**CHAPTER SIX: True Names and Privacy**  
  
All those who used their knowledge in a bid to enact social change saw cryptography as a tool to enhance individual privacy and to shift power from big, central institutions to the human beings who live in their orbit. —Paul Vigna  
  
The world needs a new paradigm of privacy because the state will always win under the old paradigm as long as it controls the Identity Industry. The industry consists of far more than government ID and forms to fill out. In the last two decades, the Identity Industry has bloated to include airport screening, biometrics, Know Your Customer regulations, clandestine data caches, and surveillance at every turn. [Alastair Berg of the RMIT Blockchain Innovation Hub observes,](https://forum.nem.io/t/the-identity-industry/16291) “These are just a handful of segments in an industry which is estimated to grow to USD16 billion by 2022.”  
  
The state will not loosen its grip on the industry because identification is an irreplaceable part of social control and the accumulation of wealth. This has been true since the Napoleonic era when [an identity card](https://www.globalresearch.ca/id-cards-an-historical-view/15231) was introduced that foreshadowed the modern ones. The purpose of the ID was to control wages by curbing the mobility of workers who wanted to move to get better jobs at higher wages. The cards were instrumental in converting a relatively free France into a police state.  
  
The state monopoly on identification needs to be broken in the same manner that crypto breaks the monetary monopoly. It should not be confronted; it should be bypassed by providing a better alternative. This not only staves off the state but also provides a free-market alternative for the valid human need for identification. Historically, identification was a free-market function; marriage certificates, for example, were a private contract between families and honored by the church. It can easily be free market again. As long as the Identity Industry is a branch of government, however, this human need will either go unfilled or be satisfied at a staggering cost to freedom.  
  
The new online paradigm for privacy is here. It is exemplified by the blockchain where interactions are transparent and real identities are protected. Privacy resides in shielding True Names—a reference to the 1981 pioneering novella by Vernor Vinge in which a group of hackers (called warlocks) penetrate computers around the world. Their real identities are secret from each other and especially from the Great Adversary—a reference to the American state. Masking real world identities is vital because anyone who knows a warlock's True Name can blackmail him or cause a True Death. Identity is literally a life and death issue.  
  
**The Origin of True Names**  
  
I think the Mailman is taking us on one at a time, starting with the weakest, drawing us in far enough to learn our True Names—and then destroying us.― Vernor Vinge, *True Names*  
  
*True Names* is one of the earliest fictional depictions of a fleshed-out cyberspace. It is widely credited with launching the cyberpunks movement, which later explored many of the themes presented in the novella.  
  
[The novella](http://www.scotswolf.com/TRUENAMES.pdf) opens:  
  
In the once-upon-a-time days of the First Age of Magic, the prudent sorcerer regarded his own true name as his most valued possession but also the greatest threat to his continued good health, for—the stories go—once an enemy, even a weak unskilled enemy, learned the sorcerer's true name, then routine and widely known spells could destroy or enslave even the most powerful. As times passed, and we graduated to the Age of Reason and thence to the first and second industrial revolutions, such notions were discredited. Now it seems that the Wheel has turned full circle (even if there never really was a First Age) and we are back to worrying about true names again.  
  
In the story, the protagonist hacker is visited by agents of the Great Enemy who have uncovered his True Name. They strong arm him into tracking down a bigger target known as The Mailman. Thus the story is highly anti-statist with a keen sense of how identity is crucial to freedom.  
  
The novella spiked the admiration of crypto-anarchists who also drew upon its vision of cyberspace. A later reprint of *True Names* includes ten articles and essays by writers who provide commentary upon Vinge's story. One is the essay "True Nyms and Crypto Anarchy" by Timothy May, author of "The Crypto Anarchist Manifesto." (Nyms is short for pseudonyms.) In the *True Names* tribute, May optimistically states:  
  
Crypto anarchy is the cyber spatial realization of anarcho-capitalism, transcending national boundaries and freeing individuals to consensually make the economic arrangements they wish to make.  
  
It ensures that men with guns cannot be brought in to interfere with mutually agreed-upon transactions, the only kind of economics interaction possible in crypto anarchy. Some people will of course scream “Unfair!” and demand government intervention, which is why strong cryptography will probably be opposed by the masses, unless of course, they are wise and take the long view. This may smack of elitism, but I have very little faith in democracy. De Tocqueville warned in 1840 that, roughly translated, “The American Republic will endure until politicians realize they can bribe the people with their own money.” We reached that point several decades ago.  
  
Strong cryptography and the privacy it offers are essential to the success of crypto-anarchy. Its antithesis is social control that requires identifying people and linking them to activities in order to be effective. Cryptography snaps this link. And not a moment too soon.  
  
Government ID is currently the only way most people can prove their offline identities in order to access the necessities of modern life. In most Western nations, undocumented people cannot board a plane, drive a car, or rent an apartment. They cannot open a bank account, acquire a credit card, access medical care, cash a check, take a visible job, attend a university, or buy a car. They become second-class citizens.  
  
Meanwhile, those with state ID become vulnerable to prosecution and persecution. In a nationalized ID and reporting system, the government knows who everyone is, what everyone owns, and where to find both. As Orwell eloquently argues in novels and essays, the nationalization of privacy is a linchpin of totalitarianism. No wonder the government’s appetite for data is so ravenous. No wonder there is a drive to strip anonymity from the Internet under the aegis of concern about bullying.  
  
What is needed now is a new paradigm for offline privacy that can work in tandem with online protections. Or, rather, an old paradigm should be revived. The offline privacy is best achieved by free-market ID that provides the benefits of identification without the liability of becoming a number in a bureaucratic file.  
  
**Free-Market ID Systems for Offline**  
  
Free-market ID is the antithesis of government ID in that it returns the power of identification back to the individual to use or not according to his own discretion. Free-market ID is a natural ally of cryptography because the goals are the same— to break the state monopoly on the Identity Industry.  
  
When commerce was on the level of barter, people usually knew or knew of the individuals with whom they traded. When commerce expanded to include complex exchanges with total strangers a world away, then direct barter was replaced by indirect exchange that often required trust or a middle-man. A bedrock of trusting someone is the ability to answer the question, “[Who am I dealing with](https://news.bitcoin.com/satoshi-revolution-chapter-2-currency-creates-freedom-and-civilization-or-oppression-part-4/)?” Thus there is a legitimate need for identification and little danger to it as long as the state is not involved.  
  
Consider a widespread method of identification from centuries ago that is making a comeback—letters of introduction. The basic dynamic: Person A carries letters of identification to Person C to whom A is a stranger. The letters are written by Person B who is a respected and mutual acquaintance. Person B vouches for the identity of the letter bearer and C is able to answer the question, “Who am I dealing with?” Such letters could be prepared by a business that verifies identities for profit.  
  
An e-version of letters of introduction occurs in crypto circles and on networks whenever a respected member vouches for an outsider who wishes to join. Given the size of the community and the fact it is under attack, introductions seem to be an increasingly popular practice.  
  
The letters embody the first and most basic service rendered by free-market ID: *authentication*. There are myriad reasons why someone would want to authenticate a person’s identity. The person could be picking up a package, confirming a reservation, joining a club, cashing a check, or applying for a job. The filter of authentication means a stranger cannot commit fraud.  
  
The free-market authentication of real identities can also be performed by companies that issue ID cards. Private ID is common today in a bastardized form that has limited value. Employers issue IDs to employees so they can unlocked offices; financial institutions offer credit cards to customers; universities hand out IDs so students can access services. But the privacy here is illusory. Before an employer or a financial institution issues ID, the recipient is screened in the hiring process or in opening an account . Student cards are prescreened by the extensive paperwork required to enroll in a university. This information is routinely reported to the state in one form or other. These semi-private IDs may be a proof of principle, but they are not free market or private.  
  
The agorist Sunni Maravillosa speculates on what free-market ID might look like in her essay “ID Without Big Brother” in the anthology *National Identification Systems: Essays in Opposition* :  
  
If an individual wants an ID that attaches a certain label to her, she has several companies to choose from. IDs R Us is a national chain that has minimal requirements for such ID, and offers fast service and low prices. However, because it has minimal requirements, its safety record isn’t that great, and many firms do not place much trust in their IDs. The most successful authentication ID issuer is Spooner’s Identity Emporium. This company also has minimal requirements for low-level name-only ID, but it takes the additional step of verifying the ID seeker’s history under that name, as well as the reputation of those who vouch for the ID-seeker. The company publishes a monthly list on its web site—usually a very short list, given its careful processing—of individuals whose ID has been revoked, along with the reason for revocation...Of course, if an individual doesn’t like the requirements of one company, she’s free to use another...  
  
Most companies would be careful about accuracy because anyone defrauded by a false document might bring legal action. They would also be careful about client privacy since discretion would be key to the marketability of its ID. If company- issued IDs facilitate fraud or if client information is leaked, then the publicity alone would damage or ruin the company’s reputation; free-market ID companies would live or die on their reputations.  
  
The second service free-market ID offers to individuals is *certification*. Letters of recommendation attest to the character, the education, and specific abilities of the bearer. Businesses would be likely to cooperate with each other in providing such letters. Maravillosa offers a hypothetical example:  
  
Banks issue “credit credentials,” which are based on an individual’s or company’s credit history with the bank, so that another individual or institution is satisfied that the entity in question is unlike to default on a loan or other credit arrangement up to a certain amount.  
  
Again, the crypto version of this service is a personal online recommendation from a trusted figure about a stranger. Alternatively, the outsider could point to certifying documents—perhaps scholarly articles he has written on relevant subjects. His reputation itself can be a certifying ID.  
  
Some forms of current ID perform a similar function. University degrees purportedly certify a level of education and intelligence; a letter of reference from an employer describes the laudable work habits of a former employee; membership in professional or charitable organizations suggests a person’s character and social skills.  
  
There is a marked downside to many current certifications, however. One of them: State licenses and diplomas frequently substitute for free-market methods of certification. Everything from neurosurgery to braiding dreadlocks requires licenses, and these tend to replace reputation as a measure of worth. An example: A non-traditional healer is well know for his skill, but he is unable to obtain a license. His reputation is stellar, but local doctors block the licensing process in order to eliminate their competition. The healer is unable to treat people without the risk of going to jail. State-mandated diplomas—even if they have value, which is increasingly in doubt—are barriers to those who are talented but not state sanctioned. In this manner, the state devalues or negates the worth of reputation.  
  
The third purpose of free-market ID is to *authorize* specific actions. Letters can assign limited rights to the bearer. An attorney’s firm might assign a limited power to one of its lawyers so he can settle a case on the behalf of a client.  
  
**Objections to Free-Market ID**  
  
Objections to free-market identification arise. The methods of identification are said to be antiquated, to not provide real anonymity, and to have no uniformity. Besides which, establishing a reputation is a slow process in a fast-moving world.  
  
*Antiquated*. Some models of identification may be outmoded. But the surest remedy for this is to open up to field and let the marketplace innovate. The most antiquated IDs are the ones produced by the stagnant state.  
  
*No Anonymity*. The primary purpose of early ID was to verify identity, not to render anonymity. And there is still a free-market demand to verify identity. There  
  
is value in anonymity; there is value in being known. The value depends on whether the individual is able to choose freely between the two.  
  
*No uniformity.* Another word for “no uniformity” is “diversity,” and it is one of the extreme advantages of free-market ID because it gives choice. Government ID is homogenized because the goal is to enforce conformity to laws and reporting requirements. When ID serves individuals, then its form is dictated by their needs and preferences, not by the state.  
  
*Slow to Establish Trust or Reputation*. It is a fast-moving world. But the fact that a reputation or a business may take time and hard work to establish is hardly a criticism. Worthwhile achievements take time and hard work.  
  
**The State’s Nuclear Option in Weaponizing Data**  
  
Privacy includes the ability to keep things secret from the government….I might be keeping secret my weakness for alcohol, or heroin, or gambling or pornography and so preventing the government from stepping in to protect me from myself….If you view government as a benevolent super being watching over you—a wise and kindly uncle with a long white beard—you will and should reject much of what I am saying. But government is not Uncle Sam or a philosopher king. Government is a set of institutions through which human beings act for human purposes. Its special feature—what differentiates political action from the other ways in which we try to get what we want—is that government is permitted to use force to make people do things.—David Friedman  
  
Government is not a wise and kindly uncle. It is self-serving institution occupied by human beings with human passions, especially for power, wealth, status, moralizing, and revenge. These days, crypto users have reason to be particularly private. A recent news story declares, “NSA Has Been Tracking Bitcoin Users Since 2013, New Snowden Documents Reveal.” An abundance of caution both online and off is not paranoia when they actually are out to get you.  
  
A February 6, 2018 headline in *Reason* magazine warns, “Governments Hate Bitcoin and Cash for the Same Reason: They Protect People’s Privacy.” The ensuing article spins off a [quote](https://www.bloomberg.com/news/articles/2018-01-12/mnuchin-warns-against-bitcoin-becoming-next-swiss-bank-account) from U.S. Treasury Secretary, Steve Mnuchin, “One of the things we will be working very closely with the G-20 on is making sure that this doesn’t become the Swiss numbered bank accounts.” Mnuchin rejects decentralized crypto as payment, investment, or savings systems because it cannot be easily tracked by government. Mnuchin’s criticism confirms that crypto is a positive good for individuals not only because it empowers them but also because it protects them from statists like him.  
  
Privacy attacks around the globe are going to get more aggressive, and quickly so. Data are being weaponized at a frightening pace, making for a tight race between privacy and totalitarianism. States are developing new ways to use  
  
databases to repress the opportunities and activities of people who make the “wrong” choices or have the “wrong” thoughts.  
  
A headline in *Reuters* read, “[China to bar people with bad ‘social credit’ from planes, trains](https://www.reuters.com/article/us-china-credit/china-to-bar-people-with-bad-social-credit-from-planes-trains-idUSKCN1GS10S?utm_campaign=trueAnthem:+Trending+Content&utm_content=5aabaabc04d30122be8c54f7&utm_medium=trueAnthem&utm_source=twitter).” [Social credit](http://theconversation.com/chinas-social-credit-system-puts-its-people-under-pressure-to-be-model-citizens-89963) (*xinyong)* is a long-standing moral concept within the Chinese tradition, which indicates the level of a person’s honesty and trustworthiness. The Chinese government now extends this moral concept to include loyalty to the state and social or political honesty; it assigns an official rank to each person. Then extreme social control is imposed on those with low scores by denying them “privileges,” such as travel and education. Social-credit offenses include using expired tickets to board a train or smoking while on it, buying too much alcohol, watching porn, returning a rented bike in a tardy manner, “not showing up to a restaurant without having canceled the reservation, cheating in online games, leaving false product reviews, and jaywalking.”  
  
The trivial offenses may seem puzzling or even funny, but they serve an important purpose for the state and a horrifying one for individuals. The trivial offenses hand the state a blank check on suppressing dissidents, political opponents, or other “undesirables” because virtually everyone commits minor infractions as part of everyday life. As Beria once said, “Show me the man, I will show you the crime.” The Chinese government can now pick and choose whom it wishes to convert into a nonperson by barring them from travel and other social interaction. The strategy is similar to that described in the book *Three Felonies a Day* by which everyone who flaunts state authority is vulnerable to criminal charges on one offense or another. Everyone is vulnerable to attack from the state. This danger also provides a huge incentive for people to obey absolutely and not to draw attention to themselves. This is true in China. It is increasingly true in many nations.  
  
The concept of social credit is not uniquely Chinese. In the U.S., passports are denied to those who are sufficiently behind in child support or tax payments, and former felons find it difficult to travel abroad. Foreigners who tell a U.S. border guard that they have smoked marijuana, whether the event occurred in a venue where it was legal or not, will be refused entry. *Global News*, a Canadian outlet,  
  
[explains](https://globalnews.ca/news/4093248/why-telling-a-u-s-border-guard-youve-smoked-pot-could-be-dangerous-even-once-its-legalized/), “they’re…told to go back to Canada, and told they are inadmissible for life. This is a lifetime ban.” Meanwhile, constitutional rights like gun ownership are being denied for an increasing long list of reasons.  
  
Government’s voracious appetite for the data required by social control is growing. [The Cloud Act](https://en.wikipedia.org/wiki/CLOUD_Act) became federal law in 2018, for example. The Act allows federal law enforcement to compel U.S.-based technology companies to provide data stored on servers regardless of where the data are stored. It strips away Fourth Amendment rights against unreasonable search and seizure by allowing the U.S. to enter into data sharing agreements with foreign countries and bypass U.S. courts. Targeted users may never know of the warrant.  
  
People need to choose their approach to privacy and prepare.  
  
**What Should You Do?**  
  
Strategies will vary from person to person because they are based on variables like personality and circumstance. There are many paths to privacy, not just one.  
  
Before answering “What should you do?,” some distinctions are useful. All information is not equal, and encrypting everything may draw unwanted attention. You might consider encrypting only information that is important to your freedom, wealth, and well-being. Everyone has at least three kinds of personal data. First, there are data that should be broadcast widely, such as an employment resume. This information requires marketing, not privacy. Second, there are facts that are harmless to disclose, such as a favorite color or a preference in potato chips. The disclosure may draw unwanted solicitations from business, but these annoyances do not jeopardize rights. Third, there are facts that bad actors can use against you. Financial data are a prime example. This is the point at which privacy becomes a survival mechanism.  
  
The next distinction is the well-trodden ground of privacy versus anonymity versus pseudonymity. I will tread it again briefly.  
  
Privacy is the act of keeping personal data or activities to yourself in its entirety or to whatever is your comfort level. What is your comfort level?  
  
Anonymity is the strategy of making content transparent but hiding True Names. Rick Falkvinge, founder of the first Pirate Party, elaborates,  
  
The typical example would be if you want to blow the whistle on abuse of power or other forms of crime in your organization without risking career and social standing in that group, which is why we typically have strong laws that protect sources of the free press. You could also post such data anonymously online through a VPN, the TOR anonymizing network, or both. This is the analog equivalent of the anonymous tip-off letter, which has been seen as a staple diet in our checks and balances.  
  
Pseudonymity is the strategy of using a fictional name rather than a True Name. It is anonymity acquired by disguise. Pseudonymity is not a recent phenomenon. The influential *The Federalist Papers* (1787-1788) were written by Publius—a collective pseudonym covering James Madison, Alexander Hamilton, and John Jay. Historians still disagree upon who wrote some of the pieces; this testifies to the effectiveness of pseudonymity.  
  
The most effective tactics to protect online data may well be [technological](http://techristic.com/20-best-tips-to-stay-anonymous-and-protect-your-online-privacy/), but this book does not [address them](https://news.bitcoin.com/category/privacy/), except in passing. Instead, the article points to privacy strategies or habits that have been used for decades, if not for centuries. Some of them will be familiar. The purpose is not to advance new or revolutionary material; it is to make people be conscious of and to think about how to maintain privacy.  
  
They have been updated to focus on crypto. Here is a sampling of some basic, effective techniques:  
  
*Obfuscate or “hide in plain sight.”* Be so inconspicuous or subtle in your outward actions and appearance as to be almost unnoticeable. Blend in and become invisible. Sometimes obfuscation involves participating at venues that are so filled with “noise” that an eavesdropper finds it difficult to distinguish your signal from any other. The core of this strategy is to avoid calling attention to yourself. When you do “noteworthy” things like calling for the overthrow of the central banking system, then do so under a pseudonym. Under your True Name, be restrained.  
  
*Avoid Centralized Exchanges and Other Data Sharing Centers.* This is an updated- for-crypto-users version of the advice to avoid data collection centers connected with the state, such as the central banks. If you want the state to have all your financial data, then you should just mail it state agencies.  
  
*Password Protect Everything and Stay Virus Free.* A password is like a lock on a door that makes it more difficult for bad actors to enter. Prevent viruses and malware through which hackers can attack your data and steal your identity. Never open unsolicited files in emails; never download files from unknown or insecure sites. Run a competent an antivirus program and prefer browsers that resist infection, such as Linux ones.  
  
*Find Discreet Ways to Cash Out.* The crypto veteran Kai Sedgwick writes,  
  
“Bitcoin transactions are semi-anonymous: every transaction on the blockchain is broadcast publicly and visible for all eternity, but the owner of each wallet is unknown. Tying addresses to real-world identities is now relatively easy for the powers-that-be, because everyone has to cash out somewhere, and that usually involves linking bitcoin addresses to bank accounts.” Don’t use trusted third parties to cash out. As much as possible, deal with people one-on-one or through decentralized exchanges that facilitate peer-to-peer buying and selling. Be inventive. Seek venues that exchange crypto for gift cards to stores at which you regularly shop, including grocery stores.  
  
*Chose a Search Engine that Respects Privacy.* Many search engines record browsing histories and use them to target ads or to generate revenue by selling them. Others, like DuckDuckGo, do not track personal data.  
  
*Use a Privacy Currency.* Dozens of such currencies exist, and more are coming because privacy is in demand. The founder of Zcash [explains](https://news.bitcoin.com/meet-top-3-coins-cryptocurrency-anonymity-race/) the philosophy behind his privacy currency. “We believe that privacy strengthens social ties and social institutions, protects societies against their enemies, and helps societies to be more peaceful and more prosperous…. A robust tradition of privacy is a common feature in rich and peaceful societies, and a lack of privacy is often found in struggling and failing societies.”  
  
*Never Give Out More Information Than Necessary.* Never volunteer information, especially in writing, whenever refusal or silence is an option. If a form is  
  
mandatory, fill out as few blanks as possible in as confusing a manner as possible. Be suspicious of any venture connected to crypto that requires more than minimal information to acquire the service or good being offered. No one in crypto needs to know a social security number, even the last four digits. Always ask those who request info “why” it is needed and the uses to which it will be put. Decide in advance how much data you are willing to disclose and in what form.  
  
*Zip It on Public Forums.* Public forums, like Facebook or Twitter, are monitored and mined by government and corporations; they are also monitored by criminals and malicious people who bear grudges. Public forums are collection points for personal data, even if a person thinks he is posting anonymously. If social media is necessary for professional reasons, then use it to the bare minimum and only for professional reasons. Never post anything on social media that you wouldn’t put on the front page of the *New York Times.*  
  
*Be Careful in Recording Information*. Do not write down private keys, for example, without having a secure, undisclosed place to store them. It makes no sense to encrypt online data if the same informative is lying in cursive form on the kitchen table.  
  
*Use Only Secure Wi-Fi Connections.* It is common for people to hook up to the free Wi-Fi at Starbucks and other venues, but there is no way to tell who may be listening in on your internet traffic. If you must use insecure Wi-Fi, then do not transmit personal data and use a VPN service to encrypt personal data.  
  
*Lie When Establishing Password Security Questions.* “What is your mother’s maiden name?” With this information, a bad actor can crack his way into your bank accounts and, perhaps, steal your identity. Do not answer this or other standard “identifier” questions truthfully. Have a standard false answer that you do not use on official or important forms that are secure. On those, tell the truth.  
  
The foregoing rudimentary precautions are meant to form the habit of privacy. Many people have a habit of disclosure, of reflexively telling the truth. A habit is nothing more than an automatic response that results from an established pattern of behavior. It may be difficult to break the habit of disclosure and replace it with discretion, but it is necessary to do so. Never lie to a friend, but do not hand a stranger the keys to your identity.  
  
The government is coming for crypto, which means it is coming for users. Its front line attack will be an assault on privacy because privacy is the backbone of crypto as a tool of freedom. Now is the time for heightened vigilance. To paraphrase the comedienne Lily Tomlin, “No matter how paranoid I get, it is never enough to keep up.”  
  
Privacy may be the front-line defense of individual freedom but decentralization is the social condition under which privacy thrives. No one can or should tell individuals which specific strategy to use. But, if you value privacy and safety, stay private and decentralize.