Schrodinger's Anonymity

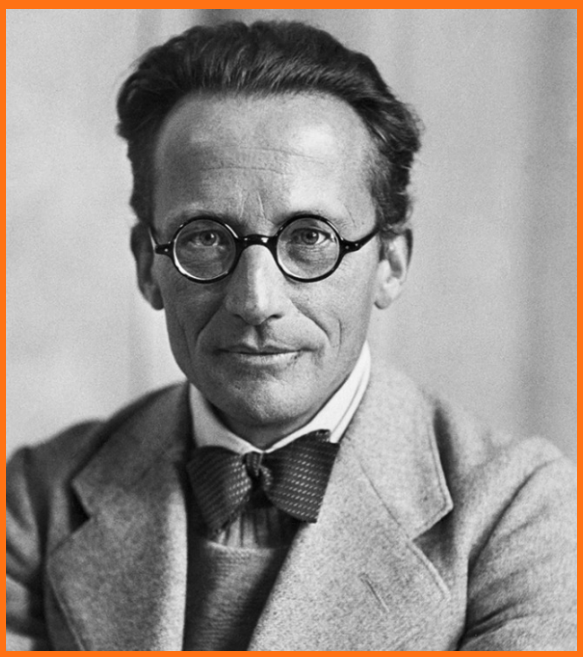
Anonymous Until Observed

INTRODUCTION

In 1935, Erwin Schrödinger proposed a thought experiment involving a cat in a sealed box with a flask of poison and a radioactive source. According to the principles of quantum superposition, until the box is opened and an observation is made, the cat is simultaneously alive and dead until observed. This paradox, known as Schrödinger's Cat, is a compelling metaphor for the nature of digital anonymity, particularly for Civil Society Organizations (CSOs) and individuals operating in sensitive environments.

Picture the internet as Schrödinger's box. Within this vast digital expanse, each user's attempt to remain anonymous exists in a state of superposition – preserved and compromised until the moment of observation. The "cat" in this scenario is the user's identity, existing in an uncertain state until someone attempts to identify them.

Just as the cat's fate remains unknown until the box is opened, a user's anonymity persists in a state of uncertainty until it's tested or challenged. This uncertainty principle of digital identity raises questions about the nature of privacy and persona for civil society organizations.



Erwin Rudolf Josef Alexander Schrödinger, sometimes written as Schroedinger or Schrodinger.

THE ANONYMITY SET

Succinctly defining anonymity starts with a universal set of all internet users. From that set, a subset of users with similar attributes can be drawn - the anonymity set. Anonymity can therefore be defined as the state of being unidentifiable within the anonymity set.

According to the International Organisation for Standardization, ISO99, anonymity requires that other users or subjects are unable to determine the identity of a user bound to a subject or operation. The concept of unlinkability is important to anonymity. Unlinkability demands that observers or adversaries are unable to determine if the same subject is responsible for specific operations or interactions in the system.

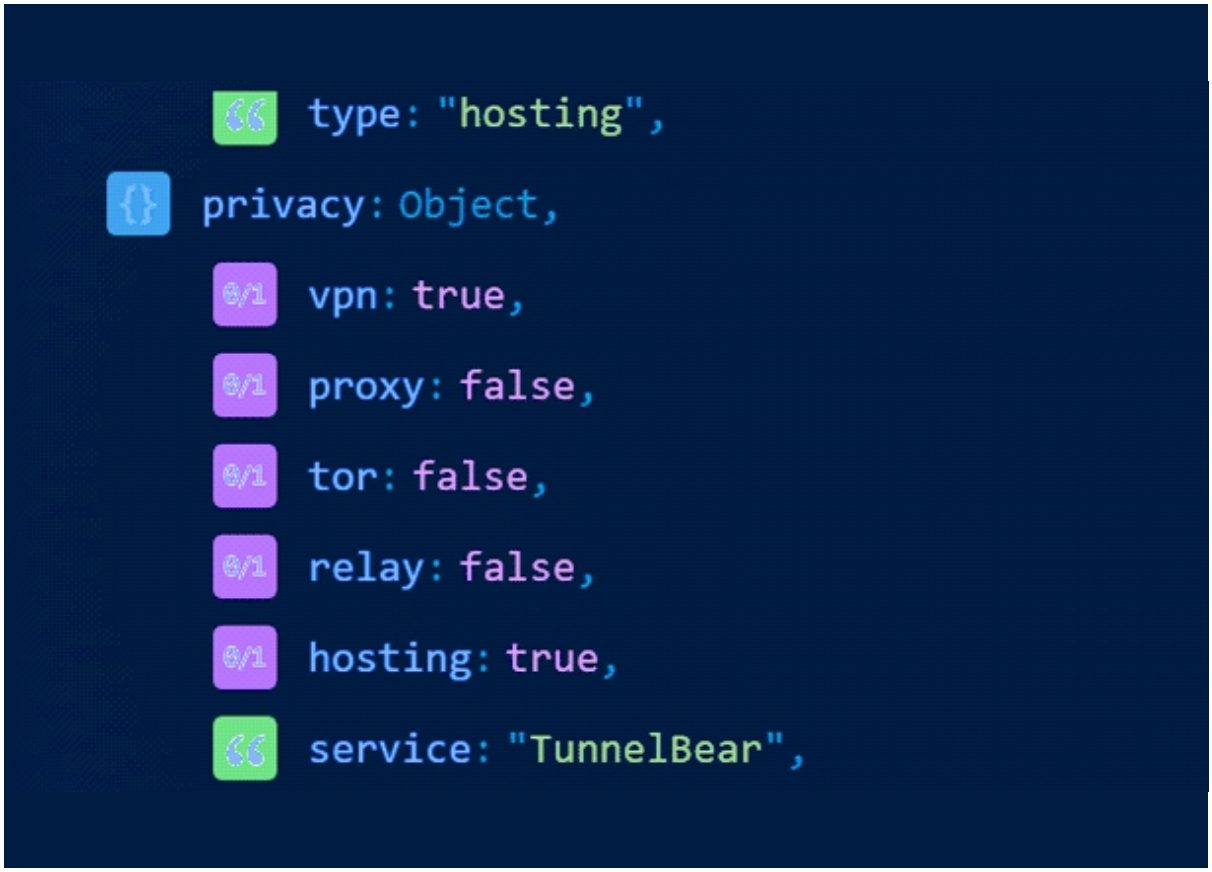
THE PARADOX OF PRIVACY-ENHANCING BEHAVIOURS

Ironically, as users and organisations take steps to protect their privacy, they may be making themselves more identifiable. Privacy-conscious users often adopt behaviours that differ significantly from those of typical internet users. These behaviours include using VPNs or Tor networks to mask their IP addresses, employing encrypted communication tools to secure their messages, regularly using private browsing modes to prevent tracking, and so on. While these actions are intended to enhance privacy, they can also cause users to stand out from the larger population of internet users who don't employ such measures.

These privacy-enhancing behaviours can create recognisable patterns across multiple websites and services, making users more trackable rather than less. This footprint, characterised by consistent use of the same set of tools or practices amongst a small set, can be observed across various platforms, allowing for identification and tracking despite attempts to stay anonymous.

By adopting uncommon privacy practices, users may inadvertently place themselves in a smaller group, reducing their anonymity. For instance, the number of Tor users is much smaller compared to the broader population of internet users, making it easier to single out individuals from within this group. Similarly, the frequent use of encrypted services can draw attention in certain contexts, marking users as outliers and making them more vulnerable to scrutiny.

These behaviours observed within a small set (the anonymity set) can lead to correlation attacks, where seemingly anonymous activities are linked together. For example, the timing of encrypted messages may be matched with other observable online actions, revealing connections between otherwise unrelated activities. Additionally, the use of specific privacy tools across multiple services can be tracked, creating a web of identifiable patterns that undermine anonymity.
Even when individual identifiers like IP addresses change due to the use of VPNs or Tor, the overall pattern of behaviour can create a persistent, unique fingerprint. This fingerprint is formed by the correlation of actions consistent with users in the anonymity set. For example, the site ipinfo.io is able to reveal the IP addresses of users as well as their service providers and if they are using a VPN service.



While they may not be able to see the content of encrypted communications, Internet Service Providers (ISPs) can observe detailed metadata about user behaviour. The timing and volume of data transfers create distinct patterns – for instance, streaming video generates a different traffic signature compared to browsing text-based websites. The true power of timing analysis was starkly demonstrated in a report from September 2024, where German authorities successfully compromised Tor's anonymity protections. By compelling major ISPs to monitor connections to specific Tor relays, law enforcement agencies were able to correlate entry and exit traffic through precise packet timing analysis. This technique allowed them to trace anonymous Tor users back to their real-world identities, effectively defeating the network's privacy protections through metadata analysis alone.

This leads to what we can describe as the "Anonymity Paradox":

1

As users take more steps to be anonymous, they often become part of a smaller, more distinct group.

2

This smaller group is easier for adversaries to monitor and analyze.

3

The very act of trying to be anonymous can become a trackable behaviour in itself.

CSOs seeking to protect their work might be putting a bigger spot on their backs as the tools and techniques they employ to protect their work and their stakeholders might be the very things that make them targets for further scrutiny.

THE STATE AND SURVEILLANCE TECHNOLOGY

Tools and networks for anonymous communication are vulnerable to many different types of attacks. While anonymity cannot be assigned a number, the adversary under consideration can determine how anonymity is measured. The most common types of adversaries are individuals or groups who can gain control of a portion of the network's nodes, and those who are state actors, having access to most passive and active communication lines within a jurisdiction.

Of the many legacies of the Second World War, the advances in electronic spying devices still present increasing threats to privacy in society. Today, governments across the world dedicate significant portions of their budget to acquiring advanced surveillance technologies. Recent research found that African governments collectively spent over $1 billion a year on digital surveillance technologies, supplied by companies in the US, the UK, China, the EU, and Israel. These technologies were used to spy on journalists and peaceful activists.

State adversaries employ a wide array of attacks and specific capabilities to obtain information and establish connections between targets and activities. The majority of these attacks result in a probability distribution that gives individuals a specific likelihood of being connected to their “anonymous” activities. The concept that even non-malicious service providers can be forced under legal or other compulsion, to reveal any information they have access to, provides a conundrum for individuals and groups seeking anonymity. Service providers have been under many circumstances forced to reveal any information they held concerning the origin or destination of a particular entity. An example of this is the PIDOM case.

CASE STUDY

The arrest of the anonymous Nigerian whistleblower operating under the pseudonym PIDOM in August 2024 highlighted the growing ability of governments to use legal and technical measures to unmask seemingly anonymous entities. PIDOM took the typical safety precautions; operated under a pseudonym, and leveraged the perceived anonymity of cryptocurrency transactions to receive support. He pinned his Tether and Bitcoin wallet addresses to his Twitter profile to keep his activities funded while circumventing the traditional banking system.

However, on August 13, 2024, Nigeria's National Security Adviser, Nuhu Ribadu, revealed that the government had frozen more than $37 million worth of cryptocurrency held in wallets believed to be owned by some organisers of #EndBadGovernance protests. Two of the addresses that were reportedly frozen by the Nigerian government were PIDOM's Tether and Bitcoin wallets.

The key to the government's ability to freeze cryptocurrency assets lies in the intersection between decentralised blockchain systems and centralised cryptocurrency exchanges. While blockchain transactions themselves are pseudonymous, the points where cryptocurrency intersects with traditional financial systems - namely, centralised exchanges - represent vulnerable chokepoints.

Subsequent analysis revealed that PIDOM's Tether address had multiple interactions with centralised exchanges like KuCoin, Binance, and OKX. The speculation that the Nigerian government compelled one of these exchanges to reveal PIDOM's identity highlights a critical vulnerability in the assumption of cryptocurrency anonymity. Governments, particularly those with significant geopolitical influence, can pressure companies operating within their jurisdiction or with ties to their financial systems.

THE WAY FORWARD / GETTING CLOSER TO ANONYMITY

By nature, the Internet's design allows service providers to observe numerous seemingly unrelated networks through cable lines and satellites. The advancement of technology (e.g. quantum computing and artificial intelligence) places a cap on the degree of anonymity that any system, tool or process can offer despite all security measures. The commodification of personal information for a range of digital services makes it difficult to separate offline identity from digital identity. Identifiers (email, usernames, phone numbers, etc) can be used to map digital identity to offline identity. While perfect anonymity remains elusive, especially against well-resourced adversaries, there are a few advanced techniques that can significantly enhance digital privacy.

DIGITAL COMMUNICATION

The options for virtual communication are many and more often than not, free. While these platforms have made it easier to communicate freely, they have also made it easier for governments, corporations, and other non-state actors to impede the right to privacy and freedom of speech. Some platforms offer messaging encryption amongst other privacy protection but that is usually not enough to maintain anonymity. Even the digital traces left by even seemingly innocuous online communications can pose a significant threat to anonymity. Metadata, the data sent over a network, can reveal communication patterns and expose participants. While end-to-end encryption may safeguard the content of a message, metadata such as message timing, size, and frequency remain vulnerable to analysis.

> *While end-to-end encryption may safeguard the content of a message, metadata such as message timing, size, and frequency remain vulnerable to analysis.*

When selecting a communication channel with the goal of anonymity, there are several key factors to be aware of to ensure your communications remain untraceable. For civil society organisations and human rights defenders operating under the threat of surveillance or persecution, the choice of communication tools can significantly impact their safety and effectiveness.

Selecting communication tools with a substantial and diverse user base in the user's location is non-negotiable, as this allows a user's activity to blend into a larger crowd, reducing the risk of standing out. The more users a network has, the harder it is to isolate and track a specific individual's communications.

The communication channel must provide robust end-to-end encryption to ensure that messages remain confidential and cannot be intercepted by unauthorised parties. While many popular messaging apps claim to offer encryption, they often fall short due to metadata collection practices. For instance, WhatsApp encrypts message content but still logs metadata from over 40 points including who communicated with whom and when. Contrary to popular opinion, Telegram is not an "encrypted messaging app", at least not by default. The app does not end-to-end encrypt messages by default. If a user wants to use end-to-end encryption in Telegram, they must manually activate a feature called

"Secret Chats" for every single private conversation they want to have.

Open-source messaging apps like Signal are ideal for anonymity. The source code is publicly available and undergoes regular audits by independent security experts, ensuring that they adhere to high standards of privacy and security. Additionally, if there was any tampering in the middle of communications, safety numbers would immediately change and the users would be immediately notified.

Another critical aspect of maintaining anonymity is the user-friendliness of the chosen communication tools. Complex systems can lead to user errors that compromise privacy, particularly if security settings are poorly labelled or difficult to navigate. A straightforward interface is essential to prevent accidental disabling of protective measures.

Furthermore, employing pseudonyms when creating accounts can significantly enhance privacy. For those seeking maximum anonymity online, utilizing the Tor network is highly effective; it masks IP addresses by routing internet traffic through multiple servers, complicating tracking efforts. Combining Tor with Tails OS—a system designed to leave no trace on the device after use—can provide robust protection against surveillance. Additionally, using a no-log VPN service alongside Tor can create layered security.

To further safeguard against prying eyes, individuals should enable two-step verification on their accounts, regularly update their software, utilize antivirus programs, and consider secure operating systems. In conclusion, while virtual communication tools have democratised interaction and made it easier for people to connect globally, they also pose significant threats to privacy. Therefore, careful selection of platforms and practices is essential for mitigating these risks effectively.

> *Selecting communication tools with a substantial and diverse user base in the user's location is non-negotiable, as this allows a user's activity to blend into a larger crowd, reducing the risk of standing out.*

FINANCIAL TRANSACTIONS

Traditional banking systems require extensive personal information for account creation, transaction processing and monitoring. This data is often stored in centralised databases that are vulnerable to breaches and governmental access requests. While these regulations aim to prevent illicit activities, they also create significant barriers to anonymity for legitimate users.

A promising alternative is the use of cryptocurrencies, which offer varying degrees of anonymity. Bitcoin, for instance, provides transparency that enhances security against fraud but it also means that anyone can trace transactions back to their origin. The points where cryptocurrency intersects with traditional financial systems, such as centralised exchanges, represent vulnerable chokepoints. These exchanges, operating within established legal and regulatory frameworks, can be compelled by governments or other powerful entities to reveal user information, effectively stripping away the veil of anonymity.

To mitigate this risk, individuals seeking anonymity can explore alternative approaches to financial transactions that enhance anonymity. One such method is Over-the-Counter (OTC) trading, which facilitates direct transactions between buyers and sellers, circumventing the need for centralized exchanges. Unlike traditional exchange trading, OTC deals are not visible on public order books; providing a discreet, direct channel between buyers and sellers. The process begins with finding a counterparty, which can be done through OTC desks run by exchanges or independent firms, via P2P platforms, or through personal networks.

Once a counterparty is found, negotiation takes place, where both parties agree on the price, quantity, and settlement terms, including any specific privacy requirements. The execution phase often involves escrow services for added security, ensuring the cryptocurrency is transferred directly between wallets. Finally, settlement occurs when both parties confirm receipt of the cryptocurrency, with any fiat currency exchanges handled separately from the digital transaction.

To maintain privacy in OTC trading, adhering to several best practices is essential. It is important to conduct due diligence to thoroughly vet OTC desks or counterparties, ensuring they prioritize client privacy and security before engaging in any trades. For transactional privacy, consider breaking large trades into smaller, less conspicuous amounts to avoid drawing attention. A multi-wallet approach on decentralized exchanges can further enhance anonymity by using separate wallets for receiving and sending cryptocurrency, making it harder to trace the flow of funds.

When combined with privacy coins (such as Monero) and mixers or tumblers—services that break transactions into smaller amounts and obscure their origins— this approach can significantly obfuscate the trail. However, cash still remains one of the most effective means of maintaining anonymity.

TRAVELLING

Many jurisdictions claim broad powers to search, seize, and even compel access to electronic devices. What might be a standard security practice in one country could be viewed as suspicious or even illegal in another. Some nations have stringent laws governing data access and surveillance that may impact how travellers use their devices while abroad. For journalists, activists, and individuals operating in high-risk environments, the integrity of personal devices is critical, as these devices often contain sensitive information that can be exploited if compromised.

The first step toward maintaining anonymity when travelling begins with meticulous evaluations. Before embarking on a trip, it is important to assess the necessity of bringing devices that store sensitive information. If a device is not essential for the trip, it is ideal to leave it at a secure location. When travel is unavoidable, using a backup device specifically configured for the trip can significantly reduce risks. Such devices should be stripped of unnecessary data and applications that could expose personal information or organisational resources.

In the absence of a travel device, the concept of "travel mode" can be adopted for primary devices. This involves creating a separate, minimalist configuration of the device that contains only the bare essentials needed for the journey. Password managers like 1Password provide this feature allowing users to remove vaults from computers and mobile devices and leave the ones safe for travel. Android devices also allow users to create multiple profiles with different email addresses and separate the data from each profile. Advanced implementations of this concept leverage sophisticated containerization or virtualization technologies to create isolated environments. These environments can be designed to leave minimal traces on the host system and can be quickly and securely erased if necessary.

When travelling with devices containing sensitive information, configuring them for maximum security becomes critical. This includes enabling full-disk encryption to protect data stored on the device. Encryption ensures that even if a device is lost or stolen, unauthorised users cannot access its contents without the appropriate decryption key.
If devices designated for sensitive operations don't have to connect to networks in foreign jurisdictions, “air gapping” is a security best practice. An air-gapped computer or network is devoid of any network interface controllers, which means it cannot be accessed remotely. The inability to connect these devices to unsecured networks means that even if an attacker gains physical access to a device, they would face significant challenges in extracting valuable data. Seemingly innocuous devices like smart hotel room systems or rental car infotainment units can potentially leave behind traceable footprints. Vigilant device management extends to disabling or physically blocking sensors and connectivity options on both personal and encountered devices.

Finally, physical security also plays a vital role in protecting devices during travel. It is important to keep devices within sight at all times and avoid leaving them unattended in public spaces or hotel rooms. Tampering detection mechanisms, ranging from tamper-evident seals to more electronic solutions that can detect and log unauthorized access attempts, should be standard practice. Upon returning from a trip, it is imperative to change passwords for any accounts accessed during travel.

Published by:

RESILIENCE
TECHNOLOGIES

www.rtafrica.org