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 governments who offer encryption in their products use. For example, Apple, who encrypts users' messages sent over iMessage, could be restricted to using an encryption 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. To me, it seems like a clear overreach for the government to prevent me from doing encryption on my own: writing an encryption scheme is Python, and communicating with a friend using my own program. The difference here is that I am not selling my encryption; I am simply using math. I would imagine that this would be allowed 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.