# True Nyms and Crypto Anarchy

**Timothy C. May**

One of the biggest issues in cyberspace these days, one that will continue to be an issue as long as there is such a venue as the Internet, is the safety of communication from prying eyes. In the detailed and persuasive essay that follows, Tim May, formerly a physicist at Intel and one of the founding members of the Cypherpunks, discusses the big issues involved—invasion of privacy, the specter of government interference in personal affairs, the use of electronically forwarded information by a variety of people, entities, and organizations for purposes other than those intended by the forwarder … these are all issues of tremendous importance to anyone who uses the Internet —and that means just about everyone, in one way or another.

In a previous age, these issues were not of such great importance, for there was never the possibility that anyone could find and gather enough information to do harm to others in the ways that are now possible with the Internet. Today, however … Read Tim May's essay and you'll never feel quite as safe as you did a moment before you read these pages. This article was written in 1996.

## The Impact of *True Names*

"True Names" came to my attention in 1986, when a friend of mine gave me a dog-eared Xerox copy and said "You need to read this." But before I even started reading this samizdat edition, the Bluejay Books trade paperback edition appeared and that's what I read, saving my eyesight and giving Vernor Vinge his proper cut of the action. *True Names* certainly riveted me, and it fit with other developments swirling around in computer circles at the time. Namely, digital money, anonymous e-mail, and all of the other issues connected with "strong cryptography" and "public key cryptography."

Some friends were setting up a company to develop "information markets" for the Net, though this was half a dozen years before the World Wide Web and wide public access to the Internet. It was clear to me that the ideas of anonymous interaction, reputation-based systems, digital pseudonyms, digital signatures, data havens, and public-key encryption in general would all be important for these markets in cyberspace. The work of Holland-based David Chaum, an American cryptographer who developed most of the early ideas about digital money and untraceable e-mail, looked to be of special relevance. Chaum's work on untraceable electronic cash, reported in a 1985 "Communications of the ACM" cover story (November 1985), sparked the realization that a digital economy could be constructed, with anonymity, untraceability, and ancillary anarcho-capitalist features, such as escrow agents to hold money for completion of services, reputation rating services and tools, and "persistence" for various kinds of constructs. In other words, a cryptographically based version of Vinge's *True Names,* and even of Ayn Rand's "Galt's Gulch" in *Atlas Shrugged.*

The full-blown, immersive virtual reality of *True Names* may still be far off, but the technologies of cryptography, digital signatures, remailers, message pools, and data havens make many of the most important aspects of

*True Names* realizable today, now, on the Net. Arguably, Mr. Slippery is already here and, as Vernor predicted, the Feds are already trying to track him down. In 1988 these ideas motivated me to write and distribute on the Net "The Crypto Anarchist Manifesto," a section of which is quoted here:

"A specter is haunting the modern world, the specter of crypto anarchy.

"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 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."

These ideas have evolved over the years since this was written, but the basic ideas remain unchanged. The Cypherpunks group has been instrumental in implementing many of the concepts.

In this article I'll be exploring some of the implications of strong cryptography and crypto anarchy and the connections with *True Names.* Because this article will be in a book, with presumably a shelf life of many years, I'm avoiding giving specific article citations and URLs to Web sites, as they tend to change quickly. Searching on the names of authors should be a more reliable way of finding current locations and information.

## Cypherpunks

The time was right in 1992 to deploy some of these new ideas swirling around in the cryptography and computer communities and reify some of these abstractions. Eric Hughes and I gathered together some of the brightest folks we knew from the annual Hackers Conference and from the Bay Area computer community to discuss the implications of these ideas, and to look into translating some of the academic work on cryptography into real-world

programs. The initial meeting led to larger, monthly meetings, and to an active mailing list. Jude Milhon suggested the pun “Cypherpunks,” a play on “cyberpunk” and on the British spelling “cypher.” The name stuck, and the Cypherpunks mailing list has been active ever since. It was on this list that several of the most important security breaches in Netscape and other Internet programs were revealed, and the Cypherpunks list has played an important role in the ongoing cryptography debate, including fruitful discussions of the Clipper chip, key escrow, export laws, private access to strong cryptography, the implications of digital money, and other issues. We were also fortunate that Phil Zimmermann’s Pretty Good Privacy, or PGP, appeared in a usable form just as we were getting started. PGP is the leading user-friendly encryption program, available on nearly all platforms, and it was used as a building block for many of the cryptographic tools we and others developed.

The Cypherpunks group is also a good example of a “virtual community.” Scattered around the world, communicating electronically in matters of minutes, and seemingly oblivious of local laws, the Cypherpunks group is indeed a community; a virtual one, with its own rules and its own norms for behavior. Some members use pseudonyms, and use anonymous remailers to communicate with the list, using PGP to digitally sign posts. These digital pseudonyms are in some sense their true names, their “true nyms.” On the Cypherpunks list, a number of well-respected nyms have appeared and are thought of no less highly than are their “real” colleagues. The whole subject of digitally authenticated reputations, and the reputation capital that accumulates or is affected by the opinions of others, is one that combines economics, game theory, psychology, and expectations. Reputations play a critical role in how anonymity and pseudonyms work in cyberspace; many of the predicted problems with nyms vanish when reputations are taken into account.

There were several books we frequently recommended to new members: *True Names* led the list, along with John Brunner’s *Shockwave Rider,* Orson Scott Card’s *Ender’s Game,* Neal Stephenson’s *Snow Crash,* Hakim Bey’s *TAZ,* and, of course, various cryptography and computer references, notably Bruce Schneier’s *Applied Cryptography*. At our first meeting, in fact, we simulated some of the notions out of “True Names,” using cryptographic

protocols. Most of the issues about pseudonyms, digital personas, and anonymity have since been explored directly using “Cypherpunks remailers” and related technologies.

## Anonymous Remailers

Anonymous remailers, also called digital mixes, provide an excellent example of the possibilities inherent in cryptographic technology. David Chaum originally developed most of the important ideas in a 1981 paper on “Untraceable E-Mail,” years before e-mail achieved the wide prominence it now has. And he later refined the ideas in a paper on so-called “DC-Nets,” an interesting topic a bit beyond the scope of this article.

There are many reasons people may wish to occasionally communicate without being traced or identified. A digital pseudonym is obviously useless if e-mail programs identify the origin of e-mail. People may wish to be anonymous for many reasons: privacy, fear of reprisal by employers or other groups, avoidance of profiles of their activities and interests, posting to controversial newsgroups or support groups (such as “alt.recovery” or rape and incest recovery groups), whistleblowing, and floating of controversial ideas. Writers have long used pseudonyms for some of the same reasons. (And the U.S. Supreme Court ruled in 1956 that writers may not be compelled to put their true names on their writing.)

To see how anonymous remailers work, imagine a person—call her Alice—trying to avoid being followed by someone—call him Bob. Wherever she goes, Bob follows. As she enters a store, Bob waits outside and watches for her to leave, and picks up the tail. However, suppose she enters a large department store, along with many others, and emerges some time later with many others, wearing different clothes and generally not being recognizable. Bob has no idea of which person leaving the store is Alice, and so he must either give up the tail, or follow all of the people leaving the store. She repeats this process many times, each time becoming more and more “mixed” with others. With even a small number of such mixings, the number of paths Bob must follow can become astronomically high. Alice has thus used department store mixes to shake her tail.

This is the way anonymous remailers or digital mixes work. An e-mail

message is sent to a remailer, encrypted to the public key of the remailer operator or his machine. The contents of the message look essentially random to any observer (who might be tapping the lines, for example). The remailer operator decrypts the message, holds it for some period of time or until sufficient other messages have accumulated, adds any needed padding to make the message size not a correlatable factor, and sends the accumulated messages out to their next destinations. Very importantly, the messages he remails are usually encrypted by the originator to the *next* remailer's public key, so any given remailer cannot read the contents of any message. Nor can any remailer in the chain modify the messages, or tag them in any way (as any modifications would make the message unreadable, undecipherable, by the next remailer in the chain). Using encryption at each stage completely obscures the mapping between origin and destination, to both the final recipient and to all of the remailers. The recipient receives only the "innermost" message, with all of the earlier stages progressively stripping off headers. Any given remailer can only open the envelope "addressed" (encrypted) to him, and cannot read the messages that remain in the text block he does see … all he can do is read the next destination, which is included in the clear. Think of envelopes within envelopes, each addressed to a particular remailer.

The originator of a message decides on a chain of remailers he plans to use, encrypts and addresses his messages in reverse order, and then sends the resulting message to the first remailer, who decrypts it and sends the result to the next remailer in the chain, and so forth. If, for example, the originator picks five remailers, and each remailer waits until ten messages have been accumulated before forwarding the accumulated batch, then in theory there are upward of one hundred thousand possible routings to be followed. There are not usually this many messages, so the correlation problem is not quite this hard. But any attempt at tracing the message is still effectively thwarted, unless the various remailers collude or are instructed by authorities to report all of the mappings between arriving and departing messages. Using some offshore remailers is an effective bar to this latter attack. And some people publish regular lists of remailers, with the results of ping tests, latency time measurements, reliability, etc.

The first Cypherpunks remailers were initially written in Perl and C by Eric Hughes and Hal Finney. They allowed e-mail to be sent to a remailer, have its origin stripped off, and then be remailed to a selected destination, including other remailers. They were first deployed in 1992, and by 1996 several dozen existed. These were used to anonymously publish ("liberate") ciphers that had not previously been published, to publish secrets of the Church of Scientology, to disclose a few military and security secrets, and, not surprisingly, for flames, insults, and anonymous attacks. Ideally, no mapping is kept of who sent what mail, so court orders and lawsuits are ineffective in revealing the identities of those sending mail. Further, hardware-based digital mixes, i.e. sealed modules with a public key present only inside the module and unreadable by outsiders, will mean no human is even involved in the process, even as a system administrator. Long chains of such mixes, operating quickly on highspeed networks, should make the task of tracing messages even more intractable. A commercial implementation of a digital mix, called MixMaster, is available; users can install such "instant mixes" on their Internet boxes and become remailers. This turns out to be a good example of what a simple application of strong cryptography, using PGP, can do. The Perl and C code is short and simple, and the security of the entire chain depends solely on the unbreakability of encrypted messages, on the number of hops, and on the unlikelihood of collusion between the various remailers. (If all of the remailers were to get together and compare notes, the system would of course be broken. But as the number of remailers increases, this strategy becomes less and less effective. Also, one can always remail messages through oneself, thus defeating most collusion or tapping efforts.)

Another approach to remailers is the one followed by Julf Helsingius, of Finland, who operated an anonymizing service that kept a database of mappings between pseudonyms and actual e-mail addresses. This system was easy to use, and allowed easy replies to senders. However, the database was a ripe target for civil lawsuit investigators (and criminal investigators), and Julf pulled the plug on his system in 1996. Cypherpunks remailers, by being distributed, in many jurisdictions, and robust against such requests, offer a more solid and scalable basis for anonymous remailer networks.

"Digital postage" is needed both to incentivize remailers to operate for-

profit sites (and thus expand the number and robustness of these sites) and to provide a more solid economic basis for e-mail in general. E-mail currently costs most users nothing to send; this has led to widespread "spamming" of the Net. (Consistent with the themes of this article, what is needed is not global regulation but a market-based pricing mechanism for e-mail.) Some work on digital postage has been done, but true progress awaits wider deployment of digital cash systems.

This use of remailers is just one concrete example of the use of cryptography to alter institutions and interactions.

## True Nyms

The controversy over naming and under what circumstances true names can be demanded is likely to rage for decades.

Why do we so often accept the notion that governments issue us our names and our identities, and that governments must ensure that names are true names? Governments like to be involved in identity issues because it gives them additional control. And it helps them to track the flow of money. For example, centuries ago, the rulers of various European countries forced the Jews to drop their traditional patronymic practices ("Jacob son of Israel") so as to allow taxes to be more efficiently collected, to monitor movements, and so forth. These rulers even sold the "best" family names to those who paid the most, leaving others with less desirable, or even insulting, names. The same practice was repeated in the U.S. with the naming of ex-slaves and the renaming of immigrants. As Nietzsche pointed out, "The master's right of naming goes so far that it is accurate to say that language itself is the expression of the power of the masters." Governments today even give themselves the rights to create/forge completely false identities, with false credit histories, false educational backgrounds, etc. Under the guise of "protecting witnesses," the Federal Witness Security Program, popularly called Witness Protection, has created upward of fifty thousand fabricated identities. The major credit reporting agencies are, of course, not fooled, as these "ghosts" pop into existence in their databases, and these agencies are most likely colluding in the support of these false identities. Imagine lending money to someone on the strength of an excellent credit report, only to find

that you lent money to a convicted scam artist who sold out his partners so he could receive a fake ID. Who would you sue? (One of the things anonymous information services, to be covered later, will be good for is soliciting the truth behind such government lies, e.g., by offering money for a CD-ROM containing the true names and locations of those in the WitSec program. Anyone with access to this database is a potential seller, and can accept payment untraceably. It's going to be an interesting world.) There are strong pressures building for issuance of national identity cards, perhaps using smart cards, especially for control of immigration, travel, "deadbeat dads," and terrorism. In a free society, those who wish to deal only with actual, provable true names would, of course, be free to refuse interactions with nyms, true names being just another credential, sometimes offered, sometimes not.

Digital pseudonyms, the creation of persistent network personas that cannot be forged by others and yet are unlinkable to the "true names" of their owners, are finding major uses in ensuring free speech, in allowing controversial opinions to be aired, and in providing for economic transactions that cannot be blocked by local governments. The technology being deployed by the Cypherpunks and others means their identities, nationalities, and even which continents they are on are untraceable—unless their owners choose to reveal this information. This alters the conventional "relationship topology" of the world, allowing diverse interactions without external governmental regulation, taxation, or interference.

## Public-Key Cryptography

Cryptography is about more than the stereotypical sending of secret messages. The combination of strong, unbreakable public-key cryptography and virtual network communities in cyberspace will produce profound changes in the nature of economic and social systems. Crypto anarchy is the cyberspatial realization of anarcho-capitalism, transcending national boundaries and freeing individuals to consensually make the economic arrangements they wish to make. The fundamental notion of modern public-key cryptography is that the key for locking, for example, a box, is different from the key for unlocking the box. The owner of a box can then publicize the form of the key needed to lock "his" box, and keep the unlocking key a secret.

Anyone can then lock a message in Bob's box with his "public-key," but no one except Bob can ever unlock that box, not even with all the computer power in the world. From this basic point flow all sorts of variations and extensions. An alternative metaphor is that of the *envelope:* anyone can place something inside one of Bob's envelopes and seal it, but only Bob can open his envelopes. (In the chains of remailers we just discussed, envelopes-within-envelopes are used, for as many stages as are desired.)

Cryptography revolves around *local control* of some secret. For example, a user has a private key which only he knows. Others can send him messages, using his *public* key, but only he can decode or decrypt them. So long as this key is kept secret, the encrypted communication cannot be read by others. The security depends on the length of the keys, the number of bits in the keys. A "weak" key of forty or fifty bits, for example, can be cracked with a personal computer. Stronger keys of sixty-four or eighty bits are preferable, though they're still not truly secure. And it is no more difficult to use ciphers with an effective strength of several hundred bits; such ciphers should withstand brute-force attacks for centuries, perhaps millennia or longer. Public-key cryptography has the important property that it is much easier to encrypt with very large keys than it is to break a message (decrypt by brute force, without the secret key). The difference in effort widens exponentially with increasing key size. Advances in computer power are more than offset by the ability to use longer keys. Likewise, "massively parallel computers," often cited by the ignorant as a possible way to break these ciphers, offer only marginal, linear speedups on brute-force cracking … utterly inconsequential compared with the efforts needed to factor large numbers. Faster computers are a big win for strong cryptography.

The important distinction between modern cryptography and conventional, or classical, cryptography is that the keys are asymmetric in modern cryptography, whereas in classical cryptography the parties to a cipher had somehow to exchange the same key. Exchanging keys with hundreds or even thousands of correspondents is much harder than simply looking up a key in a public-key directory, or asking for it to be sent in e-mail. More important for our purposes here, only the public-key approach allows the uses described here. For example, digital signatures rely on

keeping the secret key a secret. If conventional ciphers were used, then anyone sharing one's private key could forge signatures, withdraw money, and generally wreak havoc. (Digital signatures exploit this asymmetry property of keys by allowing anyone to easily authenticate a signature without having access to the key that would allow forgery of a signature.)

Appropriately for this book, encryption is like an unbreakable "force field" around an encrypted item, much like the "bobbles" described in Vinge's *The Peace War*. The amount of energy required to run the computers —not to mention the number of such computers and the time involved!—can be shown to be greater than all of the energy all of the stars in the universe will ever produce. This for a sufficiently large key, one with an RSA modulus of a few thousand digits. (This has not yet been mathematically proved, in that factoring large numbers has not been proved to be "hard." It is remotely possible that some fast factoring breakthrough will be discovered, but this is considered by nearly all mathematicians to be extremely unlikely. The speculation that the NSA knows how to quickly factor large numbers, and thus break RSA, seems equally unlikely.)

## The Encryption Controversy

Governments are clearly afraid of strong cryptography in the hands of the citizenry. Governments around the world have attempted to deal with the implications of this threat by limiting the size of keys that citizens may use, by limiting the types of algorithms that may be used, by demanding that citizen-units "escrow" (deposit) their keys with the government or with registered government agents, and by banning strong cryptography altogether. This is a battle over whether one's thoughts and messages may be placed inside sealed envelopes or must be written on "postcards," for the government to read, as Phil Zimmermann points out. One U.S. government proposal, repeated in several variants, is that messages may be sealed in envelopes, but only if the government has a special key to open them. This is like allowing citizens to have curtains on windows, but only if the local police can trigger a special transparency mode. And the issues are quite comparable. Encryption, as we will see, makes certain kinds of crimes and revolutionary activities much more feasible, but so do locked doors, curtains, and whispered

conversations. And yet we would not consider outlawing locked doors, curtains, and whispered conversations. As Zimmermann notes, “I should be able to whisper in your ear, even if you’re a thousand miles away,” referring of course to e-mail or to voice-scrambling technology (public-key cryptography is fast enough, when combined cleverly with conventional ciphers, to allow real-time audio and video streams to be encrypted). There are profound constitutional issues involved, in the U.S. at least. The various rights enumerated in the Bill of Rights would seem to make it impossible for the U.S. government to specify the forms of speech, to insist that locks have keys escrowed with the police, and so forth. Many observers expect cryptography restrictions to face strong challenge on constitutional grounds, and, in fact, a few cases are in the court system, challenging various provisions of U.S. cryptography policy (especially the export provisions of the Munitions Act and related restrictions).

This debate is still going on, and it’s too soon to tell if the “Great Crypto Crackdown” will succeed. Certainly there are many reasons to expect that it’s far too late to suppress such technologies, that millions of users will not lightly go to “postcards” for their communications, and that concerns about government corruption, secret FBI dossiers, and economic espionage will undermine Big Brother’s efforts to control the communications of “citizen-units.”

## Digital Money and Electronic Commerce

This is one of the most exciting frontiers, and one of the most publicized. But it is also one of the hardest to implement correctly. Money intrinsically involves stores of value, transfers of value, institutions, and various interlocking webs of regulations, so implementing digital money correctly has not come easily. In fact, the history of digital money lies mostly in the future. The early years of the new century should see many of the current problems resolved.

Digital cash, untraceable and anonymous (like real cash), is coming, though various technical and practical hurdles remain. What have been dubbed “Swiss banks in cyberspace” will make economic transactions much more liquid and much less subject to local rules and regulations. Tax

avoidance is likely to be a major attraction for many. One example to consider is the work under way to develop anonymous, untraceable systems for “cyberspace casinos.” While not as attractive to many as elegant casinos, the popularity of “numbers games” and bookies in general suggests an opportunity to pursue; this is but one of many new opportunities digital money will offer.

By digital money I do not mean the various kinds of electronic funds transfers, automated teller machine transactions, wire transfers, etc. that already exist in so many forms. Nor do I mean the various “smart card” systems that some claim to be “digital money,” even “untraceable digital cash” (in some notorious examples involving flawed protocols). Rather, our focus is on instruments that are actually *untraceable* in a strong sense. Again, Chaum was the pioneer in this area, and his company DigiCash is the exemplar of digital money at this time, with several large banks cooperating in joint ventures to issue DigiCash. Digital money probably will not be “digital currency,” in the sense that dollars, yen, and marks are currency. Rather, it will be more like the various financial instruments, denominated in various currencies, such as checks, bearer bonds, letters of credit, promissory notes, chop marks, and even IOUs.

Alice and Bob can exchange digital cash in this way: Alice goes to a bank, submits to the bank a kind of number, and receives a modified form of this number from the bank. It’s as if the bank has stamped her number with a “Good for 100 Digimarks” stamp. Ordinarily this number would of course be traceable, but Alice can perform a special operation on this number (“unblinding” it) which makes it unlinkable to her original purchase of the number. She can then send this number to Bob, perhaps even through an anonymous remailer, and Bob can then present this number to the bank for redemption. The bank can recognize the number as one that it issued, through some manipulations, but cannot link it with Alice. Full-blown digital cash is both payer- and payee-unlinkable. Some of the current proposals being floated limit the untraceability to only partial untraceability, presumably to satisfy the concerns of government and law-enforcement critics of full untraceability. Cypherpunks Ian Goldberg, Doug Barnes, and others have developed methods to make even this partially traceable form fully

untraceable.

The actual details involve some complicated math and need careful thought to get straight, which this article cannot cover. Bruce Schneier's *Applied Cryptography* has a good explanation of how Chaumian digital cash works, and *Scientific American* has also carried some good articles.

It is often claimed that "digital currencies" will not gain widespread acceptance, let alone the support of governments. If digital money is viewed as a transfer mechanism, and not as a competitor to currency or specie (gold, silver, etc.), then the support of governments is less of an issue, perhaps even a non-issue, because banks have done quite well without explicit governmental sanction of their instruments. And in the international realm, there already is not much of a governmental role: banks have worked out mechanisms for dealing with each other, and for dealing with entities with a reputation for misbehavior. As we will see, international trade represents a kind of anarchy.

There are many reasons for using untraceable digital cash. Some people simply prefer to pay cash for various reasons, and see no reason why electronic transactions should have more traceability than ordinary folding-money transactions have. Others fear the compilation of dossiers on spending habits, travel agendas, and so forth. Untraceable digital money protects the privacy of economic transactions, just as cash does today. With increasingly powerful networks of ATM and check-processing systems, the development of "shopping profiles" is a concern for anyone interested in privacy. Having insurance companies and employers gaining access to purchasing habits is undesirable; such access could, at its extreme, lead to law enforcement midnight raids on persons suspected of various crimes because of legal purchases they might have made. Untraceable digital money provides protection against this.

Making automated toll-road payments with untraceable digital cash is one obvious use. Digicash is working with European governments to deploy digital money for this sort of application.

There are, of course, various transactions involving anonymity, digital pseudonyms, and illegal items that only an untraceable digital cash system makes possible. And some novel applications are new. For example,

"perpetual trusts" could be constructed by purchasing a large number of digital money instruments, perhaps being converted regularly to other such instruments. Because they are untraceable, there is no means of, say, canceling the numbers to stop the perpetual trust. Thus, as a hypothetical, no one—certainly not the bankers—will know that which of the instruments are part of the perpetual trust Bill Gates creates in 2010 with ten billion dollars … and this trust could still exist a century later, untouched by taxation and not even really domiciled in any particular nation. Contracts using such digital money instruments could similarly be of this "fire and forget" sort. Thus can fortunes be directed toward specific purposes, beyond the reach of governments. (For the curious, digital time-stamping and cryptographic timed-release techniques are needed to insure that the humans involved don't violate the contract originally set up.)

There are, of course, many reasons *not* to use untraceable digital cash. Businesses typically need to show records of expenses to deduct against gross sales. The simplest example of this involves anonymous payments to employees: few corporations would be interested in doing this, even if they satisfied themselves that they wouldn't get caught, because they then could not use the employee expenses as a deduction against raw income. (One can imagine many situations where an employer *would* be interested in such arrangements, and under-the-table payments are common practice in certain types of businesses.)

There is still the possibility of fraud, of dissatisfaction with transactions, and of improperly completed transactions. Cryptography obviously cannot completely eliminate such disputes. But various measures, such as reputation-rating services, digital signatures, etc., should work fairly well in controlling these kinds of problems. Trade has been conducted for millennia without governments playing a central role; in fact, international trade is often cited as an example of anarchy in action, as clearly the laws of any one country are not easily applicable. That trade works so well is evidence that actions have consequences, that repeat business matters, and that even in a relative anarchy, behavior matters. An excellent survey of this kind of trade anarchy is contained in Bruce Benson's *The Enterprise of Law*.

The argument often made by critics of untraceable e-cash, that issuers will

renege or abscond, refusing to honor their instruments, ignores the nature of e-cash. Because e-cash is untraceable, an issuer never really knows when he's merely being "tested" by a rating service (or, more direly, when the client might be a member of the Mafia!). Reliability testing and reputation ratings are important.

True digital cash—the fully untraceable form—admittedly will allow some new channels for criminal activity. Privacy has its price. The ability of people to plot crimes and commit them behind closed doors is obvious, and yet we don't demand secret cameras in homes, apartments, and hotel rooms. Some of the disadvantages of anonymous systems will be discussed later, along with some of the proposals by various governments to limit or even completely ban strong cryptography.

## The Surveillance Society

Imagine you are entering a bar or nightclub, or a movie. You are asked to produce identification as proof that you are of legal age. Currently, these "credentials" are presumably only glanced at briefly. With the advent of computer scanners, bar codes, and networks, the very real possibility exists that such credentials will be scanned, read, and fed into various databases. Maybe for customer profiling, maybe for compliance auditing, maybe for other reasons. But the effect is that one's movements, habits, and preferences are now in a database, perhaps even fed to the local police (as is the custom in many countries). Even if the collected data is not explicitly planned for a dossier, or for the government, a trail is still created, and this presents serious problems, especially as networks and computers get much faster.

David Chaum, along with his other work, has also developed schemes for presenting a credential of some sort without revealing identity. Though this sounds impossible, modern cryptography provides an approach. Think of it as a sealed envelope with a movable transparent window that can be moved over, say, an "age" field. The owner of such a credential could present proof that he is of some age, or past some age, without providing his identity or any other information. How this works, and how forgeries are prevented, is beyond the scope of this chapter. Cryptographic protocols are used, and biometric authentication is generally needed, to prevent such a credential

from being easily lent or sold to others.

One obvious use is for automated toll-road tokens that can be read remotely, either authorizing the holder to travel on the road, or, using digital cash, make a payment remotely. The dangers of having one's movements on toll roads compiled into records is obvious to nearly everyone, though Singapore has adopted just such a citizen-unit-tracking system!

This is a good example of how technology can provide the kind of protection that well-meaning "privacy laws" cannot actually provide. While special interest groups lobby the government for new laws and new wrinkles on old laws, technology can directly provide the protection many want. For example, which approach better solves the problem of people using scanners to monitor cellular telephone conversations: passing more laws saying such monitoring is illegal (except for the police), or adding encryption to cell phones? A basic credo of the Cypherpunks movement has been that technological solutions are preferable to administrative or legislative solutions.

The growing use of government-approved picture IDs for travel is becoming the modern equivalent of travel documents in the U.S. While I cannot see a situation in which citizen-units are ever told they may not travel without authorization, I can quite easily see the situation emerging in which airlines, bus companies, car rental agencies, hotels, and gas stations are expected to "run your card through." This is already the case with many hotels and nearly all car and truck rental agencies demanding credit cards (partly to insure payment, but also for law-enforcement purposes). This produces a de facto movement-tracking system. Expect more scrutiny, perhaps even time-consuming and hassling scrutiny, for those who try to pay in cash and for those who are reluctant to have their ID cards run through the system. Since 1995, airlines have insisted on picture IDs, on orders of the government.

As with the government interest in true names and the naming process for tracking, such ID cards are an essential tool for tracking movements, collecting taxes, and establishing dossiers on citizen-units. Credentials without identity are an important technology to have and to deploy widely. A recurring theme here is that technology, not so-called privacy laws (from

which governments nearly always exempt themselves anyway), is the best protection against such a surveillance state.

## Data Havens and Information Markets

Another science fiction writer, Bruce Sterling, popularized “data havens” in his 1988 novel *Islands in the Net.* He focused on *physical* data havens, but cyberspace data havens are more interesting, and are likely to be more important. That they are distributed in many legal jurisdictions, and may not even be traceable to any particular jurisdiction, is crucial. A data haven is a place, physical or virtual, where information may be stored or accessed. The usual connotation is that the data are illegal in some jurisdictions, but not in the haven.

Data havens and information markets are already springing up, using the methods described to make information retrievable anonymously and untraceably. Using networks of remailers and, of course, encryption, messages may be posted in public forums like the Usenet, and read by anyone in the world with access, sort of like a cyberspatial “Democracy Wall” where controversial messages may be posted. These “message pools” are the main way cyberspatial data havens are implemented. Offers may be in plaintext, so as to be readable by humans, with instructions on how to reply (and with a public key to be used). This allows fully untraceable markets to develop.

It is likely that services will soon arise which archive articles for fees, to ensure that a URL (Uniform Resource Locator) is “persistent” over a period of many years. Ross Anderson’s “Eternity Service” provides a means of distributing the publication of something so that even later attempts to withdraw all copies are thwarted. This has obvious value in fighting censorship, but will also have implications when other types of publication occur (for example, a pirated work would not be withdrawable from the system, leaving it permanently liberated).

Examples of likely data haven markets are credit databases, doctor and lawyer databases, and other heavily regulated (or even unallowed) databases: information on explosives, drug cultivation and processing, methods for suicide, and other such contraband information. Data havens may also carry copyrighted material, sans payment to holders, and various national and trade

secrets.

As one example, the “Fair Credit Reporting Act” in the U.S. limits the length of time credit records may be kept (to seven or eight years) and places various restrictions on what data may be collected or reported. What if Alice “remembers” that Bob, applying for credit from her, declared bankruptcy ten years earlier, and ran out on various debts? Should she be banned from taking this into account? What if she accesses a database that is *not* bound by the FCRA, perhaps one in a data haven accessible over the Net? Can Alice “sell” her remembrances to others? (Apparently not, unless she agrees to the various terms of the FCRA. So much for her First Amendment rights.) This is the kind of data haven application I expect will develop over the next several years. It could be in a jurisdiction that ignores such things as the FCRA, such as a Caribbean island nation, or it could be in cyberspace, using various cryptographic protocols, Web proxies, and remailers for access.

Imagine the market for access to databases on “bad doctors” and “rip-off lawyers.” There are many interesting issues involved in such databases: inaccurate information, responses by those charged, the basis for making judgments, etc. Some will make malicious or false charges. This is ostensibly why such databases are banned, or heavily regulated. Governments reserve the right to make such data available. Of course, these are the same governments that falsify credit records for government agents and that give the professional guilds like the American Medical Association and the American Bar Association the power to stop competitors from entering their markets.

Information markets match potential buyers and sellers of information. One experimental “information market” is BlackNet, a system I devised in 1993 as an example of what could be done, as an exercise in guerrilla ontology. It allowed fully anonymous, two-way exchanges of information of all sorts. The basic idea was to use a “message pool,” a publicly readable place for messages. By using chains of remailers, messages could be untraceably and anonymously deposited in such pools, and then read anonymously by others (because the message pool was broadcast widely, *à la* Usenet). By including public keys for later communications, two-way unreadable (to others) communication could be established, all within the

message pool. Such an information market also acts as a distributed data haven.

As Paul Leyland succinctly described the experiment:

> Tim May showed how mutually anonymous secure information trading could be implemented with a public forum such as Usenet and with public key cryptography. Each information purchaser wishing to take part posts a sales pitch and a public key to Usenet. Information to be traded would then have a public key appended so that a reply can be posted and the whole encrypted in the public key of the other party. For anonymity, the keys should contain no information that links it to an identifiable person. May posted a 1024-bit PGP key supposedly belonging to "Blacknet". As May's purpose was only educational, he soon admitted authorship.

An example of an item offered for sale early on, in plaintext, was proof that African diplomats were being blackmailed by the CIA in Washington and New York. A public key for later communications was included.

There are reports that U.S. authorities have investigated this market because of its presence on networks at Defense Department research labs. There's not much they can do about it, of course, and more such entities are expected. The implications such tools hold for espionage are profound, and their impact largely unstoppable. Anyone with a home computer and access to the Net or the Web, in various forms, can use these methods to communicate securely, anonymously or pseudonymously, and with little fear of detection. "Digital dead drops" can be used to post information obtained, far more securely than the old physical dead drops … no more messages left in Coke cans at the bases of trees on remote roads. Payments can also be made untraceably; this of course opens up the possibility that anyone in any government agency may act as a part-time spy.

Matching buyers and sellers of organs is another example of such a market, although one that clearly involves some real-world transfers (and so it cannot be as untraceable as purely cyberspatial transactions can be). There is huge demand for such transfers, but various laws tightly control such markets, thus forcing them into Third World nations. Fortunately, strong cryptography allows market needs to be met without interference by governments. (Those who are repelled by such markets are of course free not to patronize them.)

Whistleblowing is another growing use of anonymous remailers, with

those fearing retaliation using remailers to publicly post their incriminating information. The Usenet newsgroups “alt.whistleblowing” and “alt.anonymous.messages” are places where anonymously remailed messages blowing the whistle have appeared. Of course, there’s a fine line between whistleblowing, revenge, and espionage. The same is true for “leaks” from highly placed sources. “Digital Deep Throats” will multiply, and anyone in Washington, or Paris, or wherever, can make his case safely and anonymously by digitally leaking material to the press. William Gibson foresaw a similar situation in his novel *Count Zero* (1987), in which employees of high-tech corporations agree to be ensconced in remote labs, disconnected from the Nets and other leakage paths. We may see a time when those with security clearances are explicitly forbidden from using the Net except through firewalled machines, with monitoring programs running.

Information selling by employees may even take whimsical forms, such as the selling of topless images of women who flashed for the video cameras on “Splash Mountain” at Disneyland (now called “Flash Mountain” by some). Employees of the ride swiped copies of the digital images and uploaded them anonymously to various Web sites. Such thievery and exposure has also been committed with the medical records of famous persons. DMV records have also been stolen by state employees with access, and sold to information brokers, private investigators, and even curious fans. The DMV records of notoriously reclusive author Thomas Pynchon showed up on the Net. It’s been rumored that information brokers are prepared to pay handsomely for a CD-ROM containing the U.S. government’s “key escrow” database.

The larger issue is that mere laws are not adequate to deal with such sales of personal, corporate, or other private information. The bottom line is this: if one wants something kept secret, it must be kept secret. In a free society, few personal secrets are compelled. Unfortunately, we have for too long been in a situation where governments insist that people give out their true names, their various government identification numbers, their medical situations, and so on. “And who shall guard the guardians?” The technology of privacy protection can change this balance of power. Cryptography provides for “personal empowerment,” to use the current phrasing.

## Holding Up the Walls of Cyberspace

In the virtual worlds described in the science fiction of Vinge, Gibson, Stephenson, and others, what holds up the "walls"? What keeps these worlds from collapsing, from crumbling to cyberdust as users poke around, as hackers try to penetrate systems? The virtual gates and doors and stone walls described in *True Names* are persistent, robust data structures, not flimsy constructs ready to collapse.

Certainly the robustness does not come from the hand-waving "consensual hallucination" referred to by some cyberspace pioneers such as Gibson (though he got it mostly right with his "ice"). Psychology and mental states will of course be important in virtual worlds, as is already so obviously the case on the Net and the Web, but true solidity and structure will come from more basic protocols.

Security and cryptography provide the ontological support for these cyberspatial worlds, for enduring structures that permit "colonization" of these spaces and structures. More precisely, the "owners" of a chunk of cyberspace—e.g., someone maintaining a virtual world on their owned machines and networks—establish the structure, persistence, access policies, and other rules. "My house, my rules." Those who disagree with the rules will be welcome to stay away. And those who disagree with the rules but want governments to change the rules will face an uphill battle. Owners can always re-site their machines in more favorable jurisdictions or choose to operate behind a veil of anonymity. The owners of cyberspaces will use cryptography and security measures to ensure against tampering by others.

Cryptography is not just about building the kinds of virtual realities described in *True Names.* The security of ordinary networks depends on cryptography. And yet the deployment of strong cryptography is being hobbled by the various laws and regulations limiting the use of cryptography, including export laws that affect domestic encryption products in several ways, especially because they decree that liability exists if a "foreign person" is "exposed" to an export-controlled product, even if he buys it in a U.S. store or sees it in a U.S. university lab! The U.S. is even limiting export and placement on public sites of virus protection and general security software, strongly suggesting they want the ability to knock out foreign sites and don't

want Americans to protect foreign sites. Is the U.S. planning for information warfare?

Proposals for mandatory “key escrow,” where the government gets access to a kind of spare key left with it, will weaken confidence in digital commerce, and could provide the “keys to the kingdom” to a spy or hostile power able to gain access to the master database. Unfortunately, the government’s plans to put “Big Brother Inside” the networks and to restrict access to proper security measures means these hostile agents will face an easier job. When considering the “bad” implications of strong cryptography, keep this in mind.

Some years back, the National Security Agency was explicitly divided into two functions, one function doing signals and communications intelligence (SIGINT and COMINT), and the other doing communications security and information security (COMSEC and INFOSEC), i.e., working on mechanisms to better secure the nation’s communications. At about this time, circa 1988, the NSA’s COMSEC folks were *explicitly* warning that DES, the Data Encryption Standard, was long overdue for replacement and that new measures were urgently needed to secure the nation’s communications and financial infrastructure. Yet, a decade later, with warnings of an impending “digital Pearl Harbor,” the NSA and FBI are doing everything they can to limit access to strong cryptography and are throwing up roadblocks to hinder the deployment of strong and secure systems.

It looks like the user community will have to ignore their demands and secure things themselves. John Gilmore’s SWAN program seeks to make links between machines on the Net routinely encrypted.

## Virtual Communities

Virtual communities, mentioned earlier, are networks of individuals or groups which are not necessarily closely connected geographically. The word “virtual” is meant to imply a nonphysical linking, but should not be taken to mean that these are any less community-like than are conventional physical communities.

The “Coven” in *True Names* is such a virtual community. Other examples include churches, service organizations, clubs, criminal gangs, cartels, fan

groups, etc. The Catholic Church and the Boy Scouts are both examples of well-established virtual communities that span the globe, transcend national borders, and create a sense of allegiance, of belonging—a sense of "community." Likewise, the Mafia, with its enforcement mechanisms, its own extralegal rules, etc., is a virtual community. There are many other examples: Masons, Triads, Red Cross, Interpol, religions, drug cartels, terrorist groups, political movements, to name a few. In an academic setting, "invisible colleges" are the communities of researchers. Linked by computer networks, these virtual communities are often of greater importance to members than are their physical communities, or even their universities.

There are undoubtedly many more such virtual communities than there are nation-states, and the ties that bind them are for the most part much stronger than are chauvinistic nationalist impulses. Each community will have its own rules, its own access policies, initiation rituals, censure policies, and so forth. Governments have had little power to penetrate such private groups, and even less penetration is likely when strong cryptography provides a new topology for connectivity. Essential to these communities is their essentially *voluntary* nature: it is difficult to coerce membership or interaction, though there are some obvious examples of such coercion. Self-selection and self-enforcement of rules are important aspects. Virtual communities may be attacked by those who disagree with their policies, or have some bone to pick; the Cypherpunks list has been attacked by spam attacks, subscribing the list to other high-volume lists, creating mail loops, posting of incredibly long rants on unrelated topics, and so forth. It is to be expected that hardening techniques will evolve to better protect such virtual communities. For the time being, kill files and twit filters are the best protection. Some on the Cypherpunks list choose to contract with others to filter for them, e.g., by creating "best of" compilations. This is the free market in action.

The corporation is a prime example of a virtual community, having scattered sites, private communication channels (generally inaccessible to the outside world, including governmental authorities), its own security forces and punishment systems (within limits), and its own goals and methods. In fact, many "cyberpunk" (not cypherpunk) fiction authors make a mistake in assuming the future world will be dominated by transnational megacorporate

“states.” Corporations are just one of many examples of such virtual communities that will be effectively on a par with nation-states.

These virtual communities are typically “opaque” to outsiders. Attempts to gain access to the internals of these communities are rarely successful. Law-enforcement and intelligence agencies may infiltrate such groups and use electronic surveillance (ELINT) to monitor these virtual communities. Not surprisingly, these communities are early adopters of encryption technology, ranging from scrambled cell phones to full-blown PGP encryption. Strong cryptography is already being used by various revolutionary and antigovernment movements, including rebels in Burma and Mexico. Usage is mounting daily; strong crypto makes for an ideal “revolutionary cell” system.

In addition to their own rules and access procedures, virtual communities typically have their own moral codes and ethical standards. Revolutionary or so-called terrorist groups are just one example; unbreakable cryptographic communications mean that the potential for coordinated activity by groups having their own moral standards is greatly increased.

A “politically incorrect” usage of these virtual communities is to use “race bits” to bar membership by certain races in such communities. This can even be done without violating the protection of a nym, using the idea of a “credential without identity.” For example, the Aryan Cybernation could demand that a credential be displayed showing one to be a Caucasian. Ironically, an equivalent example, but one which is deemed politically correct by many, is the example of “women-only” forums on the Net. In this case, a woman could gain access to a women-only forum by demonstrating possession of a credential with the appropriate gender bit set. (At the simplest level, this can be done by having other women “vouch” for a candidate, digitally signing a statement the candidate presents.) A more robust system, with less opportunity for false use or false transfer, would be to implement Chaum’s credentials-without-identity scheme. But the point is to show how virtual communities can establish their own access rules and their own enforcement mechanisms.

In this example, if the nexus of the virtual community is not known to be in a specific jurisdiction, but is “virtual,” enforcement of national laws is

problematic. Nations can ban membership in such unapproved groups, of course, but then members will access them through remailers, etc. (Which would inevitably lead to the next step: banning remailed messages, banning encrypted messages, registering personal computers and software, etc.)

The use of encryption by "evil" groups, such as child pornographers, terrorists, money launderers, and racists, is cited by those who wish to limit civilian access to crypto tools. I call these the "Four Horseman of the Infocalypse," as they are so often cited as the reason why ordinary citizen-units of a nation-state are not to have access to crypto. Newspaper headlines scream "Child Pornography Ring Using Secret Codes to Communicate," and the U.S. Department of Justice and the FBI send spokesmen out to speak at public conferences on the dangers of encryption.

This is clearly a dangerous argument to make, for various good reasons. The basic right of free speech is the right to speak in a language one's neighbors or governing leaders may not find comprehensible: encrypted speech.

Many of us believe we are already seeing the imminent end of nation-states, with virtual communities attaining greater importance for many people. Certainly many of us are "closer" to our neighbors in cyberspace—those with whom we share certain interests—than we are to our physical neighbors. And the passions of these special interest groups (think of Aryan Nation, Greenpeace, Sendero Luminoso, Scientologists, etc.) are often vastly more intense than normal nationalistic sentiments. (This was the rap against the Catholic Church: that Catholics were often more loyal to the Pope and the Vatican than to their various provinces and kingdoms. Whether true or not, it has clearly been a concern for many centuries.)

In such "discretionary" communities, the time-honored enforcement mechanism of "shunning" is gaining new popularity. Using kill files or twit filters, nobody in these communities has to read the messages of those they dislike. They can just filter them out.

## Reputations Matter

What will keep people from reneging on digital deals? What will keep them honest? If the government and the courts cannot track a person down,

because they used untraceable or anonymous systems, how will digital societies and economies work?

Well, for starters, the systems are not really purely “anonymous.” The ability to use digital signatures and persistent digital pseudonyms, or “true nyms,” means that behaviors can and will be attributed to nyms. Some nyms will establish the reputation of being straight in dealings, others will establish a less savory reputation.

How does an escrow service (the classical definition of escrow, not the newspeak definition used by the U.S. government for key escrow) survive and prosper? By being in the business of releasing funds when conditions are met, and not otherwise. By not absconding with the funds. In the real world escrow services do quite well because the continuing future revenue stream from their good reputation exceeds what they could get by “burning” any particular customer. Sometimes this involves putting up a bond, which is a kind of secondary escrow.

Digital escrow services will operate along similar lines, with reputation playing the major role. Also, escrow services can be “pinged” (tested) by lots of small transactions. Inasmuch as digital money is untraceable, lots of small interactions can be used to test the trustworthiness of any bank or escrow service. Brand names, image, and product ratings will be as important in cyberspace as they are today, perhaps more so.

## Private Law

As noted, virtual communities have their own rules, with usually little involvement of the outside world in the internal operations of the community. In some important examples, the virtual community is explicitly outside the law, as with the Mafia, Triads, and other such “outlaw” or “underworld” organizations—the very names suggest the status vis-à-vis the conventional legal system. For those who think of these groups as essentially criminal and coercive, à la truck hijackings and protection rackets, think also of the market services provided by the Mafia because government has decided to outlaw certain services: gambling, prostitution, high-risk loans, and “recreational” drugs. Since a bookie cannot use the court system to collect on bad debts, he has to use “private justice” systems, e.g., breaking legs. Other virtual

communities have equally well developed private legal systems. The killing of informants is one obvious example. (Note that I am not condoning the killing of informants, cheats, whatever. I'm merely noting such examples in the context of this discussion.)

But more than just "voluntary" interactions are involved: the role of contracts becomes central. And contracts can be enforced in cyberspace. Bonding entities or escrow agents can hold digital money until some service is satisfactorily completed.

Most interactions in the real world depend more on these reputational effects than on actual enforcement of laws by governments. A "reputable" mail order company, for example, ships products because that's a more important longterm business for it to be in than ripping off a few customers would be. Just about any bank could, quite easily, forge simplistic withdrawal signatures and claim that a customer had withdrawn his money. That they don't do such things has a lot more to do with what banks perceive their business to be than with any technological or legal limitations.

In other words, reputations matter. And in cyberspace, they matter even more than in the outside world, where some people have shown irksome tendencies to declare bankruptcy to escape the obligation of repaying a debt, and then seek the protection of the American legal system, and where honesty, it sometimes seems, is presumed to be something for suckers. Under crypto anarchy, a nym's reputation is all he has, and honesty once again becomes a valuable trait.

What form legal structures may take in cyberspace is unclear. But the role of traditional legal structures is likely to diminish, unless governments around the world are successful in stamping out strong cryptography use. This lesser role for the formal legal system is especially likely as the Net becomes increasingly global, with even more tools for anonymous or pseudonymous interaction. Tools to make digital signatures and digital time-stamping more common will help to build what Nick Szabo calls "smart contracts." Escrow services—even anonymous or pseudonymous ones—will make it possible to have "completion bonds" for cyberspace activities.

Individuals interacting in cyberspace will generally have to be more competent about arranging their fiduciary and contractual relationships, and

less reliant on having government offices and agents bail them out of foolish actions. Caveat emptor. Of course, they are always free to contract to have a "nanny" screen their interactions and tell them what to do. They could even call this their "government." They just can't force others to obey their nanny.

## Crypto Anarchy

"The Net is an anarchy." This truism is the core of crypto anarchy. No central control, no ruler, no leader (except by example, reputation), no "laws." No single nation controls the Net, no administrative body sets policy. The Ayatollah in Iran is as powerless to stop a newsgroup—alt.wanted.moslem.women or alt.wanted.moslem.gay come to mind—he doesn't like as the President of France is as powerless to stop, say, abuse of the French in soc.culture.french. Likewise, the CIA can't stop newsgroups, or sites, or Web pages, that give away their secrets. At least not in terms of the Net itself. What non-Net steps might be taken is left as an exercise for the paranoid and the cautious.

This essential anarchy is much more common than many think. Anarchy—the absence of a ruler telling one what to do—is common in many walks of life: choice of books to read, movies to see, friends to socialize with, etc. Anarchy does not mean complete freedom—one can, after all, only read the books that someone has written and had published—but it does mean freedom from external coercion. And anarchy does not mean an absence of local hierarchies, or an absence of rules. Groups outside the direct control of local governmental authorities may still have leaders, rulers, club presidents, or elected bodies. Many will not, though.

Anarchy as a concept, though, has been tainted by other associations. The anarchy here is not the anarchy of popular conception—lawlessness, disorder, chaos. Nor is it the bomb-throwing anarchy of the nineteenth-century "black" anarchists, usually associated with Russia and labor movements. Nor is it the black flag anarcho-syndicalism of leftist writers such as Proudhon and Goldstein. Rather, the anarchy being spoken of here is the anarchy of "absence of government" (literally, "an arch," without a chief or head). It's the same anarchy of "anarcho-capitalism," the libertarian free market ideology that promotes voluntary, uncoerced economic transactions. "Crypto

anarchy" is a pun on crypto, meaning "hidden," on the use of "crypto" in combination with political views (as in Gore Vidal's famous charge to William F. Buckley: "You crypto fascist!"), and of course because the technology of crypto makes this form of anarchy possible. The first presentation of this was in my 1988 "Crypto Anarchist Manifesto," whimsically patterned after another famous manifesto.

Politically, virtual communities outside the scope of local governmental control may present problems of law enforcement and tax collection. Avoidance of coerced transactions can mean avoidance of taxes, of laws that dictate to whom one can sell and to whom one can't, and so forth. It is likely that many will be unhappy that some are using cryptography to avoid laws designed to control behavior.

National borders are becoming ever more transparent to data. A flood of bits crosses the borders of most developed countries: phone lines, cables, fibers, satellites, and millions of diskettes, tapes, CDs, etc. A single CD or DAT can contain hundreds of megabytes of data—just the least significant bits (LSBs) of a musical recording can be replaced by a hundred megabytes of data without any means of distinguishing the data from ordinary audio noise. Stopping data at the borders is hopeless, with every tourist able to carry in and out vast amounts of data, undetectably.

## Regulatory Arbitrage

The movement of cyberspace operations from nation to nation will rival or exceed the movement of economic production from nation to nation. Just as tax and financial policies of one nation can trigger movements of factories and offices to more favorable climes, so too can data and privacy policies trigger movements of cyberspace-oriented operations to more favorable locales. And this movement can happen as fast as typing a few keystrokes to whisk the site and its files to a new host system.

The issues of international enforcement of various laws and of regularizing laws across national borders have always been problematic; the ability of anyone from the privacy of their home or business to connect with sites nearly anywhere in the world catapults this issue to the forefront. The first international conference on "financial cryptography" was held in 1997 in

Anguilla, a Caribbean tax haven.

The ability to move data around the world at will, to communicate with remote sites at will, means that what has been dubbed "regulatory arbitrage" can be used to avoid legal limits in any given country. For example, when remailing into the U.S. from a site in the Netherlands, whose laws apply? (If one thinks that U.S. laws should apply to sites in the Netherlands, does Iraqi law apply in the U.S.?)

This regulatory arbitrage is also useful for avoiding the welter of laws and regulations that operations in one country may face, including the "deep pockets" lawsuits so many in the U.S. face. Moving operations on the Net outside a litigious jurisdiction is one way to reduce this business liability. Law professor Michael Froomkin has written extensively about regulatory arbitrage and the implications of strong cryptography; his Web site has several interesting articles.

The implications for taxation policy are especially interesting. Incomes will tend to be less visible, as is already the case with international consultants. Imputing incomes and assets already requires intrusive probes into bank accounts, restrictions on funds transfers, and a loss of anonymity and privacy in financial transactions. An alternative—assuming taxes survive, which they probably will—is to tax real, physical assets, such as real property. Or to establish sales taxes and value-added taxes (VATs). Or, of course, to drastically reduce the size of governments and have people make their own arrangements for purchase of any services they may need, save perhaps for only the few services that only a larger group can purchase. David Friedman has discussed such matters in *The Machinery of Freedom.*

It seems unlikely that any sort of "new world order" will be universally adopted. Thus, governments face the prospect of either limiting communication with sites in "rogue jurisdictions," or accepting that this skirting of their laws will happen. Unfortunately, the U.S. has been showing disturbing signs of pushing for just such an international agreement, on crypto and Net access policy, despite the inevitable failure it faces, and the odd moral position of having the U.S. enforcing, say, Islamic nations' laws against mentioning certain topics. It is doubtful the Supreme Court would uphold any such attempts to limit speech in this way.

The whole issue has resonances with age and decency restrictions on material. The Net has made it easy for users of all ages to access any material they wish. This has resulted in calls for limits on material "harmful to minors," à la the U.S. Communications Decency Act. But, of course, connecting to a foreign site would bypass even the CDA, exactly as Muslims, say, can connect to U.S. or European sites where discussions of pork, homosexuality, and other "banned" (to Muslims) topics are freely available.

## The Morality of Crypto Anarchy

The political and moral implications of crypto anarchy as a form of government (or nongovernment) would itself require a long essay. Suffice it to say that many of us think giving power back to people to make their own choices in life without government interference would be a good thing. And regardless of whether it's a good thing or not, it doesn't appear that this trend toward crypto anarchy can be stopped.

Crypto anarchy ensures that men with guns cannot be brought in to interfere with mutually agreed-upon transactions, the only kind of economic 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.

Another positive effect is to put an end to the modern form of guilds: the professional cartels that limit entry into some professions and confer special rights on certain groups. For example, the various medical and legal societies, which have various legal rights not given to, say, the local stamp-collecting club members. It may be argued that these special provisions are for the protection of patients and clients. But in a free society, persons are free to make arrangements to check the credentials of service providers as they see fit, not as some committee has decreed. This applies to all forms of professional licensing. Caveat emptor!

The printing press was a technology that destroyed the medieval guilds, as the once-protected knowledge of the guilds could be distributed to a wider audience. Eventually the kings and queens stopped throwing people into prison for the crime of making leather without a royal license, and the guilds collapsed, no doubt bemoaning the "anarchy" that had been unleashed upon the world.

To put it bluntly, crypto anarchy basically undermines democracy: it removes behaviors and transactions from the purview of the mob. And once crypto is deeply entwined into the fabric of life and commerce, it will be too late to pull the plug.

## The Social Consequences of Crypto Anarchy

Can "bad things" happen with strong cryptography? Of course. I've cited several examples of things that are in some sense dangerous or bad to at least some people. But of course all technologies have both light and dark aspects. … The forty thousand Americans killed every year in traffic accidents, for example, are certainly a dark aspect of an otherwise helpful technology.

Not all aspects of untraceability are positive. People often want accountability, they want a "true name" attached to their interactions, a name and address they can go after if a transaction is unsatisfactory. They don't want to send money to a "nym" who may vanish. Fortunately, there are lots of ways of dealing with such issues. Reputations can be associated with nyms, as with writers who have used pseudonyms successfully. Digital signatures strengthen the process, making forgeries all but impossible. And expect to see "reputation rating" services and even "bonding" services, analogous to title companies, escrow services, and *Good Housekeeping* sorts of seals of approval (with digital signatures, of course).

What will happen to tax policies? How will ordinary taxpayers react to reports that digital-money transactions are escaping taxation, that some elite of crypto-savvy entrepreneurs are evading and avoiding taxes by moving transactions to places the government cannot monitor? There may be a backlash against such uses, but there may also be an increase in the numbers of folks using such methods. (This repeats a pattern seen with offshore investments: where once such approaches were exclusively the domain of the

super-rich, now even moderately wealthy individuals can use offshore investments as part of estate planning, avoidance of “deep pockets” lawsuit claims, and even for tax avoidance.)

Of great concern are the effects of anonymity and untraceability on certain types of crimes. Abhorrent markets may arise. For example, anonymous systems and untraceable digital cash have some obvious implications for the arranging of contract killings, extortion, and kidnapping. The greatest risk in arranging for such services is that physical meetings expose the buyers and/or sellers of such services to the scrutiny of law enforcement and to the setup of sting operations. Asking around at a bar if anyone knows who can do some “discreet work” is an invitation for the FBI to get involved (and I’m certainly not arguing against such FBI or law-enforcement involvement). Crypto anarchy lessens, or even eliminates, this risk, by allowing for untraceable communication to be set up. And untraceable payment. Think back to the BlackNet example, where two-way anonymous contact occurs. The risks to the actual killers are not lessened, as their physical act is not untraceable, but this is a risk the buyers need not worry about (and I surmise that the greater risks lie in the set up and payment steps). Think of anonymous escrow services that hold the digital money until the deed is done.

The implications for corporate and national espionage have already been touched upon. Combined with data havens and liquid markets in information, secrets may become much harder to keep. Imagine a *Digital Jane’s,* after the military weapons handbooks, anonymously compiled and sold for digital money, beyond the reach of various governments that don’t want their secrets revealed. Similarly, whether one views it as espionage or as journalistic whistleblowing, the publication of various secrets will be much easier. Anyone in an organization with an ax to grind only has to connect to a service like BlackNet.

On the issue of terrorists, child molesters, and other Horsemen using PGP, PGPhone, and other crypto tools, how else could it be? After all, the use of PGP is being promoted widely for the protection of privacy. The child molesters, Mafiosos, money launderers, Palestinian sympathizers, nuclear material smugglers, and other assorted miscreants (or heroes, depending on one’s outlook) are surely thinking about securing their communications. And

certain types of terrorism are becoming more possible every day, already, as communications technologies make far-flung organizations possible.

So what? After all, criminals and conspirators also have locks on their doors, use curtains on their windows, keep their voices down when speaking among themselves in public, rent hotel rooms to plot crimes, and generally use various methods to better insure privacy and secrecy. And yet the Constitution is pretty clear that we don't insist windows be uncurtained, conversations be recorded, and locks have keys "escrowed." We cannot know, in advance of an arrest and a trial, who are the criminals and who are the law-abiding citizens, which is why talk of abandoning privacy protections to "catch criminals" is so fatuous.

Nevertheless, the inevitable use of strong crypto by some criminals, perhaps even involving some particularly heinous crimes, will surely be used as an argument to restrict crypto. As some wag put it, "National security is the root passphrase to the Constitution."

Crypto anarchy has some messy aspects, of this there can be little doubt. All technological and economic revolutions have produced dislocations and rearrangements. Crypto anarchy is no different. From relatively unimportant things like price-fixing and insider trading; to more serious things like economic espionage, the undermining of corporate knowledge ownership; to extremely dark things like anonymous markets for killings. But let's not forget that nation-states have killed more than one hundred million people in this century alone: Mao, Stalin, Hitler, and Pol Pot, just to name the most extreme examples. It is hard to imagine any level of digital contract killings ever coming close to nation-state barbarism. (But this is something we cannot accurately speak about; I don't think we have much of a choice in embracing crypto anarchy or not, so I choose to focus on the bright side.)

It is hard to argue that the risks of anonymous markets and tax evasion are justification for worldwide suppression of communications and encryption tools. People have always killed each other, and governments have not stopped this (arguably, they make the problem much worse, as the wars of this century have shown). Also, there are various steps that can be taken to lessen the risks of crypto anarchy impinging on personal safety. The importance of blood relations will likely become more important, as has long

been the case in Asian and Middle Eastern economies. The hiring of private protection agencies will also help.

## Big Brother Inside?

Governments are afraid of strong, unbreakable crypto in the hands of their subjects. Governments see their powers eroded by these technologies, and are taking various steps to try to limit the use of strong crypto. The U.S. has several well-publicized efforts, including the Clipper chip, the Digital Telephony wiretap law, and proposals for "voluntary" escrow of cryptographic keys. Carl Ellison has dubbed these schemes "GAK," for "Government Access to Keys." These voluntary programs are not likely to remain so.

Cypherpunks and others expect these efforts to ultimately be bypassed. Technology has let the genie out of the bottle. Crypto anarchy is liberating individuals from coercion by their physical neighbors—who cannot know who they are on the Net or what they are doing—and from governments. For libertarians, strong crypto provides the means by which government will be avoided.

Digital cash and digital banks are likely targets for legislative moves to limit the deployment of crypto anarchy and digital economies. Whether through banking regulation or tax laws, it is not likely that digital money will be deployed easily. But as noted in the discussion on extortion, many of the more interesting results of crypto anarchy can occur if even *some* issuers of untraceable digital money exist, anywhere.

The proposals to restrict access to strong cryptography bear a definite resemblance to the "War on Drugs." As Whit Diffie, one of the inventors of public-key cryptography, has noted, the War on Drugs effectively pressed corporations into service as drug warriors. Under threat of forfeiture of corporate assets (trucks, boats, warehouses) if drugs were found in them, and loss of government business, corporations adopted random searches of employee lockers, and urine sampling, and placed "Just Say No" posters in cafeterias and work areas. Hence the reliance in the "War on Crypto" on systems to force corporations to adopt "key recovery" systems. (After all, corporations might be colluding, or price-fixing, or conspiring to violate the

various laws they are subject to … hence the government wants access to such secret communications.) Such pressure on corporations will have effects on ordinary citizen-units. There are now requirements in some jurisdictions that all candidates for public office be tested for drug use; if such policies are upheld by the Supreme Court, expect drug tests in other state-licensed matters, such as driver's licenses and work permits. Clearly the state has gone far beyond any conception the framers of the Constitution may have had.

The unhealthily close relationship between large corporations and governments often causes various deals and quid pro quos to be made. Various corporations seek to be the vendor of choice for government-approved, key-escrowed cryptography. Various "initiatives" and "alliances" are the avenue for this deal-making. Economists call this "rent-seeking." The medieval guilds were an example of the same phenomenon.

Government spokesvermin often talk about "legitimate needs for key recovery," as when a person wants a spare key stored with his lawyer, or in a safe deposit box, or when companies want critical information encrypted in such a way that the material is not lost forever if the encryptor loses his key, forgets his passphrase, dies, leaves the company, etc. The government claims this as support for its "key recovery" initiatives, its programs to force users to allow access to keys. But this argument is misleading and has major flaws.

First, if there is a compelling need, the private enterprise system will surely meet it—the "help" of the government is not needed, nor are the proposed restrictions imposed on by business. Second, there is a huge difference between the storage of files and their transmission. When Alice uses encryption to store her files she uses a different key than what she uses for transmitting files to Bob (probably Bob's public key, in fact). There is thus no pressing business need for recovery of *transmission* keys. Both parties have the material in their local storage, presumably. And yet the government's key recovery proposals specifically focus on encryption methods for *message transmission.* Guess who the main party interested in reading intercepted transmissions is? Finally, the restrictions on *export* of cryptography systems, requiring key escrow, obviously have nothing whatsoever to do with meeting the "needs" of businesses. It will be interesting to see how foreign governments react to having escrowed systems in which

the U.S. has special access to communications of their corporations and citizens. My guess is that they'll react about the same way the U.S. would react if Iraq were exporting special "Saddam-readable" crypto software to the U.S.

Any system which allows government to act to trace a transaction, or to trace a message, or to gain access to keys, essentially throws away the liberty-enhancing advantages of cryptography completely. If this is not evident, ask yourself whether the government of Burma, known as SLORC, would not use its "Government Access to Keys" to round up the dissidents communicating with laptops and PGP in the jungle? Would Hitler and Himmler have used "key recovery" to determine who the Jews were communicating with so they could all be rounded up and killed? Contact tracing is to be one of the most powerful tools in suppressing groups. Would the East German Staasi have traced e-cash transactions? The answers are obvious. For every government extant on the planet one can easily think of dozens of examples where access to keys, access to diaries, access to spending records, etc., would be exploited by the party in power. What a government considers "criminal" or "suspicious" is often what it considers threatening to its exercise of power. Rhetoric about "catching criminals" misses this point: that governments typically use surveillance powers to control citizens. Fortunately, a crackdown on crypto will not be easy to successfully implement in the U.S. and in Western nations.

Some domestic (U.S.) restrictions on cryptography and digital money seem likely, despite what many think the Constitution says. Think it can't happen? How can government require ID cards and tracking mechanisms for cash purchases? And people are finding that carrying their own cash around in cars and on planes can subject them to "forfeiture" of this cash, with no trial and no mechanism for redress (the Orwellian name for this is along the lines of "illegal use of currency").

The U.S. government continues to push for its notion of "Key Recovery," or key registration, and for limits on the strength of cryptographic systems. A purely voluntary key-recovery system is unobjectionable, as what people do with their own keys is of course their business. The danger, however, is that a widely deployed, ostensibly voluntary system could be made mandatory by

the vote of Congress or a Presidential order. This sort of sword of Damocles is always worrisome, whether the proposed system is gun registration (which can then easily lead to confiscation, as happened in Nazi Germany), implantable ID units, video cameras in public places, "voluntary self-ratings" on writings or speech, or wider use of government-approved ID cards. It has been clear for a long time that the U.S. government's interest in pushing Clipper, Tessera, and the various other GAK proposals was to make escrowed encryption widespread, with non-GAK crypto ultimately to be phased out. This would be no easy thing to accomplish, for many reasons, some discussed here. A firestorm of protest awaits any attempt to ban cryptography. As one wag put it several years ago, "They'll get my crypto keys when they pry my cold, dead fingers off my keyboard."

The widespread use of strong crypto means that "rogue crypto" (terrorists, crypto anarchists, freedom fighters) gets lost in the blizzard of other uses. And shutting down all crypto means shutting down business use of crypto to protect secrets, and probably means an end to digital commerce, a price that is almost certainly too high to pay. This is another reason to delay action on crypto for as long as possible: make encrypted communications so widespread in commerce that to pull the plug would mean a financial calamity.

## Colonizing Cyberspace

How will these ideas affect the development of cyberspace? "You can't eat cyberspace" is a criticism often leveled at arguments about the role of cyberspace in everyday life. The argument is that money and resources accumulated in some future cyberspatial system will not be able to be transferred or laundered into the real world. Even such a prescient thinker as Neal Stephenson, in *Snow Crash*, had his protagonist a vastly wealthy man in "the Multiverse," but a pauper in the physical world. And Vernor Vinge has his protagonist slip up and get caught by the Feds because he was too successful in "both planes."

This inability to move money from one realm to another is implausible for several reasons. First, we routinely see transfers of wealth from the abstract world of stock tips, arcane consulting knowledge, etc., to the real world.

Second, a variety of means of laundering money, via phony invoices, uncollected loans, art objects, etc., are well known to those who launder money.… These methods, and more advanced ones to come, are likely to be used by those who wish their cyberspace profits moved into the real world. Third, many of those who exploit the opportunities provided by crypto anarchy will not choose to live in surveillance states and high-tax-rate jurisdictions. Duncan Frissell refers to "perpetual tourists," much like the old "jet set."

Most Net and Web users already pay little attention to the putative laws of their local regions or nations, apparently seeing themselves more as members of various virtual communities than as members of locally governed entities. This trend is accelerating. Encryption makes it easy and even safe to ignore most local laws about what can be done in cyberspace. Most importantly, information can be bought and sold—anonymously, too—and then used in the real world. There is no reason to expect that this capability won't be a major reason to at least partly move into cyberspace. The World Wide Web is growing at an explosive pace. Combined with cryptographically protected communication and digital cash of some form, this should accelerate the long-awaited colonization of cyberspace.

## But Will It Happen?

Strong crypto provides new levels of personal privacy, all the more important in an era of increased surveillance, monitoring, and the temptation to demand proofs of identity and permission slips. The power of nation-states will be lessened, tax collection policies will have to be changed, and economic interactions will be based more on personal calculations of right and wrong than on societal mandates. This is the true horror to many, that the individual becomes empowered to make his own decisions about what is right and what is wrong and to then act as he wishes, to join the virtual communities he wishes to, to pay for the services he wishes, and to ignore the will of the democratic herd.

If strong cryptography and the related ideas discussed here do produce a kind of "crypto singularity," I don't believe the other side of that singularity is quite as opaque as, say, the AI and nanotechnology sorts of singularities

Vernor Vinge has discussed.

Strong crypto provides a technological means of ensuring the practical freedom to read and write what one wishes to. (Albeit perhaps not in one's true name, as the nation-state-democracy will likely still try to control behavior through majority votes on what can be said, not said, read, not read, etc.) And of course if speech is free, so are many classes of economic interaction that are essentially tied to free speech.

While many may recoil from the ideas discussed here, it is already apparent that others are embracing this world. And that's enough to make things interesting.

## A Phase Change

We are in a "race to the fork in the road." The fork in the road being essentially the point of no return, beyond which things are either pulled strongly to one side or the other, the sides being:

- a surveillance state, with restrictions on cryptography, the spending of money, the holding of various items (besides just traditional things like guns and drugs), restrictions on the dissemination of information, and of course controls on lots of other things; and
- a libertarian or anarcho-capitalist state, with people using a variety of secure and private channels to interact, exchange information, buy and sell goods and services, and communicate transnationally. The "anarchy" being the same kind of anarchy seen in so many areas of life: reading choices, eating choices, forums in cyberspace, and so on.

It is difficult to imagine stable states in between. The forces pulling to one side or the other are quite strong. In the language of chaos theory, there are two "attractors."

Each major terrorist or criminal "incident"—Oklahoma City, TWA flight 800, pedophile rings on the Net, etc.—jumps us forward toward a totalitarian surveillance state. However, each new anonymous remailer, each new Web site, each new T1 link, etc., moves us forward in the direction of crypto anarchy. Which side will win is unclear at this time, though my hunch is that we passed the point of no return some years ago and are now irreversibly on the road to crypto anarchy.

The faster and more ubiquitously we can deploy as much strong crypto as possible—remailers, strong crypto, offshore havens, digital money, encrypted Internet links, information markets—the greater the likelihood we'll win. Once enough strong, encrypted, black channels are available, it will essentially be too late to crack down and stop them. The horse will be out the barn door—arguably this has already happened. Add to the mix steganographic channels, lots of bandwidth over several types of channels, and it's too late to go back; the tipping point will have been passed.

A phase change is coming, a kind of "crypto singularity" (to morph a use coined by Vernor Vinge). Virtual communities are in their ascendancy, displacing conventional notions of nationhood. Voluntary economic and social relationships, with true freedom of association. Virtual communities, connected with black pipes opaque to outsiders, bound by their own rules and their own standards of behavior.

The fundamental battle is already under way between the forces of big government and the forces of liberty and crypto anarchy. Pandora's box has been opened and we might as well make the most of it.

## Acknowledgments

My thanks for the many discussions over the years with the dozens of core contributors to the Cypherpunks list, including both the physical and the virtual discussions. Thanks especially to Eric Hughes, Hal Finney, Lucky Green, Hugh Daniel, Nick Szabo, Robin Hanson, Duncan Frissell, Black Unicorn, Sandy Sandfort, Jim Bell, Bill Stewart, Jim Bennett, Doug Barnes, Keith Henson, Peter Hendrickson, Michael Froomkin, the late Phil Salin, Bob Fleming, Cherie Kushner, Chip Morningstar, Mark Miller, David Friedman, and the many others who critiqued or contributed ideas.