Privacy as invisibility (by default)

Bridging the gap between anarcho-capitalists and cypherpunks

Andrea Togni

MoneroKon 2022

Lisbon, 18-19 June

Who I am

- PhD in philosophy of perception (2018)
- History and philosophy teacher
- Libertarian (anarcho-capitalist)
- Self-taught Bitcoin and Monero enthusiast since 2017

Summary

1. Definitions of privacy
2. The problem with anarcho-capitalism and the current war on privacy
3. The metaphysics of privacy
4. Implications for Monero

Classic paradigms of privacy

- The right to be left alone (Westin)
- Social theories of privacy (Waldman)
- The right to control when, how and to whom personal information is made available to others
- Pseudonimity (Satoshi)
- Untraceability and unlinkability (von Saberhagen)
- Hiding, obfuscation, steganography...

Libertarian reductionism

- ✗ Privacy is *not* a natural right (Rothbard)
- ✗ Privacy is not an economic good (Klein)

Privacy as invisibility (by default)

- Privacy is the ability to make property invisible by default to enemies and visible by choice to trusted peers
- Exclusion and cooperation
- “Crypto” means “hidden”, “secret”

Ancaps or losers?

- The market provides better services at better costs than the state
- Why is it that the state always wins, while ancaps always lose?

The war on privacy

- Social credit score, digital IDs, cashless society…
- Criminalization, universality, capillarity, ostracism...

Resisting the war on privacy

- Axiom of resistance (Voskuil)
- Privacy is a strategy for liberty
- Avoiding the cockroach fallacy (Voskuil)

A better metaphysics of privacy

Realm	**Property**	**Privacy**
Body and mind	- Inalienable - Completely exclusive	- Gradual - It can never go to zero
External physical property	- Alienable - Exclusive until exchanged	- Gradual - It can go to zero
Information (ideas, data...)	**- Alienable** **- Constant homesteading of public knowledge**	**- All or nothing** **- Threat from aggregation**

Privacy as a strategy for liberty

Realm	**Privacy as a strategy for liberty**
Body and mind	*Ex ante* defense of property
External physical property	*Ex ante* defense of property
Information (ideas, data...)	**Condition of existence of property**

Ancaps, cypherpunks and...

- “The history of mankind is the history of ideas” (Mises)
- “Cypherpunks write code” (Hughes)
- “Computer technology is on the verge of providing the ability for individuals and groups to communicate and interact with each other in a totally anonymous manner” (May)
- “We don't much care if you don't approve of the software we write. We know that software can't be destroyed and that a widely dispersed system can't be shut down” (Hughes)

...Monero

- Playing at home
- No need for a widespread social upheaval
- Saving technology > NgU (NGMI) technology