

4 Summing it up

The last section, instead of providing a clear answer to question of encryption, brought up some important points that need to be addressed in order to come to satisfying answer. The aim of this section is to highlight those points, as they should be useful to future work.

In the crowded room hypothetical situation, we concluded that is was unclear, or situational, if we had a right to a private conversation, and our argument was that in order to have a private conversation, we would have to inconvenience others. Unfortunately, this hypothetical situation lacks parallelism to using encryption because using encryption does not inconvenience anyone. That is, if I use encryption on the internet, then it has no effect on your internet experience. Hence, we must ask the question, if we can hold a private conversation in the crowded room without inconveniencing others, should we? One argument in the negation of the question is that it would be

rude to leave others out - the others are in the room, and they can listen to our conversation if they want to. This argument appeals to the slogan, "you have nothing to worry about if you have nothing to hide", where just because I have no reason to have a private conversation, I should not be holding one. I am not persuaded by this argument because sometimes I talk and I just don't want a certain group of people to be privy to my conversation. If I were not able to prevent a group of people from listening to me, it would restrict what I would say. This line of thinking opens a number of questions, such as: by refusing to not eavesdrop, is that group really restricting my speech? Are they restricting my access to speech? Encryption would solve the problem because they could not listen to me and I can say what I want, so do I have a right to encryption if it increases my right or access to speech? Unfortunately, I lack the time and space to delve into these problems, but they are a sample of the problems that fall out of digging to the crowded room hypothetical. Suffice it to say that the crowded room hypothetical is a useful method for approaching the question of encryption.

The second point is really a sub-problem that needs to be addressed to resolve the encryption question. The sub-problem asks, "do the institutions that run the internet have the right to read the contents of the messages they are handling?" In section 3.0.3 I introduced formal notation for what it means to send a message x over the internet. When a message is sent over the internet, we put the internet into an envelope, creating $e(x)$, such that for the handlers of the internet to read the message they need to open the envelope. In the real world, opening the envelope could take many forms; for example, the handlers of the internet could simply save the message after

they process it; such an action is above and beyond the duty of the runners of the internet - they do not need to save the message to perform their job, but it may be useful for the internet provider to save some data about the messages it processes so that it can improve its operations. This sub-problem can likely be addressed by appealing to business ethics: to what extent can a business investigate the input to a request from a client without violating the client's privacy?

5 Conclusion

We need to address many problems before we can come to a good understanding and conclusion to whether we have a right to use encryption over the internet. The aim of this paper was to start the process for thinking through the question. Another easy step forward is see how the arguments for and against encryption fall into the tropes of new and emerging science and technology (NEST) ethics.