CY 2550 – Foundations of Cybersecurity – VSD Homework

80 points, due March 20 by 11:59pm.

Note: Please complete this assignment in groups of approximately 4 students.

In this assignment, you will perform part of a Value Sensitive Design (VSD) critique of the so-called "going dark" debate. This is an exercise in applied ethics, critical thinking, and creativity – we expect written answers, not code, pseudocode, or mathematical formulas. For your reference, there is general information available about VSD and the methods it employs at the following website: https://vsd.ccs.neu.edu.

Summary of the problem: In the U.S., law enforcement agencies may obtain legal access to computing devices and electronic communications. For example, the police may obtain a warrant that permits them to seize and analyze a computer belonging to a suspect in a crime, in order to search for evidence. The police may also obtain a warrant for a wiretap that allows them to surveil the electronic communications of a suspect. Finally, the police may obtain a subpoena that compels a communication company (e.g., a phone company or online messaging service like Facebook) to turn over electronic records and communications relating to a suspect.

In recent years, however, powerful encryption has begun to proliferate across the consumer electronics space. Laptops and smartphones are often "encrypted by default", meaning that a password or cryptographic key must be provided to unlock the data stored on the device. Similarly, end-to-end encrypted messaging apps like Signal are free and widely available. In both cases, the secrets necessary to decrypt the data are known only to end-users. Even if law enforcement were to try to compel the device maker, software developer, or service provider to grant access to data, they cannot comply – only end-users can decrypt their data.

Law enforcement agencies claim that they are "going dark" because of the proliferation of strong cryptography. They claim that data that is necessary to solve crimes, and that they otherwise have lawful access to, is now inaccessible. High-profile law enforcement officials like James Comey, Rod Rosenstein, and William Barr have called on tech companies to develop solutions that preserve the lawful access capabilities of law enforcement agencies to digital data and communications.

For their part, tech companies and cryptographers assert that they cannot comply with the demands of law enforcement officials. They argue that any "back door" added to encryption systems to facilitate access by law enforcement would inevitably also be exploited by adversaries – in other words, that there is no way to build a back door just for the "good guys". Further, this side argues that if U.S. law enforcement were to demand back door access to data and communications, law enforcement officials in other (possibly more authoritarian) countries would also demand similar access capabilities.

Question 1 (20 points): List the *direct* and *indirect stakeholders* in the going dark debate. For each stakeholder, briefly explain the most important *values* they may have that are implicated in this debate.

- Direct Stakeholders (and associated values)

- Indirect Stakeholders (and associated values)

Question 2 (10 points): Imagine that the U.S. Congress passed a law mandating that all encryption systems have a back door that allows lawful access by law enforcement agencies. Briefly describe some of the worst-case scenarios that could result due to this law (i.e., after U.S.-based encryption systems are updated to comply with the new law). What bad thing(s) could happen? To which stakeholders? What stakeholder's values or interests would be adversely impacted?

Note: you don't need to be 100% comprehensive. You only need to identify scenarios that are foreseeable, consequential, and likely. You don't need to talk about extreme event like alien invasions.

Question 3 (10 points): Imagine that U.S. law does not change, and that powerful encryption-by-default becomes the norm across all electronic devices and communication services. Briefly describe some of the worst-case scenarios that could occur in this situation. What bad thing(s) could happen? To which stakeholders? What stakeholder's values or interests would be adversely impacted?

Note: as above, you don’t need to be 100% comprehensive.

Question 4 (30 points): It seems highly unlikely that a technical solution (e.g., a new cryptographic algorithm) can be developed that will resolve the going dark debate in a way that satisfies all stakeholders. In the absence of such a solution, tradeoffs must be made between the values of different stakeholders.

If you were able to decide the outcome of the going dark debate, what outcome would you choose, and why? In answering this, make sure to explain: (i) which stakeholders and values your outcome favors, and which stakeholders and values are compromised; and (ii) why these value tradeoffs are appropriate.

Hint: Are any stakeholder values illegitimate in this context? Are there rights that need to be respected? And which of the remaining values are strongest?

Question 5 (10 points): Thus far, our analysis of the going dark debate has assumed a U.S. context. Would your proposal for how to resolve this debate (question 4) change if the debate was being held in a different country? Why or why not? What factors are relevant here?

List all of your group members (gitlab usernames):