Encryption Prevention

(1) Should we prevent encryption from being used without a backdoor for law enforcement?

I am against the idea of creating a backdoor for law enforcement. As previously defined, we have considered privacy as a "zone of inaccessibility". Relatedly, the question of allowing a backdoor for law enforcement is a focus on whether or not we should believe that some of our data should be private and inaccessible to outside sources.

Duan et. al (2018) states, "The benefits of an encryption backdoor that proponents have offered so far are currently only theoretical and are most often presented within the scenario of a hypothetical criminal or terrorist using secure lines and encrypted phones." As they assert, there is only weak or circumstantial evidence of the help that an encryption backdoor might play; even in the case of the San Bernardino terrorist attacks, an encryption backdoor was eventually unnecessary. At present, there does not appear to be substantial need for a backdoor, as there has been a largely insufficient use of available techniques.

The Washington Post opinion article (2014) further asserts that the use of a traditional backdoor is "undesirable — a back door can and will be exploited by bad guys, too... perhaps Apple and Google could invent a kind of secure golden key they would retain and use only when a court has approved a search warrant." Their solution is a middle-ground that gives preferential access to certain parties. However, Keybase, a key and encryption company, counters that this interpretation is nonsensical, "Practically speaking, the Washington Post has proposed the impossible. If Apple, Google and Uncle Sam hold keys to your documents, you will be at great risk." Instead, Keybase asserts that by allowing Apple and companies to continue to encrypt, and consumers to continue to protect their information with a single password, it protects against hackers, foreign governments, human error, and future-proofing omnipresent, ever-existent cloud data. The complexities of creating, keeping, and protecting a "golden key" would be great, and expensive.

Thus, from a utilitarian perspective, we could assert that there is little current quantifiable benefit to allowing a backdoor or "golden key", but much potential risk. Instead, we should acknowledge the importance of encryption to protect from the very real threat of cybercriminals and outside entities, as well as the danger of forgoing more rights to the central government. Moreover, from a Kantian perspective, I find it unlikely we could generalize either the rule of prevention of all encryption or incorporating backdoors in all encryption- there are significant benefits and importance of the privacy and protections afforded by encryption. Threatening the security of all parties by asking them to forgo inbuilt protections to their own data for the end of a greater possibility of protecting and prosecuting future attacks seems like specious reasoning, at best, and a use of citizens as an end. In a look at internet freedoms, Allen (2013) asserts, "Privacy is a requirement of our freedom, our dignity, and our good character." (6). To consider the importance and promotion of privacy as a virtue, I would suggest that the prevention of encryption, a method of privacy, should not be encouraged by virtue ethics, even if the individual lives righteously, with nothing to hide.

On a more fundamental level, I remain convinced that citizens deserve a right to some digital privacy, or at least a belief in such. The overarching question is whether or not citizens have a right to privacy of data. The attacks on Apple's security by the DOJ as cited by Techdirt (2), or recent legislation such as the Lawful Access to Encrypted Data Act, aimed at expanding the scope of government overreach (5) appear to be further curtailing those rights, threatening the 4th and 5th amendments. From our shared social contract, we acknowledge the importance of privacy and unreasonable search and seizure, with a presumption of innocence.

Duan, C., Rizer, A., Graves, Z., & Godwin, M. (2018). (Rep.). R Street Institute. Retrieved October 21, 2020, from http://www.jstor.org/stable/resrep19128

1. https://www.washingtonpost.com/opinions/compromise-needed-on-smartphone-encryption/2014/10/03/96680bf8-4a77-11e4-891d-713f052086a0_story.html
2. https://www.google.com/search?q=keybase+io&rlz=1C1CHBF_enUS909US909&oq=keybase&aqs=chrome.0.69i59j0i433i457j69i57j0i433j69i60l2j69i61j69i60.1253j0j7&sourceid=chrome&ie=UTF-8
3. https://www.techdirt.com/articles/20151024/04573732612/doj-claims-apple-should-be-forced-to-decrypt-iphones-because-it-customers-only-license-operating-system.shtml
4. https://cyberlaw.stanford.edu/blog/2020/06/there%E2%80%99s-now-even-worse-anti-encryption-bill-earn-it-doesn%E2%80%99t-make-earn-it-bill-ok
5. https://cyberlaw.stanford.edu/blog/2020/06/there%E2%80%99s-now-even-worse-anti-encryption-bill-earn-it-doesn%E2%80%99t-make-earn-it-bill-ok
6. https://scholarship.law.upenn.edu/cgi/viewcontent.cgi?article=1450&context=faculty_scholarship