Breaking Encryption for Law Enforcement Purposes: *Invasive or Protective?*

Nia Lam and Niki Jiang

CS Ethics

Breaking Encryption for Law Enforcement Purposes:
Protective.

Laws & Legal Access

- **Foreign Intelligence Surveillance Act (FISA)**
  - **Foreign Intelligence Surveillance Court (FISC):** individually approve electronic surveillance of U.S. citizens or foreigners who are suspected of being a threat to national security
- **Electronic Communications Privacy Act (ECPA)**
  - requires police investigators to obtain a **court-approved search warrant** before they can eavesdrop or gather private data.

Encryption and Crime

- **<u>Apple vs FBI, 2016</u>**
  - Syed Rizwan Farook killed 14 people on December 2015 terrorist attack in San Bernardino.
  - The judge ask that the FBI have access to the information on the phone with that hope of discovering additional threats to national security
  - Apple said no
- **Mumbai Terrorists Attacks in India (2008):**
  - At least 174 people died
  - It was found out that these terrorists used Blackberry devices to communicate
- Between 2017 and 2018, the spread of unchecked, fake and malicious information were found to be **directly linked to mob violence.**
  - 34 people across 9 indian states were lynched due to misinformation on social media

Encryption and Crime Cont.

- Between 1998 and 2017, India reports the **highest number of child pornography cases worldwide**, and encrypted communications makes it difficult to identify parties involved
  - The **Playpen Case:** the largest child pornography website
    - Access through the Tor browser that made it untraceable
- **Selling and distribution of drugs** on the darknet
  - Online black market sites like Silk Road (SR) provide sites for the sale of illegal drugs. Though SR did shut down, other sites made up for it

Conclusion

Going dark is a term that refers to the process of encryption or techniques that obscure information in ways that prevent the government from accessing it, even when the government is authorized by law to do so. Encryption can be used by criminals, hackers, and terrorists which makes it harder for the government to track their activities and stop their plans. When it comes to investigations of terrorist plans, child pornography, selling illegal drugs, and other major crimes, the government should have the right to access encrypted data to ensure national safety and protect the public.

Breaking Encryption for Law Enforcement Purposes:
Invasive.

Security Risks and Public Safety

- Providing the government with a backdoor creates vulnerabilities that malicious actors can exploit, causing harm to innocent people
  - The very criminals that the government wants to catch with this technology may actually be able to abuse this technology
- **Apple**
  - Refused to provide technology that grants infinite number of password attempts and prevention of data deletion
- **End-to-End Encryption**
  - Encrypted data securely transmitted from one user's device that can only be decrypted by end user's device
- Private and secure encryption for users and law enforcement decryption keys are mutually exclusive; it is technically impossible
  - Continuous, blanket storage of private user data
  - Keys to break end-to-end encryption
  - Not possible to create backdoor decryption that safely targets only one person
  - Weakens encryption overall, affecting security for innocent people

Economic Impact

- The effects on tech companies and the economy
- Studies show that small investments in accelerating deployment of encryption results in significant gains for the economy
  - The internal rate of return NIST's investment in promoting AES was 81% while the cost of capital was 7%
  - Aggregate net benefits to economy exceeded $USD 250 billion
- Laws allowing the government to break encryption lead to business uncertainty
- Encryption backdoor threatens relative perception of trust, sales, and incurs operating costs
  - Buyers are likely to be more wary, knowing that the devices they purchase may not be as safe and secure

Privacy Rights of the People

- Providing the government with these tools may increase security risks not only with malicious third-party actors, but also with the government itself
  - Government hacking
- **Threatens Anonymity and Freedom of Expression**
  - People may be afraid to express themselves fully and freely online with the knowledge that the government may have unlimited surveillance on their messaging
  - Journalists and whistleblowers lose their protective cover of anonymity
- **Human Rights Violations**
  - Violates human right to privacy
  - The European Court of Human Rights (ECtHR) ruled that weakening encryption can lead to general and indiscriminate surveillance on everyone
- **Protecting Civil Liberties**

Conclusion

While the government argues for breaking encryption to protect people from criminals, hackers, and terrorists, providing backdoor decryption for the government only worsens the issues. It is not possible to have safe and secure encryption while also providing the government to keys to that encryption. The overall security of the system is compromised, and the keys may be exploited by the very people the government claims to protect people from. In addition, there is no certainty that the government itself may abuse this power. Breaking encryption for law enforcement purposes is a violation of the human right to privacy.