Discussing end to end encryption that caused changes in encryption standards

Technology, Information Technology

End to end encryption post-snowden has dramatically altered the landscape of encryption standards. Today, companies are more paranoid of data leaks and as such request stronger security — unbreakable even in the cases when need be such as law enforcement. The private sector claims that it is not only in their business interest but within their rights to manufacture such a system. The problem then lies that in cases of law enforcement, damning evidence is suddenly out of the reach of due process of law. Understanding the fundamental security situation, a system must be put in place to obtain backdoors in case data needs to be examined by a third party because it is ethical to do so.

The heart of the argument comes from accessibility relating to crimes. Companies who serve clients with sensitive data are pressured into developing more advanced encryption schemes. These companies argue that implementing a double key system — or any other proposed backdoor system makes their entire infrastructure semantically insecure. They claim these schemes “ poke a hole in mobile devices and countless other critical systems” (Perlroth). These companies also have to deal with many hands — although many people hold the data they are in the end responsible for the security increasing pressure to encrypt the data. The expectation of risk is what frightens many sensitive data users — making them think that it becomes immoral for their data to have even infinitesimally more risk than already existing in the system. From financial groups to personal phone, users have been bamboozled into thinking that any sort of back door could stop their entire system. Between common password frequencies and inadequacies in operating systems (Android Camera Backdoor and IOS

Keychain) users systems are already exposed to multiple vantage points. Now, that is not to say that it is alright to create another hole in the system is wholly ethical, but the implications of keeping data fully encrypted are much more detrimental than allowing for that small amount of risk with the backdoor leaking out (imagining a non-universal backdoor).

But this begs the question, even if we can implement encryption effectively, would said risk be morally acceptable given the alternative? In this case, it would be. In fact, this data privacy needs to be striped away in the case when a court of law decides otherwise. There are numerous cases of phone data, email data, and other personal data being used to indict horrible criminals — some cases where that was the damning evidence (Comey). To use former ethics, individuals have the right to personal privacy and privacy from searches and seizures until a courts deem it sufficient and necessary for those rights to be taken for the due process of law. Implementing end to end peer encryption violates that ethical principal (mutual respect) because there is a center subset of people who are suddenly above the law through a somewhat arbitrary means of random number generating. Technical expertise should not beget one this power. The tech giants side that it is within their right to exercise encryption algorithms. McConnell simply leaves it as “[The Government] will develop technologies and techniques to meet their legitimate mission goals”. Although as computer professionals we know the time complexity behind all of these issues, we need to be weary that it is wrong for us to do so: even if it is to appease the next bank account user or

private database conglomerate — not to imply that all computer professionals are moralistic as well.

It follows that it is immoral to create end to end encryption schemes with no backdoor. To clarify, this would not be a universal backdoor key that could solve all encryptions but more granulated to keep the element of random guessing due to time at a maximum. Using a consequence or a duty based system leads to no conclusion in terms of an argument — there are positives and negatives where one cannot weigh on a moral agent without a subjective evaluation. Using a contract based system, we can equate this issue to one of a contract with the U. S. constitution — logically extending to the virtual era. Director of the FBI James Comey commented on this exact extension, saying “[End to end encryption is] the equivalent of a closet that can’t be opened. A safe that can’t be cracked. And my question is, at what cost?” (Comey) — he was referring to the extension of the fourth amendment for searches. Although the analogy doesn’t follow directly, seizures in houses don’t automatically make houses insecure, the implicit rule is what rings clear. End to end encryption can be used to protect drug/human trafficking, child abuse, sexual crimes, anything where the evidence is all but cleared up physically and the courts need the data to convict. This essentially makes security and privacy incompatible; the law abiding citizen must be put under the same vigilant eye as the criminal. Also, character based ethics tells through virtue tells us that if were put in a scenario where data was needed to convict or free that a backdoor would be beneficial from both sides — should that occur.

In the end, this issue is nothing more than a logical extension of the law. It is agreed that the third party doctrine applies because this is a logical extension of the law. Although that one has to give up much to the malicious hackers in order to insure the rights and system is preserved, we as computer professionals must implement the back doors and figure out other methods to safeguard data and keep with the law.