Meta Problems: Government Access to Data in the Metaverse

Simon Sun (sunchi@iu.edu)
S.J.D. Candidate, Indiana University Maurer School of Law

Atta Tantratian (attantra@iu.edu)
S.J.D. Candidate, Indiana University Maurer School of Law

Mar Diez Henao (mardiezhenao97@gmail.com)
RegTech Analyst, ECIX Tech

1 Research Question

The Metaverse offers boundless possibilities for users, ...
yet concurrently presents new avenues for... CRIMINAL ACTIVITIES.

Given the following activities happened in the Metaverse:

- Abuse and harassment
- Drugs dealing
- Child pornography screening
- Money laundering using digital currencies

Metaverse is commonly understood as an interconnected realm of virtual landscapes and augmented reality domains, facilitating user interactions of diverse forms.

Search warrant
upon probable cause

OR

Court order / Subpoena
less stringent than probable cause

A research question arises: Which search standard should apply when the government accesses your data in the Metaverse?

The Metaverse, DAO, and Your Data

2 Ideally!

The governance of Decentralized Autonomous Organization (DAO) would avoid the 4th Amendment privacy concerns.

- In a DAO, personal information or transaction details are typically stored on a blockchain. Blockchains are **decentralized**, **pseudonymized**, and **transparent** by design, so the data isn't "given" to a singular third party and identities are secured.

From:	0xb26370...4fd55407
Interact With (To):	0x70916c...93A0a87D
Tokens Transferred:	**From** 0xb26370...4fd55407 **To** 0x70916c...93A0a87D **For** 879.999 ($333)
Value:	0 ETH ($0.00)
Transaction Fee:	0.00161699... ETH ($2.99)
Gas Price:	29.80694... Gwei (0.000000029806 ETH)

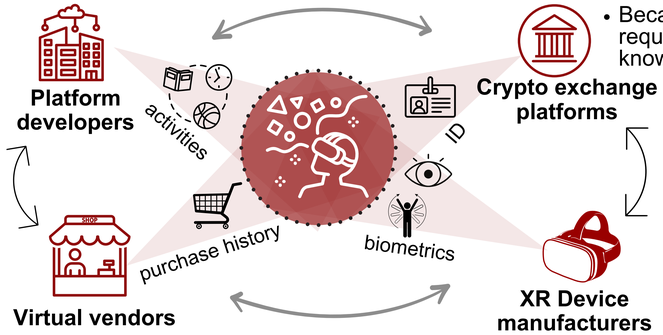
Who?

- **The notion of control is instrumental here. This creates the user's ability to control its data, assets, and identity.**

However!

3

Due to prevailing scalability concerns, a complete DAO is an ideal, where achieving a fully decentralized DAO is an ongoing journey. Today's norm remains the utilization of centralized, private storages from THIRD PARTIES.



- Because of the KYC requirement, they must know who you are!

Case Review:

- In *U.S. v. Gratkowski* (2020), law enforcement subpoenaed Coinbase, a crypto exchange platform, and obtained access to Gratkowski's identity without a warrant.
  - The court held that the defendant lacked a privacy interest in his personal data (1) located on Coinbase and (2) located directly on the blockchain.
  We disagree as it disregards the critical distinction between Blockchain and third party crypto exchange, lowering the standard of a search.

4 The 4th Amendment & The 3rd-Party Doctrine

For criminal prosecutions, law enforcement may need to obtain data about you from these third parties, giving rise to concerns regarding your expectation of privacy!

The **4th Amendment** requires that law enforcement obtains a warrant upon probable cause from court before conducting search. However, there exists **3rd-Party Doctrine** **exempting search warrant** for information held by 3rd parties.

The doctrine assumes that you have no expectation of privacy over information you already disclosed to someone else.

(No warrant needed)

Property

Historically, the Supreme Court's analysis of the Fourth Amendment relied on doctrines of "common-law trespass" in property law, such as in Olmstead v. U.S. (1928).

Expectation of Privacy

Later recognizing that "the Fourth Amendment protects people, not places," the Supreme Court in Katz v. U.S. (1967). The Fourth Amendment protects the "expectations of privacy consisting of the actual expectation (subjective) and one that society is prepared to recognize as 'reasonable' (objective)."

Property-based privacy

In response, textualist justices insisted that property is a basis for Fourth Amendment consideration, clarifying that the Katz's privacy test is merely an addition, not a substitution.

5 Current Regulations

To extend the 4th Amendment protection to include electronic communications, Congress passed the **Stored Communications Act (SCA)** in 1986. **(Too old!)**

Search rules under the SCA

- To access your **communications data** (180 days old or less),the police need a **warrant upon probable cause** from court!

(Warrant needed)

- **However, for other data**, the police merely need a **subpoena** (easier to obtain). The following become less protected data:

Older or opened communications data
"read" "seen"
180+ d/o

Personal info.
of you and your friends
- Name
- Date of birth
- Bank account
- etc.

Your **data captured by XR devices**
- Room environment
- Biometrics and possible inferences

Note that while the SCA protects data at rest, the **Wiretap Act protects data in transit.**

- To **intercept** your communications, the police need a **warrant upon probable cause**!
- **But will this rule apply to police patrolling in the Metaverse?**

Gap: As the SCA generally applies to phone/internet service providers--your data held by third parties like crypto exchanges and device manufacturers are less likely protected by the SCA.

Our Proposal: THE THEORY OF CONTROL

We believe the search standard under the 4th Amendment consideration in the Metaverse should focus on **the notion of control.**

Property (Control over one's space) ▶▶ **Expectation of Privacy** (Control over secrecy) ▶▶ **Property-Based Privacy** (Control over secrecy considering one's space)

→ **Control**

The reasons are that:

1) "Control" is an underlying component discussed in court decisions.

2) "Control" is instrumental to those who envision the Metaverse being a DAO.

We propose that "Control" in the Metaverse (C) directly correlates with the Government's search standard (S):

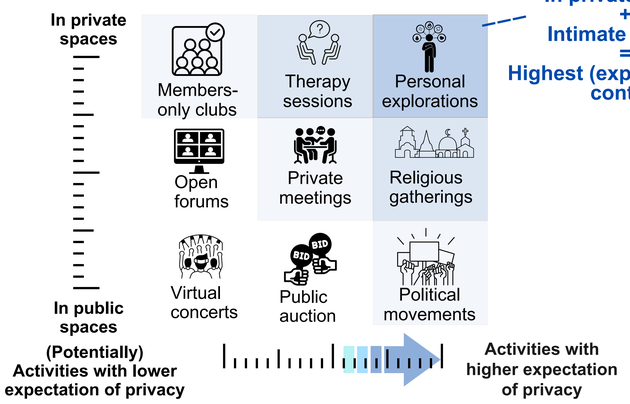
- **When C increases, S proportionally rises.** **C↑ = S↑**
- **Users maintain different levels of control, depending on the space they choose.**

1) The degree of decentralization
The higher degree of decentralization = the higher control

Decentralization degree can be determined by these factors...

- Administrative
  - Peer-to-peer connection
  - Node distribution
- Policital
  - Reg. compliance
  - Transparency / openness
  - Ownership structure
- Fiscal
  - Economic incentives

2) The nature of spaces and activities



In private space + Intimate activity = Highest (expectation of) control

HYPOTHETICAL CASE

A user built a **personal space** for their **self-explorations**. Although the platform is run by a third party, the user **implemented most controls** available (such as creating a world that can only be accessed through an NFT-key and trusting a platform that is fully administratively decentralized).

- As such, regardless of what activities the user did or items the user had in that space, **the government cannot ask the third party to disclose such information without a warrant upon probable cause.**