Assuming society is likely to collect a lot more information about us as individuals ,is this good or is this bad.

This depends on our private perspective.

We must be informed about the good and bad.

Spreading information might make our lives easier.

Information about ourselves being passed on to doctors and chemists so we can know what illnesses we will suffer from in future.

If the authorities can take in and process all information about individuals, we will have societies where we can more easily find those individuals who are bad for society.

Privacy enhancement tools

Cookies help to simulate sessions in HTTP protocol. Such as when we do shopping on a website.

Cookie – token that contains information about state of transaction on a network.

Although transaction can be any client-server interaction, cookie is used term in reference to interactions between web browsers and web servers.

Cookies minimize storage requirements of servers ,put burden of maintaining required information on the client(web browser).

Cookies used for more than session management.

Cookies used for keeping track of what users do and what users like.

Cookies consist of several values.

1)Name (or key) and value encoded into the cookie and represent the state. Interpretation is name has an associated value.

2) Expires field indicates when cookie is valid. Expired cookies are discarded.

If field not present cookie deleted at end of session.

3)Domain states domain for which cookie is intended. Consists of last n fields of domain name of server. Cookie sent to servers in that domain. Example, domain =.adv.com specifies cookie is to be sent to any server in adv.com domain.

4)Path further restricts dissemination of the cookie.

When web server requests cookie ,it provides a domain. Cookies that match domain maybe sent to server.

5)If secure field is set, cookie will be sent only over secured connections.

(HTTPS)

Ex – Caroline logs into web server ,www.books.com and adds 2 books to cart.

Web server sends a cookie with name bought and value BK=124 & BK-544.The domain of cookie is .books.com.

When she goes to buying page ,server asks for cookie with name bought.

Some websites allow tracking companies to add cookies on their site.

VPN’s and privacy

relationships between VPN’s and privacy

Have a network and a client who needs to talk privately within the network.

Client is located somewhere else.

Want to make a connection between a client and a server.

A tunnel with a protective barrier for communication between client and server.

A VPN, or Virtual Private Network, is a service that creates a secure, encrypted connection over a less secure network, such as the internet.

The primary purpose of a VPN is to provide privacy and security to users by creating a private network from a public internet connection.

1. **Encryption**: Data transmitted over a VPN is encrypted, meaning that it's turned into a code to prevent unauthorized access. This protects your data from hackers, ISPs, and government surveillance.
2. **Masking Your IP Address**: VPNs hide your IP address, making it appear as though your internet traffic is coming from the VPN server's IP address, not your own. This can help maintain anonymity online and prevent websites from tracking your location.
3. **Bypassing Geo-restrictions**: Since you can appear as though you are browsing from the VPN server’s location, you can access content that is geo-blocked or restricted in your actual location.
4. **Secure Use of Public Wi-Fi**: Using a VPN on public Wi-Fi networks helps protect your personal information from being intercepted by others on the same network.
5. **Remote Access**: VPNs are commonly used by businesses to allow employees to securely connect to the company's internal network from remote locations.
6. **Avoidance of Censorship**: VPNs can be used to bypass internet censorship in countries where internet access is restricted or controlled.

Anonymity VPN’s

Anonymity VPNs are specialized VPN services that focus on providing users with an anonymous browsing experience.

They take additional steps to ensure that a user's identity and activity online are not traceable back to them. Here's how they differ from standard VPN services:

1. **No Logs Policy**: Anonymity VPNs often have a strict no-logs policy, meaning they do not keep any records of user activity, connection logs, or any data that could be used to identify a user.
2. **Shared IP Addresses**: They typically use shared IP addresses, which means many users are assigned the same IP address, making it more difficult to trace activity back to a single user.
3. **Secure Protocols**: They utilize strong encryption protocols to ensure that all data transmitted through the VPN is secure and private.
4. **Kill Switch**: An automatic kill switch disconnects the user from the internet if the VPN connection drops, preventing data leaks.
5. **DNS Leak Protection**: Anonymity VPNs provide DNS leak protection to ensure that all DNS requests are routed through the VPN, preventing ISPs or third parties from seeing your DNS requests.
6. **Payment Anonymity**: These services often allow users to pay with cryptocurrencies or other methods that do not require personal information, adding an extra layer of anonymity.
7. **Tor Over VPN**: Some anonymity VPNs offer the option to route traffic through the Tor network in addition to the VPN, providing an additional layer of anonymity and security.

Remailers

A remailer is a service that anonymizes email content by stripping out header information from the email, thus concealing the sender's identity.

It functions as an intermediary that forwards email messages on behalf of its users, making it appear as though the email originated from the remailer service rather than the actual sender.

There are several types of remailers, with the two most common being:

1. **Pseudonymous Remailers (Type I)**: These remailers replace the sender's email address with a pseudonym. Although they provide anonymity, they don't necessarily hide all metadata. Users can receive replies at a pseudonymous address that the remailer knows to forward back to the user's actual address.
2. **Anonymous Remailers (Type II - Cypherpunk)**: These remailers use encryption and chaining to provide a higher degree of anonymity. The message is encrypted with multiple layers corresponding to multiple remailers in the chain. Each remailer in the chain decrypts one layer and forwards the message to the next remailer, without knowing the original sender or the final recipient. Replies, however, are often not possible with this type.
3. **Mixmaster Remailers (Type III)**: These are designed to resist traffic analysis.

Mixmaster remailers use a series of techniques to improve anonymity, such as fixed-length messages, padding, reordering of messages, and batching, which makes tracing the email back to the sender even more difficult.

Remailers are a part of the broader category of anonymity services on the internet, which aim to protect users' identities for privacy and security reasons. They can be essential tools for whistleblowers, political dissidents, and others who need to communicate sensitive information without revealing their identity. However, the use of remailers can be controversial, as they can also be used for malicious purposes due to the anonymity they provide.

Top of Form

How to have strong(proper) anonymity over web?

Remailers – general concept for ways to anonymize email

Let’s imagine have a situation where I want to on my laptop somehow send messages to someone else on the big internet.

I want to assure myself that recipient cannot know who I am.

Being a good guy but fear retribution from somebody.

Set up a pseudonymous remailer

This is a service out on the net whereby I can send emails specifying where I want them to go.

Have the recipient marked in my special anonymous email packages.

pseudonymous remailer strips all headers away from email.

Thing it passes on will not have any of original headers.

What headers look like in email?

View – message source

Can then see email SMTP headers

Headers continue until there is blank space.

This data can show who message comes from.

Simplest form of remailer – pseudonymous remailer.

If a government agency can break their way into a remailer then they can keep an eye on the traffic.

They will discover who is sending these things.

If I send things to a journalist, it would be nice if journalist could also reply and ask for clarification.

Can we have anonymity where we strip headers but allow someone to reply to the message?

Remailers manage these by having tables with mappings between real addresses and pseudo addresses.

If receiver reply to the pseudo address, the remailer will send it to original email id using the table they are keeping.

Still wanting to send an email anonymously and we reached a realization here that , if do it through box ,I have things to worry about. Can I trust the people to make it a very secure box.

If any one party could monitor the input and output of a remailer ,

A mixnet , short for mix network, is a routing protocol designed to anonymize the origin of data communications by using a chain of proxy servers called mixes.

Each mix collects and shuffles data before passing it on to the next, obscuring the trail back to the source.

The concept was originally developed by David Chaum in the 1980s as a way to provide anonymous email services.

Here's a simplified explanation of how mixnets work:

1. **Message Input**: A user sends a message intended for a recipient, but instead of sending it directly, the message is sent through a mixnet.
2. **Layered Encryption**: The message is encrypted in layers with the public keys of the mix nodes it will pass through. This is similar to the concept used by onion routing, which is the foundation of the Tor network.
3. **Mix Nodes**: Each node in the mixnet is a mix that performs a set of operations when it receives a batch of messages:
   * It decrypts the outer layer of encryption from each message, revealing the next destination and the remaining encrypted message.
   * It delays messages and reorders them, which breaks the timing and sequence patterns that could otherwise be used to trace messages.
   * It may also add dummy messages or split messages into smaller pieces, further obscuring the original message's path.
4. **Anonymity**: By the time the message exits the last mix in the chain, it is practically impossible to trace it back to the original sender, as the temporal and order patterns have been disrupted.
5. **Receipt by Recipient**: The intended recipient gets the message without knowing which path the message took through the mixnet or who originally sent it.

Mixnets are designed to defend against traffic analysis, a form of network surveillance that tracks the communication patterns between parties, rather than the content of the communications (which are encrypted). They are useful for any application where strong anonymity is desired, such as private messaging, secure voting systems, and circumventing censorship.

While mixnets offer robust anonymity, they can be slower than traditional networks due to the inherent delays introduced by the mixing process, and the need for multiple layers of encryption and decryption. Despite this trade-off, they are a critical technology for preserving privacy in an increasingly surveilled digital environment.

Mixnets and remailers both aim to provide anonymity for users, but they have different approaches and, as a result, different advantages. Here are some advantages of mixnets over remailers:

1. **Resistance to Traffic Analysis**: Mixnets are specifically designed to defend against traffic analysis. They do this by batching and mixing messages to make it difficult to trace the path of any single message. Remailers can also resist traffic analysis to some extent, but mixnets often use more sophisticated mixing strategies that can offer stronger protection.
2. **Timing Attack Protection**: Mixnets introduce variable delays and reorder messages, which helps protect against timing attacks. These are attacks where an adversary attempts to correlate the timing of messages sent and received to uncover the path of communication. Remailers may introduce delays, but mixnets often have more robust systems to randomize message delivery times.
3. **Scalability and Flexibility**: Mixnets can be designed to handle a large volume of diverse traffic, not just emails. This makes them suitable for a wider range of applications, including instant messaging, file sharing, and even web browsing, whereas remailers are typically specialized for email.
4. **Robustness and Redundancy**: The design of mixnets often incorporates redundancy, with messages able to take multiple paths through the network. This can make the system more robust against nodes being compromised or taken offline.
5. **Advanced Encryption Techniques**: Mixnets usually employ advanced encryption techniques and can be combined with other cryptographic systems (like public key cryptography) to further secure messages against potential interception.
6. **Support for Real-time Communication**: Some modern mixnets are designed to support near real-time communication, which is a significant improvement over traditional remailers that can introduce considerable latency.

However, it's important to note that the increased complexity of mixnets can also be a disadvantage in terms of higher computational overhead, potentially slower message delivery compared to some remailer services, and the need for more sophisticated software and protocols to manage the mixing process. Despite these trade-offs, mixnets provide a high degree of anonymity and are a critical technology for privacy-preserving communication on the internet.

Traffic analysis is a method of surveillance that examines the communication patterns between parties rather than the content of the communications themselves. Even if the content is encrypted and cannot be read, traffic analysis can reveal a significant amount of information. It's a form of network analysis that focuses on who is talking to whom, when, and how often.

Here are some aspects of communications that traffic analysis might study:

1. **Source and Destination**: Identifying the sender and recipient of messages or other data packets sent over a network.
2. **Frequency**: How often communications occur between certain parties, which can indicate the level of communication or the relationship's nature.
3. **Volume**: The size of messages or data transfers can sometimes indicate the type of communication (e.g., text message vs. file transfer).
4. **Timing**: The time at which messages are sent and received can reveal patterns of behavior and coordination between parties.