16.21. Cyberspace, private spaces, enforcement of rules, and technology

---

16.21.1. Consider the "law" based approach

- a discussion group that wants no men involved ("a protected space for womyn")
  - so they demand the civil law system enforce their rules
  - practical example: sysadmins yank accounts when "inappropriate posts" are made
  - the C&S case of spamming is an example
- Note: The Net as currently constituted is fraught with confusion about who owns what, about what are public and what are private resources, and about what things are allowed. If Joe Blow sends Suzy Creamcheese an "unwanted" letter, is this "abuse" or "harassement"? Is it stealing Suzy's resources? (In my opinion, of course not, but I agree that things are confusing.)

16.21.2. The technological approach:

- spaces created by crypto...unbreachable walls
- example: a mailing list with controls on membership
  - could require nomination and vouching for by others
- presentation of some credential (signed by someone), e.g. of femaleness
  - pay as you go stops spamming

16.21.3. This is a concrete example of how crypto acts as a kind of building

material

- and why government limitations on crypto hurt those who wish to protect their own spaces
- a private mailing list is a private space, inaccessible to those outside
- "There are good engineering approaches which can force data to behave itself. Many of them involve cryptography. Our government's restrictions on crypto limit our ability to build reliable computer systems. We need strong crypto for basic engineering reasons." [Kent Borg, "Arguing Crypto: The Engineering Approach," 1994-06-29]

16.21.4. Virtual Communities-the Use of Virtual Networks to Avoid Government

- that is, alternatives to creating new countries (like the Minerva project)
- the Assassin cult/sect in the mountains of Syria, Iraq, Afghanistan, etc. had a network of couriers in the mountain fastnessess
- pirate communities, networks of trading posts and watering holes, exempt-if only for a few years-from the laws of the imperial powers

16.21.5. These private spaces will, as technology makes them more "livable" (I don't mean in a full sense, so don't send me notes about how "you can't eat cyberspace"), become full- functioned "spaces" that are outside the reach of governments. A new frontier, untouchable by outside, coercive governments.

- Vinge's "True Names" made real

16.21.6. "Can things really develop in this "cyberspace" that so many of us talk about?"

- "You can't eat cyberspace!' is the usual point made. I argue, however, that abstract worlds have always been with us, in the forms of commerce, reputations, friends, etc. And this will continue.
- Some people have objected to the sometimes over- enthusiastic claims that economies and socities will flourish in computer-mediated cyberspaces. The short form of the objection is: "You can't eat cyberspace." Meaning, that profits and gains made in cyberspace must be converted to real world profits and gains.
- In "Snow Crash," this was made out to be difficult...Hiro Protagonist was vastly wealthy in the Multiverse, but lived in a cargo container at LAX in the "real world." A fine novel, but this idea is screwy.

- There are many ways to transfer wealth into the "real" world:
  - all the various money-laundering schemes

- money in offshore accounts, accessible for vacations, visits, etc. - phony purchase orders
- my favorite: Cyberspace, Inc. hires one as a "consultant" (IRS cannot and does not demand proof of work being done, the nature of the work, one's qualifications to perform the work, etc...In fact, many consultants are hired "on retainer," merely to be available should a need arise.)
  - information-selling
  - investments

16.21.7. Protocols for this are far from complete

- money, identity, walls, structures
- a lot of basic work is needed (though people will pursue it locally, not after the work is done...so solutions will likely be emergent)

16.22. Data Havens

16.22.1. "What are data havens?"

- Places where data can be hidden or protected against legal action.
  - Sterling, "Islands in the Net," 1988
  - Medical experiments, legal advice, pornography, weapons

- reputations, lists of doctors, lawyers, rent deadbeats, credit records, private eyes
  - What to do about the mounting pressure to ban certain kinds of research?
- One of the powerful uses of strong crypto is the creation of journals, web sites, mailing lists, etc., that are "untraceable." These are sometimes called "data havens," though that term, as used by Bruce Sterling in "Islands in the Net" (1988), tends to suggest specific places like the Cayman Islands that corporations might use to store data. I prefer the emphasis on "cypherspace."
- "It is worth noting that private "data havens" of all sorts abound, especially for financial matters, and most are not subject to governmental regulation...Some banks have research departments that are older and morecomprehensive than credit reporting agencies. Favored customers can use them for evaluation of private deals...Large law firms maintain data banks that approach those of banks, and they grow with each case, through additions of private investigators paid for by successive clients...Security professionals, like Wackenhut and Kroll, also market the fruits of substantial data collections...To these add those of insurance, bonding, investment, financial firms and the like which help make or break business deals." [John Young, 1994-09-07]

16.22.2. "Can there be laws about what can be done with data?"

- Normative laws ("they shouldn't keep such records and hence we'll outlaw them") won't work in an era of strong crypto and privacy. In fact, some of us support data havens precisely to have records of, say, terminal diseases so we'll not lend money to Joe-who-has-AIDS. It may not be "fair" to Joe, but it's my money. (Same idea as in using offshore or cryptospatial data havens to bypass the nonsense in the "Fair Credit Reporting Act" that outlaws the keeping of certain kinds of facts about credit applicants, such as that they declared bankruptcy 10 years ago or that they left a string of bad debts in Germany in the 1970s, etc.)

16.22.3. Underground Networks, Bootleg Research, and Information Smuggling

- The Sharing of Forbidden Knowledge

- even if the knowledge is not actually forbidden, many people relish the idea of trafficking in the forbidden + Some modern examples + drugs and marijuana cultivation
- drugs for life extension, AIDS treatments

- illegal drugs for recreational use

- bootleg medical research, AIDS and cancer treatments, etc.

- for example, self-help user groups that advise on treatments, alternatives, etc.

- lockpicking and similar security circumvention techniques

- recall that possession of lockpicks may be illegal
- what about manuals? (note that most catalogs have a disclaimer: "These materials are for educational purposes only, ...")
- defense-related issues: limitations on debate on national security matters may result in "anonymous forums"

- BTW, recent work on crab shells and other hard shells has produced even stronger armor!
  - this might be some of the genetic research that is highly classified and is sold on the anonymous nets + Alchemists and the search for immortality
- theory that the "Grandfather of all cults" (my term) started around 4500 B.C.

- in both Egypt and Babylonia/Sumeria

- ancestor of Gnostics, Sufis, Illuminati, etc.

- The Sufi mystic Gurdjieff claimed he was a member of a mystical cult formed in Babylon about 4500 B.C.
- spider venom?

- Speculation: a group or cult oriented toward life extension, toward the search for immortality-perhaps a link to The Epic of Gilgamesh.
- The Gilgamesh legend

- Gilgamesh, Akkadian language stone tablets in Nineveh
- made a journey to find Utnapishtim, survivor of Babylonian flood and possessor of secret of immortality (a plant that would renew youth)
- but Gilgamesh lost the plant to a serpent

- Egyptians

- obviously the Egyptians had a major interest in life extension and/or immortality

- Osiris, God of Resurrection and Eternal Life

- also the Dark Companion of Serius (believed to be a neutron star?)
- they devoted huge fraction of wealth to pyramids, embalming, etc. (myrhh or frankincense from desert city in modern Oman, discovered with shuttle imaging radar)

- "pyramid power": role on Great Seal, as sign of Illuminati, and of theories about cosmic energy, geometrical shapes, etc.

- and recall work on numerological significance of Great Pyramid dimensions

- Early Christianity

- focus on resurrection of Jesus Christ

- Quest for immortality is a major character motivation or theme
- arguably for all people: via children, achievements, lasting actions, or even "a good life"

- "Living a good life is no substitute for living forever"
- but some seek it explicitly
- "Million alive today will never die." (echoes of past religious cults...Jehovah's Witnesses?)
- banned by the Church (the Inquisition)

- research, such as it was, was kept alive by secret orders that communicated secretly and in code and that were very selective about membership

- classes of membership to protect against discovery (the modern spy cell system)
- red herrings designed to divert attention away

- all of this fits the structure of such groups as the Masons, Freemason, Illuminati, Rosicrucians, and other mystical groups

- with members like John Dee, court astrologer to Queen Elizabeth

- a genius writer-scientist like Goethe was probably a member of this group

- Faust was his message of the struggle
- with the Age of Rationalism, the mystical, mumbo-jumbo aspects of alchemical research were seen to be passZ, and groups like Crowleys O.T.O. became purely mystical showmanship

- but the need for secrecy was now in the financial arena, with vast resources, corporate R & D labs, and banks needed

- hence the role of the Morgans, Rothschilds, etc. in these conspiracies

- and modern computer networks will provide the next step, the next system of research

- funded anonymously
- anonymous systems mean that researchers can publish results in controversial areas (recall that cryobiologists dare not mention cryonics, lest they be expelled from American Cryobiology xxx)
    - Bootleg Medical Research (and Cryonics)

    - Cryonics Research and Anti-aging Treatments
        - Use of Nazi Data
- hypothermia experiments at Dachau + Anti-aging drugs and treatments
- fountain of youth, etc.
- many FDA restrictions, of course
- Mexico

- Switzerland

- foetal calf cells?
- blood changing or recycling? + Illegal Experiments
- reports that hyperbaric oxygen may help revival of patients from neat-death in freezing accidents
    - Black Markets in Drugs, Medical Treatments
        - RU-486, bans on it
- anti-abortion foes
- easy to synthesize
- NOW has indicated plans to distribute this drug themselves, to create networks (thus creating de facto allies of the libertarian-oriented users) + Organ Banks

- establishing a profit motive for organ donors

- may be the only way to generate enough donations, even from the dead
- some plans are being made for such motives, especially to motivate the families of dying patients
- ethical issues

- what about harvesting from the still-living?

- libertarians would say: OK, if informed consent was given
- the rich can go to overseas clinics

- AIDS patients uniting via bulletin boards to share treatment ideas, self-help, etc.

- with buying trips to Mexico and elsewhere
- authorities will try to halt such BBSs (on what grounds, if no money is changing hands?)

- Doctors may participate in underground research networks to protect their own reputations and professional status

- to evade AMA or other professional organizations and their restrictive codes of ethics + or lawsuits and bad publicity
- some groups, the "Guardian Angels" of the future, seek to expose those who they think are committing crimes: abortionists (even though legal), etc.
- "politically incorrect" research, such as vitamin therapy, longevity research, cryonics
- breast implant surgery may be forced into black markets (and perhaps doctors who later discover evidence of such operations may be forced to report such operations)

    - Back Issues of Tests and Libraries of Term Papers
    - already extant, but imagine with an AMIX-like frontend? + Different kinds of networks will emerge, not all of them equally accessible

- the equivalent of the arms and drug networks-one does not gain entree merely by asking around a bit - credibility, reputation, "making your bones" - these networks are not open to the casual person
- Some Networks May Be For the Support of Overseas Researchers
    - who face restrictions on their research

- e.g., countries that ban birth control may forbid researchers from communication with other researchers

- suppose U.S. researchers are threatened with sanctions-loss of their licenses, censure, even prosecution-if they participate in RU-486 experiments?

- recall the AIDS drug bootleg trials in SF, c. 1990
    - or to bypass export restrictions
- scenario: several anonymous bulletin boards are set up-and then closed down by the authorities-to facillitate anonymous hookups (much like "anonymous FTP")

- Groups faced with debilitating lawsuits will "go underground"

- Act Up! and Earth First! have no identifiable central office that can be sued, shut down, etc.
    - and Operation Rescue has done the same thing

16.22.4. Illegal Data

- credit histories that violate some current law about records
    - bootleg medical research
    - stolen data (e.g., from competitors...a GDS system could allow remote queries of a database, almost "oracular," without the stolen data being in a U.S. jurisdiction)
- customers in the U.K or Sweden that are forbidden to compile data bases on individuals may choose to store the data offshore and then access it discreetly (another reason encryption and ZKIPS must be offered)

16.22.5. "the Switzerland of data"

- Brussells supposedly raises fewer eyebrows than Lichtenstein, Luxembourg, Switzerland, etc.
    - Cayman Islands, other small nations see possibilities

16.22.6. Information markets may have to move offshore, due to licensing and other restrictions

- just as stock brokers and insurance brokers are licensed, the government may insist that information resellers be licensed (pass exams, be subject to audits and regulations)

16.23. Undermining Governments--Collapse of the State

16.23.1. "Is it legal to advocate the overthrow of governments or the breaking of laws?"

- Although many Cypherpunks are not radicals, many others of us are, and we often advocate "collapse of governments" and other such things as money laundering schemes, tax evasion, new methods for espionage, information markets, data havens, etc. This rasises obvious concerns about legality.
- First off, I have to speak mainly of U.S. issues...the laws of Russia or Japan or whatever may be completely different. Sorry for the U.S.-centric focus of this FAQ, but that's the way it is. The Net started here, and still is dominantly here, and the laws of the U.S. are being propagated around the world as part of the New World Order and the collapse of the other superpower.
- Is it legal to advocate the replacement of a government? In the U.S., it's the basic political process (though cynics might argue that both parties represent the same governing philosophy). Advocating the *violent overthrow* of the U.S. government is apparently illegal, though I lack a cite on this.

- Is it legal to advocate illegal acts in general? Certainly much of free speech is precisely this: arguing for drug use, for boycotts, etc.
- The EFF gopher site has this on "Advocating Lawbreaking, Brandenburg v. Ohio. ":

- "In the 1969 case of Brandenburg v. Ohio, the Supreme Court struck down the conviction of a Ku Klux Klan member under a criminal syndicalism law and established a new standard: Speech may not be suppressed or punished unless it is intended to produce 'imminent lawless action' and it is 'likely to produce such action.' Otherwise, the First Amendment protects even speech that advocates violence. The Brandenburg test is the law today. "

16.23.2. Espionage and Subversion of Governments Will be Revolutionized by Strong Crypto

- (I think they see what we see, too, and this is a motivation for the attempts to limit the use of strong crypto. Besides some of the more conventional reasons.)
  - Digital dead drops will revolutionize espionage

- spies and their controllers can communicate securely, relatively quickly, without fear of being watched, their drops compromised, etc.

- no more nooks of trees, no more chalk marks on mailboxes to signal a drop to be made
  - this must be freaking out the intelligence community!
- more insights into why the opposition to crypto is so strong
  - Cell-Based Systems and Conventional Protection Systems
    - Cells are a standard way to limit the damage of exposure
- the standard is the 3-person cell so common in the early days of Soviet espionage in the U.S.
- but computer systems may allow new kinds of cells, with more complicated protocols and more security

- Keeping files for protection is another standard protection method
- and with strong crypto, these files can be kept encrypted and in locations not apparent (e.g., posted on bulletin boards or other such places, with only the key needed at a later time to open them)

- a la the "binary files" idea, wherein encrypted files are widely available for some time before the key is distributed (thus making it very hard for governments to halt the distribution of the raw files)

16.23.3. "Xth Column" (X = encrypted)

- The possible need to use strong cryptography as a tool to fight the state.

- helping to undermine the state by using whistleblowers and anonymous information markets to leak information

- the 63,451 people given false identities in the WitSec program...leak their names, watch them be zapped by vengeful enemies, and watch the government squirm
- auction off the details of the 1967 Inspector General's report on CIA assassinations

16.23.4. use of clandestine, cell-based systems may allow a small group to use "termite" methods to undermine a society, to destroy a state that has become too repressive (sounds like the U.S. to me)

- encrypted systems, anonymous pools, etc., allow truly secure cell-based systems (this is, by the way, one of the concerns many countries have about "allowing" cryptography to be used...and they're right abou the danger!)
- subversion of fascist or socialist governments, undermining the so-called democratic governments

16.23.5. "Why won't government simply ban such encryption methods?" + This has always been the Number One Issue!

- raised by Stiegler, Drexler, Salin, and several others (and in fact raised by some as an objection to my even discussing these issues, namely, that action may then be taken to head off the world I describe)
  - Types of Bans on Encryption and Secrecy
    - Ban on Private Use of Encryption
    - Ban on Store-and-Forward Nodes
    - Ban on Tokens and ZKIPS Authentication
    - Requirement for public disclosure of all transactions

- Recent news (3-6-92, same day as Michaelangelo and Lawnmower Man) that government is proposing a surcharge on telcos and long distance services to pay for new equipment needed to tap phones! - S.266 and related bills

- this was argued in terms of stopping drug dealers and other criminals
- but how does the government intend to deal with the various forms fo end-user encryption or "confusion" (the confusion that will come from compression, packetizing, simple file encryption, etc.)
    - Types of Arguments Against Such Bans
        - The "Constitutional Rights" Arguments
        - The "It's Too Late" Arguments
- PCs are already widely scattered, running dozens of compression and encryption programs...it is far too late to insist on "in the clear" broadcasts, whatever those may be (is program code distinguishable from encrypted messages? No.)
- encrypted faxes, modem scramblers (albeit with some restrictions)
- wireless LANs, packets, radio, IR, compressed text and images, etc...all will defeat any efforts short of police state intervention (which may still happen)
    - The "Feud Within the NSA" Arguments
        - COMSEC vs. PROD
    - Will affect the privacy rights of corporations
- and there is much evidence that corporations are in fact being spied upon, by foreign governments, by the NSA, etc.
    - They Will Try to Ban Such Encryption Techniques
        - Stings (perhaps using viruses and logic bombs)
            - or "barium," to trace the code

- Legal liability for companies that allow employees to use such methods

- perhaps even in their own time, via the assumption that employees who use illegal software methods in their own time are perhaps couriers or agents for their corporations (a tenuous point)

16.23.6. "How will the masses be converted?"

- Probably they won't. Things will just happen, just as the masses were not converted on issues of world financial markets, derivative instruments, and a lot of similar things.
    - Crypto anarchy is largely a personal approach of withdrawal, of avoidance. Mass consensus is not needed (unless the police state option is tried).
- Don't think in terms of selling crypto anarchy to Joe Average. Just use it.

16.23.7. As things seem to be getting worse, vis-a-vis the creation of a police

state in the U.S.--it may be a good thing that anonymous assassination markets will be possible. It may help to level the playing field, as the Feds have had their hit teams for many years (along with their safe houses, forged credentials, accommodation addresses, cut-outs, and other accouterments of the intelligence state).

- (I won't get into conspiracies here, but the following terms may trigger some memories: Gehlen Org, Wackenhut, McKee Team, Danny Casolaro, Cabazon Indians, Gander crash, Iraq arms deals, Pan Am 103, Bridegrooms of Death, French Connection, Fascist Third Position, Phoenix Program, Bebe Rebozo, Marex, Otto Skorzeny, Nixon, P-2, Klaus Barbie, etc.)
- Plenty of evidence of misbehavior on a massive scales by the intelligence agencies, the police forces, and states in general. Absolute power has corrupted absolutely.
- I'm certainly not advocating the killing of Congressrodents and other bureaucrats, just noting that this cloud may have a silver lining.

16.24. Escrow Agents and Reputations

16.24.1. Escrow Agents as a way to deal with contract renegging

- On-line clearing has the possible danger implicit in all trades that Alice will hand over the money, Bob will verify that it has cleared into hisaccount (in older terms, Bob would await word that his Swiss bank account has just been credited), and then Bob will fail to complete his end of the bargain. If the transaction is truly anonymous, over computer lines, then of course Bob just hangs up his modem and the connection is broken. This situation is as old as time, and has always involved protcols in which trust, repeat business, etc., are factors. Or escrow agents.
- Long before the "key escrow" of Clipper, true escrow was planned. Escrow as in escrow agents. Or bonding agents.
- Alice and Bob want to conduct a transaction. Neither trusts the other; indeed, they are unknown to each other. In steps "Esther's Escrow Service." She is *also utraceable*, but has established a digitally-signed presence and a good reputation for fairness. Her business is in being an escrow agent, like a bonding agency, not in "burning" either party. (The math of this is interesting: as long as the profits to be gained from any small set of transactions is less than her "reputation capital," it is in her interest to forego the profits from burning and be honest. It is also possible to arrange that Esther cannot profit from burning either Alice or Bob or both of them, e.g., by suitably encrypting the escrowed stuff.)
    - Alice can put her part of the transaction into escrow with Esther, Bob can do the same, and then Esther can release the items to the parties when conditions are met, when both parties agree, when adjudication of some sort occurs, etc. (There a dozen issues here, of course, about how disputes are settled, about how parties satisfy themselves that Esther has the items she says she has, etc.)

16.24.2. Use of escrow services as a substute for government

- as in underworld deals, international deals, etc.
    - "Machinery of Freedom" (Friedman), "The Enterprise of Law" (Benson)

- "It is important to note in any case that the use of third- party escrow as a substitute for Government regulation was a feature of the Northern European semi-anarchies of Iceland and Ireland that have informed modern libertarian thought." [Duncan Frissell, 1994-08-30]

16.24.3. Several people have raised the issue of someone in an anonymous transaction simply taking the money and not performing the service (or the flip

side). This is where *intermediaries* come into the picture, just as in the real worl (bonds, escrow agents, etc.).

16.24.4. Alice and Bob wish to conduct an anonymous transaction; each is unknown to the other (no physical knowledge, no pseudonym reputation knowledge). These "mutually suspicious agents," in 1960s- and 70s-era computer science lingo, must arrange methods to conduct business while not trusting the other.

16.24.5. Various cryptographic protocols have been developed for such things as "bit commitment" (useful in playing poker over the phone, for example). I don't know of progress made at the granularity of anonymous transactions, though. (Though the cryptographic protocol building blocks

at lower levels--such as bit commitment and blobs--will presumably be used eventually at higher levels, in markets.)

16.24.6. I believe there is evidence we can shorten the cycle by borrowing noncryptographic protocols (heresy to purists!) and adapting them. Reputations, for example. And escrow agents (a form of reputation, in that the "value" of a bonding entity or escrow agent lies in reputation capital).

16.24.7. if a single escrow agent is suspected of being untrustworthy (in a reputation capital sense), then can use *multiple* escrows

- with various protocols, caveat emptor
- n-out-of-m voting schemes, where n escrow agents out of m are required to complete a transaction
- hard to compromise them all, especially if they have no idea whether they are being "legitimately bribed" or merely pinged by a reputation-rating service
- Hunch: the work of Chaum, Bos, and the Pfaltzmanns on DC- nets may be direcly applicable here...issues of collusion, sets of colluders, detection of collusion, etc.

16.25. Predictions vs. Implications

16.25.1. "How do we know that crypto anarchy will 'work,' that the right institutions will emerge, that wrongs will be righted, etc.?"

- We don't know. Few things are certain. Only time will tell. These are emergent situations, where evolution will determine the outcome. As in other areas, the forms of solutions will take time to evolve.
- (The Founders could not have predicted the form corporate law would take, as but one example.)

16.25.2. My thinking on crypto anarchy is not so much *prediction* as examination of trends and the implications of certain things. Just as steel girders mean certain things for the design of buildings, so too does unbreakable crypto mean certain things for the design of social and economic systems.

16.25.3. Several technologies are involved:

- Unbreakable crypto
- Untraceable communication
- Unforgeable signatures

16.25.4. (Note: Yes, it's sometimes dangerous to say "unbreakable," "untraceable," and "unforgeable." Purists eschew such terms. All crypto is economics, even information-theoretically secure crypto (e.g., bribe someone to give you the key, break in and steal it, etc.). And computationally-secure crypto-such as RSA, IDEA, etc.--can in *principle* be brute-forced. In reality, the costs may well be exhorbitantly high...perhaps more energy than is available in the entire universe would be needed. Essentially, these things are about as unbreakable, untraceable, and unforgeable as one can imagine.)

16.25.5. "Strong building materials" implies certain things. Highways, bridges, jet engines, etc. Likewise for strong crypto, though the exact form of the things that get built is still unknown. But pretty clearly some amazing new structures will be built this way.

16.25.6. Cyberspace, walls, bricks and mortar...

16.25.7. "Will strong crypto have the main effect of securing current freedoms, or will it create new freedoms and new situations?"

- There's a camp that believe mainly that strong crypto will ensure that current freedoms are preserved, but that this will not change things materially, Communications can be private, diaries can be secured, computer security will be enhanced, etc.
- Another camp--of which I am a vocal spokesman--believes that qualitatively different types of transactions will be made possible. In addition, of course, to the securing of liberties that the first camp things is the main effect.
    - These effects are specultative, but probably include:
- increased hiding of assets through untraceable banking systems
    - markets in illegal services
    - increased espionage
    - data havens

16.25.8. "Will all crypto-anarchic transactions be anonymous?"

- No, various parties will negotiate different arrangements. All a matter of economics, of enforcement of terms, etc. Some will, some won't. The key thing is that the decision to reveal identity will be just another mutually negotiated matter. (Think of spending cash in a store. The store owner may *want* to know who his customers are, but he'll still take cash and remain ignorant in most cases. Unless a government steps in and distorts the market by requiring approvals for purchases and records of identities--think of guns here.)
- For example, the local Mob may not lend me money if I am anonymous to them, but they have a "hook" in me if they know who I am. (Aspects of anonymity may still be used, such as systems that leave no paper or computer trail pointing to them or to me, to avoid stings.)
- "Enforcement" in underground markets, for which the conventional legal remedies are impossible, is often by means of physical force: breaking legs and even killing welshers.
- (Personally, I have no problems with this. The Mob cannot turn to the local police, so it has to enforce deals its own way. If you can't pay, don't play.)

16.26. How Crypto Anarchy Will Be Fought

16.26.1. The Direct Attack: Restrictions on Encryption

- "Why won't government simply ban such encryption methods?"
  - This has always been the Number One Issue!

- raised by Stiegler, Drexler, Salin, and several others (and in fact raised by some as an objection to my even discussing these issues, namely, that action may then be taken to head off the world I describe)
  - Types of Bans on Encryption and Secrecy
    - Ban on Private Use of Encryption
    - Ban on Store-and-Forward Nodes
    - Ban on Tokens and ZKIPS Authentication
- Requirement for public disclosure of all transactions + Recent news (3-6-92, same day as Michaelangelo and Lawnmower Man) that government is proposing a surcharge on telcos and long distance services to pay for new equipment needed to tap phones!

- S.266 and related bills
- this was argued in terms of stopping drug dealers and other criminals
- but how does the government intend to deal with the various forms fo end-user encryption or "confusion" (the confusion that will come from compression, packetizing, simple file encryption, etc.)
    - Types of Arguments Against Such Bans
        - The "Constitutional Rights" Arguments
        - The "It's Too Late" Arguments
- PCs are already widely scattered, running dozens of compression and encryption programs...it is far too late to insist on "in the clear" broadcasts, whatever those may be (is program code distinguishable from encrypted messages? No.)
- encrypted faxes, modem scramblers (albeit with some restrictions)
- wireless LANs, packets, radio, IR, compressed text and images, etc...all will defeat any efforts short of police state intervention (which may still happen) + The "Feud Within the NSA" Arguments
- COMSEC vs. PROD + Will affect the privacy rights of corporations
- and there is much evidence that corporations are in fact being spied upon, by foreign governments, by the NSA, etc.
    - They Will Try to Ban Such Encryption Techniques
        - Stings (perhaps using viruses and logic bombs)
- or "barium," to trace the code

- Legal liability for companies that allow employees to use such methods

- perhaps even in their own time, via the assumption that employees who use illegal software methods in their own time are perhaps couriers or agents for their corporations (a tenuous point)
    - restrictions on: use of codes and ciphers

- there have long been certain restrictions on the use of encryption

- encryption over radio waves is illegal (unless the key is provided to the government, as with Morse code)
    - in war time, many restrictions (by all governments)
- those who encrypt are ipso facto guilty and are shot summarily, in many places
- even today, use of encryption near a military base or within a defense contractor could violate laws
    - S.266 and similar bills to mandate "trapdoors"

- except that this will be difficult to police and even to detect - so many ways to hide messages - so much ordinary compression, checksumming, etc.
    - Key Registration Trail Balloon
        - cite Denning's proposal, and my own postings

16.26.2. Another Direct Attack: Elimination of Cash

- the idea being that elimination of cash, with credit cards replacing cash, will reduce black markets

- "one person, one ID" (goal of many international standards organizations)
- this elimination of cash may ultimately be tied in to the key registration ideas...government becomes a third party in all transactions
  - a favorite of conspiracy theorists
- in extreme form: the number of the Beast tattooed on us (credit numbers, etc.)
- currency exchanges (rumors on the Nets about the imminent recall of banknotes, ostensibly to flush out ill-gotten gains and make counterfeiting easier)

- but also something governments like to do at times, sort of to remind us who's really in charge - Germany, a couple of times - France, in the late 1950s - various other devaluations and currency reforms
  - Partial steps have already been made

- cash transactions greater than some value-$10,000 at this time, though "suspicious" sub-$10K transactions must be reported-are banned

- large denomination bills have been withdrawn from circulation - used in drug deals, the argument goes

- Massachussetts has demanded that banks turn over all account records, SS numbers, balances, etc.

- "If what you're doing is legal, why do you need cash for it?"

- part of the old American dichotomy: privacy versus "What have you got to hide?"
  - But why the outlawing of cash won't work
    - if a need exists, black markets will arise
- i.e., the normal tradeoff between risk and reward: there may be some "discounts" on the value, but cah will still circulate
  - too many other channels exist: securities, secrets, goods

- from trading in gold or silver, neither of which are outlawed any longer, to trading in secrets, how can the government stop this?

- art being used to transfer money across international borders (avoids Customs)
- "consideration" given, a la the scam to hide income + total surveillance?
- it doesn't even work in Russia

- on the other hand, Russia lacks the "point of sale" infrastructure to enforce a cashless system

16.26.3. Another Direct Attack: Government Control of Encryption, Networks, and Net Access

- a la the old Bell System monopoly, which limited what could be hooked up to a phone line

- the government may take control of the networks in several ways:
- FCC-type restrictions, though it is hard to see how a private network, on private property, could be restricted - as it is not using part of the "public spectrum"

- but it is hard to build a very interesting network that stays on private property...and as soon as it crosses public property, BINGO!

- "National Data Highway" could be so heavily subsidized that alternatives will languish (for a while)

- the Al Gore proposals for a federally funded system (and his wife, Tipper, is of course a leader of the censorship wing)
- and then the government can claim the right and duty to set the "traffic" laws: protocols, types of encryption allowed, etc.
- key patents, a la RSA (if in fact gov't. is a silent partner in RSA Data Security)

16.26.4. An Indirect Attack: Insisting that all economic transactions be "disclosed" (the "Full Disclosure Society" scenario)

- this sounds Orwellian, but the obvious precedent is that businesses must keep records of all financial transactions (and even some other records, to see if they're colluding or manipulating something)
  - for income and sales tax reasons
  - and OSHA inspections, INS raids, etc.
- there is currently no requirement that all transactions be fully documented with the identies of all parties, except in some cases like firearms purchases, but this could change

- especially as electronic transactions become more common: the IRS may someday insist on such records, perhaps even insisting on escrowing of such records, or time-stamping

- this will hurt small businesses, due to the entry cost and overhead of such systems, but big businesses will probably support it (after some grumbling)

- big business always sees bureaucracy as one of their competitive advantages

- and individuals have not been hassled by the IRS on minor personal transactions, though the web is tightening: 1099s are often required (when payments exceed some amount, such as $500) - small scale barter transactions
- but the nature of CA is that many transactions can be financial while appearing to be something else (like the transfer of music or images, or even the writing of letters)

- which is why a cusp is coming: full disclosure is one route, protection of privacy is another

- the government may cite the dangers of a "good old boy network" (literally) that promulgates racist, sexist, and ableist discrimination via computer networks

- i.e., that the new networks are "under-representing people of color"
  - and how can quotas be enforced in an anonymous system?
- proposals in California (7-92) that consultants file monthly tax statements, have tax witheld, etc.
- a strategy for the IRS: require all computer network users to have a "taxpayer ID number" for all transactions, so that tax evasion can be checked

16.26.5. Attempts to discredit reputation-based systems by deceit, fraud, nonpayment, etc.

- deliberate attacks on the reputation of services the government doesn't want to see
- there may be government operations to sabotage businesses, to undermine such efforts before they get started
  - analogous to "mail-bombing" an anonymous remailer

16.26.6. Licensing of software developers may be one method used to try to control the spread of anonymous systems and information markets

- by requiring a "business license" attached to any and all chunks of code

- implemented via digital signatures, a la the code signing protocols mentioned by Bob Baldwin as a means of reducing trapdoors, sabotage, and other modifications by spies, hackers, etc.

- proposals to require all chunks of code to be signed, after the Sililcon Valley case in mid-80s, where spy/saboteur went to several s/w companies and meddled with code
- "seals" from some group such as "Software Writers Laboratories," with formal specs required, source code provided to a trusted keeper, etc.

- such licensing and inspection will also serve to lock-in the current players (Microsoft will love it) and make foreign competition in software more difficult

- unless the foreign competition is "sanctioned," e.g., Microsoft opens a code facility in India

16.26.7. RICO-like seizures of computers and bulletin board systems - sting operations and setups

- Steve Jackson Games is obvious example
- for illegal material (porno, drug advocacy, electronic money, etc.) flowing through their systems
- even when sysop can prove he did not know illegal acts were being committed on his system (precedents are the yachts seized because a roach was found)
  - these seizures can occur even when a trial is never held
- e.g., the "administrative seizure" of cars in Portland in prostitution cases
- and the seizures are on civil penalties, where the standards of proof are much lower

- in some cases a mere FBI investigation is enough to get employees fired, renters kicked out, IRS audits started
- reports that a woman in Georgia who posted some "ULs" (unlisted numbers?) was fired by her company after the FBI got involved, told by her landlord that her lease was not being extended, and so forth - "We don't truck with no spies"

- the IRS audit would not ostensibly be for harassment, but for "probable cause" (or whatever term they use) that tax avoidance, under-reporting, even money-laundering might be involved

16.26.8. Outlawing of Digital Pseudonyms and Credentialling + may echoe the misguided controversy over Caller ID

- misguided because the free market solution is clear: let those who wish to hide their numbers-rape and battering support numbers, police, detectives, or even just citizens requesting services or whatever-do so
- and let those who refuse to deal with these anonymous callers also do so (a simple enough programming of answering machines and telephones)
- for example, to prevent minors and felons from using the systems, "true names" may be required, with heavy fines and forfeitures of equipment and assets for anybody that fails to comply (or is caught in stings and setups)

- minors may get screened out of parts of cyberspace by mandatory "age credentialing" ("carding")

- this could be a major threat to such free and open systems, as with the various flaps over minors logging on to the Internet and seeing X-rated images (however poorly rendered) or reading salacious material in alt.sex
- there may be some government mood to insist that only "true names" be used, to facillitate such age screening (Fiat-Shamir passports, papers, number of the Beast?)

- the government may argue that digital pseudonyms are presumptively considered to be part of a conspiracy, a criminal enterprise, tax evasion, etc.
  - the old "what have you got to hide" theory

- closely related to the issue of whether false IDs can be used even when no crimes are being committed (that is, can Joe Average represent himself by other than his True Name?)
  - civil libertarians may fight this ban, arguing that Americans are not required to present "papers" to authorities unless under direct suspicion for a crime (never mind the loitering laws, which take the other view)

16.26.9. Anonymous systems may be restricted on the grounds that they constitute a public nuisance

- or that they promote crime, espionage, etc.

- especially after a few well-publicized abuses
  - possibly instigated by the government?

- operators may have to post bonds that effectively drive them out of business

16.26.10. Corporations may be effectively forbidden to hire consultants or subcontractors as individuals

- the practical issue: the welter of tax and benefit laws make individuals unable to cope with the mountains of forms that have to be filed

- thus effectively pricing individuals out of this market + the tax law side: recall the change in status of consultants a few years back...this may be extended further
- a strategy for the IRS: require all computer network users to have a "taxpayer ID number" for all transactions, so that tax evasion can be checked
- not clear how this differs from the point above, but I feel certain more such pressures will be applied (after all, most corporations tend to see independent contractors as more of a negative than a positive)
- this may be an agenda of the already established companies: they see consultants and free lancers as thieves and knaves, stealing their secrets and disseminating the crown jewels (to punningly mix some metaphors)
- and since the networks discussed here facilitate the use of consultants, more grounds to limit them

16.26.11. There may be calls for U.N. control of the world banking system in the wake of the BCCI and similar scandals

- to "peirce the veil" on transnationals
- calls for an end to banking secrecy
- talk about denying access to the money centers of New York (but will this push the business offshore, in parallel to the Eurodollar market?)
  - motivations and methods
    - recall the UNESCO attempt a few years back to credential reporters, ostensibly to prevent chaos and "unfair" reporting...well, the BCCI and nuclear arms deals surfacing may reinvigorate the efforts of "credentiallers"

- the USSR and other countries entering the world community may sense an opportunity to get in on the formation of "boards of directors" of these kinds of banks and corporations and so may push the idea in the U.N.

- sort of like a World Bank or IMF with even more power to step in and take control of other banks, and with the East Bloc and USSR having seats!

16.26.12. "National security"

- if the situation gets serious enough, a la a full-blown crypto anarchy system, mightn't the government take the step of declaring a kind of national emergency?
  - provisions exist: "401 Emergency" and FEMA plans
- of course, the USSR tried to intitiate emergency measures and failed
- recall that a major goal of crypto anarchy is that the systems described here will be so widely deployed as to be essential or critical to the overall economy...any attempt to "pull the plug" will also kill the economy

16.26.13. Can authorities force the disclosure of a key?

- on the "Yes" side:
- is same, some say, as forcing combination to a safe containing information or stolen goods

- but some say-and a court may have ruled on this-that the safe can always be cut open and so the issue is mostly moot - while forcing key disclosure is compelled testimony
  - and one can always claim to have forgotten the key
  - i.e., what happens when a suspect simply clams up?
- but authorities can routinely demand cooperation in investigations, can seize records, etc.
  - on the "No" side:
- can't force a suspect to talk, whether about where he hid the loot or where his kidnap victim is hidden
- practically speaking, someone under indictment cannot be forced to reveal Swiss bank accounts...this would seem to be directly analogous to a cryptographic key
- thus, the key to open an account would seem to be the same thing
- a memorized key cannot be forced, says someone with EFF or CPSR
- on balance, it seems clear that the disclosure of cryptographic keys cannot be forced (though the practical penalty for nondisclosure could be severe)
  - but this has not really been tested, so far as I know
- and many people say that such cooperation can be demanded...

16.27. How Crypto Anarchy Advocates Will Fight Back

16.27.1. Bypassing restrictions on commercial encryption packages by not making them "commercial"

- public domain
- freely distributed
- after all, the basic algorithms are simple and don't really deserve patent protection: money will not be made by the originators of the code, but by the actual providers of services (for transmission and storage of packets)

16.27.2. Noise and signals are often indistinguishable

- as with the LSB audio signal approach...unless the government outlaws live recordings or dubs on digital systems...

16.27.3. Timed-release files (using encryption) will be used to hide files, to ensure that governments cannot remove material they don't like

- easier said than done

16.27.4. Legal approaches will also be taken: fundamental constitutional issues

- privacy, free speech, free association

16.27.5. The Master Plan to Fight Restrictions on Encryption

- "Genie out of the bottle" strategy: deploy crypto widely

- intertwined with religions, games, whistleblower groups, and other uses that cannot easily just be shut down
  - scattered in amongst many other activities
  - Media attention: get media to report on value of encryption, privacy, etc.
  - Diffusion, confusion, and refusion
    - Diffuse the use by scattering it around
    - Confuse the issue by fake religions, games, other uses
    - Refuse to cooperate with the government
- Free speech arguments: calling the discussions free speech and forcing the government to prove that the free speech is actually an economic transaction
  - links with religions, corporations, etc.
    - private meetings protected
    - voting systems

16.28. Things that May Hide the Existence of Crypto Anarchy

16.28.1. first and foremost, the incredible bandwidth, the bits sloshing around the world's networks...tapes being exchanged, PCs calling other PCs, a variety of data and compression formats, ISDN, wireless transmission, etc.

16.28.2. in the coming years, network traffic will jump a thousandfold, what with digital fax, cellular phones and computers, ISDN, fiber optics, and higher-speed modems

- and these links will be of all kinds: local, private, corporate, business, commercial, bootleg (unrecorded), cellular radio, etc.

16.28.3. corporations and small groups will have their own private LANs and networks, with massive bandwidth, and with little prospects that the government can police them-there can be no law requiring that internal communications be readable by the government!

- and the revelations that Ultra Black has been used to read messages and use the information will be further proof to corporations that they need to adopt very strong security measures
- and "partnerships" can be scattered across the country, and even internationally, and have great lattitude in setting up their own communication and encryption systems
  - recall Cargill case
- and also remember that the government may crack down on these systems

16.28.4. AMIX-like services, new services, virtual reality (for games, entertainment, or just as a place of doing business) etc.

- many users will encrypt their links to VR servers, with a decryption agent at the other end, so that their activities (characters, fantasies, purchases, etc.) cannot be monitored and logged
- this will further increase the bandwidth of encrypted data and will complicate further the work of the NSA and similar agencies

- attempts to force "in the clear" links will be doomed by the welter of PC standards, compression utilities, cellular modems, and the like...there will be no "cleartext" that can be mandated

16.28.5. steganography

- in general, impossible to know that a message contains other encypted messages
  - except in stings and setups, which may be ruled illegal
  - the LSB method, and variants
- LSB of DAT, DCC, MD, etc., or even sound bites (chunks of sampled sounds traded on bulletin boards)

- especially of live or analog-dubbed copies (the noise floor of a typical consumer-grade mike is much higher than the LSB of DAT)
  - of images, Adobe Photoshop images, artwork, etc.

- imagine an "Online Art Gallery" that is used to store messages, or a "Photo Gallery" that participants post their best photos to, offering them for sale

- Sturges case
- LSB method

- gets into some theoretical nitpicking about the true nature of noise, especially if the entire LSB channel is uncharacteristic of "real noise"

- but by reducing the bandwidth somewhat, the noise profile can be made essentially undistinguishable from real noise
- and a 2 GB DAT produces 130 MB of LSB, which is a lot of margin!
  - what could the government do?
- stings and setups to catch and scare off potential users

- an attempt to limit the wide use of digital data-hopeless! + a requirement for government-approved "dithering"?
- this would be an enforcement nightmare

- and would only cause the system to be moved into higher bits

- and with enough error correction, even audible dithering of the signal would not wipe out the encrypted signal
  - variants: text justification, word selection
    - bandwidth tends to be low
    - but used in Three Days of the Condor

- virtual reality art may further enable private communications
  - think of what can be encrypted into such digital images!

- and user has total privacy and is able to manipulate the images and databases locally

16.28.6. in the sense that these other things, such as the governments own networks of safe houses, false identities, and bootleg payoffs, will tend to hide any other such systems that emerge

- because investigators may think they've stumbled onto yet another intelligence operation, or sting, or whatever
  - this routinely cripples undercover investigations

- scenario: criminals even float rumors that another agency is doing an operation...?

16.28.7. Government Operations that Resemble Cryptoanarchy will Confuse the Issues

- various confidential networks already exist, operated by State, DoD, the services, etc.

- Witness Protection Program (or Witness Relocation Program)

    - false IDs, papers, transcripts

- even money given to them (and the amounts seem to be downplayed in the press and on t.v., with a sudden spate of shows about how poorly they do in the middle of middle America-sounds like a planted story to me)
- cooperation with certain companies and schools to assist in this aspect
    - Payoffs of informants, unofficial agents
        - like agents in place inside defense contractors
- vast amount of tips from freelancers, foreign citizens, etc.
    - operators of safe houses (like Mrs. Furbershaw)
    - Networks of CIA-funded banks, for various purposes
        - a la the Nugan-Hand Bank, BCCI, etc.
        - First American, Bank of Atlanta, Centrust Savings, etc.
- these banks and S&Ls act as conduits for controversial or secret operations, for temporary parking of funds, for the banking of profits, and even for the private retirement funds of agents (a winked-at practice)
    - Confidential networks over computer lines
        - e.g., encrypted teleconferencing of Jasons, PFIAB, etc.
        - these will increase, for many reasons
            - concerns over terrorism
- demands on time will limit travel (especially for groups of non-fulltime committee members)
- these suspected government operations will deter investigation

16.28.8. Encrypted Traffic Will Increase Dramatically

- of all kinds
- mail, images, proposals, faxes, etc.
- acceptance of a P-K mail system will make wide use of encryption nearly automatic (though some fraction, perhaps the majority, will not even bother)

- there may even be legal reasons for encryption to increase:

- requirements that employee records be protected, that medical records be protected, etc.
- "prudent man" rules about the theft of information (could mean that files are to be encrypted except when being worked on)
    - digital signatures
- echoes of the COMSEC vs. SIGINT (or PROD) debate, where COMSEC wants to see more encryption (to protect American industry against Soviet and commercial espionage)
    - Selling of "Anonymous Mailers"?
        - using RSA
        - avoiding RSA and the P-K patent morass

        - could sell packets of one-time pads

- no effective guarantee of security, but adequate for many simple purposes
- especially if buyers swap them with others

- but how to ensure that copies are not kept? - idea is to enable a kind of "Democracy Wall"
    - prepaid "coins," purchased anonymously
        - as with the Japanese phone cards
- or the various toll booth electronic tokens being developed

16.28.9. Games, Religions, Legal Consultation, and Other "Covers" for the Introduction and Proliferation of Crypto Anarchy

- won't be clear what is real encryption and what is gameplaying
    - imagine a game called "Cryptoanarchy"!
    - Comment on these "Covers"
- some of these will be quite legitimate, others will be deliberately set up as covers for the spread of CA methods
- perhaps subsidized just to increase traffic (and encrypted traffic is already expected to increase for a variety of reasons)
    - people will have various reasons for wanting anonymity
    - Games
        - "Habitat"-style games and systems
- with "handles" that are much more secure than at present (recall Chip's comments)

- behaviors that are closely akin to real-world illegal behaviors:

- a thieves area
- an espionage game
- a "democracy wall" in which anything can be posted anonymously, and read by all
    - MUDs (Multi-user Domains, Multi-User Dungeons)
        - lots of interest here
- topic of discussion at a special Cypherpunks meeting, early 1994.

- interactive role-playing games will provide cover for the spread of systems: pseudonyms will have much more protection than they now have

- though various methods may exist to "tag" a transaction (a la barium), especially when lots of bandwidth is involved, for analysis (e.g., "Dark Dante" is identified by attaching

specific bits to stream) + Dealing with Barium Tracers
- code is allowed to simmer in an offsite machine for some time (and with twiddling of system clock)
- mutations added
  - Shared Worlds
- authors, artists, game-players, etc. may add to these worlds - hypertext links, reputation-based systems

- hypothesize a "True Names" game on the nets, based *explicitly* on Vinge's work

- perhaps from an outfit like Steve Jackson Games, maker of similar role-playing games - with variable-resolution graphics (a la Habitat) - virtual reality capabilities

- a game like "Habitat" can be used as a virtual Labyrinth, further confusing the line between reality and fantasy

- and this could provide a lot of bandwidth for cover
- the Smalltalk "Cryptoids" idea is related to this...it looks like a simulation or a game, but can be used by "outsiders"
  - Religions

- a nearly ironclad system of liberties, though *some* limits exist

- e.g., a church that uses its organization to transport drugs or run a gambling operation would be shut down quickly (recall the drug church?)
- and calls for tax-break limitations (which Bill of Rights says nothing about)
- still, it will be *very* difficult for the U.S. government to interfere with the communications of a "religion."
  - "ConfessionNet"

- a hypothetical anonymous system that allows confessions to be heard, with all of the privileges of privacy that normal confessions have

- successors to 900 numbers?

- virtually ironclad protections against government interference

- "Congress shall make no law..."

- but governments may try to restrict who can do this, a la the restrictions in the 70s and 80s on "instant Reverends"

- Kirby J. Hensley's Univeral Life Church
- various IRS restrictions, effectively establishing two classes of religions: those grandfathered in and given tax breaks and the like, and those that were deemed invalid in some way

- Scenario: A Scientology-like cult using CA as its chief communications system? - levels of initiation same as a cell system - "clearing"

- New Age garbage: Ascended Masters, cells, money flowing back and forth - blackballing
  - Digital Personals
- the "personals" section of newspapers currently requires the newspaper to provide the anonymity (until the parties mutually agree to meet)
  - what about on AMIX or similar services?
- a fully digital system could allow self-arranging systems + here's how it could work:
- Alice wants to meet a man. She writes up a typical ad, "SWF seeks SWM for fun and walks on the beach..."
- Alice encloses her specially-selected public key, which is effectively her only name. This is probably a onetime deal, unlinkable to her in any way.
- She encrypts the entire package and sends it through a remailing chain (or DC-Net) for eventual posting in a public place.
- Everyone can download the relevant area (messages can be sorted by type, or organized in interest groups), with nobody else knowing which messages they're reading.
- Bob reads her message and decides to repond. He digitizes a photo of himself and includes some other info, but not his real name. He also picks a public key for Alice to communicate with him.
- Bob encrypts all of this with the public key of Alice (though remember that he has no way of knowing who she really is).
- Bob sends this message through a remailing chain and it gets posted as an encrypted message addressed to the public key of Alice. Again, some organization can reduce the total bandwidth (e.g., an area for "Replies").
- Alice scans the replies and downloads a group of messages that includes the one she can see-and only she can see!-is addressed to her.
- This has established a two-way communication path between Alice and Bob without either of them knowing who the other one is or where they live. (The business about the photos is of course not conducive to anonymity, but is consistent with the "Personals" mode.)
- If Alice and Bob wish to meet in person it is then easy for them to communicate real phone numbers and the like.
  - Why is this interesting?
    - it establishes a role for anonymous systems
    - it could increase the bandwidth of such messages

- Legal Services (Legitimate, i.e., not even the bootleg stuff)
  - protected by attorney-client privileges, but various Bar Associations may place limits on the use of networks

- but if viewed the way phones are, seems unlikely that Bars could do much to limit the use of computer networks
- and suppose a Nolo Press-type publishing venture started up on the Nets? (publishing self-help info under pseudonyms)
- or the scam to avoid taxes by incorporating as a corporation or nonprofit?
  - Voting Systems

        - with and without anonymity
        - Board of Directors-type voting
- with credentials, passwords, and (maybe) anonymity (under certain conditions)
    - Blackballing and Memberships
        - generally anonymous
- blackballing may be illegal these days (concerns about racism, sexism, etc.)
- cf. Salomaa for discussion of indistinguishability of blackballing from majority voting
    - Consumer Ratings and Evaluations
- e.g., there may be "guaranteed anonymous" evalution systems for software and other high-tech items (Joe Bluecollar won't mess with computers and complicated voting systems)
    - Politically Active Groups May Have Anonymous Voting
        - to vote on group policies, procedures, leadership
- or on boycott lists (recall the idea of the PC-Card that doesn't allow politically incorrect purchases)

- this may be to protect themselves from lawsuits (SLAPP) and government harassment

- they fear government infiltrators will get the names of voters and how they voted
    - Official Elections
- though this is unlikely for the barely-literate majority
- the inevitable fraud cases will get wide exposure and scare people and politicians off even more
    - unlikely in next decade + Journal Refereeing
- some journals, such as Journal of Cryptology, appropriately enough, are already using paper-based versions of this + Xanadu-like systems may be early adopters
- there are of course reasons for just the opposite: enhanced used of reputations
- but in some cases anonymity may be preferred
    - Groupware
- anonymous comment systems (picture a digital blackboard with anonymous remarks showing up)
- these systems are promoted to encourage the quiet to have an equal voice
- but they also provide another path to anonymous and/or reputation-based systems
    - Psychological Consultations
- will require the licensing of counselors, of course (under U.S. laws)
    - what if people call offshore counselors?
    - and various limitations on privacy of records exist
        - Tarisoff [spelling?]
        - subpoenas
        - record-keeping required
    - may be used by various "politically correct" groups
        - battered women
        - abused children
- perhaps in conjunction with the RU-486-type issues, some common ground can be established (a new kind of Underground Railroad)
    - Advice on Medicine (a la AIDS, RU 486)

    - anonymity needed to protect against lawsuits and seizure
- NOW and other feminist groups could use crypto anarchy methods to reduce the risks to their organizations
    - Anonymous Tip Lines, Whistleblower Services

- for example, a newspaper might set up a reward system, using the crypto equivalent of the "torn paper" key - where informant holds onto the torn off "key"

- even something like the James Randi/Yuri Geller case reveals that "anonymous critics" may become more common

- corporate and defense contractor whistleblowers may seek protection through crypto methods

- a "Deep Throat" who uses bulletin boards to communicate with DS?

- this presumes much wider use of computers and modems by "average" people...and I doubt "Prodigy"-type systems will support these activities!

- but there may be cheap systems based on video game machines, a la the proposed Nintendo computers
- environmentalists set up these whistleblower lines, for people to report illegal logging, spraying, etc.
    - Online, "Instant" Corporations

- shell companies, duly incorporated in Delaware or wherever (perhaps even foreign sites) are "sold" to participants who wish to create a corporate cover for their activities

- so that AMIX-like fees are part of the "internal accounting"
    - Anonymous collaborative writing and criticism
        - similar to anonymous voting

16.28.10. Compressed traffic will similarly increase

- and many compression algortithms will offer some form of encryption as a freebie
- and will be difficult to decypher, based just on sheer volume
- files will have to at least be decompressed before key word searches can be done (though there may be shortcuts)

16.29. The Coming Phase Change

16.29.1. "We'd better hope that strong cypto, cheap telecoms and free markets can provide the organizing basis for a workable society because it is clear that coercion as an organizing principle ain't what it used to be." [Duncan Frissell, in his sig, 4-13-94]

16.29.2. "What is the "inevitability" argument?"

- Often made by me (Tim May), Duncan Frissell, Sandy Sandfort, and Perry Metzger (with some twists). And Hal Finney takes issue with certain aspects and contributes incisive critiques.
  - Reasons:
    - borders becoming more transparent to data flow
    - encryption is not detectable/stoppable
- derivative financial instruments, money sloshing across borders
  - transnationalism
  - cash machines, wire transfers
  - "permanent tourists"
- Borders are becoming utterly transparent to massive data flows. The rapid export of crypto is but an ironic example of this. Mosaid, ftp, gopher, lynx...all cross borders fluidly and nearly untraceably. It is probably too late to stop these systems, short of "pulling the plug" on the Net, and this pulling the plug is simply too expensive to consider. (If the Feds ever really figure out the long- range implications of this stuff, they may try it...but probably not.)

16.29.3. "What is the "crypto phase change"?"

- I'm normally skeptical of claims that a "singularity" is coming (nanotechnology being the usual place this is claimed, a la Vinge), but "phase changes" are more plausible. The effect of cheap printing was one such phase change, altering the connectivity of society and the dispersion of knowledge in a way that can best be described as a phase change. The effects of strong crypto, and the related ideas of digital cash, anonymous markets, etc., are likely to be similar.
  - transition
  - tipping factors, disgust by populace, runaway taxation
  - "leverage effect"
    - what Kelly called "the fax effect"
    - crypto use spreads, made more popular by common use
- can nucleate in a small group...doesn't need mass acceptance

16.29.4. "Can crypto anarchy be stopped?"

- A goal is to get crypto widely enough deployed that it cannot then be stopped

- to the point of no return, where the cost of withdrawing or banning a technology is simply too high (not always a guaranteee)
- The only recourse is a police state in which homes and businesses are randomly entered and searched, in which cryptography is outlawed and vigorously prosecuted, in which wiretaps, video surveillance, and other forms of surveillance are used aggressively, and in which perhaps the very possession of computers and modems is restricted.
- Anything short of these police state tactics will allow the development of the ideas discussed here. To some extent. But enough to trigger the transition to a mostly crypto anarchic situation.
- (This doesn't mean everyone, or even most, will use crypto anarchy.)

16.29.5. Need not be a universal or even popular trend

- even if restricted to a minority, can be very influential
- George Soros, Quantum fund, central banks, Spain, Britain, Germany
  - and a minority trend can affect others

16.29.6. "National borders are just speedbumps on the digital superhighway."

16.29.7. "Does crypto anarchy have to be a mass movement to succeed?" - Given that only a tiny fraction is now aware of the implications...

- Precedents for "vanguard" movements
  - high finance in general is an elite thing
    - Eurodollars, interest rate swaps, etc...not exactly Joe Average...and yet of incredible importance (George Soros has affected European central bank policy)
  - smuggling is in general not a mass thing
  - etc.
- Thus, the users of crypto anarchic tools and instruments can have an effect out of proportion to their numbers
  - others will start to use
  - resentment by the "suckers" will build

- the services themselves--the data havens, the credit registries, the espionage markets--will of course have a real effect

16.29.8. Strong crypto does not mean the end to law enforcement

- "...cryptography is not by any means a magic shield for criminals. It eliminates, perhaps, one avenue by which crimes might be discovered. However, it is most certainly not the case that someone who places an open anonymous contract for a murder in an open forum is doing so "risk free". There are *plenty* of ways she might be found out. Likewise, big secret societies that nefariously undermine the free world via cryptography are as vulnerable as ever to the motivations of their own members to expose the groups in a double-cross." [Mike McNally, 1994-09-09]

16.30. Loose Ends

16.30.1. governments may try to ban the use of encryption in any broadcast system, no matter how low the power, because of a realization that all of them can be used for crypto anarchy and espionage

- a losing battle, of course, what with wireless LANs of several flavors, cellular modems, the ability to hide information, and just the huge increase in bandwidth

16.30.2. "tontines"

- Eric Hughes wrote up some stuff on this in 1992 [try to get it]
  - Italian pseudo-insurance arrangements
  - "digital tontines"?

16.30.3. Even in market anarchies, there are times when a top-down, enforced set of behaviors is desirable. However, instead of being enforced by threat of violence, the market itself enforces a standard.

- For example, the Macintosh OS, with standardized commands that program developers are "encouraged" to use. Deviations are obviously allowed, but the market tends to punish such deviations. (This has been useful in avoiding modal software, where the same keystroke sequence might save a file in one program and erase it in another. Sadly, the complexity of modern software has outpaced the Mac OS system, so that Command-Option Y often does different things in different programs.)

    - Market standards are a noncoercive counter to total chaos.

16.30.4. Of course, nothing stops people from hiring financial advisors, lawyers, and even "Protectors" to shield them from the predations of others. Widows and orphans could choose conservative conservators, while young turks could choose to go it alone.

16.30.5. on who can tolerate crypto anarchy

- Not much different here from how things have been in the past. Caveat emptor. Look out for Number One. Beware of snake oil.

16.30.6. Local enforcement of rules rather than global rules

- e.g., flooding of Usenet with advertising and chain letters
    - two main approaches

- ban such things, or set quotas, global acceptable use policies, etc. (or use tort law to prosecute & collect damages)
- local carrriers decide what they will and will not carry, and how much they'll charge
    - it's the old rationing vs. market pricing argument

16.30.7. Locality is a powerful concept

- self-responsibility

- who better to make decisions than those affected?
- tighter feedback loops
- avoids large-scale governments

- Nonlocally-arranged systems often result in calls to stop "hogging" of resources, and general rancor and envy
- water consumption is the best example: anybody seen "wasting" water, regardless of their conservations elsewhere or there priorities, is chastised and rebuked. Sometimes the water police are called.

- the costs involved (perhaps a few pennies worth of water, to wash a car or water some roses) are often trivial...meanwhile, billions of acre-feet of water are sold far below cost to farmers who grow monsoon crops like rice in the California desert
- this hypocrisy is high on my list of reasons why free markets are morally preferable to rationing-based systems

---

Revision #1
Created 23 June 2022 04:03:45 by c0mmando
Updated 23 June 2022 04:04:11 by c0mmando