10. Legal Issues

10.1. copyright

10.2. SUMMARY: Legal Issues

10.2.1. Main Points

10.2.2. Connections to Other Sections

- Sad to say, but legal considerations impinge on nearly every aspect of crypto

10.2.3. Where to Find Additional Information

10.2.4. Miscellaneous Comments

- "I'm a scientist, Jim, not an attorney." Hence, take my legal comments here with a grain of salt, representing only hints of the truth as I picked them up from the discussions on the various forums and lists.

10.3. Basic Legality of Encryption

10.3.1. "Is this stuff legal or illegal?"

- Certainly the *talking* about it is mostly legal, at least in the U.S. and at the time of this writing. In other countries, you prison term may vary.

- The actions resulting from crypto, and crypto anarchy, may well be illegal. Such is often the case when technology is applied without any particular regard for what the laws say is permitted. (Pandora's Box and all that.)

- Cypherpunks really don't care much about such ephemera as the "laws" of some geographic region. Cypherpunks make their own laws.
  - There are two broad ways of getting things done:
- First, looking at the law and regulations and finding ways to exploit them. This is the tack favored by lawyers, of whic$are many in this country.
- Second, "just do it." In areas where the law hasn't caught up, this can mean unconstrained technological developement. Good examples are the computer and chip business, where issues of legality rarely arose (except in the usual areas of contract enforcement, etc.). More recently the chip business has discovered lawyering, with a vengeance.
- In other areas, where the law is centrally involved, "just do it" can mean many technical violations of the law. Examples: personal service jobs (maids and babysitters), contracting jobs without licenses, permissions, etc., and so on. Often these are "illegal markets," putatively.
- And bear in mind that the legal system can be used to hassle people, to pressure them to "plead out" to some charges, to back off, etc. (In the firearms business, the pressures and threats are also used to cause some manufacturers, like Ruger, to back off on a radical pro-gun stance, so as to be granted favors and milder treatment. Pressure on crypto-producing companies are probably very similar. Play ball, or we'll run you over in the parking lot.)

10.3.2. "Why is the legal status of crypto so murky?"

- First, it may be murkier to me than it it to actual lawyers like Mike Godwin and Michael Froomkin, both of whom have been on our list at times. (Though my impression from talking to Godwin is that many or even most of these issues have not been addressed in the courts, let alone resolved definitively.)
- Second, crypto issues have not generally reached the courts, reflecting the nascent status of most of the things talked about it here. Things as "trivial" as digital signatures and digital timestamping have yet to be challenged in courts, or declared illegal, or anything similar that might produce a precedent-setting ruling. (Stu Haber agrees that such tests are lacking.)

- Finally, the issues are deep ones, going to the heart of issues of self-incrimination (disclosure of keys, contempt), of intellectual property and export laws (want to jail someone for talking about prime numbers?), and the incredibly byzantine world of money and financial instruments.
- A legal study of crypto--which I hear Professor Froomkin is doing--could be very important.

10.3.3. "Has the basic legality of crypto and laws about crypto been tested?"

- As usual, a U.S. focus here. I know little of the situation in non-U.S. countries (and in many of them the law is whatever the rulers say it is).
  - And I'm not a lawyer.
  - Some facts:
- no direct Constitutional statement about privacy (though many feel it is implied)
- crypto was not a major issue (espionage was, and was dealt with harshly, but encrypting things was not a problem per se)

- only in the recent past has it become important...and it will become much more so - as criminals encrypt, as terrorists encrypt - as tax is avoided via the techniques described here

- collusion of business ("crypto interlocking directorates," price signalling) - black markets, information markets
  - Lawrence Tribe..new amendment
    - scary, as it may place limits... (but unlikely to happen)
  - Crypto in Court
    - mostly untested
    - can keys be compelled?
    - Expect some important cases in the next several years

10.3.4. "Can authorities force the disclosure of a key?"

- Mike Godwin, legal counsel for the EFF, has been asked this queston *many* times:

- "Note that a court could cite you for contempt for not complying with a subpoena duces tecum (a subpoena requiring you to produce objects or documents) if you fail to turn over subpoenaed backups...To be honest, I don't think *any* security measure is adequate against a government that's determined to overreach its authority and its citizens' rights, but crypto comes close." [Mike Godwin, 1993-06-14]

- Torture is out (in many countries, but not all). Truth serum, etc., ditto.
  - "Rubber hose cryptography"
  - Constitutional issues
    - self-incrimination
  - 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
  - "Safe" analogy
    - You have a safe, you won' tell the combination
      - you just refuse
      - you claim to have forgotten it
      - you really don't know it
- cops can cut the safe open, so compelling a combination is not needed
  - "interefering with an investigation"
- on balance, it seems clear that the disclosure of cryptographic keys cannot be forced (though the practical penalty for nondisclosure could be severe)
  - Courts
    - compelled testimony is certainly common
- if one is not charged, one cannot take the 5th (may be some wrinkles here) - contempt
  - What won't immunize disclosure:
    - clever jokes about "I am guilty of money laundering"
- can it be used?
- does judge declaring immunity apply in this case?
- Eric Hughes has pointed out that the form of the statement is key: "My key is: "I am a murderer."" is not a legal admission of anything.
- (There may be some subtleties where the key does contain important evidence--perhaps the location of a buried body- -but I think these issues are relatively minor.)
  - but this has not really been tested, so far as I know
- and many people say that such cooperation can be demanded...
  - Contempt, claims of forgetting

10.3.5. Forgetting passwords, and testimony

- This is another area of intense speculation:
  - "I forgot. So sue me."

- "I forgot. It was just a temporary file I was working on, and I just can't remember the password I picked." (A less in-your-face approach.)

- "I refuse to give my password on the grounds that it may tend to incriminate me."
- Canonical example: "My password is: 'I sell illegal drugs.'"

- Eric Hughes has pointed out this is not a real admission of guilt, just a syntactic form, so it is nonsense to claim that it is incriminating. I agree. I don't know if any court tests have confirmed this.

- Sandy Sandfort theorizes that this example might work, or at least lead to an interesting legal dilemma:
  - "As an example, your passphrase could be: I shot a cop in the back and buried his body under the porch at 123 Main St., anywhere USA. The gun is wrapped in an oily cloth in my mother's attic. "I decline to answer on the grounds that my passphrase is a statement which may tend to incriminate me. I will only give my passphrase if I am given immunity from prosecution for the actions to which it alludes." "Too cute, I know, but who knows, it might work." [S.S., 1994-0727]

10.3.6. "What about disavowal of keys? Of digital signatures? Of contracts?

- In the short term, the courts are relatively silent, as few of these issues have reached the courts. Things like signatures and contract breaches would likely be handled as they currently are (that is, the judge would look at the circumstances, etc.)

- Clearly this is a major concern. There are two main avenues of dealing with this"

- The "purist" approach. You *are* your key. Caveat emptor. Guard your keys. If your signature is used, you are responsible. (People can lessen their exposure by using protocols that limit risk, analogous to the way ATM systems only allow, say, $200 a day to be withdrawn.)
- The legal system can be used (maybe) to deal with these issues. Maybe. Little of this has been tested in courts. Conventional methods of verifying forged signatures will not work. Contract law with digital signatures will be a new area.

- The problem of *repudiation* or *disavowal* was recognized early on in cryptologic circles. Alice is confronted with a digital signature, or whatever. She says; "But I didn't sign that" or "Oh, that's my old key--it's obsolete" or "My sysadmin must have snooped through my files," or "I guess those key escrow guys are at it again."
- I think that only the purist stance will hold water in the long run.(A hint of this: untraceable cash means, for most transactions of interest with digital cash, that once the crypto stuff has been handled, whether the sig was stolen or not is moot, because the money is gone...no court can rule that the sig was invalid and then retrieve the cash!)

10.3.7. "What are some arguments for the freedom to encrypt?"

- bans are hard to enforce, requiring extensive police intrusions
  - private letters, diaries, conversations
  - in U.S., various provisions
  - anonymity is often needed

10.3.8. Restrictions on anonymity

- "identity escrow" is what Eric Hughes calls it
- linits on mail drops, on anonymous accounts, and--perhaps ultimately--on cash purchases of any and all goods

10.3.9. "Are bulletin boards and Internet providers "common carriers" or not?"

- Not clear. BBS operators are clearly held more liable for content than the phone company is, for example.

10.3.10. Too much cleverness is passing for law

- Many schemes to bypass tax laws, regulations, etc., are, as the British like to say, "too cute by half." For example, claims that the dollar is defined as 1/35th of an ounce of gold and that the modern dollar is only 1/10th of this. Or that Ohio failed to properly enter the Union, and hence all laws passed afterward are invalid. The same could be said of schemes to deploy digital cash be claiming that ordinary laws do not apply. Well, those

who try such schemes often find out otherwise, sometimes in prison. Tread carefully.

10.3.11. "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. "

10.4. Can Crypto be Banned?

10.4.1. "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)

10.4.2. The long-range impossibility of banning crypto

- stego

- direct broadcast to overhead satellites
- samizdat
- compression, algorithms, ...all made plaintext hard to find

10.4.3. Banning crypto is comparable to

- banning ski masks because criminals can hide their identity

- Note: yes, there are laws about "going masked for the purpose of being masked," or somesuch

- insisting that all speech be in languages understandable by eavesdroppers

- (I don't mean "official languages" for dealing with the Feds, or what employers may reasonably insist on)
- outlawing curtains, or at least requiring that "Clipper curtains" be bought (curtains which are transparent at wavelengths the governments of the world can use)
- position escrow, via electronic bracelets like criminals wear
  - restrictions on books that possibly help criminals
  - banning body armor (proposed in several communities)
  - banning radar detectors
- (Note that these bans become more "reasonable" when the items like body armor and radar detectos are reached, at least to many people. Not to me, of course.)

10.4.4. So Won't Governments Stop These Systems?

- Citing national security, protection of private property, common decency, etc.
  - Legal Measures
    - Bans on ownership and operation of "anonymous" systems
    - Restrictions on cryptographic algorithms
      - RSA patent may be a start
    - RICO, civil suits, money-laundering laws
      - FINCEN, Financial Crimes Information Center
      - IRS, Justice, NSA, FBI, DIA, CIA
- attempts to force other countries to comply with U.S. banking laws

10.4.5. Scenario for a ban on encryption

- "Paranoia is cryptography's occupational hazard." [Eric Hughes, 1994-05-14]

- There are many scenarios. Here is a graphic one from Sandy Sandfort:
- "Remember the instructions for cooking a live frog. The government does not intend to stop until they have effectively eliminated your privacy. STEP 1: Clipper becomes the de facto encryption standard. STEP 2: When Cypherpunks and other "criminals" eschew Clipper in favor of trusted strong crypto, the government is "forced" to ban non-escrowed encryption systems. (Gotta catch those pedophiles, drug dealers and terrorists, after all.) STEP 3: When Cypherpunks and other criminals use superencryption with Clipper or spoof LEAFs, the government will regretably be forced to engage in random message monitoring to detect these illegal techniques. Each of these steps will be taken because we wouldn't passively accept such things as unrestricted wiretaps and reasonable precautions like digital telephony. It will portrayed as our fault. Count on it." [Sandy Sandfort, 6-14-94]

10.4.6. Can the flow of bits be stopped? Is the genie really out of the bottle?

- Note that Carl Ellison has long argued that the genie was never *in* the bottle, at least not in the U.S. in nonwartime situations (use of cryptography, especially in communications, in wartime obviously raises eyebrows)

10.5. Legal Issues with PGP

10.6. Legal Issues with Remailers

10.7. Legal Issues with Escrowed Encryption and Clipper

10.8. Legal Issues with Digital Cash

10.8.1. "What's the legal status of digital cash?"

- It hasn't been tested, like a lot of crypto protocols. It may be many years before these systems are tested.

10.8.2. "Is there a tie between digital cash and money laundering?"

- There doesn't have to be, but many of us believe the widespread deployment of digital, untraceable cash will make possible new approaches
- Hence the importance of digital cash for crypto anarchy and related ideas.
- (In case it isn't obvious, I consider money-laundering a non-crime.)

10.8.3. "Is it true the government of the U.S. can limit funds transfers outside the U.S.?"

- Many issues here. Certainly some laws exist. Certainly people are prosecuted every day for violating currency export laws. Many avenues exist.
- "LEGALITY - There isn't and will never be a law restricting the sending of funds outside the United States. How do I know? Simple. As a country dependant on international trade (billions of dollars a year and counting), the American economy would be destroyed." [David Johnson, privacy@well.sf.ca.us, "Offshore Banking & Privacy," alt.privacy, 1994-07-05]

10.8.4. "Are "alternative currencies" allowed in the U.S.? And what's the implication for digital cash of various forms?

- Tokens, coupons, gift certificates are allowed, but face various regulations. Casino chips were once treated as cash, but are now more regulated (inter-casino conversion is no longer allowed).
- Any attempt to use such coupons as an alternative currency face obstacles. The coupons may be allowed, but heavily regulated (reporting requirements, etc.).
- Perry Metzger notes, bearer bonds are now illegal in the U.S. (a bearer bond represented cash, in that no name was attached to the bond--the "bearer" could sell it for cash or redeem it...worked great for transporting large amounts of cash in compact form).

- Note: Duncan Frissell claims that bearer bonds are *not* illegal.

- "Under the Tax Equity and Fiscal Responsibility Act of 1982 (TEFRA), any interest payments made on *new* issues of domestic bearer bonds are not deductible as an ordinary and necessary business expense so none have been issued since then. At the same time, the Feds administratively stopped issuing treasury securities in bearer form. Old issues of government and corporate debt in bearer form still exist and will exist and trade for 30 or more years after 1982. Additionally, US residents can legally buy foreign bearer securities." [Duncan Frissell, 1994-08-10]
- Someone else has a slightly different view: "The last US Bearer Bond issues mature in 1997. I also believe that to collect interest, and to redeem the bond at maturity, you must give your name and tax-id number to the paying agent. (I can check with the department here that handles it if anyone is interested in the pertinent OCC regs that apply)" [prig0011@gold.tc.umn.edu, 1994-08-10]
- I cite this gory detail to give readers some idea about how much confusion there is about these subjects. The usual advice is to "seek competent counsel," but in fact most lawyers have no clear ideas about the optimum strategies, and the run-of-the-mill advisor may mislead one dangerously. Tread carefully.
    - This has implications for digital cash, of course.

10.8.5. "Why might digital cash and related techologies take hold early in illegal markets? That is, will the Mob be an early adopter?"

- untraceability needed
- and reputations matter to them
- they've shown in the past that they will try new approaches, a la the money movements of the drug cartels, novel methods for security, etc.

10.8.6. "Electronic cash...will it have to comply with laws, and how?"

- Concerns will be raised about the anonymity aspects, the usefulness for evading taxes and reporting requirements, etc.
- a messy issue, sure to be debated and legislated about for many years

- split the cash into many pieces...is this "structuring"? is it legal?

- some rules indicate the structuring per se is not illegal, only tax evasion or currency control evasion
- what then of systems which *automatically*, as a basic feature, split the cash up into multiple pieces and move them?

10.8.7. Currency controls, flight capital regulations, boycotts, asset seizures, etc.

- all are pressures to find alternate ways for capital to flow
- all add to the lack of confidence, which, paradoxically to lawmakers, makes capital flight all the more likely

10.8.8. "Will banking regulators allow digital cash?"

- Not easily, that's for sure. The maze of regulations, restrictions, tax laws, and legal rulings is daunting. Eric Hughes spent a lot of time reading up on the laws regarding banks, commercial paper, taxes, etc., and concluded much the same. I'm not saying it's impossible--indeed, I believe it will someday happen, in some form--but the obstacles are formidable.
  - Some issues:
    - Will such an operation be allowed to be centered or based in the U.S.?
- What states? What laws? Bank vs. Savings and Loan vs. Credit Union vs. Securities Broker vs. something else?

- Will customers be able to access such entities offshore, outside the U.S.?

- strong crypto makes communication possible, but it may be difficult, not part of the business fabric, etc. (and hence not so useful--if one has to send PGP- encrypted

instructions to one's banker, and can't use the clearing infrastructure...)
    - Tax collection, money-laundering laws, disclosure laws, "know your customer" laws...all are areas where a "digital bank" could be shut down forthwith. Any bank not filling out the proper forms (including mandatory reporting of transactions of certain amounts and types, and the Social Security/Taxpayer Number of customers) faces huge fines, penalties, and regulatory sanctions.
- and the existing players in the banking and securities business will not sit idly by while newcomers enter their market; they will seek to force newcomers to jump through the same hoops they had to (studies indicate large corporations actually *like* red tape, as it helps them relative to smaller companies)
    - Concluson: Digital banks will not be "launched" without a *lot* of work by lawyers, accountants, tax experts, lobbyists, etc. "Lemonade stand digital banks" (TM) will not survive for long. Kids, don't try this at home!
- (Many new industries we are familiar with--software, microcomputers--had very little regulation, rightly so. But the effect is that many of us are unprepared to understand the massive amount of red tape which businesses in other areas, notably banking, face.)

10.8.9. Legal obstacles to digital money. If governments don't want anonymous cash, they can make things tough.

- As both Perry Metzger and Eric Hughes have said many times, regulations can make life very difficult. Compliance with laws is a major cost of doing business.

- ~"The cost of compliance in a typical USA bank is 14% of operating costs."~ [Eric Hughes, citing an "American Banker" article, 1994-08-30]

- The maze of regulations is navigable by larger institutions, with staffs of lawyers, accountants, tax specialists, etc., but is essentially beyond the capabilities of very small institutions, at least in the U.S.

- this may or may not remain the case, as computers proliferate. A "bank-in-a-box" program might help. My suspicion is that a certain size of staff is needed just to handle the face-to-face meetings and hoop-jumping.
    - "New World Order"
- U.S. urging other countries to "play ball" on banking secrecy, on tax evasion extradition, on immigration, etc.
- this is closing off the former loopholes and escape hatches that allowed people to escape repressive taxation...the implications for digital money banks are unclear, but worrisome.

10.9. Legality of Digital Banks and Digital Cash?

10.9.1. In terms of banking laws, cash reporting regulations, money laundering statutes, and the welter of laws connected with financial transactions of all sorts, the Cypherpunks themes and ideas are basically *illegal*. Illegal in the sense that anyone trying to set up his own bank, or alternative currency system, or the like would be shut down quickly. As an informal, unnoticed *experiment*, such things are reasonably safe...until they get noticed.

10.9.2. The operative word here is "launch," in my opinion. The "launch" of the BankAmericard (now VISA) in the 1960s was not done lightly or casually...it

required armies of lawyers, accountants, and other bureacrats to make the launch both legal and successful. The mere 'idea" of a credit card was not enough...that was essentially the easiest part of it all. (Anyone contemplating the launch of a digital cash system would do well to study BankAmericard as an example...and several other examples also.)

10.9.3. The same will be true of any digital cash or similar system which intends to operate more or less openly, to interface with existing financial institutions, and which is not explicity intended to be a Cypherpunkish underground activity.

10.10. Export of Crypto, ITAR, and Similar Laws

10.10.1. "What are the laws and regulations about export of crypto, and where can I find more information?"

- "The short answer is that the Department of State, Office of Defense Trade Controls (DOS/DTC) and the National Security Administration (NSA) won't allow unrestricted export (like is being done with WinCrypt) for any encryption program that the NSA can't crack with less than a certain amount (that they are loathe to reveal) of effort. For the long answer, see ftp://ftp.csn.net/cryptusa.txt.gz and/or call DOS/DTC at 703-875-7041." [Michael Paul Johnson, sci.crypt, 1994-0708]

10.10.2. "Is it illegal to send encrypted stuff out of the U.S.?"

- This has come up several times, with folks claiming they've heard this.
- In times of war, real war, sending encrypted messages may indeed be suspect, perhaps even illegal.
- But the U.S. currently has no such laws, and many of us send lots of encrypted stuff outside the U.S. To remailers, to friends, etc.
- Encrypted files are often tough to distinguish from ordinary compressed files (high entropy), so law enforcement would have a hard time.
  - However, other countries may have different laws.

10.10.3. "What's the situation about export of crypto?"

- There's been much debate about this, with the case of Phil Zimmermann possibly being an important test case, should charges be filed.

- as of 1994-09, the Grand Jury in San Jose has not said anything (it's been about 7-9 months since they started on this issue)
- Dan Bernstein has argued that ITAR covers nearly all aspects of exporting crypto material, including codes, documentation, and even "knowledge." (Controversially, it may be in violation of ITAR for knowledgeable crypto people to even leave the country with the intention of developing crypto tools overseas.)
- The various distributions of PGP that have occurred via anonymous ftp sources don't imply that ITAR is not being enforced, or won't be in the future.

10.10.4. Why and How Crypto is Not the Same as Armaments

- the gun comparison has advantages and disadvantages
- "right to keep and bear arms"
- but then this opens the door wide to restrictions, regulations, comparisons of crypto to nuclear weapons, etc.

- "Crypto is not capable of killing people directly. Crypto consists

- entirely of information (speech, if you must) that cannot be
  - interdicted. Crypto has civilian use.
  - <Robert Krawitz rlk@think.com, 4-11-94, sci.crypt>

10.10.5. "What's ITAR and what does it cover?"

- ITAR, the International Trafficking in Arms Regulations, is the defining set of rules for export of munitions--and crypto is treated as munitions.
  - regulations for interpreting export laws
  - NSA may have doubts that ITAR would hold up in court

- Some might argue that this contravenes the Constitution, and hence would fail in court. Again, there have been few if any solid tests of ITAR in court, and some indications that NSA lawyers are reluctant to see it tested, fearing it would not pass muster.
- doubts about legality (Carl Nicolai saw papers, since confirmed in a FOIA)
  - Brooks statement
  - Cantwell Bill
  - not fully tested in court

- reports of NSA worries that it wouldn't hold up in court if ever challenged
  - Carl Nicolai, later FOIA results, conversations with Phil
  - Legal Actions Surrounding ITAR

- The ITAR laws may be used to fight hackers and Cypherpunks...the outcome of the Zimmermann indictment will be an important sign.
  - What ITAR covers
    - "ITAR 121.8(f): ''Software includes but is not limited to the system functional design, logic flow, algorithms, application programs, operating systems and support software for design, implementation, test, operation, diagnosis and repair.'' [quoted by Dan Bernstein, talk.politics.crypto, 1994-07-14]

- joke by Bidzos about registering as an international arms dealer
  - ITAR and code (can code be published on the Net?)
    - "Why does ITAR matter?"
    - Phil Karn is involved with this, as are several others here

- Dan Bernstein has some strongly held views, based on his long history of fighting the ITAR - "Let's assume that the algorithm is capable of maintaining secrecy of information, and that it is not restricted to decryption, banking, analog scrambling, special smart cards, user authentication, data authentication, data compression, or virus protection. "The algorithm is then in USML Category XIII(b)(1). "It is thus a defense article. ITAR 120.6. " [Dan Bernstein, posting code to sci.crypt, talk.politics.crypto, 1994-08-22] - "Sending a defense article out of the United States in any manner (except as knowledge in your head) is export. ITAR 120.17(1). "So posting the algorithm constitutes export. There are other forms of export, but I won't go into them here. "The algorithm itself, without any source code, is software." [Dan Bernstein, posting code to sci.crypt, talk.politics.crypto, 1994-08-22]
  - "The statute is the Arms Export Control Act; the regulations are the International Traffic in Arms Regulations. For precise references, see my ''International Traffic in Arms Regulations: A Publisher's Guide.''" [Dan Bernstein, posting code to sci.crypt, talk.politics.crypto, 1994-08-22]
- "Posting code is fine. We do it all the time; we have the right to do it; no one seems to be trying to stop us from doing it." [Bryan G. Olson, posting code to sci.crypt, talk.politics.crypto, 1994-08-20] - Bernstein agrees that few busts have occurred, but warns: "Thousands of people have distributed crypto in violation of ITAR; only two, to my knowledge, have been convicted. On the other hand, the guv'mint is rapidly catching up with reality, and the Phil Zimmermann case may be the start of a serious crackdown." [Dan Bernstein, posting code to sci.crypt, talk.politics.crypto, 1994-08-22]

- The common view that academic freedom means one is OK is probably not true.

- Hal Finney neatly summarized the debate between Bernstein and Olsen:

- "1) No one has ever been prosecuted for posting code on sci.crypt. The Zimmermann case, if anything ever comes of it, was not about posting code on Usenet, AFAIK. "2) No relevant government official has publically expressed an opinion on whether posting code on sci.crypt would be legal. The conversations Dan Bernstein posted dealt with his requests for permission to export his algorithm, not to post code on sci.crypt. "3) We don't know whether anyone will ever be prosecuted for posting code on sci.crypt, and we don't know what the outcome of any such prosecution would be." [Hal Finney, talk.politics.crypto, 1994-008-30]

10.10.6. "Can ITAR and other export laws be bypassed or skirted by doing

development offshore and then *importing* strong crypto into the U.S.?"

- IBM is reportedly doing just this: developing strong crypto products for OS/2 at its overseas labs, thus skirting the export laws (which have weakened the keys to some of their network security products to the 40 bits that are allowed).
  - Some problems:
- can't send docs and knowhow to offshore facilities (some obvious enforcement problems, but this is how the law reads)
- may not even be able to transfer knowledgeable people to offshore facilities, if the chief intent is to then have them develop crypto products offshore (some deep Constitutional issues, I would think...some shades of how the U.S.S.R. justified denying departure visas for "needed" workers)
- As with so many cases invovling crypto, there are no defining legal cases that I am aware of.

10.11. Regulatory Arbitrage

10.11.1. Jurisdictions with more favorable laws will see claimants going there.

10.11.2. Similar to "capital flight" and "people voting with their feet."

10.11.3. Is the flip side of "jurisdiction shopping." wherein prosecutors shop around for a jurisdiction that will be likelier to convict. (As with the Amateur Action

BBS case, tried in Memphis, Tennessee, not in California.)

10.12. Crypto and Pornography

10.12.1. There's been a lot of media attention given to this, especially pedophilia (pedophilia is not the same thing as porn, of course, but the two are often discussed in articles about the Net). As Rishab Ghosh put it: "I think the pedophilic possibilities of the Internet capture the imaginations of the media -- their deepest desires, perhaps." [R.G., 1994-07-01]

10.12.2. The fact is, the two are made for each other. The untraceability of remailers, the unbreakability of strong crypto if the files are intercepted by law

enforcement, and the ability to pay anonymously, all mean the early users of commercial remailers will likely be these folks.

10.12.3. Avoid embarrassing stings! Keep your job at the elementary school! Get re-elected to the church council!

10.12.4. pedophilia, bestiality, etc. (morphed images)

10.12.5. Amateur Action BBS operator interested in crypto...a little

bit too late

10.12.6. There are new prospects for delivery of messages as part of stings or entrapment attacks, where the bits decrypt into incriminating evidence when the right key is used. (XOR of course)

10.12.7. Just as the law enforcement folks are claiming, strong crypto and remailers will make new kinds of porn networks. The nexus or source will not be known, and the customers will not be known.

- (An interesting strategy: claim customers unknown, and their local laws. Make the "pickup" the customer's responsibility (perhaps via agents).

10.13. Usenet, Libel, Local Laws, Jurisdictions, etc.

10.13.1. (Of peripheral importance to crypto themes, but important for issues of coming legislation about the Net, attempts to "regain control," etc. And a bit of a jumble of ideas, too.)

10.13.2. Many countries, many laws. Much of Usenet traffic presumably violates various laws in Iran, China, France, Zaire, and the U.S., to name f ew places which

have laws about what thoughts can be expressed.

10.13.3. Will this ever result in attempts to shut down Usenet, or at least the feeds into various countries?

10.13.4. On the subject of Usenet possibly being shut-down in the U.K. (a recent rumor, unsubstantiated), this comment: " What you have to grasp is that USENET type networks and the whole structure of the law on publshing are fundamentally incompatiable. With USENT anyone can untracably distribute pornographic, libelous, blasphemous, copyright or even officially secret information. Now, which do you think HMG and, for that matter, the overwhealming majority of oridnary people in this country think is most

important. USENET or those laws?" [Malcolm McMahon, malcolm@geog.leeds.ac.uk, comp.org.eff.talk, 1994--08-26]

10.13.5. Will it succeed? Not completely, as e-mail, gopher, the Web, etc., still offers access. But the effects could reach most casual users, and certainly affect the structure as we know it today.

10.13.6. Will crypto help? Not directly--see above.

10.14. Emergency Regulations

10.14.1. Emergency Orders

- various NSDDs and the like
- "Seven Days in May" scenario

10.14.2. Legal, secrecy orders

- George Davida, U. oif Wisconsin, received letter in 1978 threatening a $10K per day fine
  - Carl Nicolai, PhasorPhone

- The NSA has confirmed that parts of the EES are patented, in secrecy, and that the patents will be made public and then used to stop competitors should the algorithm become known.

10.14.3. Can the FCC-type Requirements for "In the clear" broadcasting (or keys supplied to Feds) be a basis for similar legislation of private networks and private use of encryption?

- this would seem to be impractical, given the growth of cellular phones, wireless LANs, etc...can't very well mandate that corporations broadcast their internal communications in the clear!
- compression, packet-switching, and all kinds of other "distortions" of the data...requiring transmissions to be readable by government agencies would require providing the government with maps (of where the packets are going), with specific decompression algorithms, etc...very impractical

10.15. Patents and Copyrights

10.15.1. The web of patents

- what happens is that everyone doing anything substantive spends much of his time and money seeking patents
- patents are essential bargaining chips in dealing with others
  - e.g., DSS, Schnorr, RSADSI, etc.
  - e.g., Stefan Brands is seeking patents
  - Cylink suing...

10.15.2. Role of RSA, Patents, etc.

- Bidzos: "If you make money off RSA, we make money" is the simple rule

- but of course it goes beyond this, as even "free" uses may have to pay

- Overlapping patents being used (apparently) to extent the life of the portfolio
  - 4/28/97 The first of several P-K and RSA patents expires
    - U.S. Patent Number: 4200770
      - Title: Cryptographic Apparatus and Method
      - Inventors: Hellman, Diffie, Merkle
      - Assignee: Stanford University
      - Filed: September 6, 1977
      - Granted: April 29, 1980
      - [Expires: April 28, 1997]

- remember that any one of these several patents held by Public Key Partners (Stanford and M.I.T., with RSA Data Security the chief dispenser of licenses) can block an effort to bypass the others - though this may get fought out in court
  - 8/18/97 The second of several P-K and RSA patents expires
    - U.S. Patent Number: 4218582
      - Title: Public Key Cryptographic Apparatus and Method
      - Inventors: Hellman, Merkle

- Assignee: The Board of Trustees of the Leland Stanford Junior University - Filed: October 6, 1977 - Granted: August 19, 1980 - [Expires: August 18, 1997]
- this may be disputed because it describe algortihms in broad terms and used the knapsack algorithm as the chief example
  - 9/19/00 The main RSA patent expires
    - U.S. Patent Number: 4405829
      - Title: Cryptographic Communications System and Method
      - Inventors: Rivest, Shamir, Adleman
      - Assignee: Massachusetts Institute of Technology
      - Filed: December 14, 1977
      - Granted: September 20, 1983
      - [Expires: September 19, 2000]

10.15.3. Lawsuits against RSA patents

- several are brewing
  - Cylink is suing (strange rumors that NSA was involved)
  - Roger Schlafly

10.15.4. "What about the lawsuit filed by Cylink against RSA Data Security Inc.?"

- Very curious, considering they are both part of Public Key Partners, the consortium of Stanford, MIT, Cylink, and RSA Data Security Inc. (RSADSI)

    - the suit was filed in the summer of 1994

- One odd rumor I heard, from a reputable source, was that the NSA had asked PKP to do something (?) and that Cylink had agreed, but RSADSI had refused, helping to push the suit along
    - any links with the death threats against Bidzos?

10.15.5. "Can the patent system be used to block government use of patents for purposes we don't like?"

- Comes up especially in the context of S. Micali's patent on escrow techniques
- "Wouldn't matter. The government can't be enjoined from using a patent. The federal government, in the final analysis, can use any patent they want, without permission, and the only recourse of the patent owner is to sue for royalties in the Court of Claims." [Bill Larkins, talk.politics.crypto, 1994-07-14]

10.16. Practical Issues

10.16.1. "What if I tell the authorities I Forgot My Password?"

- (or key, or passphrase...you get the idea)
- This comes up repeatedly, but the answer remains murky

10.16.2. Civil vs. Criminal

- "This is a civil mattep, and the pights of ppivaay one haq in cpiminal mattepq

- tend to vaniqh in aivil litigation. The paptieq to a lawquit hate
    - tpemeldouq powepq to dopae the othep qide to peteal ildopmatiol peletalt
    - to the aaqe, <@pad Templetol, 4-1-94, aomp,opg,edd,tal

10.16.3. the law is essentially what the courts say it is

10.17. Free Speech is Under Assault

10.17.1. Censorship comes in many forms. Tort law, threats of grant or contract removal, all are limiting speech. (More reasons for anonymous speech, of course.)

10.17.2. Discussions of cryptography could be targets of future crackdowns. Sedition laws, conspiracy laws, RICO, etc. How long before speaking on these matters earns a warning letter from your university or your company? (It's the "big stick" of ultimate government action that spurs these university and company

policies. Apple fears being shut down for having "involvement" with a terrorist plot, Emory University fears being sued for millions of dollars for "conspiring" to degrade wimmin of color, etc.)

How long before "rec.guns" is no longer carried at many sites, as they fear having their universities or companies linked to discussions of "assault weapons" and "cop-killer bullets"? Prediction: Many companies and universities, under pressure from the Feds, will block groups in which encrypted files are posted. After all, if one encrypts, one must have something to hide, and that could expose the university to legal action from some group that feels aggrieved.

10.17.3. Free speech is under assault across the country. The tort system is being abused to stifle dissenting views (and lest you think I am only a capitalist, only a free marketeer, the use of "SLAPP suits"--"Strategic Lawsuits Against Public Participation"--by corporations or real estate developers to threaten those who dare to publicly speak against their projects is a travesty, a travesty that the courts have only recently begun to

correct).

We are becoming a nation of sheep, fearing the midnight raid, the knock on the door. We fear that if we tell a joke, someone will glare at us and threaten to sue us *and* our company! And so companies are adopting "speech codes" and other such baggage of the Orwell's totalitarian state. Political correctness is extending its tendrils into nearly every aspect of life in America.

10.18. Systems, Access, and the Law

10.18.1. Legal issues regarding access to systems

- Concerns: - access by minors to sexually explicit material + access from regions where access "should not be permitted"
  - export of crypto, for example
  - the Memphis access to California BBS
- Current approach: taking the promise of the accessor
  - "I will not export this outside the U.S. or Canada."
  - "I am of legal age to access this material."
- Possible future approaches:
  - Callbacks, to ensure accessor is from region stated
    - easy enough to bypass with cut-outs and remailers
  - "Credentials"
    - a la the US Postal Service's proposed ID card (and others)
    - cryptographically authenticated credentials
      - Chaum's credentials system (certainly better than many non-privacy-preserving credentials systems)

10.18.2.

one?"

- (This topic has significance a vis whether remailers carriers.)
- Common carriers are what the phone and package delivery services are. They are not held liable for the contents of phone calls, for the contents of packages (drugs,

pornography, etc.), or for illegal acts connected with their services. One of the deals is that common carriers not examine the insides of packages. Common carriers essentially agree to take all traffic that pays the fee and not to discriminate based on content. Thus, a phone service will not ask what the subject of a call is to be, or listen in, to decide whether to make the connection.

- Some say that to be a common carrier requires a willingness to work with law enforcement. That is, Federal Express is not responsible for contents of packages, but they have to cooperate in reasonable ways with law enforcement to open or track suspicious packages. Anybody have a cite for this? Is it true?
- Common carrier status is also cited for bookstores, which are not presumed to have read each and every one of the books they sell...so if somebody blows their hand off in a an experiment, the bookstore is not liable. (The author/publisher may be, but that's a?nt issue.)
- How does one become a common carrier? Not clear. One view is that a service should "behave like" a common carrier and then hope and pray that a court sees it that way.

- Are computer services common carriers? A topic of great interest.
  - "According to a discussion I had with Dave Lawrence (postmaster at UUNET, as well as moderator of news.admin.newgroups), UUNET is registered with the FCC as an "Enhanced Service Provider," which, according to Dave, amounts to similar protection as "Common Carrier." ("Common Carrier" seems to not be appropriate yet, since Congress is so behind the tech curve)." [L. Todd Masco, 1994-08-11] As for remailer networks totally unclear at this being treated as common carriers time. Certainly the fact that packets are fully encrypted and unreadabel goes to part of the issue about agreeing not to screen. More on the common carrier debate:

- "Ah, the eternal Common Carrier debate. The answer is the same as the last few times. "Common Carrier" status has little to do with exemption from liability. It has most to do with being unable to reject passengers, goods, or phone calls...Plenty of non-common carrier entities are immune from prosecution for ideas that they unkowingly communicate -- bookstores for example (unless they are *knowingly* porno bookstores in the wrong jurisdiction)...Compuserve was held not liable for an (alleged) libel by one of its sysops. Not because of common carrier but because they had no knowledge or control...Remailers have no knowledge or control hence no scienter (guilty knowledge) hence no liability as a matter of law---not a jury question BTW." [Duncan Frissell, 1994-08-11]

10.19. Credentials

10.19.1. "Are credentials needed? Will digital methods be used?"

10.19.2. I take a radical view. Ask yourself why credentials are *ever* needed. Maybe for driving a car, and the like, but in those cases anonymity is not needed, as the person is in the car, etc.

Credentials for drinking age? Why? Let the parents enforce this, as the argument goes about watching sex and violence on t.v. (If one accepts the logic of requiring bars to enforce children's behavior, then one is on a slippery slope toward requiring television set makers to check smartcards of viewers, or of requiring a license to access the Internet, etc.) In almost no cases do I see the need to carry "papers" with me. Maybe a driver's license, like I said. In other areas, why?

10.19.3. So Cypherpunks probably should not spend too much time worrying about how permission slips and "hall passes" will be handled. Little need for them.

10.19.4. "What about credentials for specific job performance, or for establishing time-based contracts?"

- Credentials that prove one has completed certain classes, or reached certain skill levels, etc.?
- In transactions where "future performance" is needed, as in a contract to have a house built, or to do some similar job, then of course the idea of on-line or immediate clearing is bogus...like paying a stranger a sum of money on his promise that he'll be back the next day to start building you a house. Parties to such long-term, non-locally-cleared cases may contract with an escrow agent, as I described above. This is like the "privately-produced law" we've discussed so many times. The essence: voluntary arrangements. Maybe proofs

of identity will be needed, or asked for, maybe not. But these are not the essence of the deal.

10.20. Escrow Agents

10.20.1. (the main discussion of this is under Crypto Anarchy)

10.20.2. 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.)

10.21. Loose Ends

10.21.1. Legality of trying to break crypto systems

- "What's the legality of breaking cyphers?"

- Suppose I find some random-looking bits and find a way to apparently decrease their entropy, perhaps turning them into the HBO or Playboy channel? What crime have I committed?
- "Theft of services" is what they'll get me for. Merely listening to broadcasts can now be a crime (cellular, police channels, satellite broadcasts). In my view, a chilling developemt, for practical reasons (enforcement means invasive monitoring) and for basic common sense ethics reasons: how can listening to what lands on your property be illegal?
- This also opens the door for laws banning listening to certain "outlaw" or "unlicensed" braodcast stations. Shades of the Iron Curtain. (I'm not talking about FCC licensing, per se.)

- "Could it ever be illegal to try to break an encryption scheme, even if the actual underlying data is not "stolen"?"
  - Criminalizing *tools* rather than actions

- The U.S. is moving in the direction of making mere possession of certain tools and methods illegal, rather than criminalizing actual actions. This has been the case--or so I hear, though I can't cite actual laws-- with "burglar tools." (Some dispute this, pointing to the sale of lockpicks, books on locksmithing, etc. Still, see what happens if you try to publish a detailed book on how to counterfeit currency.) - Black's law term for this?

- To some extent, it already is. Video encryption is this way. So is cellular.

- attendees returning from a Bahamas conference on pirate video methods (guess why it was in the Bahamas) had their papers and demo materials seized by Customs
  - Counterfeiting is, I think, in this situation, too. Merely exploring certain aspects is verboten. (I don't claim that all aspects are, of course.)
- Interception of broadcast signals may be illegal-satellite or cellular phone traffic (and Digital Telephony Act may further make such intercepts illegal and punishable in draconian ways)

- Outlawing of the breaking of encryption, a la the broadcast/scanner laws
  - (This came up in a thread with Steve Bellovin)
  - Aspects
- PPL side...hard to convince a PPL agent to "enforce" this

- but market sanctions against those who publically use the information are of course possible, just as with those who overhear conversations and then gossip widely (whereas the act of overhearing is hardly a crime)

- statutory enforcement leads to complacency, to below- par security
- is an unwelcome expansion of power of state to enforce laws against decryption of numbers
- and may lead to overall restrictions on crypto use

10.21.2. wais, gopher, WWW, and implications

- borders more transparent...not clear *where* searches are taking place, files being transferrred, etc. (well, it is deterministic, so some agent or program presumably knows, but it's likely that humans don't)

10.21.3. "Why are so many prominent Cypherpunks interested in the law?"

- Beats me. Nothing is more stultfyingly boring to me than the cruft and "found items" nature of the law.
- However,, for a certain breed of hacker, law hacking is the ultimate challenge. And it's important for some Cypherpunks goals.

10.21.4. "How will crypto be fought?"

- The usual suspects: porn, pedophilia, terrorists, tax evaders, spies
  - Claims that "national security" is at stake
- As someone has said, "National security is the root password to the Constitution"
  - claims of discrimination
- as but one example, crypto allows offshore bank accounts, a la carte insurance, etc...these are all things that will shake the social welfare systems of many nations

10.21.5. Stego may also be useful in providing board operators with "plausible deniabillity"--they can claim ignorance of

the LSB contents (I'm not saying this will stand up in court very well, but any port in a storm, especially port 25).

10.21.6. Can a message be proved to be encrypted, and with what key? .21.7. Legality of digital signatures and timestamps?

- Stu Haber confirms that this has not been tested, no precedents set

10.21.8. A legal issue about proving encryption exists

- The XOR point. Any message can be turned into any other message, with the proper XOR intermediate message. Implications for stego as well as for legal proof (difficulty of). As bits leave no fingerprints, the mere presence of a particular XOR pad on a defendant's disk is no proof that he put it there...the cops could have planted the incriminating key, which turns "gi6E2lf7DX01jT$" into "Dope is ready." (I see issues of "chain of evidence" becoming even more critical, perhaps with use of independent "timestamping authorities" to make hashes of seized evidence--hashes in the cryptographic sense and not hashes in the usual police sense.)

10.21.9. "What are the dangers of standardization and official sanctioning?"

- The U.S. has had a disturbing tendency to standardize on some technology and then punish deviations from the standard. Examples: telephones, cable (franchises granted, competitors excluded)
  - Franchises, standards...

- My concern: Digital money will be blessed...home banking, Microsoft, other banks, etc. The Treasury folks will sign on, etc.

- Competitors will have a hard time, as government throws roadblocks in front of them, as the U.S. makes international deals with other countries, etc.

10.21.10. Restrictions on voice encryption?

- may arise for an ironic reason: people can use Net connections to talk worldwide for $1 an hour or less, rather than $1 a minute; this may cause telcos to clamor for restrictions

- enforcing these restrictions then becomes problematic, unless channel is monitored
  - and if encrypted...

10.21.11. Fuzziness of laws

- It may seem surprising that a nation so enmeshed in complicated legalese as the U.S., with more lawyers per capita than any other large nation and with a legal code that consists of hundreds of thousands of pages of regulations and interpretations, is actually a nation with a legal code that is hard to pin down.
- Any system with formal, rigid rules can be "gamed against" be an adversary. The lawmakers know this, and so the laws are kept fuzzy enough to thwart mechanistic gaming; this doesn't stop there from being an army of lawyers (in fact, it guarantees it). Some would say that the laws are kept fuzzy to increase the power of lawmakers and regulators.
- "Bank regulations in this country are kept deliberately somewhat vague. The regulator's word is the deciding principle, not a detailed interpretation of statute. The lines are fuzzy, and because they are fuzzy, the banks don't press on them nearly as hard as when there's clear statutory language available to be interpreted in a court. "The uncertainty in the regulatory environment *increases* the hold the regulators have over the banks. And the regulators are known for being decidedly finicky. Their decisions are largely not subject to appeal (except for the flagrant stuff, which the regulators are smart enough not to do too often), and there's no protection against crosslinking issues. If a bank does something untoward in, say, mortgage banking, they may find, say, their interstate branching possibilities seem suddenly much dimmer. "The Dept. of Treasury doesn't want untraceable transactions." [Eric Hughes, Cypherpunks list, 1994-8-03]
- Attempts to sneak around the laws, especially in the context of alternative currencies, Perry Metzger notes: "They are simply trying to stop you from playing games. The law isn't like geometry -- there aren't axioms and rules for deriving one thing from another. The general principle is that they want to track all your transactions, and if you make it difficult they will either use existing law to jail you, or will produce a new law to try to do

the same." [Perry Metzger, 1994-08-10]

- This fuzziness and regulatory discretion is closely related to those wacky schemes to avoid taxes by claiming , for example, that the "dollar" is defined as 1/35th of an ounce of gold (and that hence one's earnings in "real dollars" are a tiny fraction of the ostensible earnings), that Ohio did not legally enter the Union and thus the income tax was never properly ratified,, etc. Lots of these theories have been tested--and rejected. I mention this because some Cypherpunks show signs of thinking "digital cash" offers similar opportunities. (And I expect to see similar scams.)
- (A related example. Can one's accumulation of money be taken out of the country? Depending on who you ask, "it depends." Taking it out in your suitcase rasises all kind of possibilies of seizure (violation of currency export

  laws, money laundering, etc.). Wiring it out may invoke

FinCEN triggers. The IRS may claim it is "capital flight" to avoid taxes--which it may well be. Basically, your own money is no longer yours. There may be ways to do this--I hope so--but the point remains that the rules are fuzzy, and the discretionary powers to seize assets are great. Seek competent counsel, and then pray.)

10.21.12. role of Uniform Commercial Code (UCC)

- not discussed in crypto circles much, but the "rules of the road"
- in many way, an implementation of anarcho-capitalism, in that the UCC is a descendant (modulo some details) of the "Law Merchant" that handled relations between sovereign powers, trade at sea, etc.
- things like electronic funds transfere, checks, liablities for forged sigs, etc.
  - I expect eventual UCC involvement in digital money schemes

10.21.13. "What about the rush to legislate, to pass laws about cyberspace, the information superduperhighway, etc.?

- The U.S. Congress feels it has to "do something" about things that many of us feel don't need regulation or "help" from Congress.
  - crypto legislation

- set-top boxes, cable access, National Information Infrastructure (Cable Version)
- information access, parental lock-outs, violence ratings, sexually explicit materials, etc.

- Related to the "do something!" mentality on National Health Care, guns, violence, etc.
  - Why not just not do anything?
  - Scary possibilities being talked about:

- giving television sets unique IDs ("V chips") with cable access through these chips

- tying national ID cards to these, e.g., Joe Citizen, of Provo, Utah, would be "allowed" to view an NC-17 violence-rated program
- This would be disastrous: records, surveillance, dossiers, permission, centralization
- The "how can we fix it?" mindset is very damaging. Many things just cannot be "fixed" by central planners...look at economies for an example. The same is usually true of technologies.

10.21.14. on use of offshore escrow agents as protection against seizures

- contempt laws come into play, but the idea is to make yourself powerless to alter the situation, and hence not willfully disobeying the court

- Can also tell offshore agents what to do with files, and when to release them
  - Eric Hughes proposes: "One solution to this is to give (or other access information) to someone it back to you if you are under duress, court order, etc. One would desire that in a jurisdiction other than where an investigation might happen." [E.H., 1994-07-26]

- Sandy Sandfort adds: "Prior to seizure/theft, you would make an arrangement with an offshore "escrow agent." After seizure you would send your computer the instruction that says, "encrypt my disk with the escrow agents public key." After that, only the escrow agent could decrypt your disk. Of course, the escrow agent would only do that when conditions you had stipulated were in effect." [S. S., 1994-07-27]
- related to data havens and offshore credit/P.I. havens

10.21.15. Can the FCC-type Requirements for "In the clear" broadcasting (or keys supplied to Feds) be a basis for similar legislation of private networks and private use of encryption?

- this would seem to be impractical, given the growth of cellular phones, wireless LANs, etc...can't very well mandate that corporations broadcast their internal communications in the clear!
- compression, packet-switching, and all kinds of other "distortions" of the data...requiring transmissions to be readable by government agencies would require providing the government with maps (of where the packets are going), with specific decompression algorithms, etc...very impractical

10.21.16. Things that could trigger a privacy flap or limitations on crypto

- Anonymously publishing adoption records [suggested by Brian Williams, 1994-08-22]
- nuclear weapons secrets (true secrets, not just the titillating stuff that any bright physics student can cobble together)
- repugant markets (assassinations, organ selling, etc.) .21.17. Pressures on civilians not to reveal crypto knowledge + Example: mobile phone crypto standards.
- "This was the official line until a few months ago - that A5 was strong and A5X a weakened export version...However, once we got hold of A5 we found that it was not particularly strong there is an easy 2Л40 attack. The government's line then changed to 'you mustn't discuss this in public because it would harm British export sales'...Perhaps it was all a ploy to get Saddam to buy A5 chips off some disreputable arms dealer type. [Ross Anderson, "mobil phone in europe , a precedence?," sci.crypt, 1994-08-15]
- Now this example comes from Britain, where the intelligence community has always had more lattitude than in the U.S. (an Official Secrets Act, limits on the press, no pesky Constitution to get in the way, and even more of an old boy's network than we have in the U.S. mil-industrial complex).
- And the threat by NSA officials to have Jim Bidzos, the president of RSA Data Security, Inc., killed if he didn't play ball. {"The Keys to the Kingdom," San Jose Mercury News]

10.21.18. "identity escrow", Eric Hughes, for restrictions on e-mail accounts and electronic PO boxes (has been talked about,

apparently...no details) .

Revision #1
Created 23 June 2022 03:53:13 by c0mmando
Updated 23 June 2022 03:53:35 by c0mmando