COURSE PROJECT

Systems Security

Fred Schneider

Faculty Author
Cornell Bowers Computing and Information Science

Cornell University

Project Completed by: Germaine Wong

eCornell

COURSE PROJECT — PART ONE

Choosing a System

1. The first step is to choose a system that you will later use as the object of your project work. Consider the four possible systems described below, and select one that best matches your interests.

- Secure anonymous communication: This system enables users to communicate with one another secretly, accurately, and anonymously. Users can specify what information other users may learn about them and their communications.
- Electronic voting system: This system enables users to privately express their preferences about some issue. The system produces a verifiably correct aggregate of all the users' preferences.
- Grade management system: This system allows student grades to be stored by course staff, which may include TAs and professors, and to be retrieved by students. Grade information is stored in a back-end file system.
- Password manager: This system allows users to create and store usernames and passwords for other systems. Users can manage their passwords across different devices.

Functional Requirements

For the system of your choice, define its intended behavior in further detail. To do so, invent a list of functional requirements. (See previous Read page for details about how "functional requirements" should be interpreted in the context of this course.)

Secure anonymous communication:

User Type	Assets	User Story
New Users	Account	As a new user, I can create a new account without providing my personal identifiable information (PII)
Authenticated End Users	Account Settings	As an authenticated end user, I can access and make changes to my settings and preferences, including MFA settings
Authenticated End Users	Messages	As an authenticated end user, I can send and receive end-to-end encrypted messages anonymously without providing personal information

Authenticated End Users	Message Settings	As an authenticated end user, I can set sensitivity levels, restricting the recipient's ability to share messages
Authenticated End Users	Authenticity	As an authenticated end user, I can verify the authenticity of a message by verifying with the sender's public key
System Administrator	System Logs	As a system administrator, I can run regular security audits and check compliance by accessing system logs
External Auditor	Anonymized datasets	As an external auditor, I can see if privacy regulations and standards are being followed and met by reviewing anonymized datasets

Facilitator’s Comments

Good job selecting the secure anonymous communication system and defining its functional requirements, which shows a solid understanding of the system's goals and user needs. Your requirements show good focus on user anonymity, security, and data protection, highlighting the system's ability to enable secure and private communication.

Grade

100%

COURSE PROJECT — PART TWO

Threat Model

1. Against what kinds of attackers will your system defend? What are their motivations, resources, and capabilities? Don't just list vague, generic threats; make them specific to your system and its functionality.

My secure anonymous communication system will defend against Class II attackers, who find and exploit vulnerabilities and/or flaws using new methods to gain access. These attackers' motivations lie both in harm and in gain. When causing harm, one intent would be to shut down communications by attacking vulnerabilities within the servers and network of the company hosting the physical infrastructure on which the software for the users runs. A second harm intent would be shutting down the access to messages for the end user by using phishing to gain access to the user's phone and/or account. When attacking for gain, the intent would be to exfiltrate data from the end user and/or communications company for the purpose of obtaining ransom, for extortion, selling the information on the dark web and/or leaking of the communications, with the main goal being profit.

The resources an attacker would use on this system include: static and dynamic analysis tools (static is used to find vulnerabilities, dynamic is used to identify bugs and look at memory usage), their own exploits that target hardware/software vulnerabilities and backdoors to change the behavior of the target system, knowledge of attack surfaces (used to gain unauthorized access to servers or employee computers and carry out an attack), moderate level of funding (~$10K-$100K), knowledge of pen testing techniques (using tools to penetrate as far as possible into a system), an advanced knowledge of how to analyze systems in order to locate specific vulnerabilities, access to high end workstations and controlled environments (isolation from external networks, use of Tor/VPNs, using air gapped systems), dark web access (using Tor to access hidden networks, a place to sell exfiltrated data, anonymization), and custom scripts.

One of the capabilities an attacker has for this system includes compute time of hours to weeks or longer, depending upon the attack level desired. Longer-term compute job of key extraction, since encryption is a big part of secure communications. In terms of memory, having enough RAM (64-128 GB) to be able to run a VM with 4-16 virtual CPUs. In terms of the high end workstations, or for large table lookups (correlation of inputs/outputs, rainbow tables to correlate encrypted content with plaintext) as well as for cryptographic attacks (i.e. collision), a minumum of a 24GB GPU with a 16 core CPU and 32-64 GB of RAM system is required.

2. If there are any non-threats, you should identify them as well. For example, you may wish to assume that some system components execute on hardware that is located in a physically secured machine room reachable only by trustworthy system operators.

Non-threats for a secure anonymous communication system include the assumption that physical access to company servers and infrastructure is only accessible by authorized workers via a combination of a key card programmed for physical access to the specific room(s) and biometric data (fingerprint, face scan, etc). Use of memory encryption, closed ports and disabling USB ports in addition to the ability to access rooms where infrastructure is located aids in this process.

Facilitator’s Comments

Good understanding here of cybersecurity risks, clearly defining the capabilities, motivations, and resources of Class II attackers targeting secure anonymous communication systems. By outlining defense strategies alongside non-threat assumptions, you show good awareness of layered security measures necessary to protect critical infrastructure.

Grade

100%

COURSE PROJECT — PART THREE

Security Goals

1. In this part of the course project, you will identify the assets and stakeholders involved with your system. This step should be easy because you already identified assets and users for each functional requirement. For each asset, identify its value to stakeholders.

With the asset of account, the value the end user gets includes: access to services and updates, enabling communication with other users, setting up MFA (how access account), continuity of access, secure way of signing into account, and the ability to access from multiple devices.

With the asset of account settings the value the end user gets includes: control over how notifications are received (or not), deciding who can see their information, being able to download any data collected, being able to delete their account or remove their personal data, having a sense of ownership, and protection against the ability to misuse the account.

With the asset messages the value the end user gets includes: identity protection, an environment that is secure so that real conversations can occur, messages are unable to be intercepted, that the intended recipient (and no one else) can read the message, knowing that the messages received/sent show a timestamp and can be verified as being from the correct person.

With the asset message settings the value the end user gets includes: selecting who can have access to their messages, ensuring anonymity, the ability to hide personal identifiers, deciding how much personal information is shared with the person receiving the messages, being able to block messages from specific senders, and the ability to send messages that delete themselves after being read to prevent storage or screenshots.

With the asset authenticity the value the end gets includes: knowing that you are communicating with the correct person, knowing that what a user sent you is not intercepted or modified en route, any messages or communications can be traced back to the proper source in the case of a legal dispute, lowers the chance of a phishing attack and/or malicious links

With the system logs the value the system administrator gets includes: allows the administrator to prevent security threats by being able to spot unusual behavior and get a baseline to help detect spikes in activity; detection of security threats by automated alerts, anomalies showing up, looking at failed logins, connections to unauthorized IPs; and provides a record that can be traced when responding to incidents.

With the anonymized datasets the value the third party auditor gets includes: the ability to analyze data handling practices while preserving the anonymity of users, evaluating system security, ensuring that the system is providing transparency about how it handles data to the users, making sure the system is behaving as it should be, and checking to see how the system performs and is able to handle increased usage.

2. Perform a harm analysis on assets; that is, identify all the things that might go wrong. You may find it helpful to use the template "Performing action on/to/with asset could cause harm." (Although you are encouraged to rewrite statements made with that template into more naturally flowing English.) Be as thorough and creative here as possible; this is the step at which you're most likely to overlook something that's important and relevant to security.

Asset: Account

-Performing account compromising on an account could cause harm.

-Performing de- anonymization on an account could cause harm.

-Performing the inability to access an account could cause harm.

-Performing social engineering on an account could cause harm.

-Performing data leaks of account could cause harm.

-Performing session hijacking on the account could cause harm.

Asset: Account Settings

-If MFA is not offered to the user in account settings, this could cause harm.

-Performing SSPR with account settings could cause harm.

-Allowing account recovery via an unsecured channel in account settings could cause harm.

-Allowing the use of defaults in account settings could cause harm.

-Not allowing a user to look at and and revoke sessions in account settings could cause harm.

Asset: Messages

-Performing tampering on messages could cause harm.

-Performing the leaking of timestamps/IP/access information on messages could cause harm.

-Messages not disappearing could cause harm. Receiver performing screen shots of messages could cause harm.

-Performing default backups of messages and keys could cause harm.

-Message body exposure without a password could cause harm.

-Performing long term storage of messages could cause harm.

-Performing malware with messages could cause harm.

-Performing forwarding/copying of messages could cause harm.

-Performing a breach of confidentiality on messages could cause harm.

-Using poor encryption practices with messages could cause harm.

-A user performing mistakes with messages could cause harm.

-Showing when a user is typing a message could cause harm.

-Lack of offline message protection could cause harm.

-Performing accidental de-anonymization with messages could cause harm.

-Allowing 3rd party links via messages could cause harm.

Asset: Message Settings

-The inability to allow or deny the forwarding of messages in message settings could cause harm.

-The inability to block screenshots in message settings could cause harm.

-Not being able to control read receipts in message settings could cause harm.

-Not being able to control notifications in message settings could cause harm.

-The inability to allow or remove timestamps in message settings could cause harm.

-The inability to set storage limits in message settings could cause harm.

Asset: Authenticity

-Performing impersonation of authenticity could cause harm.

-A breach of trust of authenticity could cause harm.

-Allowing non-rotating keys or non-revocation of keys for authenticity could cause harm.

-Not performing verification of users for authenticity could cause harm.

-Performing key reuse across multiple systems in regards to authenticity could cause harm.

-Performing key spoofing in authenticity could cause harm. Having a centralized key trust compromised that helps authenticity could cause harm.

Asset: System Logs

-Abused privileges by administrators on system logs could cause harm.

-Performing data leaks of system logs could cause harm.

-Performing log injection on system logs could cause harm.

-Performing longer log retention of system logs could cause harm.

-System logs being stored in plaintext could cause harm.

-Lack of access controls on system logs could cause harm.

-Administrators de-anonymizing users with system logs could cause harm.

Asset: Anonymized Datasets

-Performing a violation of GDPR/CCPA or other privacy standards of anonymized datasets could cause harm.

-Linking public or leaked datasets with anonymized datasets could cause harm.

3. Now transform the harms you've identified into security goals using the template "The system shall prevent/detect action on/to/with asset." Label each goal as being exactly one of confidentiality, integrity, or availability. Examine the feasibility of each goal in light of your threat analysis; if necessary, relax goals so that it is feasible to achieve them.

Account:

-The system shall attempt to detect a compromised account via comparison of current activity to baseline access through a new device or IP address or impossible device location movement. Integrity.

-The system shall prevent de-anonymization of an account with well designed protocols and strict security. Confidentiality.

-The system shall detect the inability to access an account on a general level like user inactivity. Availability.

-The system shall try to prevent social engineering on an account through education. Integrity.

-The system shall prevent data leaks of an account. Confidentiality.

-The system shall attempt to detect session hijacking on an account through careful and safeguarded session handling. Integrity.

Account Settings:

-The system shall provide MFA to the user in account settings while carefully balancing privacy, security and usability. Confidentiality.

-The system shall prevent SSPR in account settings as it is a good way to preserve privacy and prevent identity leakage. Confidentiality.

-The system shall prevent account recovery via an unsecured channel through account settings that rely on cryptographic mechanisms. Confidentiality.

-The system shall prevent the use of defaults in account settings by enforcing user-designed settings. Integrity.

-The system shall allow the user to look at and revoke sessions in account settings through the removal of tokens/keys tied to the session. Integrity.

Messages:

-The system shall prevent tampering of messages by using end-to-end encryption and digital signatures. Integrity.

-The system shall prevent the leakage of timestamps/IP/access information about messages by following strict logging policies. Integrity.

-The system shall remove self-destruct messages via auto-deletion. Integrity.

-The system shall educate regarding the use of screenshots of messages. Integrity.

-The system shall minimize backup exposure of messages and keys. Confidentiality.

-The system shall prevent message body exposure without a password with messages by balancing convenience and security. Confidentiality.

-The system shall prevent the long term storage of messages. Integrity.

-The system shall prevent most malware from being shared in messages by incorporating the use of a malware scanner. Integrity.

-The system shall use a multi-layered approach to attempt to prevent a breach of confidentiality of messages. Confidentiality.

-The system shall prevent poor encryption practices on messages. Integrity.

-The system shall detect a user making mistakes with messages with real-time alerts. Integrity.

-The system shall prevent showing when a user is typing a message. Integrity.

-The system shall provide offline protection for messages that users will have to set up through FDE. Confidentiality.

-The system shall work to prevent accidental de-anonymization in conjunction with a vigilant user. Confidentiality.

-The system shall prevent the use of 3rd party links in messages by blocking/filtering those with external URLs but needs to balance this with usability. Integrity.

Message Settings:

-The system shall give the option to allow or deny the forwarding of messages in message settings only within the application. Integrity.

-The system shall include the option to use watermarking in message settings to deter the use of screenshots. Confidentiality.

-The system shall prevent external monitoring and prevent data leakage in order to control read receipts in message settings. Confidentiality.

-The system shall prevent the inability to control notifications in message settings by prioritizing privacy and usability. Integrity.

-The system shall prevent the inability to toggle timestamps in message settings by using attention to metadata management. Integrity.

-The system shall allow the user to set storage limits in message settings including notifications of impending removal and ensuring the data is securely deleted. Integrity.

Authenticity:

-The system shall prevent impersonation on authenticity. Confidentiality.

-The system shall prevent a breach of trust on authenticity through careful design. Integrity.

-The system shall combine secure key management with cryptography to prevent the non-rotation or non-revocation of keys used in authenticity. Integrity.

-The system shall enforce the verification of users through verifiable credentials in order to maintain authenticity. Confidentiality.

-The system shall prevent key reuse across multiple systems through sophisticated mechanisms (PKI, decentralized key management systems) for authenticity. Integrity.

-The system shall balance user experience and privacy with security to prevent and detect key spoofing for authenticity. Confidentiality.

-The system shall prevent having the centralized key trust compromised through key escrow and redundancy to ensure authenticity. Confidentiality.

System Logs:

-The system shall prevent abused privileges by the system administrator on system logs by using the principle of least privilege and RBAC. Integrity.

-The system shall detect data leaks of system logs through a combination of best practices and technical measures. Integrity.

-The system shall use a multi-layered approach to prevent and detect log injection on system logs. Integrity.

-The system shall prevent longer log retention of system logs through mitigating risks. Integrity.

-The system shall use a combination of security measures to prevent the use of plaintext to store system logs. Integrity.

-The system shall have access controls like RBAC on system logs. Integrity.

-The system shall use procedural safeguards and technical controls to prevent system administrators from de-anonymizing users with system logs. Confidentiality.

Anonymized Datasets:

-The system, designed with proper data management policies and privacy safeguard, shall prevent a violation of GDPR/CCPA and other privacy standards with anonymized datasets. Confidentiality.

-The carefully designed system shall prevent the ability to link public or leaked datasets with the anonymized datasets. Confidentiality.

Facilitator's Comments

Nicely done. You've done a good job identifying assets and stakeholders, performing a harm analysis, and transforming harms into security goals for various system components. Your work shows a good understanding of potential security risks and threats, and your security goals are well-defined and categorized into confidentiality, integrity, and availability.

Grade

100%

COURSE PROJECT — PART FOUR

Enforcement

1. For each security goal, explain how you might enforce it. Consider whether it would be best enforced by prevention, recovery, or deterrence. Attenuate your goals where appropriate to ensure that they can be met by the corresponding security mechanism.

For each of your recovery goals, identify which principals will need to be authenticated, what those principals are authorized to do, and what actions or states would need to be audited to enable recovery or deterrence.

Account Goals:

-The system shall attempt to detect a compromised account via comparison of current activity to baseline access through a new device/IP address or impossible device location movement. Enforcement: Prevention, because it's a proactive measure. How it would be enforced: monitoring, security policy, behavioral sensors, IDS, vulnerability scanning.

-The system shall prevent de-anonymization of an account with well designed protocols and strict security. Enforcement: Prevention. How it would be enforced: encryption, compliance checks.

-The system shall detect the inability to access an account on a general level like user activity. Enforcement: Recovery, need secure account recovery or re-authentication workflow. How it would be enforced: security awareness and training programs.

-The system shall try to prevent social engineering on an account through education. Enforcement: Prevention. How it would be enforced: DLP, encryption, IDS.

-The system shall prevent data leaks of an account. Enforcement: Prevention. How it would be enforced: use DLP to stop leaks before they happen, encryption, IDS.

-The system shall attempt to detect session hijacking on an account through careful and safeguarded session handling. Enforcement: Prevention. How it would be enforced: monitoring, security policy, IAM, behavioral. sensors, IDS, vulnerability scanning.

Account Settings Goals:

-The system shall provide MFA to the user in account settings while carefully balancing privacy, security, and usability. Enforcement: Prevention. How it would be enforced: MFA is a prevention control, authentication mechanisms, IAM.

-The system shall prevent SSPR in account settings as it's a good way to preserve privacy and prevent identity leakage. Enforcement: Prevention. How it would be enforced: avoid the use of insecure recovery channels, access controls.

-The system shall prevent account recovery via an unsecured channel through account settings that rely on cryptographic mechanisms. Enforcement: Prevention. How it would be enforced: cryptography, mandatory access controls.

-The system shall prevent the use of defaults in account settings by enforcing user-designed settings. Enforcement: Prevention. How it would be enforced: forcing customization makes it harder for attackers to rely on weak configs via mandatory access controls, upon account creation the program immediately goes to account settings and gives requirements.

-The system shall allow the user to look at and revoke sessions in account settings through the removal of tokens or keys tied to the session. Enforcement: Recovery. How it would be enforced: damage control and remediation by user to regain control over account, user would need to be authenticated an authorized to revoke active/previous sessions, session states, system and processes would need to be audited to enable recovery.

Messages goals:

-The system shall prevent tampering of messages by using end-to-end encryption and digital signatures. Enforcement: Prevention, proactive. How it would be enforced: encryption and digital signatures.

-The system shall prevent the leakage of timestamps, IP addresses and access information about a message by following strict logging policies. Enforcement: prevention. How it would be enforced: strict logging policies.

-The system shall remove self-destruct messages via auto-deletion. Enforcement: prevention. How it would be enforced: message removal by design that developers include in the application code.

-The system shall educate regarding the use of screenshots of messages. Enforcement: Deterrence. How it would be enforced: security awareness and training programs.

-The system shall minimize backup exposure of messages and keys. Enforcement: Prevention.

How it would be enforced: retention labels, retention policies, label policies.

-The system shall prevent message body exposure without a password with messages by balancing convenience and security. Enforcement: Prevention. How it would be enforced: security policies, encryption of data at rest, secure enclave.

-The system shall prevent the long term storage of messages: Enforcement: Prevention. How it would be enforced: retention labels, retention policies, label polcies.

-The system shall prevent most malware from being shared in messages by incorporating the use of a malware scanner. Enforcement: Prevention. How it would be enforced: malware scanners.

-The system shall use a multi-layered approach to prevent a breach of confidentiality of messages. Enforcement: prevention. How it would be enforced: defense in depth, IDS.

-The system shall prevent poor encryption practices on messages. Enforcement: Prevention. How it would be enforced: proper key management, code signing, digital signatures.

-The system shall prevent showing when a user is typing a message. Enforcement: Prevention. How it would be enforced: exclude the feature.

-The system shall provide offline protection for messages that users will have to set up through FDE. Enforcement: Prevention. How it would be enforced: encryption of data at rest, bitlocker/firevault.

-The system shall work to prevent accidental de-anonymization in conjunction with a vigilant user. Enforcement: Prevention. How it would be enforced: masked identifiers, system design.

-The system shall prevent the use of 3rd party links in messages by blocking or filtering those with external URLs but needs to balance this with usability. Enforcement: Prevention. How it would be enforced: check link against allow/deny list, only download content if user allows.

Message Settings Goals:

-The system shall give the option to allow or deny the forwarding of messages in message settings only within the app. Enforcement: Prevention. How it would be enforced: limit data flow within the system.

-The system shall include the option to use watermarking in message settings to deter the use of screenshots. Enforcement: Deterrence. How it would be enforced: associate identifiable info with messages.

-The system shall prevent external monitoring and prevent data leakage in order to control read receipts in message settings. Enforcement: Prevention. How it would be enforced: secure key management - decentralized, rotated, PKI; metadata; user behavior.

-The system shall prevent the inability to control notifications in message settings by prioritizing privacy and usability. Enforcement: prevention. How it would be enforced: privacy controls.

-The system shall prevent the inability to toggle timestamps in message settings by using attention to metadata management. Enforcement: Prevention. How it would be enforced: metadata management, labels.

-The system shall allow the user to set storage limits in message settings, including notifications of impending removal and ensure the data is securely deleted. Enforcement: Recovery. In order to recover, use a post-use data lifecycle, mitigate residual data risks. Notification prepares a user regarding cleanup of messages. The principal to be authenticated is the user, who is allowed to ensure the correct messages and data are being removed.

Authenticity Goals:

-The system shall prevent impersonation on authenticity. Enforcement: Prevention. How it would be enforced: authentication and authorization mechanisms.

-The system shall prevent a breach of trust on authenticity through careful design. Enforcement: Prevention. How it would be enforced: identity models, IAM.

-The system shall combine secure key management with cryptography to prevent the non-rotation or non-revocation of keys used in authenticity. Enforcement: Prevention. How it would be enforced: decentralized key management, cryptography, PKI.

-The system shall enforce the verification of users through verifiable credentials in order to maintain authenticity. Enforcement: Prevention. How it would be enforced: IAM.

-The system shall prevent key reuse across multiple systems through sophisticated mechanisms (PKI, decentralized key management) for authenticity. Enforcement: Prevention. How it would be enforced: PKI, unique key use enforcement.

-The system shall balance user experience and privacy with security to prevent and detect key spoofing for authenticity. Enforcement: Prevention. How it would be enforced: system design, technical safeguards.

-The system shall prevent having the centralized key trust compromised through key escrow and redundancy to ensure authenticity. Enforcement: Prevention. How it would be enforced: key escrow, redundancy, quick shutdown in case of an emergency.

System Logs Goals:

-The system shall prevent abused privileges by the system administrator on system logs by using the principle of least privilege. Enforcement: Prevention. How it would be enforced: least privilege, log auditing, RBAC, privilege access management (PAM), continuous monitoring.

-The system shall detect data leaks of system logs through a combination of best practices and technical measures. Enforcement: Recovery. To recover, security team/IR team identifies incidents so can be recovered from/contained, state of the system and processes would need to be audited. After mitigation, rescan, audit the results, verify the results and report findings.

-The system shall use a multi-layered approach to prevent and detect log injections on system logs. Enforcement: Prevention. How it would be enforced: input sanitization, logging security, read only access.

-The system shall prevent longer log retention of system logs through mitigating risks. Enforcement: Prevention. How it would be enforced: data retention policies.

-The system shall use a combination of security measures to prevent the use of plaintext to store system logs. Enforcement: Prevention. How it would be enforced: encryption, controls, cryptography.

-The system shall have access controls like RBAC on system logs. Enforcement: Prevention. How it would be enforced: RBAC, least privilege, insider risk management, JIT, JEA, PAM.

-The system shall use procedural safeguards and technical controls to prevent system administrators from de-anonymizing users with system logs. Enforcement: Prevention. How it is enforced: prevention by design, insider risk management.

Anonymized Datasets Goals:

-The system, designed with proper data management policies and privacy safeguards, shall prevent a violation of GDPR/CCPA and other privacy standards with anonymized datasets. Enforcement: Prevention. How it would be enforced: compliance and anonymization mechanisms, data geofencing by design, no PII included in information.

-The carefully designed system shall prevent the ability to link public or leaked datasets with the anonymized datasets. Enforcement: Prevention. How it would enforced: privacy-preserving techniques, including differential privacy (add mathematical noise), read only access.

Facilitator's Comments

Nice job on a comprehensive set of security goals for your system, ranging from preventing account compromise and message tampering to ensuring log integrity and protecting anonymized datasets. Your detailed enforcement strategies, emphasizing prevention through encryption, access controls, and vigilant monitoring, along with considerations for recovery and deterrence, show a good understanding of holistic cybersecurity design.

Grade

100%

COURSE PROJECT — PART FIVE

Public Policy

1. Discuss any ways your system could intrude on existing laws or affect social values.

There are multiple ways that a secure, anonymous communication system could intrude on existing laws. Legal tension arises from the concepts of privacy, anonymity, and free expression, which bump up against complying with legal obligations like law enforcement. The GDPR doesn't allow data storage or transferral outside of EU/EEA countries to any country that does not have what they consider to be stringent enough data protection levels (i.e. the United States) in addition to EU/EEA member states having their own supervisory authority that is in charge of investigating potential violations and handling complaints against companies. When anonymous systems support communications for terrorists or criminal organizations it conflicts with national security and law enforcement trying to identify and track these people, however, due to encryption, users are unable to be attributed to messages. It conflicts with privacy rights and the question of if the system provider will have to hand over data. The system also conflicts with the ability to disallow classified information from being shared on a platform, in violation of the Classified Information Procedures Act (sharing using a non-approved channel), The National Security Act of 1947 (using improper channels or disclosing to unauthorized persons even if encrypted if it pertains to intelligence or national defense), and The Federal Records Act (classified information shared outside approved systems). The Electronics Communications Privacy Act (ECPA) works to balance privacy with the need of law enforcement to have access to data when doing criminal investigations. Technology companies say encryption is needed to protect their users' privacy and may refuse to decrypt data.

There are many ways that social values can be affected by a secure, anonymous communication system. The first is that it can reshape how people relate to freedom, trust, accountability, safety, and social norms. When given the freedom of expression it can encourage open dialogue among people, and can also protect journalists, whistleblowers, and marginalized voices through anonymization and privacy, encouraging private thought and dissent. In low trust societies (authoritarian regimes, political instability, surveillance states, ongoing civil war) it has the ability to lower the fear of someone "outing" you and allows for communications of actions that are not being reported by the media, what people are witnessing, and guidance on how to stay safe. Increased surveillance can drive users to an anonymous communication system due to the lack of privacy. But in high trust societies (low levels of corruption, sense of shared values, government institutions that are accountable, etc) it can be a place to spread conspiracy theories - an "echo chamber" of sorts, to anonymously engage with people who think and feel the way you do which discourages civil discourse. When hidden behind a screen and anonymous, divisive rhetoric is more easily spread. This leads to the question of how do we distinguish between genuine communication and communication used for manipulation of facts? How do we hold people accountable for their speech, especially if they are leading a call to incite violence?

Facilitator’s Comments

Nicely done on &nbsp;how a secure, anonymous communication system can create legal conflicts around privacy, data protection, and law enforcement access, especially with regulations like GDPR and national security laws. Your work also shows understanding of the social impacts, recognizing both the benefits for free expression and privacy as well as the risks of misuse, echo chambers, and challenges in accountability.

Grade

100%

eCornell

Provide Feedback on this PDF

Submit Feedback