4. Goals and Ideology -- Privacy, Freedom, New Approaches

4.1. copyright

4.2. SUMMARY: Goals and Ideology -- Privacy, Freedom, New Approaches

4.2.1. Main Points

4.2.2. Connections to Other Sections

- Crypto Anarchy is the logical outgrowth of strong crypto.

4.2.3. Where to Find Additional Information

- Vernor Vinge's "True Names"
- David Friedman's "Machinery of Freedom"

4.2.4. Miscellaneous Comments

- Most of the list members are libertarians, or leaning in that direction, so the bias toward this is apparent.
- (If there's a coherent *non*-libertarian ideology, that's also consistent with supporting strong crypto, I'm not sure it's been presented.)

4.3. Why a Statement of Ideology?

4.3.1. This is perhaps a controversial area.

So why include it? The main reason is to provide some grounding for the later comments on many issues.

4.3.2. People should not expect a uniform ideology on this list.

Some of us are anarcho-capitalist radicals (or "crypto anarchists"), others of us are staid Republicans, and still others are Wobblies and other assored leftists.

4.4. "Welcome to Cypherpunks"

4.4.1. This is the message each new subscriber to the Cypherpunks lists gets

, by Eric Hughes:

4.4.2. "Cypherpunks assume privacy is a good thing

and wish there were more of it. Cypherpunks acknowledge that those who want privacy must create it for themselves and not expect governments, corporations, or other large, faceless organizations to grant them privacy out of beneficence. Cypherpunks know that people have been creating their own privacy for centuries with whispers, envelopes, closed doors, and couriers. Cypherpunks do not seek to prevent other people from speaking about their experiences or their opinions. "The most important means to the defense of privacy is encryption. To encrypt is to indicate the desire for privacy. But to encrypt with weak cryptography is to indicate not too much desire for privacy. Cypherpunks hope that all people desiring privacy will learn how best to defend it. "Cypherpunks are therefore devoted to cryptography. Cypherpunks wish to learn about it, to teach it, to implement it, and to make more of it. Cypherpunks know that cryptographic protocols make social structures. Cypherpunks know how to attack a system and how to defend it. Cypherpunks know just how hard it is to make good cryptosystems. "Cypherpunks love to practice. They love to play with public key cryptography. They love to play with anonymous and pseudonymous mail forwarding and delivery. They love to play with DC-nets. They love to play with secure communications of all kinds. "Cypherpunks write code. They know that someone has to write code to defend privacy, and since it's their privacy, they're going to write it. Cypherpunks publish their code so that their fellow cypherpunks may practice and play with it. Cypherpunks realize that security is not built in a day and are patient with incremental progress. "Cypherpunks don't care if you don't like the software they write. Cypherpunks know that software can't be destroyed. Cypherpunks know that a widely dispersed system can't be shut down. "Cypherpunks will make the networks safe for privacy." [Eric Hughes, 1993-07-21 version]

4.5. "Cypherpunks Write Code"

4.5.1. "Cypherpunks write code" is almost our mantra.

4.5.2. This has come to be a defining statement.

Eric Hughes used it to mean that Cypherpunks place more importance in actually changing things, in actually getting working code out, than in merely talking about how things "ought" to be.

- Eric Hughes statement needed here:
- Karl Kleinpaste, author of one of the early anonymous posting services (Charcoal) said this about some proposal made: "If you've got serious plans for how to implement such a thing, please implement it at least skeletally and deploy it. Proof by example, watching such a system in action, is far better than pontification about it." [Karl_Kleinpaste@cs.cmu.edu, news.admin.policy, 1994-06-30]

4.5.3. "The admonition, "Cypherpunks write code," should be taken metaphorically.

I think "to write code" means to take unilateral effective action as an individual. That may mean writing actual code, but it could also mean dumpster diving at Mycrotronx and anonymously releasing the recovered information. It could also mean creating an offshore digital bank. Don't get too literal on us here. What is important is that Cypherpunks take personal responsibility for empowering themselves against threats to privacy." [Sandy Sandfort, 1994-07-08]

4.5.4. A Cypherpunks outlook: taking the abstractions of academic conferences and making them concrete

- One thing Eric Hughes and I discussed at length (for 3 days of nearly nonstop talk, in May, 1992) was the glacial rate of progress in converting the cryptographic primitive operations of the academic crypto conferences into actual, workable code. The basic RSA algorithm was by then barely available, more than 15 years after invention. (This was before PGP 2.0, and PGP 1.0 was barely available and was disappointing, with RSA Data Security's various products in limited niches.) All the neat stuff on digital cash, DC- Nets, bit commitment, olivioius transfer, digital mixes, and so on, was completely absent, in terms of avialable code or "crypto ICs" (to borrow Brad Cox's phrase). If it took 10-15 years for RSA to really appear in the real world, how long would it take some of the exciting stuff to get out?
  - We thought it would be a neat idea to find ways to reify these things, to get actual running code. As it happened, PGP 2.0 appeared the week of our very first meeting, and both the Kleinpaste/Julf and Cypherpunks remailers were quick, if incomplete, implementations of David Chaum's 1981 "digital mixes." (Right on schedule, 11 years later.)
- Sadly, most of the abstractions of cryptology remain residents of academic space, with no (available) implementations in the real world. (To be sure, I suspect many people have

cobbled-together versions of many of these things, in C code, whatever. But their work is more like building sand castles, to be lost when they graduate or move on to other projects. This is of course not a problem unique to cryptology.)

- Today, various toolkits and libraries are under development. Henry Strickland (Strick) is working on a toolkit based on John Ousterhout's "TCL" system (for Unix), and of course RSADSI provides RSAREF. Pr0duct Cypher has "PGP Tools." Other projects are underway. (My own longterm interest here is in building objects which act as the cryptography papers would have them act...building block objects. For this, I'm looking at Smalltalk of some flavor.)
- It is still the case that most of the modern crypto papers discuss theoretical abstractions that are *not even close* to being implemented as reusable, robust objects or routines. Closing the gap between theoretical papers and practical realization is a major Cypherpunk emphasis.

4.5.5. Prototypes, even if fatally flawed, allow for evolutionary learning and improvement. Think of it as engineering in action.

4.6. Technological empowerment

4.6.1. (more needed here...)

4.6.2. As Sandy Sandfort notes, "The real point of Cypherpunks is that it's better to use strong crypto than weak crypto or no crypto at all.

Our use of crypto doesn't have to be totally bullet proof to be of value. Let *them* worry about the technicalities while we make sure they have to work harder and pay more for our encrypted info

than they would if it were in plaintext." [S.S. 1994-07-01]

4.7. Free Speech Issues

4.7.1. Speech

- "Public speech is not a series of public speeches, but rather one's own words spoken openly and without shame...I desire a society where all may speak freely about whatever topic they will. I desire that all people might be able to choose to whom they wish to speak and to whom they do not wish to speak. I desire a society where all people may have an assurance that their words are directed only at those to whom they wish. Therefore I oppose all efforts by governments to eavesdrop and to become unwanted listeners." [Eric Hughes, 1994-02-22]
- "The government has no right to restrict my use of cryptography in any way. They may not forbid me to use whatever ciphers I may like, nor may they require me to use any that I do not like." [Eric Hughes, 1993-06-01]

4.7.2. "Should there be *any* limits whatsoever on a person's use of cryptography?"

- No. Using the mathematics of cryptography is merely the manipulation of symbols. No crime is involved, ipso facto.
- Also, as Eric Hughes has pointed out, this is another of those questions where the normative "should" or "shouldn't" invokes "the policeman inside." A better way to look at is to see what steps people can take to make any question of "should" this be allowed just moot.
- The "crimes" are actual physical acts like murder and kidnapping. The fact that crypto may be used by plotters and planners, thus making detection more difficult, is in no way different from the possibility that plotters may speak in an unusual language to each other (ciphers), or meet in a private home (security), or speak in a soft voice when in public (steganography). None of these things should be illegal, and *none of them would be enforceable* except in the most rigid of police states (and probably not even there).
- "Crypto is thoughtcrime" is the effect of restricting cryptography use.

4.7.3. Democracy and censorship

- Does a community have the right to decide what newsgroups or magazines it allows in its community? Does a nation have the right to do the same? (Tennessee, Iraq, Iran, France. Utah?)
- This is what bypasses with crypto are all about: taking these majoritarian morality decisions out of the hands of the bluenoses. Direct action to secure freedoms.

4.8. Privacy Issues

4.8.1. "Is there an agenda here beyond just ensuring privacy?"

- Definitely! I think I can safely say that for nearly all political persuasions on the Cypherpunks list. Left, right, libertarian, or anarchist, there's much more to to strong crypto than simple privacy. Privacy qua privacy is fairly uninteresting. If all one wants is privacy, one can simply keep to one's self, stay off high-visibility lists like this, and generally stay out of trouble.
- Many of us see strong crypto as the key enabling technology for a new economic and social system, a system which will develop as cyberspace becomes more important. A system which dispenses with national boundaries, which is based on voluntary (even if anonymous) free trade. At issue is the end of governments as we know them today. (Look at interactions on the Net--on this list, for example--and you'll see many so-called nationalities, voluntary interaction, and the almost complete absence of any "laws." Aside from their being almost no rules per se for the Cypherpunks list, there are essentially no national laws that are invokable in any way. This is a fast-growing trend.)
  - Motivations for Cypherpunks
- Privacy. If maintaining privacy is the main goal, there's not much more to say. Keep a low profile, protect data, avoid giving out personal information, limit the number of bank loans and credit applications, pay cash often, etc.
  - Privacy in activism.

- New Structures. Using cryptographic constructs to build new political, economic, and even social structures.

- Political: Voting, polling, information access, whistleblowing
- Economic: Free markets, information markets, increased liquidity, black markets - Social: Cyberspatial communities, True Names
- Publically inspectable algorithms always win out over private, secret algorithms

4.8.2. "What is the American attitude toward privacy and encryption?"

- There are two distinct (and perhaps simultaneously held) views that have long been found in the American psyche:

- "A man's home is his castle." "Mind your own business." The frontier and Calvinist sprit of keeping one's business to one's self.
- "What have you got to hide?" The nosiness of busybodies, gossiping about what others are doing, and being suspicious of those who try too hard to hide what they are doing.

- The American attitude currently seems to favor privacy over police powers, as evidenced by a Time-CNN poll:

- "In a Time/CNN poll of 1,000 Americans conducted last week by Yankelovich Partners, two-thirds said it was more important to protect the privacy of phone calls than to preserve the ability of police to conduct wiretaps. When informed about the Clipper Chip, 80% said they opposed it." [Philip Elmer-Dewitt, "Who Should Keep the Keys," *TIME*, 1994-03-04.]
- The answer given is clearly a function of how the question is phrased. Ask folks if they favor "unbreakable encryption" or "fortress capabilities" for terrorists, pedophiles, and other malefactors, and they'll likely give a quite different answer. It is this tack now being taken by the Clipper folks. Watch out for this!
  - Me, I have no doubts.
- As Perry Metzger puts it, "I find the recent disclosures concerning U.S. Government testing of the effects of radiation on unknowing human subjects to be yet more evidence that you simply cannot trust the government with your own personal safety. Some people, given positions of power, will naturally abuse those positions, often even if such abuse could cause severe injury or death. I see little reason, therefore, to simply "trust" the U.S. government -and given that the U.S. government is about as good as they get, its obvious that NO government deserves the blind trust of its citizens. "Trust us, we will protect you" rings quite hollow in the face of historical evidence. Citizens must protect and preserve their own privacy -- the government and its centralized cryptographic schemes emphatically cannot be trusted." [P.M., 1994-01-01]

4.8.3. "How is 1994 like 1984?"

- The television ad for Clipper: "Clipper--why 1994 *will* be like 1984"
  - As Mike Ingle puts it:
- 1994: Wiretapping is privacy Secrecy is openness Obscurity is security

4.8.4. "We anticipate that computer networks will play a more and more important role in many parts of our lives.

But this increased computerization brings tremendous dangers for infringing privacy. Cypherpunks seek to put into place structures which will allow people to preserve their privacy if they choose. No one will be forced to use pseudonyms or post anonymously. But it should be a matter of choice how much information a person chooses to reveal about himself when he communicates. Right now, the nets don't give you that much choice. We are trying to give this power to people." [Hal Finney, 1993-02-23]

4.8.5. "If cypherpunks contribute nothing else we can create a real privacy advocacy group,

advocating means of real selfempowerment, from crypto to nom de guerre credit cards, instead of advocating further invasions of our privacy as the so-called privacy advocates are now doing!" [Jim Hart, 199409-08]

4.9. Education Issues

4.9.1. "How can we get more people to use crypto?"

- telling them about the themes of Cypherpunks
- surveillance, wiretapping, Digital Telephony, Clipper, NSA, FinCEN, etc...these things tend to scare a lot of folks
- making PGP easier to use, better integration with mailers, etc.
- (To be frank, convincing others to protect themselves is not one of my highest priorities. Then why have I written this megabyte-plus FAQ? Good question. Getting more users is a general win, for obvious reasons.)

4.9.2. "Who needs to encrypt?"

- Corporations
  - competitors...fax transmissions
  - foreign governments
    - Chobetsu, GCHQ, SDECE, Mossad, KGB
  - their own government
    - NSA intercepts of plans, investments
- Activist Groups

- Aryan Nation needs to encrypt, as FBI has announced their intent to infiltrate and subvert this group
  - RU-486 networks
  - Amnesty International
  - Terrorists and Drug Dealers
- clearly are clueless at times (Pablo Escobar using a cellphone!)
  - Triads, Russian Mafia, many are becoming crypto-literate
  - (I've been appoached-'nuff said)
  - Doctors, lawyers, psychiatrists, etc.
- to preserve records against theft, snooping, casual examination, etc.
- in many cases, a legal obligation has been attached to this (notably, medical records)
- the curious situation that many people are essentially *required* to encrypt (no other way to ensure standards are met) and yet various laws exists to limit encryption...ITAR, Clipper, EES
  - (Clipper is a partial answer, if unsatisfactory)

4.9.3. "When should crypto be used?"

- It's an economic matter. Each person has to decide when to use it, and how. Me, I dislike having to download messages to my home machine before I can read them. Others use it routinely.

4.10. Libertarian Issues

4.10.1. A technological approach to freedom and privacy:

- "Freedom is, practically, given as much (or more) by the tools we can build to protect it, as it is by our ability to convince others who violently disagree with us not to attack us. On the Internet we have tools like anon remailers and PGP that give us a great deal of freedom from coercion even in the midst of censors. Thus, these tools piss off fans of centralized information control, the defenders of the status quo, like nothing else on the Internet." [an50@desert.hacktic.nl (Nobody), libtech- l@netcom.com, 1994-06-08]
    - Duncan Frissell, as usual, put it cogently:
- "If I withhold my capital from some country or enterprise I am not threatening to kill anyone. When a "Democratic State" decides to do something, it does so with armed men. If you don't obey, they tend to shoot...[I]f technological change enhances the powers of individuals, their power is enhanced no matter what the government does. "If the collective is weakened and the individual strengthened by the fact that I have the power of cheap guns, cars, computers, telecoms, and crypto then the collective has been weakened and we should ease the transition to a society based on voluntary rather than coerced interaction. "Unless you can figure out a new, improved way of controlling others; you have no choice." [D.F., Decline and Fall, 1994-06-19]

4.10.2. "They that can give up essential liberty to obtain a little temporary safety deserve neither liberty nor safety."

[Benjamin Franklin]

4.10.3. a typical view of government

- "As I see it, it's always a home for bullies masquerading as a collective defense. Sometimes it actually it actually has to perform its advertised defense function. Like naked quarks, purely defensive governments cannot exist. They are bipolar by nature, with some poles (i.e., the bullying part) being "more equal than others." [Sandy Sandfort, 199409-06]

4.10.4. Sadly, several of our speculative scenarios for various laws have come to pass. Even several of my own, such as:

- "(Yet Another May Prediction Realized)...The text of a "digital stalking bill" was just sent to Cyberia-l." [L. Todd Masco, 1994-08-31] (This was a joking prediction I made that "digital stalking" would soon be a crime; there had been news articles about the horrors of such cyberspatial stalkings, regardless of there being no real physical threats, so this move is not all that surprising. Not surprising in an age when free speech gets outlawed as "assault speech.")

4.10.5. "Don't tread on me."

4.10.6. However, it's easy to get too negative on the situation,

to assume that a socialist state is right around the corner. Or that a new Hitler will come to power. These are unlikely developments, and not only because of strong crypto. Financial markets are putting constraints on how fascist a government can get...the international bond markets, for example, will quickly react to signs like this. (This is the theory, at least.)

4.10.7. Locality of reference, cash, TANSTAAFL, privacy

- closure, local computation, local benefits
- no accounting system needed
- markets clear
- market distortions like rationing, coupons, quotas, all require centralized record-keeping
- anything that ties economic transactions to identity (rationing, entitlements, insurance) implies identitytracking, credentials, etc.

- Nonlocality also dramatically increases the opportunities for fraud, for scams and con jobs

- because something is being promised for future delivery (the essence of many scams) and is not verifiable locally
  - because "trust" is invoked
- Locality also fixes the "policeman inside" problem: the costs of decisions are borne by the decider, not by others.

4.11. Crypto Anarchy

4.11.1. The Crypto Anarchy Principle:

Strong crypto permits unbreakable encrypion, unforgeable signatures, untraceable electronic messages, and unlinkable pseudonomous identities. This ensures that some transactions and communications can be entered into only voluntarily. External force, law, and regulation cannot be applied. This is "anarchy," in the sense of no outside rulers and laws. Voluntary arrangements, backstopped by voluntarily-arranged institutions like escrow services, will be the only form of rule. This is "crypto anarchy."

4.11.2. crypto allows a return to contracts that governments cannot breach

- based on reputation, repeat business
- example: ordering illegal material untraceably and anonymously,,,governments are powerless to do anything
- private spaces, with the privacy enforced via cryptographic permissions (access credentials)
  - escrows (bonds)

4.11.3. Technological solutions over legalistic regulations

- Marc Ringuette summarized things nicely:

- "What we're after is some "community standards" for cyberspace, and what I'm suggesting is the fairly libertarian standard that goes like this: " Prefer technological solutions and self-protection solutions over rule-making, where they are feasible. "This is based on the notion that the more rules there are, the more people will call for the "net police" to enforce them. If we can encourage community standards which emphasize a prudent level of self-protection, then we'll be able to make do with fewer rules and a less intrusive level of policing."[Marc Ringuette, 1993-03-14]

- Hal Finney has made cogent arguments as to why we should not become too complacent about the role of technology visa-vis politics. He warns us not to grow to confident:

- "Fundamentally, I believe we will have the kind of society that most people want. If we want freedom and privacy, we must persuade others that these are worth having. There are no shortcuts. Withdrawing into technology is like pulling the blankets over your head. It feels good for a while, until reality catches up. The next Clipper or Digital Telephony proposal will provide a rude awakening." [Hal Finney, POLI: Politics vs Technology, 1994-

01-02]

- "The idea here is that the ultimate solution to the low signal-to-noise ratio on the nets is not a matter of forcing people to "stand behind their words". People can stand behind all kinds of idiotic ideas. Rather, there will need to be developed better systems for filtering news and mail, for developing "digital reputations" which can be stamped on one's postings to pass through these smart filters, and even applying these reputations to pseudonyms. In such a system, the fact that someone is posting or mailing pseudonymously is not a problem, since nuisance posters won't be able to get through." [Hal Finney, 199302-23]

4.11.4. Reputations

4.11.5. I have a moral outlook

that many will find unacceptable or repugnant. To cut to the chase: I support the killing of those who break contracts, who steal in serious enough ways, and who otherwise commit what I think of as crimes.

- I don't mean this abstractly. Here's an example:

- Someone is carrying drugs. He knows what he's involved in. He knows that theft is punishable by death. And yet he steals some of the merchandise.
- Dealers understand that they cannot tolerate this, that an example must be made, else all of their employees will steal.
- Understand that I'm not talking about the state doing the killing, nor would I do the killing. I'm just saying such things are the natural enforcement mechanism for such markets. Realpolitik.
- (A meta point: the drug laws makes things this way. Legalize all drugs and the businesses would be more like "ordinary" businesses.)
- In my highly personal opinion, many people, including most Congressrodents, have committed crimes that earn them the death penalty; I will not be sorry to see anonymous assassination markets used to deal with them.

4.11.6. Increased espionage

will help to destroy nation-state-empires like the U.S., which has gotten far too bloated and far too dependent on throwing its weight around; nuclear "terrorism" may knock out a few cities, but this may be a small price to pay to undermine totally the socialist welfare states that have launched so many wars this century.

4.12. Loose Ends

4.12.1. "Why take a "no compromise" stance?"

- Compromise often ends up in the death of a thousand cuts. Better to just take a rejectionist stance.
- The National Rifle Association (NRA) learned this lesson the hard way. EFF may eventually learn it; right now they appear to be in the "coopted by the power center" mode, luxuriating in their inside-the-Beltway access to the Veep, their flights on Air Force One, and their general schmoozing with the movers and shakers...getting along by going along.
- Let's not compromise on basic issues. Treat censorship as a problem to be routed around (as John Gilmore suggests), not as something that needs to be compromised on. (This is directed at rumblings about how the Net needs to "police itself," by the "reasonable" censorship of offensive posts, by the "moderation" of newsgroups, etc. What should concern us is the accomodation of this view by well-meaning civil liberties groups, which are apparently willing to play a role in this "self-policing" system. No thanks.)
- (And since people often misunderstand this point, I'm not saying private companies can't set whatever policies they wish, that moderated newsgroups can't be formed, etc. Private arrangements are just that. The issue is when censorship is forced on those who have no other obligations. Government usually does this, often aided and abetted by corporations and lobbying groups. This is what we need to fight. Fight by routing around, via technology.)

4.12.2. The inherent evils of democracy

- To be blunt about it, I've come to despise the modern version of democracy we have. Every issue is framed in terms of popular sentiment, in terms of how the public would vote. Mob rule at its worst.
- Should people be allowed to wear blue jeans? Put it to a vote. Can employers have a policy on blue jeans? Pass a law. Should health care be provided to all? Put it to a vote. And so on, whittling away basic freedoms and rights. A travesty. The tyranny of the majority.
- De Toqueville warned of this when he said that the American experiment in democracy would last only until citizens discovered they could pick the pockets of their neighbors at the ballot box.
- But maybe we can stop this nonsense. I support strong crypto (and its eventual form, crypto anarchy) because it undermines this form of democracy. It takes some (and perhaps many) transactions out of the realm of popularity contests, beyond the reach of will of the herd. (No, I am not arguing there will be a complete phase change. As the

saying goes, "You can't eat cyberspace." But a lot of consulting, technical work, programming, etc., can in fact be done with crypto anarchic methods, with the money gained transferred in a variety of ways into the "real world." More on this elsewhere.)

- Crypto anarchy effectively allows people to pick and choose which laws they support, at least in cyberspatial contexts. It empowers people to break the local bonds of their majoritarian normative systems and decide for themselves which laws are moral and which are bullshit.

- I happen to have faith that most people will settle on a relatively small number of laws that they'll (mostly) support, a kind of Schelling point in legal space.

4.12.3. "Is the Cypherpunks agenda *too extreme*?"

- Bear in mind that most of the "Cypherpunks agenda," to the extent we can identify it, is likely to provoke ordinary citizens into *outrage*. Talk of anonymous mail, digital money, money laundering, information markets, data havens, undermining authority, transnationalism, and all the rest (insert your favorite idea) is not exactly mainstream.

4.12.4. "Crypto Anarchy sounds too wild for me."

- I accept that many people will find the implications of crypto anarchy (which follows in turn from the existence of strong cryptography, via the Crypto Anarchy Principle) to be more than they can accept.
- This is OK (not that you need my OK!). The house of Cypherpunks has many rooms.

Revision #1
Created 23 June 2022 03:41:33 by c0mmando
Updated 23 June 2022 03:41:58 by c0mmando