Creative Destruction in the Philosophy of Technology

Alex Ledger

1 Introduction

Over the last few years, namely since the Snowden revelations in 2013, issues concerning privacy, anonymity and surveillence on the internet have come to the forefront of our cultural discussions. Snowden surprised many people when he said provided evidence that the NSA has access to our internet activity, and moreover, 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 *encrytion* to protect their privacy. Encryption is means of obfuscating a message - if two people use encryption, they can talk to each other without an eavesdropper reading their message, or with extra pre-cautions, from learning their identities.

With the advent of the Snowden revelations came the slogan, "you have nothing worry about if you have nothing to hide," in effect painting encryption as unpatriotic act of rebellion.

Another debate has emerged over how encryption may undermine the

efforts of the law-enforcement community: encryption allows criminals to communicate, allowing them to elude law-enforcement and hence presenting a security risk to the citizenry. 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 encrpytion would hold (e.g., Apple or Google), would allow the law-enforcement agency to unlock encrypted messages.

The goal of this paper is to take a step back from the politicized arguments surrounding encryption and anonymity and ask a basic question: do we have a right to encryption? Is ethically permissible to restrict public access to encryption, or is it unethical to give criminals easy-access to encryption? {AL-0: Talk about structure of paper}

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 use 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 encryption has been described as an act of rebellion, and something that should potentially be restricted; my suspicion is that the main reason for this that we all know have access to encryption, as opposed to states, and so it needs to be restricted, perhaps to support a state that

uses surveillence.

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: math enables use to communicate privately. 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.

In contrast, the government could 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 in the previous paragraph is that I am not selling encrpytion; rather, I am simply doing math. I believe that regulating encryption on the indvidiaul level is clearly a governmental overreach. I would imagine that such regulations would be illegal by freedom of speech - the freedom to write a program - but I have been surprised by laws and court decisions before.

The final fact to be aware of is that by requiring encryption schemes that use a master-key, the governemnt 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

In this section we present a variety of situations that are similar and disimilar to encryption to help us think about whether we have a fundamental right to encrytion.

First a few definitions. Encryption, as I will be thinking about 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.

{AL-1: other definitions if needed}

3.0.1 Private Room, Private Converstation

One way to think about encryption is verbally talking to another party in a private room, in which case we ask the question: 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, the conversors, have received no indication that someone might be listening to our conversation. In this case, it seems reasonable for us to expect a private conversation - if you take issue with

this, then you may ignore the following analysis.

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 am standing on one side of the room, and the person to whom I am speaking is standing on the other side. We wish to communicate without others in the room from listening. We can achieve this using public-key encryption: we can each do some math, shout at each other, let everyone listen to our shouts, and in the end communicate some message that everyone else is oblivious to.

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 if we want to have a private conversation, we are required to use public-key encryption. This situation is much more similar to using encryption over the internet: the internet is accessible to the public, so in order to converse privately over the internet, we are required to use public-key encryption.

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 message and open. 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 a desired destination, the USPS does internal work to get the letter to the destination, and you eventually receive the letter. In this framing, it feels like the USPS is doing me a favor; they are 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 be able to open my letter and read it. My letter is private, and I am paying them for their communication services, so they should communicate 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 appeals to national security, then I may not have the same right to encryption. National security effort need to be able to read my letter if it's bad, so I don't have a right to encrypt it. This line of reasoning returns to the slogan, "you have nothing to worry about if you have nothing to hide."

Another way to think about the USPS reading letters is to think about the question using business ethics. First, I formalize the proble. Suppose the USPS were a private company 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. In fact, I put x into an envelope or letter, call this $l(x)$. I actually give the USPS $l(x)$ and they return $S(l(x))$. The question then is if the USPS does not need to open $l(x)$ (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 inputs. I am paying them to perform the service, and 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 of that they learn about x should be upper bounded by some value. That is, they can learn some things, because it's unreasonable to hold them an absurdly high standard of respecting my privacy, but they shouldn't 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 becomes a messier issue.

3.0.4 National Security

Many arguments for regulating encryption focus on the fact that weaker encryption would aid 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 national security. And 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 the efficacy. There is some sweet spot where privacy and national security are 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.