**SECTION TWO: THE IMPERATIVE OF PRIVACY**  
  
**CHAPTER FIVE: When Privacy Is Criminalized, Only Criminals Will Be Private**  
  
I grew up with the understanding that the world I lived in was one where people enjoyed a sort of freedom to communicate with each other in privacy, without it being monitored, without it being measured or analyzed or sort of judged by these shadowy figures or systems, any time they mention anything that travels across public lines.—Edward Snowden  
  
I want my tombstone to read, “I lived. I died. Now mind your own damned business.” What do I have to hide? Everything! Which is to say, any information I am required to reveal is data I decline to disclose.  
  
A fundamental question floats over the rhetoric, however. What is privacy? **What is Privacy?**  
  
A famous answer comes from an article by the American attorneys Samuel Warren and Louis Brandeis, which appeared in a 1890 issue of the *Harvard Law Review*. It is one of the most influential pieces in the history of Western legal theory. “ [The Right to Privacy](http://faculty.uml.edu/sgallagher/Brandeisprivacy.htm)” has been called the first prominent call for privacy as a concept to be cemented into law. The article opens:  
  
THAT the individual shall have full protection in person and in property is a principle as old as the common law; but it has been found necessary from time to time to define anew the exact nature and extent of such protection.  
  
Elsewhere, privacy is defined as the right to be left alone.  
  
The article argues for privacy as a “foundational” or basic human right upon which all other rights rest. “The right of property in its widest sense including all rights and privileges, and hence embracing the right to an inviolate personality, affords  
  
alone that broad basis upon which the protection which the individual demands can be rested.” Privacy is a prerequisite for all other rights: freedom of speech, sexuality, freedom of conscience, and financial security depend upon it because no right can be exercised in the presence of storm troopers smashing through the door. The right to lock the front door behind you is essential.  
  
Interestingly, the Brandeis-Warren article was in response to technological developments that were seen to threaten personal privacy. One of the developments was the portable camera with which journalists photographed prominent people in venues that were formerly private such as restaurants, weddings, and funerals. Today, the focus of protecting privacy has shifted from journalists to the government for which “privacy” is a synonym for “secrecy.” Privacy is no longer a right but a probable cause for suspicion. The shift in definition reflects how powerful government has become since the 1890s—and how diminished the individual.  
  
Although privacy has been a theme both in common law and Western societies, its legal status has been vague. Indeed, before “The Right to Privacy,” the legal protection of privacy was splintered across specific issues. Laws against trespassing existed, for example, but codification of the broad concept of privacy did not.  
  
After all, what does the “right to be left alone” mean? Much of this chapter explores an answer.  
  
Everyone knows a woman’s purse should not be snatched, her window peeped through, or her house burglarized. These are obviously and intuitively cases of privacy violations, but they are not the type of violation that crypto users are likely to confront. Crypto users will deal with their personal information being mined and monitored—often covertly—in order to use against them in some manner. With the government, the goal of mining and monitoring is social control, taxation, confiscation, or imprisonment. With criminals, the goal is theft, blackmail, or extortion.  
  
Peeping through a bedroom window may be an obvious breach of privacy, but what about eavesdroppers who access public information like that embedded in the blockchain? The blockchain’s open ledger allows unwanted parties to monitor financial transactions that users voluntarily make public. If an eavesdropper analyzes the pattern of transfers and unmasks a user’s identity, then has privacy been violated? The blockchain is a public place where people voluntarily exchange in a manner they know is transparent and recorded. Eavesdropping is akin to listening to people who are speaking audibly in public. Is listening a culpable act, especially when done by state agents or other bad actors? Certainly, how the state or other criminals use the information is wrong, but this issue is distinct from whether the act of listening itself is wrong.  
  
Assessing the question means putting privacy in the context of other human rights.  
  
**The Human Rights Context of Privacy**  
  
Murray Rothbard claims that all human rights are property rights. That is, all rights come down to the question of who properly controls the use and disposal of a thing, whether the thing is a widget, an idea, or a human body. It is always possible to use force to usurp control of anything, of course, but the question of who is the *proper* owner remains.  
  
Rothbard answers: The owner is the individual who holds valid title to the thing. True ownership is not a matter of control that can be acquired by brute force, but of *rightful* control that comes from peacefully acquiring title. There can be no more obvious or valid title than the one individuals have over their own bodies. Indeed, trying to deny this title reduces either to obscenity or absurdity. There are only three positions possible on who owns a person’s body: the person himself (freedom), someone else (slavery), or it is unclaimed baggage. Those who value freedom and human rights argue for self-ownership.  
  
Again, the classic definition of self-ownership: Every human being has a moral and logical jurisdiction over his own body and the peaceful use thereof, including the products of his labor. No right is more fundamental than self-ownership because it is the wellspring of all other rights. Freedom of conscience and speech exist only because individuals have the capacity to think and speak, both of which are aspects of the human body. The right of self-defense exists only because people own their bodies and have a right to protect their property. The flip side of rights is duty. Just as every other human being is morally and logically prohibited from initiating force against you, you have a duty to desist from initiating force against them.  
  
If there is a right to privacy, then it must be rooted in self-ownership. It must be what is called a natural right. And, if privacy is a right, then other people have a duty to desist from violating it.  
  
The issue is non-trivial. Self-ownership and privacy are under concerted attack by the biggest eavesdropper in human history—the state. The state intends to use the data it collects against people with extreme prejudice. In his book [*Seeing Like a State: How Certain Schemes to Improve the Human Condition Have Failed*](http://mises.org/daily/5101/Seeing-Like-a-State), the political scientist James C. Scott comments on the role that just one form of data collection has played in the rise of the modern state: the census. “If we imagine a state that has no reliable means of enumerating and locating its population, gauging its wealth, and mapping its land, resources, and settlements, we are imagining a state whose interventions in that society are necessarily crude.” The current state is sophisticated and complex.  
  
Information is power, both for the individual and for the government. One reason government succeeds at acquiring data is that privacy is an ill-defined concept that people do not understand in the broader context of rights. Another reason is  
  
that information is ephemeral and seems less prone to ownership than a table or car.  
  
The assessment of whether data privacy is a natural right hinges on two questions. As a prelude to considering them, ponder whether you have a right of ownership over your thoughts and their expression, including the expression of personal information. This broad question is key to the issue of intellectual property, which is the claim that ideas and their expression can be owned. People reach dramatically different conclusions, and intellectual property is frequently claimed as a natural right. The same question confronts privacy, which also addresses the ownership of personal information and its expression.  
  
Question #1: *Who owns what is in your mind?*  
  
Most people would loudly declare, “no one owns what’s in my mind!” Your thoughts are your own for the same reason as your fingers and eyes are; they are part of your body, and your body is who you are. It *is* you. No one else has any business claiming jurisdiction over your body. But what if the thought in your mind is a chemical formula originated by a co-worker and written on a chalkboard during a lecture you attended? The formula is now part of your mind as well as his and, if he can claim a right to use it because it is part of his body, then shouldn’t you be able to make the same claim?  
  
At this point, the co-worker’s argument usually shifts ground. He *originated* the idea, he maintains, which makes the formula a product of his labor, and owning the products of your labor is an extension of self-ownership. It doesn’t matter if the idea is in *your* mind now; it is *his* idea. He found it first.  
  
Putting aside the fact that the co-worker almost certainly utilized the ideas and work of hundreds of people before him—that is, the formula is a product of their labor as well—let’s assume that he added a totally original refinement. What of it? The instant you glimpsed the formula, the concept changed. The formula integrated with every other concept you have about chemistry, technology, and life in general. The formula in your mind is slightly or considerably different than the one on the chalkboard or in the mind of your co-worker. How then can he claim property rights in an idea based on other people’s prior work while denying your property rights in an idea that is based on his prior work?  
  
The bottom line of the scenario: no one has a right to what is in your mind. What is called privacy in this circumstance reduces to self-ownership. You own what is beneath your skin, including ideas. The 19th-century libertarian James Walker  
  
[states](http://www.libertarian.co.uk/lapubs/libhe/libhe014.htm), “My thoughts are my property as the air in my lungs is my property…” When you exhale, however, you lose all claim to ownership of the air expelled. The same is true of ideas or information that are thrown into a public realm; y ou lose all privacy claim except and unless there is a prior nondisclosure agreement in place. In that circumstance, your claim to privacy or information ownership is not a matter of natural rights but of contractual rights.  
  
The parallel to financial information: Crypto users lose any reasonable expectation of privacy or ownership of information once it goes onto the blockchain or another public form. An eavesdropper who accesses the data does nothing more than view what is public knowledge. The eavesdropper may use the knowledge in a vicious way that harms a user, but the use of information is a different matter than how it was obtained.  
  
*Question #2: How was the data obtained?*  
  
The answer to this question is to distinguish between legitimate eavesdropping and a criminal act. Legitimate eavesdroppers access publicly or freely disclosed information and in no way violate rights. By contrast, criminal eavesdroppers violate private property rights in order to access data. Tapping a phone or a computer is like breaking into a person’s home to rummage through a file cabinet or desk. A census taker who threatens an unresponsive person with fines or arrest is using criminal means to access information. The litmus test to distinguish between legitimate eavesdropping and a crime is whether the acquisition of data involves a violation of rights.  
  
Rothbard argues, "there is no such thing as a right to privacy except the right to protect one's property from invasion." In other words, there is no natural right to privacy per se. Information is private by virtue of being protected by other rights. A person has a right to conceal information, for instance, because the right to free speech includes the right to remain silent, and breaching a determined silence requires threats or violence. Equally, a person has the right to close his door behind him, and information in the papers on his desk is protected from intruders by his right of property in the house. The privacy of the information is shielded by the wall of rights surrounding it, but this does not make privacy a right in and of itself.  
  
By contrast, if a person shouts personal information in a public square or if he throws his papers out the window into the wind, it is no longer protected by his property rights. He has placed it into the public sphere and abandoned the claim to exclusive control.  
  
The Satoshi approach to privacy has a foot in both worlds—public abandonment of information along with a privacy protected by natural rights. A transparent blockchain functions with anonymous or pseudonymous users who employ both public and private keys. The transactions have been thrown into the wind, but the identities are protected by other rights. In other words, to unmask someone’s identity or his private key requires a violation of the property rights that surround and protect them—the person’s right to his computer, for example. Ownership consists of the exclusive right to control and to use a thing; if government accesses the computer with no regard to the consent of the real owner, then the government usurps ownership of the computer and unabashedly violates the rights of the real owner.  
  
**A Dramatic Shift in the Paradigm of Privacy**  
  
The Satoshi approach may confuse some people. As long as they cleave to the old paradigm of privacy—that is, privacy equals concealment—then the transparency of the blockchain sounds like a death knell. But the new paradigm of privacy is the transparency of information and the protection of identity. The focus has shifted from information on activities to information on True Names.  
  
The transparency of transactions serves a vital purpose. For the sake of honesty and efficiency, the blockchain publishes every single activity. The protection of True Names also serves a vital purpose. For the sake of personal freedom, participants mask their identities at will and with ease. The blockchain does not require the verification of ID anymore than a grocery store records the names of those who buy milk with cash. Let everyone see, let everyone verify the truth of the transaction. Let no one demand personal information about the who and why of the exchange. Both honesty and privacy are preserved, but the link between a transaction and a True Name is broken. Forcibly reestablishing this link threatens users’s wealth and freedom.  
  
In the past, the focus of government and other Eves has been on the forced disclosure or surveillance of information about activities because the state had cornered the “identity industry.” From birth onward, people are registered, certified, recorded, and processed according to the numbers and other identifiers issued by the state. David Friedman observes in his essay [“The Case for Privacy,”](https://nakamotoinstitute.org/the-case-for-privacy/)  
  
“It is hard to pass through the world without leaving tracks. Somewhere there is a record of every car I have registered, every tax form I have filed, two marriages, one divorce, the birth of three children, thousands of posts to online forums on a wide variety of subjects, four published books, medical records and a great deal more.”  
  
The identity or True Name of individuals has been far better known than their interactions have, many of which may take place in secret and silence. The Satoshi model turns this situation on its head. It makes all interactions public with all identities remaining private at the discretion of the individuals. Government no longer controls identity and, without such control, access to all other information has little value. The state is well aware of this.  
  
The digital age has changed the cultural, political, and psychological zeitgeist of privacy. “Mind your own damned business!” was once a respected attitude, but government has slowly eroded the idea that innocent people need privacy. The new zeitgeist: Only those who have something to hide refuse to answer questions or to undergo scrutiny. “Only criminals fear government surveillance” is a common response to anyone who defends privacy today. But every peaceful person is now a criminal with [something to hide](https://mic.com/articles/86797/8-ways-we-regularly-commit-felonies-without-realizing-it#.5mWiyKsxJ). Why? Because everyone has exceeded the speed limit, taken an illegal drug, smuggled cheap booze or cigarettes across a border, made “unauthorized” additions to a house, fibbed to a government agent, understated their income, or violated one of the tens of thousands of statute laws that criminalize harmless behavior and do so in an  
  
omnipresent manner. Most people are not aware of how many laws they break in the course of conducting a peaceful daily life.  
  
In his book *Three Felonies A Day: How the Feds Target the Innocent*, attorney Harvey Silverglate details how the average American wakes up and goes about his daily route, not knowing that he is likely to commit several federal crimes as he does so. The number of federal crimes has soared exponentially in recent decades and prosecutors can now choose between a cornucopia of vaguely defined crimes with which to charge peaceful individuals of every background, profession, and status. A combination of broad and ill-defined laws, the drug war, and career-building prosecutors who are immune to consequences has turned justice into a conscience-free bureaucracy that seems to care nothing for innocence or guilt. Silverglate notes a standard procedure for the justice bureaucrats:  
  
Prosecutors are able to structure plea bargains in ways that make it nearly impossible for normal, rational, self-interest calculating people to risk going to trial. The pressure on innocent defendants to plead guilty and “cooperate” by testifying against others in exchange for a reduced sentence is enormous—so enormous that such cooperating witnesses often fail to tell the truth, saying, instead, what prosecutors want to hear.  
  
Silverglate’s book is chillingly reminiscent of an infamous Soviet-era quotation from the despised Beria, Stalin’s head of the secret police. “Show me the man, and I will find you the crime.” When someone asks you, “What do you have to hide?,” you should answer, “From Beria and his ilk, everything, especially my identity (the man).”  
  
Or, as Ayn Rand once explained, “The only power any government has is the power to crack down on criminals. Well, when there aren’t enough criminals, one makes them. One declares so many things to be a crime that it becomes impossible for men to live without breaking laws.”  
  
Crypto users who demand privacy are especially vulnerable to cultural and political assumptions that strongly favor state control rather than individual freedom.  
  
The strong assumptions against privacy include:  
  
• The presumption of innocence belongs to government, not to individuals. • A double standard of morality is applied to government and to individuals. • Privacy is equated with concealment.  
  
*The Presumption of Innocence.* The legal term “presumption of innocence” is sometimes expressed by the Latin phrase “*ei incumbit probatio qui dicit, non qui negat,*” which means the burden of proof is with the accuser and not with the accused. The accused is presumed innocent until proven guilty. The legal doctrine rests on the belief that most people are not criminals, so criminality cannot be  
  
presumed; it must be demonstrated. The doctrine also acknowledges a fundamental principle of logic; because it is impossible to [prove a negative](https://en.wikipedia.org/wiki/Burden_of_proof_(philosophy)#Proving_a_negative), the burden of proof rests upon the person making a positive assertion. Someone may claim you are a thief. And even massive evidence of your honesty will not dispel the accusation because you could be lying about a past misdeed or concealing evidence. That is why the accuser is asked to specify what you have stolen and to provide evidence of the crime.  
  
The presumption of innocence is the cornerstone of due process and a wall of protection against arbitrary prosecution by the state. It is a defining feature of a free society as opposed to a totalitarian one. The renowned British barrister Sir John Clifford Mortimer—best known as the creator of the beloved fictional defense barrister Horace Rumpole—was far from alone in viewing the presumption of innocence as “the golden thread” that weaves justice together.  
  
The golden thread has unraveled.  
  
In the name of security, the public has lost the presumption of innocence even in the absence of accusations. Border and airport agents fingerprint, frisk, interrogate, and bark “Your papers!” to queued hordes; individuals who do not comply are automatically yanked out of line and processed like criminals. Police officers demand ID and arrest those who refuse, whether or not the arrest is legal. After all, government agents are assumed to protect security and to enforce the peace. This means those who resist are against security and the peace. Few people ask where law enforcement obtains the right to demand obedience from people who are doing no harm. The presumption of innocence has transferred from individuals to government agents, which reverses the legal concept’s original intent of protecting individuals *from* the state.  
  
The logical principle of being unable to prove a negative has been replaced with the fallacy known as “[the argument or appeal from ignorance](https://en.wikipedia.org/wiki/Argument_from_ignorance).” Here “ignorance” refers to a lack of contrary evidence—a situation deemed suffice to prove the truth of an assertion. In short, an accusation is true because it is not proven to be false. The criminality of an individual becomes a given because it is not disproven. Why else, the state asks, would he refuse to cooperate with authorities?  
  
It is difficult to overstate the importance of the shift in a presumption of innocence from the individual to state agents. Just as the presumption of innocence is the golden thread of justice, the presumption of guilt for individuals is its death. It obliterates due process and slides society directly into totalitarianism. That’s the political meaning and consequence of the question “What do you have to hide?” Government-issued ID is crucial to the process. After your True Name is known, then all other social control becomes possible.  
  
*Double Standard of Morality.* A double standard of morality is at work in society— one for individuals and one for government. What is *im*moral for an individual to do has become moral for the state. If you take money from a neighbor at gun point, it is an act of theft for which you are justly arrested. If a government agent  
  
does the same thing, it is an act of taxation by which the miscreant pays his “fair share” of earnings and for which the agent receives a salary and a pension. Modern morality is now defined by who is performing the act, not by the act itself. The impenetrable secrecy of the state is prudent while the privacy of individuals is criminal.  
  
No voice rang out more clearly against a double standard of morality than that of the libertarian publisher Raymond Cyrus Hoiles who created the media chain Freedom Communications. Hoiles believed the double standard was more destructive to society than any other concept, and his ferocious attacks upon it blasted frequently through his newspapers.  
  
In an editorial entitled “The Most Harmful Error Most Honest People Make” (December 17, 1956), which appeared in the *Santa Ana Register*, Hoiles [explai ns the error](https://www.fff.org/explore-freedom/article/libertarian-legacy-rc-hoiles-part-1/). It “is the belief that a group or a government can do things that would be harmful and wicked if done by an individual and produce results that are not harmful, unjust and wicked. It is the belief that a number of people doing a thing that is wrong for an individual to do can make it right and just.” Hoiles most often critiqued the error with reference to taxation. Again, if it was wrong for a neighbor to steal your goods, then it was equally wrong for a group of neighbors or their appointed representative (government) to perform the same act.  
  
The critique of a double standard did not start with Hoiles, of course. A 1657 pamphlet ascribed to the rebel Colonel Titan [argue](https://tinyurl.com/yc5a2rfx)s: “What can be more absurd in nature and contrary to all common sense than to call him Thief and kill him that comes alone… and to call him Lord Protector and obey him that robs me with regiments and troops? As if to rove with two or three ships were to be a pirate, but with fifty an admiral?” Yet this absurdity is what the state enforces when it acts in a manner that would not be tolerated from individuals.  
  
Again, no one asks where government acquires these sweeping so-called rights. Since the only rights that exist are individual ones against which no one can rightfully aggress, if the government wishes to claim legitimate ownership of the private information of others, then it must produce proof of voluntary disclose, a transfer or sharing of title. Otherwise, the so-called rights are nothing more than the assertion of raw violence.  
  
What applies to taxation applies no less to the violation of privacy. If it is wrong for a neighbor to pat down your body and that of your child without consent, then it is wrong for a government agent to do so in an airport. If it is wrong for a neighbor to tap your phone, to record your financial transactions, and to peek through your windows, then it is wrong for the government to do so. Individuals in a group do not relinquish personal responsibility because acts are always committed by an individual, and they are always a matter of personal responsibility. Gang rape is no less rape and the individual rapists are no less personally responsible simply because they were the second or third in line.  
  
Nevertheless, people buy into a double standard that exempts state agents from moral and legal responsibility. If state agents, from the president to post-office workers, were bound by the same standards of decency and legal accountability as individuals are, then the current government would crumble.  
  
*Privacy is equated with concealment.* Redefining “privacy” as “having a shameful something to hide” is a sleight of hand. In his excellent [essay](https://tinyurl.com/yau8me3g) “’I’ve Got Nothing to Hide’ and Other Misunderstandings of Privacy,” Professor Daniel J. Solove explains the metamorphosis of privacy into concealment. “The argument that no privacy problem exists if a person has nothing to hide is frequently made…When the government engages in surveillance, many people believe that there is no threat to privacy unless the government uncovers unlawful activity, in which case a person has no legitimate justification to claim that it remain private.” Oddly enough, people who make the “nothing to hide” argument also hang curtains on their windows and close them when undressing. They do not give their wallets or purses to strangers to rummage through. They close the door before having sex, and they object to their naked photos being posted online. What are they hiding? As Solove comments, privacy is “not about anything to hide, it’s about things not being any one else’s business.”  
  
The assault on individual privacy is toxic to society as a whole.  
  
Consider freedom of speech. I remember being in a restaurant when a relative went on a post-9/11 rant about how the atmosphere in U.S. was beginning to feel like Cuba from which he had escaped. His wife tried to silence him, declaring in an adamant whisper, “You can’t say those things in public.” She was nervous as she glanced around to see who might have overheard. Surveillance and informants make people reluctant to express opinions that could be used against them in a legal or political manner. Property can be seized, families destroyed, and prison ensue. Why would anyone speak out if his children could lose a parent as a result?  
  
Until recently, many incursions on privacy did not occur for no other reason than that they were difficult to execute. Then technology arrived. Surveillance now is far more efficient with less effort. Even notoriously incompetent bureaucracies are able to surveil as never before. Many people are afraid or complacent regarding surveillance. Some simply no longer believe in the possibility of privacy. The government benefits immensely from the Big Lie that privacy is now impossible due to the omnipotent and omniscient of the state. Balderdash. First of all, technology almost always empowers the individual as much or more than it does the government. Second, there is a world of difference between more difficult and impossible. Privacy may well be more difficult than before or, perhaps, its requirements have merely changed and different protections are needed than before. Perhaps privacy takes more innovation and work.  
  
**The Value of Privacy to Society**  
  
A healthy society requires privacy. When a government monitors general communication, people do not interact freely. This is especially true of dissenters,  
  
the peacefully aberrant, writers, whistle blowers, drug users, government critics, skeptics, defense attorneys, artists… Anyone who is different in lifestyle or in opinion feels the chill of being watched by authorities who wave guns and jail cells. The bleak gray society of the Soviet Union and other communist states provides a cautionary tale of how fear crushes creativity and discussion. Surveillance strips society of color and vibrancy because it drains individuals of life, and individuals collectively *are* society.  
  
It also prevents people from rising up against injustice. A defense of privacy is a defense of human rights. Financial privacy may not be the issue with which to enter a discussion of this link, however, because money arouses immediate cynicism. But the link must be established.  
  
Consider freedom of religion and due process instead. A 16th century insurrection defined the evolution of both and their connection to privacy. The revolt revolved around a person’s right to keep his religious beliefs private so they could not be used against him in a court of law. A current version of this right is called “taking the fifth”—invoking the due process right against self-incrimination. It is called “taking the fifth” because the Fifth Amendment of the U.S. Bill of Rights provides, “No person...shall be compelled in any criminal case to be a witness against himself.” Although this mainstay of due process is often portrayed as a recourse for the guilty, the overwhelming beneficiary is the innocent man on the street who is protected against the exercise of arbitrary power, whether he realizes it or not.  
  
The 16th century insurrection: Henry VIII denied papal authority and established the Church of England, which claimed new authority over people’s souls. Protestants, called dissenters, were often tried for heresy with torture commonly accompanying trial. In the late 1530s, the Protestant John Lambert was burnt alive for heresy. During his trial Lambert became the first Englishman known to proclaim it was illegal under God and the common law to compel a man to accuse himself. He appealed to the privacy of conscience.  
  
In 1563, the dissenter John Foxe published the immensely influential *Book of Martyrs*, a book of Protestant history and martyrology that has been called a “libertarian primer” on procedural rights. He argues for the right to remain silent in order to keep personal information private. Famously, the Leveller and libertarian John Lilburne employed Foxe’s procedures in 1637 when he was brought before the Court of Star Chamber for circulating Puritan books. (The term “Star Chamber” has become a synonym for elitist and abusive courts that meet in secret.) Refusing to take the customary oath, Lilburne declined to answer questions that bore witness against himself. He was fined, whipped, pilloried, and sentenced to prison until he complied. While there, he penned an account of his brutal treatment, which was entitled *The Work of the Beast.* A few years later*,* the much-hated Star Chamber was abolished and the right to remain silent—the right to privacy—was established.  
  
The right against self-incrimination—the right of privacy in personal information— lies at the core of due process. It is historically anchored in the quest for religious  
  
freedom, but it applies no less to other freedoms, including economic ones. The demand for privacy did not merely protect individuals, however, it also inflamed societies toward freedom.  
  
It is only a slight exaggeration to say that the American Revolution might not have occurred if colonists had not demanded the right of privacy in person and property. Privacy is a revolutionary principle and virtue that prompted American colonists to [slam the door](https://www.juancole.com/2013/07/unreasonable-documents-revolution.html) in the face of British officials both literally and figuratively. The [Third Amendment of the U.S. Constitution](https://constitutioncenter.org/interactive-constitution/amendments/amendment-iii), for example, prohibits the then-widespread practice of forcibly quartering soldiers in private homes, even during peace time. The Amendment sounds antiquated to modern ears, but the violation was important enough for revolutionaries to rank it third in the list of liberties declared by the Bill of Rights. The Third Amendment asserts the right of privacy against government’s intrusion into that most personal of all realms—the home. As outmoded as the Amendment may seem, no great leap is needed to apply its principle to the current assault against all other forms of privacy.  
  
[The Fourth Amendment](https://nccs.net/online-resources/us-constitution/amendments-to-the-us-constitution/the-bill-of-rights-amendments-1-10/amendment-4-protection-from-unreasonable-searches-and-seizures) also asserts privacy. It opens by defending “[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures.” In terms of crypto privacy, the important word is “papers” because it can be extrapolated to apply to emails and other computer data, including real identities.  
  
[The Fifth Amendment](https://en.wikipedia.org/wiki/Fifth_Amendment_to_the_United_States_Constitution#Text) champions privacy by delineating the right of an individual *not to* bear “witness against himself” in criminal cases.  
  
In 18th-century parlance, when the state surveils computers and crypto accounts, it is seizing “papers.” Physical-evidence rules do not always cleanly apply to digital evidence, however, and inconsistent rulings by courts on crypto privacy cause confusion. Insight into the growing legal mess over privacy may lie in the Fourth Amendment word—“papers.” The Amendment [states](https://www.usconstitution.net/xconst_Am4.html) that both “papers, and effects, [are protected] against unreasonable searches and seizures.” But the common law, upon which Western jurisprudence is based, has tended to grant greater protection to “papers” than to “effects,” perhaps because papers are seen as a violation of person rather than property.  
  
Law professor Donald A. Dripps opens his pioneering [essay](http://scholarlycommons.law.northwestern.edu/jclc/vol103/iss1/2/) *“*’Dearest Property’: Digital Evidence and the History of Private ‘Papers’ as Special Objects of Search and Seizure” with two questions. “Why does the Fourth Amendment distinctly refer to ‘papers’ prior to ‘effects’? Why should we care?” Dripps asks in order “to ground special Fourth Amendment rules for digital evidence” within statute law to restrict “the volume of innocent and intimate information that must be exposed [or demanded] before the criminal material is discovered.” Again, the American Revolution provides insight.  
  
In the 1760s, British warrants for papers began to issue against colonial authors and publishers who were suspected of sedition. [*Entick v. Carrington*](https://everything2.com/title/Entick+v.+Carrington) (1765) is probably the most influential legal case of the time. The bare facts of the case:  
  
John Entick published a paper that opposed the Crown. In 1762, officers broke into Entick’s home and stole hundreds of papers in a search for evidence of treason. Entick sued. Entick won. The presiding judge, Lord Camden, offered a famous dictum. “If it is law, it will be found in our books. If it is not to be found there, it is not law.” The government’s purported right to seize papers was not in the statutes, therefore, it was not law.  
  
Subsequent analysis of the *Entick* case found four aspects of the government’s raid to be legally obnoxious; all of them apply to the current surveillance and seizure of financial information. The warrant was *indiscriminate.* The seizure *expropriated* the papers, denying their use to the plaintiff. The warrant was *unregulated* because there was no neutral oversight or avenue of appeal. The seizure was *inquisitorial* because it gave the government information about the private workings of Entick’s mind. Counsel for Entick declared: “No power can lawfully break into a man’s house and study to search for evidence against him; this would be worse than the Spanish inquisition; for ransacking a man’s secret drawers and boxes to come at evidence against him, is like racking his body to come at his secret thoughts.” Seizing papers was an attack against person, not property.  
  
Any judge who subsequently considered issuing a warrant for papers had to consider Lord Camden‘s ruling that an alleged offense needed to be in the statute books if it was to exist in law. Moreover, warrants on papers increasingly ran afoul of state constitutions.  
  
War changes laws, especially laws protecting individual rights. Dripps continues, “America...refused to modify the common law ban by statute until the Civil War.” The excise tax was the federal government’s major source of funding for the war, but tax evasion was rampant. In response, a unique statute was passed. “[This] act of 1863 was the first act in this country...or in England, so far as we have been able to ascertain, which authorized the search and seizure of a man’s private papers, or the compulsory production of them, for the purpose of using them in evidence against him in a criminal case, or in a proceeding to enforce the forfeiture of his property.” Seizure of papers was now in the statutes.  
  
The question of papers versus effects legally zigzagged after the Civil War. Arguably, the most important shift came in 1886 when *Boyd v. United States* was decided by the U.S. Supreme Court. “The story of the Boyd case,” Dripps writes, “properly begins with a statute authorizing customs officers to seize the books and papers of importers suspected of evading taxes.” The Supreme Court [ruled in Boyd’s favor, saying](https://www.csoonline.com/article/2220119/microsoft-subnet/in-this-digital-age--what-the-heck-happened-to-the-constitution-.html) :  
  
The principles laid down in this opinion affect the very essence of constitutional liberty and security. They...apply to all invasions on the part of the government and its employees of the sanctity of a man’s home and the privacies of life. It is not the breaking of his doors and the rummaging of his drawers that constitutes the essence of the offense; but it is the invasion of his indefeasible right of personal security, personal liberty, and private  
  
property, where that right has never been forfeited by his conviction of some public offense, it is the invasion of this sacred right which underlies and constitutes the essence of Lord Camden’s judgment.  
  
The *Boyd* ruling reinstated greater Constitutional protection to papers than to effects, and it bears directly upon digital papers. The protection was never absolute, however, and it has severely eroded. Dripps explains, “During the last quarter of the twentieth century, the Supreme Court began effectively to equate ‘papers’ and ‘effects’. Another line of modern cases established ‘bright-line rules’ that gave the same constitutional treatment to all ‘effects’.” Papers not only lost their special status under common and Constitutional law, they also came closer to becoming legally interchangeable with every other effect. This offered far weaker protection. Nevertheless, the precedent of *Boyd* prevailed for almost a century, and it is still not toothless.  
  
The importance of papers is inextricably connected to the value of privacy to individuals. When the government steals data, it does not violate “property” in the legal sense of the word; it violates person.  
  
Privacy is part of a healthy, creative, and self-reflecting life. Since childhood I’ve kept a diary into which I pour hopes, confusion, disappointments, and desires. When I read pages from the past, I connect viscerally to who I was at ten years old, and I better understand the person I am today. These diaries are private, not because I am ashamed of them, but because they are *personal*. In his dystopian novel [*1984*](http://www.george-orwell.org/1984/), George Orwell stresses the importance of diaries:  
  
The thing that he was about to do was to open a diary. This was not illegal (nothing was illegal, since there were no longer any laws), but if detected it was reasonably certain that it would be punished by death.  
  
*1984*‘s protagonist discovers his individualism. In this journey, the diary represents the freedom of speech and conscience that are essential to a sense of self—so essential that the state will kill him for this act of privacy.  
  
Every infringement of privacy erodes the human spirit. A word is not spoken for fear of being overheard; a thought is not formed for fear it will become a word; a feeling is never expressed and, perhaps in time, not even felt. Then, one day, the outer silence becomes an inner one through the now automatic habit of self- censorship. People no longer question. Perhaps they no longer even notice that they no longer question. They have developed the habit of not being an individual, and they have become part of a collective will instead.  
  
Everyone has areas of privacy to protect. Some wear lockets with photos of dead relatives; others harbor a forbidden love; some bolt the door to luxuriate in a hot bath without being disturbed; or they hide a sexual preference that confuses them. Every human being has a right to draw lines that harm no one else, lines that no one else should cross without an invitation. Slam the door in the face of anyone who says differently!  
  
Crypto focus on privacy is more than the desire to retain wealth, as is usually claimed. It is a desire to retain individuality, the human spirit, and freedom.