Deliverables:

- PDF in each partner's **work** repo, subject to these guidelines:
    - links to primary sources included
    - summary of issue or newsworthy development
- Other supporting files may be added to ethicacy folder. Each partners' folder must contain all files.
- Digital components saved in ethicacy0 dir in root of work repo.

Presentation

- *GOAL: Each partner takes a side (of an at-least-2-sided issue), and audience gets to hear each argument.*
    - ~5min per side.
        - (shorter: topic not rich enough)
        - (longer: topic not distilled enough)
    - solicit questions/comments/concerns
- Ethicacy will take place at the beginning of each class session. Q&A thereafter.

Online Follow-Up, or "I'm here for the comments."

- By the next class session, each audience member will weigh in…
    - clearly indicating chosen side
    - supporting their choice with supporting documentation, by referencing personal experience, and/or by expanding upon comments from live presentation or preceding discussion.

Presentation Order / Teams

- CSV of randomized date assignments:
- *Duos are expected to establish intra-team communications as soon as possible, and collaborate to maximize presentation quality.*

Topics:

1. Breaking encryption for law enforcement purposes
2. "User engagement" : biz-speak for "addiction"
3. "Always-on" expectation in workplace and/or educational sphere

Requirements

- links to primary sources included
- summary of issue or newsworthy development

- GOAL: Each partner takes a side (of an at-least-2-sided issue), and audience gets to hear each argument.
    - ~5min per side.
        - (shorter: topic not rich enough)
        - (longer: topic not distilled enough)
    - solicit questions/comments/concerns

Encryption and Law

Breaking encryption for law enforcement purposes
https://www.american.edu/sis/centers/security-technology/encryption.cfm

Other Sources

https://www.thirdway.org/report/weakened-encryption-the-threat-to-americas-national-security
https://cepa.org/comprehensive-reports/encryption-its-not-about-good-and-bad-guys-its-about-all-of-us/
https://www.dwt.com/blogs/privacy--security-law-blog/2019/11/the-battle-over-encryption
https://www.malwarebytes.com/blog/news/2020/05/going-dark-encryption-and-law-enforcement
http://dspace.mit.edu/bitstream/handle/1721.1/97690/MIT-CSAIL-TR-2015-026.pdf?sequence=8&isAllowed=y

JSTOR Resources:

- Dispute between US law enforcement agencies and tech companies
    - EX: apple as of 2022 said that all the data that been encrypted (end to end encryption) so that only user can use
        - Therefore the police are concerned as crime investigation (kidnapping, terrorism, child abuse) will be hindered
        - But an argument against this: the police must have a valid reason to even TAKE away the device

Encryption: A Tradeoff Between User Privacy and National Security

https://www.american.edu/sis/centers/security-technology/encryption.cfm

- Whether law enforcement should have a “backdoor,” access key for encrypted messages (enabled/provided by the companies)

- Argument arose in early 1990s, but heated up due to high casualty terrorist attacks
    - Terrorist attack at the Inland Regional Center in California
        - FBI filed an order for Apple to unlock iPhone of one of the perpetrators
        - Apple refused to provide “U.S. law enforcement with special iOS technology that would grant an infinite number of password attempts to unlock the phone and avoid data deletion, which typically happens after a certain number of failed attempts”
- Justice department: William Barr
- Gov attempt at “breaking encryption” - backdoor
    - 1993 NSA, “Skipjack” was developed to be used solely by the government to decrypt messages
        - Encrypt and decrypt messages using identical keys: symmetric-key algorithm
        - Gov thought open access to encryption would allow criminals to use that in conversation
    - 1994 Clinton administration, Clipper Chip
        - Used Skipjack’s encryption algorithm to scramble conversations on mobile devices and provide a record of each key, which could be used by gov to intercept and decrypt messages
    - Clipper Chip failed
        - Intense backlash from cryptography community and privacy advocates
        - Encryption software was becoming ubiquitous → public already accustomed to private communications
        - Hardware-based technology complicated rollout - placing in each individual device was expensive and tedious
- CURRENT FOCUS of debate: end-to-end encryption
    - End-to-end encryption: encrypted data securely transmitted from one user’s device that can only be decrypted by the end user’s device
    - MUTUALLY EXCLUSIVE: private & secure encryption for users and law enforcement decryption keys
        - (Tech companies)
        - Technically impossible
- Tech companies fear that a backdoor will leave customers unprotected from malicious actors
- Tech companies claim they do not retain users’ messages for an extended period of time, technology to break encryption algorithms themselves
- Giving law enforcement the tools can lead to increased security risks and grave human rights violations → government hacking
    - 2016: https://www.accessnow.org/wp-content/uploads/2016/09/GovernmentHackingDoc.pdf

        - Threatens anonymity → whistleblowers and journalists
    - **Such laws have already been passed in UK & Australia**
        - Giving law enforcement legal authority to require tech companies to creat algorithms that provide government access to encrypted messages
        - These corporations operate worldwide
    - 2015 Paris terrorist attack (encrypted devices)
    - BOTH HOLD ABSOLUTIST POSITIONS - SECURITY VS SECURITY
    - Potential variables?
        - Quantum computing → enable quick decryption of even most complicated technologies
        - Likely adoption of “user-controlled” encryption → gives end user total control over keys required to recover their data
            - 2019: https://carnegieendowment.org/research/2019/04/likely-future-adoption-of-user-controlled-encryption?lang=en
    - “The conversation must move past the broad and absolutist positions of each side by breaking the encryption argument down into its component parts. Focusing on smaller debates, like mobile phone encryption for data at rest—meaning data that isn’t actively transmitting information between devices—could alleviate the concern that exceptional access for law enforcement would leave data vulnerable to foreign adversaries and other criminal activity. Ultimately, any technical solution and subsequent policy proposal should hold up against important principles that allow for limited access for law enforcement while addressing privacy and equity concerns of consumers. The debate surrounding open encryption remains fraught, but by focusing on smaller, short-term solutions, both sides might find small compromises in this crucial privacy/security conundrum.”

Australia data encryption laws explained

https://www.bbc.com/news/world-australia-46463029
2018

- Laws: Tech companies must grant law enforcement access to encrypted messages
    - Necessary to combat terrorism and crime?
    - Global weak point?
- Hand over suspect's communication to police
    - Possible if service provider uses form of encryption that allows them to view a user’s message
    - HOWEVER services have added additional layer of security: end-to-end encryption
        - Service provider cannot unscramble it
- End-to-end encryption is banned in China, Russia, and Turkey

- Australia
    - Police can force companies to create technical function that gives them access to encrypted messages *without the user's knowledge*
        - "It's not possible to create a 'back door' decryption that would safely target just one person
        - Any backdoor would weaken existing encryption scheme, *affecting security for overall innocent people*
        - Could be exploited by criminals
        - Law offers a safeguard: "decryptions won't go ahead if they create a systemic weakness"
            - Critics say this definition is vague and its application is unclear
        - Lacks sufficient checks and balances?
        - "The Electronic Frontier Foundation has said police could order individual IT developers to create technical functions without their company's knowledge."

Apple Said No

[Weakened Encryption: The Threat to America's National Security]

Summary + Points:

- During covid, more people were interested in securing their information.
    - There were cases of zoom bombing hosted by **Alcohol Anonymous** (these are organization that conduct sensitive and private information)
    - Due to this, zoom allowed the users to have end to end encryption to make sure cases like these don't happen
    - Congress members also support this with the Senate Sergeant at Arms approving the use of **Signal**, an encrypted messaging app, for staffers in 2017.
        - Congress members were also advised not to use zoom since it was not encrypted
- The danger of foreign actors and its role in encryption
    - What are foreign actors
        - People who are trying to get into sensitive US information
            - EX: hack of the Office of Personnel Management files by Chinese intelligence services in 2015
            - earlier hack of the US military's classified computer networks by Russian intelligence
        - The danger
            - Cyberattacks to find cracks in our national security system
            - Personal and commercial information can be exposed and therefore interfered with
            - Supply chain with encryption devices can be controlled by foreign players

- If there was a backdoor for companies to decrypt the information, foreign countries can have a better chance of getting that private information
- Even encrypted data could travel across devices and platforms that are controlled by foreign actors (companies like Huawei have a close relationship with China) . It just wouldn't be able to be understood but if it is decrypted then anyone within that network could read it. A system of encryption with built in vulnerabilities (like having that master key) can give the illusion of security
- Encryption in national security
    - Secure info about troop communications, information about troop movements, and unclassified but sensitive military research and technology

Weakening Encryption Violates Fundamental Rights

https://www.eff.org/deeplinks/2024/03/european-court-human-rights-confirms-undermining-encryption-violates-fundamental

- Case of Podchasov, European Court of Human Rights (ECtHR) ruled that weakening encryption can lead to general and indiscriminate surveillance of the communications of ALL users
- Violates HUMAN RIGHT TO PRIVACY
- 2017: Russia's government required providers to store and supply all communication data and content
    - Telegram refused, was blocked, fuel added to fire
- Infringes on: "Everyone has the right to respect for his private and family life, his home and his correspondence (Article 8 ECHR, right to respect for private and family life, home and correspondence)"
- Also protects right to FREEDOM OF EXPRESSION - international human rights law
- Continuous, blanket storage of private user data interferes with right to privacy

Economic Impact of Encryption Laws

www.internetsociety.org/wp-content/uploads/2021/05/The_Economic_Impact_of_Laws_that_Weaken_Encryption-EN.pdf

- Increase in business uncertainty
- Studies show that small investments in accelerating deployment of encryption capabilities resulted in very large gains to economy
    - The NIST (2018) study estimated that the internal rate of return on NIST's investment in promoting AES was 81%, significantly more than NIST's 7% cost of capital (under government regulations), and the aggregate net benefits to the

economy exceeded $USD 250 billion once all direct and indirect spillover effects are computed.

- Better brand image → higher sales over time and higher market value
    - Encryption backdoor threatens relative perception of trust
- Lost sales
    - Reduced consumption by buyers, shift to a competitor
- Operating costs

Encryption and India's Security and Law Enforcement Challenges

- Indian gov weakening encryption due to national security and law enforcement reasonings
- Gov officials pointed out to trouble in preventing terrorism, fake news, and crime against women and children
    - EXAMPLE OF THIS:
        - Attack in Mumbai in 2008 where terrorists were caught using Blackberry devices
        - Since 2017: mob violence and lynching that were incited due to misinformation shared on Whatsapp. Between 2017 and 2018, the spread of unchecked, fake and malicious information were found to be directly linked to mob violence. It was said that 34 people across 9 indian states were lynched due to misinformation on social media
        - Between 1998 and 2017, India reports the highest number of child pornography cases worldwide, and encrypted communications makes it difficult to identify culpable parties

Surveillance and Encryption

- What is gov surveillance: any activity whereby intelligence or police officials: (a) intercept communications in transit or (b) access stored communications.
- Encryption can make it more difficult for law enforcement to access these communications, while at the same time protecting user data from criminal hackers.
- When it comes to national security programs, the most important law is the **Foreign Intelligence Surveillance Act (FISA).**
    - Under this act, there is a **Foreign Intelligence Surveillance Court (FISC)** that must individually approve electronic surveillance of U.S. citizens or foreigners who are suspected of being a threat to national security
- Congress and the courts have imposed major restrictions on the ability of law enforcement agencies to gather electronic evidence. Most importantly, the **Electronic**

Communications Privacy Act (ECPA) requires police investigators to obtain a **court-approved search warrant** before they can eavesdrop or gather private data.
    - To this end, a law called the Communications Assistance for Law Enforcement Act (CALEA) lays out how telecommunications providers must help police enforce search warrants.
- Some degree of government surveillance is therefore necessary to keep the public safe.
    - **A surveillance authorized by FISA was critical to foiling a 2009 terrorist plot to bomb the subway in New York City**
- Fourth Amendment generally requires that government agents obtain a judicially approved search warrant before they can search someone's house, belongings, or—in many cases—electronic communications.
- Organizations like al Qaeda and ISIS use the Internet to spread their propaganda, attract recruits, and remotely plot terrorist attacks from relative safety. Their communications are needles in a massive haystack of global data. Even if intelligence agencies can single out their targets, terrorists can use encryption to make their messages unreadable.

POLICY APPROACHES TO THE ENCRYPTION DEBATE

- A term used in the law enforcement field, **"going dark"** refers to the process by which encryption or other techniques obscure information in ways that prevent the government from accessing it, even in situations wherein the government is otherwise authorized by law to do so
    - The FBI has expressed a "fear of missing out" on preventable crimes or prosecutable criminals, arguing that it cannot access the necessary evidence.
- The most commonly proposed solution is the installation of a "backdoor,"which is a way that enables the government or law enforcement to read encrypted communications and stored data
    - (Technology cannot inherently distinguish between good guys and bad guys, and thus any backdoor will open at least some possibility that hackers and rogue government officials will gain access.)
- Advocates on the law enforcement side have claimed that, with increasing prevalence of "default-on" encryption, to deny law enforcement a mechanism to access encrypted information will lead to more crimes going unsolved and further threats to public safety
-

What is end to end encryption: https://www.youtube.com/watch?v=c2OkOckSD20

https://www.jstor.org/stable/pdf/resrep25138.5.pdf?refreqid=fastly-default%3A8537103172420270506f32a2e0e0af8f&ab_segments=0%2Fbasic_search_gsv2%2Fcontrol&initiator=&acceptTC=1

Names: Nia Lam, Niki Jiang

What is encryption?

Encryption is the process of taking information and scrambling it to make it unreadable. This way the message is confidential as it's transmitted through a network like the internet. Once the message is received by the recipient, it's decrypted, translated back into its original form with an encryption key.

The Issue: Should law enforcements be allowed to break encrypted data?

Con for Law Enforcement Accessing Encrypted Data:

Law enforcement should not be able to break encrypted data because not only is it a violation of the people's privacy and influence the people's freedom of speech, it allows a weakness in a nation's national security, allowing foreign actors to potentially hack and see the nation's top information. In addition, encryption has shown more benefits to businesses, boosting the economy. Therefore to protect the public's trust, ensure the public's privacy and freedom of expression is protected, law enforcement should not be able to break encryption.

Pro for Law Enforcement Accessing Encrypted Data:

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.

Links:
Terror in the Dark
POLICY APPROACHES TO THE ENCRYPTION DEBATE
Surveillance and Encryption
Encryption and India's Security and Law Enforcement Challenges