Journal of Libertarian Studies
Volume 26, No. 1 (2022): XX–XX

Privacy as Invisibility (by Default): Bridging the Gap between Anarcho-Capitalists and Cypherpunks

Andrea Togni

ABSTRACT: This article argues that privacy (here defined as invisibility by default) is one of the best weapons to defend property rights. Privacy cannot be owned, but it is necessary to preserve property. Physical and tangible objects behave differently from information, ideas, and data with regard to property and privacy: while ownership of the latter is lost as soon as adversaries see them, this is not the case for the former. In both cases, however, making property invisible is crucial to keeping it safe. Ultimately, privacy is the ability to make property invisible by default to enemies and visible by choice to trusted peers.

A BRIEF OVERVIEW OF THE NATURE OF PRIVACY

This article shows why attaining invisibility is a prerequisite for any free society. In this paragraph, some of the most popular theories on privacy are discussed and contextualized. The next section provides some conceptual clarifications useful to better understand the purpose of this work. The third paragraph addresses the question of why the private sector has not been successful in replacing governments despite being able to provide better services at better prices. Lastly, the concept of privacy as invisibility (by default) with a special consideration of the digital realm is explained, and in doing so, the article calls for a structural

Andrea Togni (andrea.togni@protonmail.com) is an independent researcher currently working on privacy and the nature of money; he is also a high school teacher of history and philosophy. In 2018, he earned a PhD in philosophy.

alliance between anarcho-capitalists and cypherpunks. To paraphrase Rothbard, the cypherpunk ethos is the fullest expression of anarcho-capitalism, and anarcho-capitalism is the fullest expression of the cypherpunk ethos.

Before presenting the theory of privacy as invisibility (by default), it is useful to briefly recollect some of the main concepts that have been deployed to make sense of privacy. The purpose is not to defend or attack the classic approaches, but to place the subsequent discussion in a broader framework. All the theories outlined below give important insights into the nature of privacy. This article focuses on three main paradigms: privacy as the right to be let alone; privacy as control over personal information; and privacy as a social tool for sharing confidential information.

First, one of the most successful and meaningful privacy paradigms posits that privacy is the right of individuals to be let alone, the right to subtract oneself from the eyes of others in order to act freely and without concerns regarding others' reactions. As Westin (1969) points out, the right to be let alone can take four different forms: complete solitude and separation from others; sharing thoughts and interacting only with a small group of people, such as family members or friends; anonymity, which allows an individual to speak and act in public places, such as a park or the internet, without fear of being identified, so that her true ideas and emotions can be shared with no retaliation; and reserve, in which individuals maintain distance from others, so that during public activities they can choose to expose their inner selves only when comfortable. With solitude, intimacy, anonymity, and reserve, people try to defend their private thoughts and property from others' observation. Different levels of privacy are expected in different situations, and those expectations play a big role in shaping behavior.

A second, related theory ties privacy to the right to voluntarily disclose information about oneself: individuals need to control when, how, and to whom their personal information is made available. It is easy to see how this approach is related to the pressing issue of data protection in the internet era. Take, for example, the notice-and-choice paradigm that governs interactions with the internet: when people browse websites, they are notified of how companies will use their data, and then they can choose which uses to allow or to refuse to navigate further if the

requests are too burdensome. Data should not be understood as isolated: rather, it's often data aggregation that threatens privacy, because only by putting information together can users' most intimate habits be exposed and exploited. Daniel Solove (2009) presents a well-developed taxonomy of privacy and data collection that distinguishes between information gathering through surveillance and interrogation; information processing through aggregation, identification, insecurity, secondary use, and exclusion; information dissemination through breach of confidentiality, disclosure, exposure, increased accessibility, blackmail, appropriation, and distortion; and invasion through intrusion and decisional interference. Solove's deep dive into these privacy issues is very useful to grasp the consequences of the everyday production of personal data.

As Raymond Wacks (2015) points out, legislators around the world are aware of the impact of data dissemination on people's lives and have been building legal guarantees aligned with a number of principles. For example, the Organization for Economic Co-operation and Development (OECD) guidelines state that data can be collected only for lawful purposes and only if subjects consent; that data must be used only for the purposes for which it has been gathered; that data must not be disclosed unknown to users; that individuals have the right to correct information about themselves; and so on. Of course, the ongoing debate on how to legally and effectively protect data is lively and not at all settled. Take, for example, websites' terms of service (TOS). Reading TOS is useful to appreciate which kind of personal information users produce and how websites and third parties profit from using it. Unfortunately, TOS are often verbose and vague, and the common internet user chooses to agree to TOS without even giving them a quick look. Thus, TOS are not effective in protecting users' privacy; probably, broader legal protections should be considered, even tough, in the end, the best way to avoid the abuse of personal data is to prevent services and third parties from accessing and collecting it in the first place.

In recent years, some have noted that privacy is not only an individual right but has an intrinsic social dimension: the need to protect one's private life needs to be balanced with the need to disclose information to others. Accordingly, privacy has been tied to the multiple social roles people play over their lives: for example,

people behave differently at work, when they interact with their parents, during a romantic dinner with their partner, and when they fight on Twitter. In each situation, individuals choose to share only a limited amount of information: only what is required to perform the role in question, only the kind of information that put them under others' prying scrutiny. Without this self-protection, people would not have the confidence to engage with the world and to fulfill their social roles. Thus, personal information is not fungible: sharing one piece of information is not the same as sharing another piece of information, and sharing information with A is not the same as sharing that information with B. Context also plays a central role in how individuals manage privacy: it is appropriate to discuss how to raise children while dining with one's partner, but doing so with a stranger at a basketball game would be weird. Ari Waldman (2018, 69) goes as far as to state that "rather than a shield separating individuals and society, privacy is an element of social structure that facilitates sharing and social interaction by constraining the power of information holders." Thus, privacy can be understood as the trust people put in others to keep information confidential: people do not expect their doctors to disclose their medical history to the other patients, and people share their inner thoughts with their partners with the belief that they will not discuss them with random people on the internet. To invade privacy, then, is to breach trust.

It is important to note that social and individualist theories of privacy are not incompatible. Seeking seclusion signals a need for space and time alone, and does not necessarily imply that a person wants permanent or total isolation. People look for anonymity in public spaces precisely because they want to act freely in public. The need to protect data exists because people generate them in interacting with others and with publicly available platforms such as Twitter or Facebook. Thus, social and individualist theories are complementary. Also, endorsing the methodological individualist view that society results from human interactions resolves the alleged dualism between individuals and the collective.

The theories of privacy as the right to be let alone, as control over personal information, and as a social tool for sharing personal information provide the basis for the theory of privacy as invisibility (by default). Before presenting it, some clarifications are needed to avoid confusion and misunderstandings.

SOME CLARIFICATIONS

The following discussion is in the context of classic libertarianism,[1] according to which property, understood as the faculty to exclude others from enjoying a scarce resource, is the foundation of all human rights. As will be shown, privacy can be viewed as one of the main tools to protect property from invasion, especially by armed governments. As Peter Klein (2019) explains, privacy is not an economic good per se, because it is not something that can be sold or bought on the market. Rather, it's possible to exchange tools that help people attain privacy, such as window shades or privacy-focused cryptocurrencies. This point is crucial when considering privacy, the internet, and personal data. As Julian Assange (2016, 24) points out, there is a general tendency to "centralize control in those people who control the physical resources". It is a fact that when end users browse the internet, they do not just stay on their own property, because they need to interact with a web of servers, cables, software, and digital spaces that they do not own nor control.[2] In fact, consumers of proprietary hardware and software cannot even attain more than a surface-level knowledge of how these tools work.[3] This is why the idea that personal digital data should be thought of as the property of users is problematic. The fact that users do not own infrastructure that generates the data in some ways legitimates governments and big tech corporations' exploitation of personal data for their own profit. The point has long been a pain in privacy advocates' necks. In the *Olmstead v. United States* case of 1928, the Supreme Court of the United States (SCOTUS) decided that federal agents enforcing Prohibition didn't violate the Fourth Amendment when wire-tapping a telephone because a physical invasion of defendant's

---

[1] In this article, I discuss mainly the anarcho-capitalist variant of libertarianism and so treat the terms "libertarianism" and "anarcho-capitalism" as synonyms, even though the former is much broader in scope.

[2] To appreciate the general tendency toward the centralization of internet infrastructure, it is enough to realize that Amazon, which almost touched a market capitalization of $1.9 trillion in the second half of 2021, made 67 percent of its 2019 operating profits from its cloud service, Amazon Web Services (AWS). Another example of this centralization is the Google and Apple duopoly on app development for smartphones.

[3] The development of free and open-source software and hardware is crucial to give users more control over their data.

property had not occurred.[4] Privacy advocates have taken issue with the decision, but the court made a good point: How can a search be illegal if there is no clear definition of the property that it violated? The hidden problem revealed by the SCOTUS decision runs parallel to the one highlighted by Klein (2019): privacy is not an economic good per se. It is not something that is owned and subject to theft or invasion. As will become evident, this does not mean that privacy and property are unrelated, only that privacy should be understood as a tool to protect property although not property itself.

Another relevant clarification concerns the relation between privacy, mental states, and mental content. In a sense, mental states are always, by definition, private. Nobody other than me can enjoy the particular mental state that I'm experiencing right now; nobody will ever be able to experience the world as I do, and I will never be able to experience the world as somebody else does. Even Thomas Hobbes, a proponent of absolutism, recognized that the mind is a private space that governments cannot ever intrude upon. However, people can make the content of their mental states public; governments and criminals have always tried to torture their way into people's minds; right now, the reader is reading these thoughts on privacy, which are therefore public. What is crucial to underscore is that once thoughts, ideas, and theories are made public, there cannot be any meaningful exclusivity claim on them, notwithstanding the fact that the particular act of thinking always remains private. As soon as this paper is published, readers cannot be prevented from using its ideas; as soon as a listener catches information, that information is duplicated in her mind instantly and effortlessly. This is also true of digital content: as soon as personal data is made visible, it can be duplicated at basically zero cost by anyone able to see it. Given that duplicable information is not scarce, it cannot be an economic good, because it can be used by anyone who comes in contact with it; on the other hand, information that has not been shared remains in the

[4] The National Security Agency holds the same position nowadays. Snowden writes: "The agency's internal policies neither regarded your data as legally protected personal property, nor regarded their collection of the data as a 'search' or 'seizure.' Instead, the NSA maintained that because you had already 'shared' your phone records with a 'third party'—your telephone service provider—you had forfeited any constitutional privacy interest you may once have had" (Snowden 2019, 230).

exclusive possession of its owner. Of course, people do try to use the law to enforce ownership of something that can be duplicated at zero cost once made public. However, a strong argument can be made that such property claims are illegitimate, because they infringe upon the freedom of others to use their physical property and their minds as they like (Kinsella 2015). Once ideas and data enter others' minds the genie cannot be put back into the bottle: no public ideas and data can be made invisible again, and therefore no exclusive ownership of the original information can be reclaimed. As the next two sections will show, this feature of data, information, and ideas has consequences for the philosophical understanding of privacy.

In what follows, I assume that privacy is a tool for individuals to protect their property. A number of objections can be raised against this individualist approach. First, it may be said that individual rights are less important than social rights. However, it has already been pointed out that social theories of privacy are not incompatible with individualist approaches once methodological individualism is embraced. If the objection rests on the thesis that society cannot be reduced to the interactions between individuals, the burden of proof is on the critic to reveal the metaphysical nature of society. Here the simple and economical ontological view that individual actions and interactions should be taken into account in order to conceptualize privacy is assumed. Second, it may be objected that individualist understandings of privacy are too idiosyncratic to serve as the basis of a coherent theory. Although it is true that different people conceptualize privacy differently, this is not an issue in the anarcho-capitalist framework. Indeed, libertarians call consistently for legal systems based on the property rights that emerge spontaneously in the marketplace through the always evolving interactions between individuals: a similar bottom-up approach, combined with theoretical rigorousness, can be applied to privacy.[5] Third, some scholars point out that privacy should not be understood in terms of property rights, but in terms

[5] Another related issue regards the alleged failure of individualist theories of privacy to make sense of important distinctions like the one between public spaces and private spaces. For example, it may be held that individuals enjoy privacy in the sanctity of their homes but not in public areas, where society's interests dominate. As a rejoinder, it is enough to point out that in a pure libertarian society based on property rights, there is no such thing as a public space; the issues related to the public-private distinction affect only existent nonlibertarian societies.

of personal autonomy. However, personal autonomy cannot be enjoyed without the full ownership of the body and mind. As will be shown, privacy is a way to protect property rights, although it is not property itself. Fourth, some try to dismiss individualist approaches to privacy by noting that individuals are always at a loss when confronted with giant corporations and powerful governments. This is not so much an objection as a fact. The fact is that individuals are always the weakest minority of any society; therefore, governments and big corporations always try to take advantage of them.[6] Rather than abandoning individualist approaches to privacy, scholars need to recognize this fact and propose suitable countermeasures. A fifth objection is that privacy and property rights are not the appropriate tools to deal with information and data that can be duplicated at zero cost, because these are not economic goods. Although it is true that data and information differ from scarce physical goods, it will be shown that this does not foreclose the existence of privacy and property rights in the digital and information realms. On the contrary, the preservation of privacy in these domains is one of the most important conditions for the defeat of violent governments and the establishment of a free society. Moreover, it is condescending to attack the so-called secrecy paradigm, according to which information loses its private nature as soon as it is shared with someone. The secrecy paradigm is the simple recognition of a fact. When people allow personal data to spill out, they should expect it to be used against their interests. When people share their thoughts with a confidant, they accept the risk of these thoughts being propagated, whether they like it or not. Notwithstanding calls to make this and other kinds of propagation illegal, libertarians cannot help but recognize that it is legitimate for adversaries to take advantage of people's negligence and to use their knowledge for their own interests, because once information is in adversaries' minds, it is theirs, and it's immoral to prevent them from using their minds as they like (unless it entails physical aggression, of course). It is people's duty to manage their privacy and to impede their enemies from gaining a competitive advantage on them.

---

[6] For example, nowadays TOS reflect the interests of big corporations more than the concerns of powerless individuals. In an anarcho-capitalist society, TOS may be seen as a particular form of contract or fiduciary agreement that has to be crafted on the market; as such, TOS do not pose a conceptual threat to the understanding of privacy, even though they pose more practical issues than ever.

THE PROBLEM WITH CLASSIC ANARCHO-CAPITALISM

Ancapistan is the fictitious place where libertarian dreams are fully realized. Two main differences exist between Ancapistan and contemporary social organizations. First, Ancapistan is an anarchist society; that is, a society without a ruler who enjoys coercive power over her fellow men. Second, in Ancapistan, individuals interacting voluntarily on the market determine the rules respecting property rights completely. The strict connection between economics and society is highlighted by Murray Rothbard's famous quote: "Capitalism is the fullest expression of anarchism, and anarchism is the fullest expression of capitalism" (Salerno and McCaffrey 2016, 39). This paper is not the place to discuss how Ancapistan is organized.[7] It is enough to say that libertarians have shown convincingly and repeatedly that private enterprises are able to supply better services than the state without violating property rights and personal freedom. This is true in every sector, including justice and security, the traditional government arenas. The question of interest for this work is why governments have not been replaced and in fact absorb ever more economic resources if private companies are conceptually and practically suited to deliver better services. Of course, there is not a simple and all-encompassing answer, but this article submits that governments' ability to systematically violate people's privacy plays a significant role. Other important factors are, for instance, government direct or indirect control of the education system, widespread cronyism, monopoly on money issuance, and so on. However, privacy violations stand out because they go hand in hand with every other state regulation. For example, in order to enforce laws in the field of education, the state has to find ways to oversee the behavior of families, teachers, and administrators.

As said above, a libertarian society is a society that fully respects property rights. Among libertarians, it is usually accepted that property rights in the physical realm can be established through homesteading and through free exchange. Tangible objects have been the main topic of discussion for classical liberals since John Locke. However, in the contemporary world there are important

[7] Actually, there is no way to know a priori how Ancapistan would be organized because it depends on market dynamics that cannot be predicted.

areas where property rights are more difficult to assess: it is hard to claim ownership of information and data because they can be duplicated at no cost by anyone able to see them. Information and data are therefore both scarce and not scarce. They are scarce in the sense that a single piece of data makes learning something specific possible; they are not scarce because they can be duplicated endlessly without costs. Data and information are valuable, as shown by governments and corporations' appetite for them; but property rights are more difficult to establish and preserve in this domain than in the everyday world of tangible objects.

The problem of understanding the metaphysical status of property rights is not new in the libertarian literature. According to the natural rights camp, rights possess ontological weight, and they have to be understood as natural rights; according to utilitarians, property rights are just the most useful tools to build a peaceful and prosperous society. While adding the adjective "natural" does not make a theory sounder, it is also true that utilitarian approaches offer few guarantees: if it could be shown that the abolition of property rights is a net good for society, then utilitarians would argue that property rights should be abolished, but this is not an outcome most libertarians would embrace. However, all libertarians can agree on one point: regardless of the metaphysical status of property rights, they are always in danger of being lost, and therefore, they need to be defended appropriately. Stated otherwise, property does not exist without the ability to defend it. Attackers are not a scarce resource, and this fact must be recognized. According to Locke, self-defense is both a right and a duty of any individual: even though he suggests creating a government to defend property more effectively, he repeatedly asserts that all people have the right and the duty to defend themselves and others.

In the realm of tangible objects, the fact that property is visible doesn't imply a loss of ownership. A thief may know that someone owns a luxurious home at a certain address, but this does not mean that he knows how to take possession of it. Usually, the law and self-defense instruments such as alarm systems and guns are fairly effective in keeping abodes safe. Certainly, visibility is a vulnerability: thieves (and governments) often know something very valuable about people—where and how their wealth is stored; and with that information, they can draft a plan to steal people's wealth. Still, seeing others' physical property is not the same as

knowing how to get around its defense. This is not the case with ideas and digital data.[8] When someone utters something, it enters other people's minds immediately and effortlessly. When data is decrypted and made visible, anyone able to see it owns it, even if she doesn't want to use it. That is, ideas, information, and data are private if and only if they are not visible to others, in which case they are completely private. But if information is shared, it can at most be regarded as confidential, not private: there is no final guarantee that even the most trusted man on Earth won't make use of it carelessly or dangerously. Some mitigation may be put in place, such as a violent threat against disclosure or a contract imposing silence, but this is only mitigation. These measures do not change the fact that any person who hears or sees information is entitled to use it, thus rendering any exclusivity claim unsubstantiated. In contrast, if someone sees someone's house and wants to take control of it, he needs to successfully carry out a legitimate (nonviolent) or illegitimate (violent) plan.

Establishing property rights in the physical realm differs from establishing property rights in the mental and digital spheres. But in both cases, making property invisible helps keep it safe. The black market is arguably the freest market because violent governments cannot see it and therefore cannot interfere with it: in black markets, individuals are free to interact as they want, without external regulations imposed through the threat of violence.[9] Agorists have understood black markets' importance to the preservation of tangible property and freedom very well (Konkin 1980; Mayweather 2021; Smuggler and XYZ 2018). Similarly, making data invisible to the prying eyes of attackers is key to protecting intangible property and should thus be a priority for anyone libertarian minded. Brunton and Nissenbaum (2016, 51, 53) point out the risks implied by the asymmetry of power that is created once we share personal information:

---

[8] In this paper, I'm not making any ontological statement on the difference in nature between physical objects and intangible information, ideas, and data. Even if the latter were regarded as physical objects based on a physicalist or reductionist view, this would not impact my analysis, which belongs to the field of political philosophy.

[9] Of course, any time tangible property is made visible to others, it may become prey to malicious attackers, so appropriate means of defense must be put in place to avoid the loss of property. This is true in black markets as well as under any other circumstances.

> Big data methods take information we have willingly shared, or have been compelled to provide, and produce knowledge from inferences that few—least of all we individual data subjects—could have anticipated. . . . Those who know about us have power on us. They can deny us employment, deprive us of credit, restrict our movements, refuse us shelter, membership, or education, and limit our access to the good life.

In the information domain, property rights are more difficult to preserve than in the physical domain because ownership of information, ideas, and data is lost as soon as others perceive them. On the other hand, tangible property can never be as secure as property in data and ideas that have not been shared with anyone.

Unfortunately, governments are well aware of the fact that property cannot be defended adequately without appropriate privacy; that is, without a well-developed strategy to keep it invisible. In most Western countries, black markets constitute only a small subset of the economy, and can exist only as long as complicit governments tolerate them. Also, governments are very successful in recording the vast majority of online events in collusion with big corporations. These facts help explain why the free market has been unable to supersede governments despite offering better services in all areas. The state will use its monopoly on violence against its competitors for as long as they fail to preserve their privacy effectively—that is, so long as people are visible and therefore attackable. It does not matter that the market is more effective than the government by any metric. What matters is that governments are stronger and more powerful than any other social actor. To believe that the state will not make use of its exorbitant force to impose its will (even retroactively and without notice) is wishful thinking. Given this reality, how can Ancapistan become reality instead of remaining utopia?

PRIVACY AS INVISIBILITY (BY DEFAULT)

In order to build a libertarian society, competition with the government on its own terrain must be avoided. The state can exploit infinite fiat money to arm itself, while common people cannot. Also, plans to use violence against the government cannot be successful without the population's full support, which is often lacking: most people see governments as legitimate powers and do not want to engage in revolutionary acts. On the rare occasions when governments are toppled, they are substituted with other governments, making all revolutionary efforts fruitless from an anarcho-capitalist perspective.

Libertarians must shift their resistance strategy to their own advantage. Privacy is their primary weapon. In this context, privacy is simply the ability to make one's property invisible to attackers, and it is a necessary condition for the enjoyment of property rights in information. Accepting this definition of privacy does not entail an attack against the other approaches discussed earlier; on the contrary, privacy as invisibility is broad enough to embrace most of the intuitions dear to privacy-loving authors. For example, being invisible by default means that people are in a position to be left alone if they so desire and that they can decide autonomously whether to share data and knowledge about themselves. The goal of invisibility (by default) does not entail being antisocial or completely isolated: rather, what is being claimed is that visibility should be optional. Privacy allows people to share something with others voluntarily, without being forced to do so. Also, privacy violation should not be conflated with violence nor with freedom per se. Accordingly, *Merriam-Webster*'s definition of privacy as "freedom from unauthorized intrusion" is somewhat simplistic. The preservation of privacy is one of the main *conditions* for the preservation of freedom, and safeguarding privacy is one of the most effective ways to hinder violence against goods, ideas, and people. However, if A violates B's privacy, it does not follow that A is doing physical violence to B, even though A is now in a better position to harm B and B's freedom to use her property away from intrusive eyes and actions is threatened. In the digital data domain, if one is not careful in covering one's tracks, adversaries gain a considerable advantage, which, unfortunately, can be transmuted into physical violence. Even though a privacy violation is not itself actualized violence, it is a *necessary* condition for actualized violence. In the physical domain, being punched by A requires that A knows where the victim is; taxation (that is, being stripped of property by the state) requires the state to locate citizens' property.[10] In the digital domain, the exploitation of data

[10] In the case of consumption taxes, the state must be able to observe that an exchange is taking place to collect its "revenue." Here the victim of privacy violation is not so much the customer, but the merchant, who is under the watch of taxmen and who needs to pay them; without this violation, customers would not be forced to pay more than market prices for goods and services. Some sort of privacy violation emerges with regard to every government regulation. For example, in order to *enforce* normative barriers to enter a business, the state needs to see and trace its citizens' activities. In general, as the Greek philosopher Antiphon underscored millennia ago, every human (positive) law is effective only if legislators

implies the ability to see it. To sum up, invisibility by default is a prerequisite for the free enjoyment of property.

Physical property and personal data need to be hidden from the prying eyes of governments. Privacy is not a black-and-white state; it is never absolute: rather, it is an endless race to hide from ever more sophisticated attacks. Agorists explained quite well how black markets and underground economies can thrive in a world mostly controlled by governments. But physical objects are always more or less visible, and therefore, privacy in the physical realm is structurally limited. This fact helps to explain the continuous existence of the state despite its well-known inefficiencies and brutalities: government agents can see the people under their jurisdiction more often than not, and therefore can seize their property and enforce state rules. Of course, people can always try to hide their property better than before, but they are at a structural disadvantage. Thus, anarcho-capitalists should look to the mental and digital domains for full vindication. As already pointed out, ideas and data are valuable, but once visible, they are easily used by adversaries for their own advantage. However, although it is true that ideas and data are more vulnerable than physical property, it is also true that privacy and invisibility can be made more resilient in the information domain than in the tangible realm. For simplicity, digital data is the focus here. The argument is that invisibility on the internet is one of the most effective weapons libertarians can develop to overthrow the state.[11]

The greatest vulnerability of digital data is that they can be copied endlessly at zero cost by anyone able to see them. The most effective defense against this problem is to not generate data in the first place: online watchers cannot exploit personal data that does not exist. However, this solution is not worth considering, given how important the internet is in everyday life. Legislation arguably provides a line of defense: privacy and property rights might be safer if government protected them. The problem with this solution is the trust that would need to be placed in the state.

---

are able to track and punish citizens who disobey it; conversely, individuals can legitimately violate any law that hinders human happiness by hiding from the intrusive watch of government agents.

[11] Importantly, what follows is not to be read as a technical discussion but as an essay in political philosophy.

It is hard to believe that the biggest violator of property rights and the biggest agent of mass surveillance, the government, can be trusted to secure personal data. In this regard, it is enough to keep in mind the National Security Agency programs that Edward Snowden exposed and law enforcement agencies' long-standing global battle against encryption. A third solution appeals to the market: companies whose main source of revenue comes from advertisements, such as Google and Facebook, may develop solutions to protect users' privacy. Although the private sector is more trustworthy than the state, it is worth noting that internet giants profit precisely from gathering massive amounts of personal information. Users of Google and Facebook do not pay for those services with money, but by giving away their intimate data, which is also a product that can be sold on the market anytime. In addition, big tech corporations are among the biggest government contractors in the world, and are actively engaged in mass surveillance programs on behalf of the state (Rectenwald 2019). Thus, although it is true that public pressure may compel big tech companies to offer better privacy-preserving technology and TOS to their users, it is also true that their economic and political incentives are structurally tilted toward some level of privacy violation. In the end, the responsibility of protecting privacy rests upon users. This is coherent with the classic liberal thesis that defense is the duty and the right of each and every individual.

A more effective way to protect personal data is to overload adversaries with information. Brunton and Nissenbaum (2016, 7), while giving a nice overview of obfuscation techniques, explain that

> obfuscation is contingent, shaped by the problems we seek to address and the adversaries we hope to foil or delay, but it is characterized by a simple underlying circumstance: unable to refuse or deny observation, we create many plausible, ambiguous, and misleading signals within which the information we want to conceal can be lost.

Of course, obfuscation is always a race against the development of techniques that can eliminate the noise and expose the real information. Encryption is also a powerful tool to attain privacy. Thanks to encryption, the meaning of visible data is hidden from attackers. Encryption is at work in a lot of services we use daily, such as messaging apps (Signal, for example, takes advantage of end-to-end encryption), secure communication protocols (the Transport Layer Security protocol is just one example), and many others.

A very important point to note for anarcho-capitalists is that cryptography and encryption are crucial to enforcing financial security and privacy. A quick look at one of the best privacy-preserving cryptocurrencies illustrates this. Monero was born in 2014 with the aim to develop an open-source, decentralized, permissionless, private, and secure payment network where anyone can transact with the peace of mind that only privacy can guarantee.[12] It "uses powerful cryptographic techniques to create a network that allows parties to interact without revealing the sender, recipient, or transaction amounts. . . . One of monero's crucial defining features is its philosophy of enforced privacy by default. Users are specifically prevented from initializing transactions that are accidentally or intentionally insecure" (SerHack 2018, 23–24). Every monero transaction is untraceable, meaning that "for each incoming transaction all possible senders are equiprobable" and unlinkable, meaning that "it is impossible to prove [that any two outgoing transactions] were sent to the same person" (Van Saberhagen 2013, 1). Because no coin's history can be revealed, monero is fungible. Privacy entails fungibility, and both are what distinguish monero from transparent networks like bitcoin, where everybody can develop techniques to see what other people are doing with their money. Given that bitcoin is not private by default, it is more difficult to make it fungible: for an external observer, one bitcoin is not the same as another bitcoin, because anybody can see their different histories, and coins with different pasts have different value. All these features make monero ideal for sharing value and keeping financial history private, away from the prying eyes of data-hungry governments, corporations, and other adversaries. Of course, monero's privacy is always in danger of being breached by new analysis heuristics, cryptographic breakthroughs, and unforeseen vulnerabilities.[13] But it works. When people pay in monero, big corporations can apply little or no behavioral analysis to their purchasing history, and the state cannot see what citizens are doing with their money, with huge implications for

[12] This discussion of monero is nontechnical and introductory only, and aims at showing how technology can be used to preserve privacy (and, consequently, freedom and property) in a world where digital surveillance seems unstoppable. For a technical and philosophical introduction to cryptocurrencies in general and bitcoin in particular, see Andreas M. Antonopoulos's works.

[13] The *Breaking Monero* series discusses some of monero's vulnerabilities.

tax collection and governments' economic resources.[14] The state's strength descends mostly from its purchasing power, but how can men with guns extort money from the people if they *cannot* know what the people are doing with their finances? Sure, the state may try to ban private means of exchange, but how would that ban be enforced? How can the state effectively prevent people from using a software? How can men with guns ban mathematics? Sure, governments do try to spy on the entry and exit points of financial networks, such as those of merchants or payment gatekeepers, and to surveil the nodes that run the networks (Jevans 2020; Erb 2020); but with private means of payment, the state loses its head start, while individuals gain a competitive advantage.[15] Any system serious about defending its users' property must enforce privacy by default.[16] For example, it takes some effort for monero users to make their transactions visible through view keys, while sending value privately is effortless; similarly, it will take great effort to deanonymize monero transactions (nobody has been successful so far). These two facts imply that monero end users enjoy a structural advantage over their adversaries, reversing the state's structural advantage in the physical world, where its monopoly on violence and means of exchange looks unbreakable. Anarcho-capitalist rebels should exploit financial tools such as monero to preserve their own property and to starve the state without resorting to violence. Best of all, anarcho-capitalists do not need to wait for a widespread social upheaval in order to initiate a revolution: any individual can opt out of the system right now, just by choosing to use privacy-preserving software to defend her property.

Enemies of privacy and freedom aim at visibility by default: the panopticon is their ideal model for society. Jeremy Bentham developed the concept of the "panopticon" in the late eighteenth

---

[14] Monero view keys assure that one's transaction history can be made visible if the holder voluntarily chooses so. Making one's view key public doesn't have any impact on the spend key: the holder is in control of her own funds.

[15] As the reader may have noted, this situation is the opposite of what happens in the tangible realm, where the government can easily see and control citizens and so enjoys a structural advantage over individuals. It does not come as a surprise, then, that the US Department of Homeland Security and the IRS are actively funding corporations to crack monero and make it traceable. However, no tools to deterministically deanonymize monero transactions have been discovered or made public so far.

[16] Of course, one is always free to choose whether to use privacy-preserving software.

century; Michel Foucault (1978) thoroughly discusses it in *Discipline and Punish: The Birth of Prison*. The panopticon is a prison in which a guard tower is surrounded by a circular building; the prison cells are in the circular outer edifice and the guards in the inner tower. The panopticon's key feature is its asymmetry of visibility: each cell is completely visible from the tower, but prisoners cannot see what happens there, and cannot even know whether the guards are watching them. In addition, the fact that prisoners do not know whether the guards are at their station causes a chilling effect: inmates *must* assume that they are constantly under watch precisely because they *may* be under surveillance at all times, so detainees cannot but police themselves. There is no privacy in the panopticon because prisoners are visible by default, while the guards are allowed to act in secret. Extending the model of the panopticon to all society is any tyrant's pipe dream because it would make everybody completely visible by default. And a citizenry under permanent watch is easily controllable through the use or threat of violence.

Central bankers are trying to implement a version of the panopticon in the digital world through the issuance of central bank digital currencies (CBDCs). Agustín Carstens, the general manager of the Bank of International Settlements, also known as the central bank of central banks, stated in an October 2020 meeting that CBDCs are the digital equivalent of cash but that there is also a «huge difference» between them and common physical currency: central bankers do not know how physical cash is being spent, but with CBDCs they "will have absolute control on the rules and regulations that will determine the use of that expression of central bank liability"; moreover, they "will have the technology to enforce that" (IMF 2020). In other words, CBDCs are meant to be visible to central authorities by default, while physical cash grants users a degree of privacy because the state cannot see and track every single bill that circulates in the economy. If CBDCs became a reality,[17] the states' power would be greater than ever because

[17] Since this paper was submitted for review, at least two three major CBDC developments have emerged. First, China tested a first implementation of the digital yuan on the ground at the Beijing Winter Olympics (Prathap 2022). Second, President Joe Biden signed an executive order encouraging the Fed "to continue to research and report on the extent to which CBDCs could improve the efficiency and reduce the costs of existing and future payments systems, to continue to assess the optimal form of a United States CBDC, and to develop a

every financial transaction would fall under their watch and control. Needless to say, "panoptical" visibility by default in every sector of physical and digital life is what governments and governmentalities such as Google and Facebook aspire to. Conversely, privacy as invisibility by default is the strongest weapon that can be employed against tyrannical governments and corporations that live off their users' data. If people's actions are invisible by default, adversaries cannot enforce their rules, even if they enjoy a monopoly on physical violence. In the physical world, invisibility is unattainable: people are material beings, and material bodies can always be seen by sharp observers.[18] In the digital realm, it is possible to push both visibility and invisibility to further extremes: on the one hand, central banks, government agencies, and big tech corporations enjoy complete control over any action that is performed through their infrastructures and tools; on the other hand, free and open-source systems such as monero are available for anyone to download and use,[19] and they allow people to carve out a niche of invisibility, privacy, and freedom for themselves.

In the prescient "Crypto Anarchist Manifesto," written in 1988, Timothy C. May ([1988] n.d.) states that

> 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. Two persons may exchange messages, conduct business, and negotiate electronic contracts without ever knowing the True Name, or legal identity, of the other. Interactions over networks will be untraceable, via extensive re-routing of encrypted packets and tamper-proof boxes which implement cryptographic protocols with nearly perfect assurance against any tampering. Reputations will be of central importance, far more important in dealings

---

strategic plan for Federal Reserve and broader United States Government action, as appropriate, that evaluates the necessary steps and requirements for the potential implementation and launch of a United States CBDC." See Exec. Order No. 14,067, 87 Fed. Reg. 14143 (Mar. 14, 2022). Third, the European Central Bank (ECB) started pushing hard towards the development of a digital euro: keeping a straight face, Christine Lagarde and Fabio Panetta stated that "introducing a digital euro would ensure that citizens can continue to trust in the monetary anchor behind their digital payments" and that "the protection of privacy must be of the highest standard" (Lagarde and Panetta 2022).

[18] Of course, this does not mean that people should stop attempting to attain an effective degree of privacy in their daily lives.

[19] It is encouraging to see the monero network continuing to show organic growth in transactions (BitInfoCharts, n.d.).

> than even the credit ratings of today. These developments will alter completely the nature of government regulation, the ability to tax and control economic interactions, the ability to keep information secret, and will even alter the nature of trust and reputation. . . . Just as the technology of printing altered and reduced the power of medieval guilds and the social power structure, so too will cryptologic methods fundamentally alter the nature of corporations and of government interference in economic transactions. Combined with emerging information markets, crypto anarchy will create a liquid market for any and all material which can be put into words and pictures.

Anarcho-capitalists need to embrace the cypherpunk ethos in order to make their theories less utopian. However, although it is useful, remarkable, and crucial that "cypherpunks write code" (Hughes 1993), libertarian and anarcho-capitalist thinking is required to defend privacy and property rights on intellectual grounds, so that the public will fall out of love with statist arguments, and, as a consequence, start actively using privacy-preserving technology. To paraphrase Rothbard: the cypherpunk ethos is the fullest expression of anarcho-capitalism, and anarcho-capitalism is the fullest expression of the cypherpunk ethos. Full property rights cannot exist without realized privacy. Cypherpunks write code, but, as Ludwig von Mises pointed out, ideas write human history: let's put libertarian ideas into code and shape an anarcho-capitalist world through cypherpunk software.

CONCLUSION

Anarcho-capitalist libertarianism sounds great in theory but in real life is often met with skepticism because of its inability to explain why the state still exists despite its well-known inefficiencies, despite its systematic violation of property rights, and despite the fact that the market has proven itself better than political institutions in basically every respect.

This article argues that a great deal of state power comes from the ability to intrude on people's lives. Libertarian reductionism maintains that only property rights exist; in this vein, privacy is not a right, but a condition for the preservation of ownership rights. Defending privacy means subtracting oneself from the preying eyes of potential adversaries—that is, privacy is the ability to make oneself visible to others and to interact with them voluntarily, without being forced to do so. Given this definition of privacy, given that the state describes itself as the sole legitimate and legal user of force in a certain territory, and given that violence can only be exercised on

visible targets, it follows that governments thrive when privacy is weak and that protecting privacy should be a top priority for anyone libertarian minded. In the information era, safeguarding privacy means more than hiding physical possessions. This is extremely clear in the field of finance, where the vast majority of transactions occur electronically. In this article, the example of monero was used to show how digital financial privacy can boost freedom and hinder panoptical surveillance. On the other hand, tools such as CBDCs are an existential threat to digital privacy and, consequently, to digital (and physical) property and freedom.

Of course, a lot of work still needs to be done. On a philosophical level, the development of a metaphysics of property and privacy that takes into account the full spectrum of similarities and differences between the physical and the information realms cannot be postponed any longer. A systematic study of the nature of surveillance is sorely needed: the enemy can only be fought if it is deeply understood. On a more practical level, new tools must be developed to protect all aspects of privacy, property, and freedom, and these must be widely available and user-friendly. Private and state actors that enjoy the technical ability to spy on people *will* use and abuse this power, because, in the end, surveillance is the prelude to violence. A renewed and strengthened alliance between anarcho-capitalists and cypherpunks offers one of the last chances to stop the construction of a Big Brother society.

REFERENCES

Assange, Julian. 2016. *Cypherpunks: Freedom and the Future of the Internet*. New York: OR Books.

BitInfoCharts. n.d. "Monero Transactions Historical Chart." Accessed May 22, 2022. https://bitinfocharts.com/comparison/monero-transactions.html#alltime.

Brunton, Finn, and Helen Nissenbaum. 2016. *Obfuscation: A User's Guide for Privacy and Protest*. Cambridge, Mass.: MIT press.

Erb, Kelly Phillips. 2020. "IRS Will Pay Up to $625,000 If You Can Crack Monero, Other Privacy Coins." *Forbes*, September 14, 2020. https://www.forbes.com/sites/kellyphillipserb/2020/09/14/irs-will-pay-up-to-625000-if-you-can-crack-monero-other-privacy-coins/.

Foucault, Michel. 1978. "Panopticism." In *Discipline and Punish: The Birth of Prison*, translated by Alan Sheridan, 195–228. Vancouver, Wash.: Vintage Books. https://foucault.info/documents/foucault.disciplineAndPunish.panOpticism/.

Hughes, Eric. 1993. "A Cypherpunk's Manifesto." Activism: Cypherpunks, March 9, 1993. https://activism.net/cypherpunk/manifesto.html.

IMF (International Monetary Fund). 2020. "Cross-Border Payments—a Vision for the Future." IMF seminar at the 2020 Annual Meetings of the International Monetary Fund and the Board of Governors of the World Bank Group. October 19, 2020. Video, 59:50. https://meetings.imf.org/en/2020/Annual/Schedule/2020/10/19/imf-cross-border-payments-a-vision-for-the-future.

Jevans, Dave. 2020. "CipherTrace Files Two Monero Cryptocurrency Tracing Patents." CipherTrace, November 20, 2020. https://ciphertrace.com/ciphertrace-files-two-monero-cryptocurrency-tracing-patents/.

Kinsella, N. Stephan. 2015. *Against Intellectual Property*. Auburn, Ala.: Ludwig von Mises Institute.

Klein, Peter G. 2019. "The Economics of Data Privacy." Lecture at Mises University, Auburn, Ala., July 19, 2019. Video, 47:56. August 9, 2019. https://www.youtube.com/watch?v=UQXwXb1FSkM.

Konkin, Samuel Edward, III. 1980. *The New Libertarian Manifesto*. Los Angeles: KoPubCo.

Lagarde, Christine and Fabio Panetta. 2022. "Key Objectives of the Digital Euro." European Central Bank, July 13, 2022. https://www.ecb.europa.eu/press/blog/date/2022/html/ecb.blog220713~34e21c3240.en.html.

May, Timothy C. (1988) n.d. "The Crypto Anarchist Manifesto." Satoshi Nakamoto Institute. Accessed May 22, 2022. https://nakamotoinstitute.org/crypto-anarchist-manifesto/.

Mayweather, Sal. 2021. *Anti-politics*. Self-published.

Prathap, Madana. 2022. "More than $300,000 of China's New CBDC Is Being Spent at the Olympics Every Day." Business Insider India, February 18, 2022. https://www.businessinsider.in/investment/news/more-than-300000-of-chinas-new-cbdc-is-being-spent-at-the-olympics-every-day/articleshow/89655765.cms.

Rectenwald, Michael. 2019. *Google Archipelago: The Digital Gulag and the Simulation of Freedom*. Nashville: New English Review Press.

Salerno, Joseph T., and Matthew McCaffrey, eds. 2016. *The Rothbard Reader*. Auburn, Ala.: Mises Institute.

SerHack. 2018. *Mastering Monero: The Future of Private Transactions*. Self-published, Lernolibro.

Smuggler and XYZ. 2018. *Second Realm: Book on Strategy*. Self-published, Liberty Under Attack Publications.

Snowden, Edward. 2019. *Permanent Record*. London: Macmillan.

Solove, Daniel J. 2009. *Understanding Privacy*. Cambridge, Mass.: Harvard University Press.

Van Saberhagen, Nicolas. 2013. *CryptoNote v 2.0*. https://web.archive.org/web/20201028121818/https://cryptonote.org/whitepaper.pdf.

Wacks, Raymond. 2015. *Privacy: A Very Short Introduction*. Oxford: Oxford University Press.

Waldman, Ari Ezra. 2018. *Privacy as Trust: Information Privacy for an Information Age*. Cambridge: Cambridge University Press.

Westin, Alan. 1967. *Privacy and Freedom*. New York: Ig Publishing.