

Libertaria in Cyberspace

Cyberspace more hospitable to ideas of liberty and crypto anarchy

Timothy C. May

September 1st, 1992

Here are a few points about why "cyberspace," or a computer-mediated network, is more hospitable than physical locations for the kind of "crypto anarchy" libertarian system I've been describing.

Several folks have commented recently about ocean-going libertarian havens, supertankers used as data havens, and so forth. In the 1970s, especially, there were several unsuccessful attempts to acquire islands in the Pacific for the site of what some called "Libertaria." (Some keywords: Vanuatu, Minerva, Mike Oliver, Tonga)

Obtaining an entire island is problematic. Getting the consent of the residents is one issue (familiar to those on this list who weathered the Hurricane Andrew diversion debate). Being _allowed_ to operate by the leading world powers is another...the U.S. has enforced trade embargoes and blockades against many nations in the past several decades, including Cuba, North Korea, Libya, Iran, Iraq, and others. Further, the U.S. has invaded some countries—Panama is a good example—whose government it disliked. How long would a supertanker "data haven" or libertarian regime last in such an environment? (Stephenson's fascinating *Snow Crash* didn't address the issue of why the "Raft" wasn't simply sunk by the remaining military forces.)

I should note that the recent splintering of countries may provide opportunities for libertarian (or PPL, if you prefer to think of it in this way) regions. Some have speculated that Russia itself is a candidate, given that it has little vested in the previous system and may be willing to abandon statism. If several dozen new countries are formed, some opportunities exist..

The basic problem is that *physical space* is too small, too exposed to the view of others. "Libertaria" in the form of, say, an island, is too exposed to the retaliation of world powers. (I won't go into the "private nukes" strategy, which I need to think about further.)

A floating private nation (or whatever it's called) is too vulnerable to a single well-placed torpedo. Even if it serves as a kind of Swiss bank, and thus gets some of the same protection Switzerland got (to wit, many leaders kept their loot there), it is too vulnerable to a single attacker or invader. Piracy will be just one of the problems.

Finally, how many of us want to move to a South Pacific island? Or a North Sea oil rig? Or even to Russia?

Cyberspace looks more promising. There is more "space" in cyberspace, thus allowing more security and more colonizable space. And this space is coterminous with our physical space,

accessible with proper terminals from any place in the world (though there may be attempts in physical space to block access, to restrict access to necessary cryptographic methods, etc.).

I won't go into the various cryptographic methods here (see my earlier posting on the "Dining Cryptographers" protocol and various other postings on public key systems, digital mixes, electronic cash, etc.). Interested readers have many sources. (I have just read a superb survey of these new techniques, the 1992 Ph.D. thesis of Jurgen Bos, "Practical Privacy," which deals with these various protocols in a nice little book.)

Alice and Bob, our favorite cryptographic stand-ins, can communicate and transact business without ever meeting or even knowing who the other is. This can be extended to create virtual communities subject only to rules they themselves reach agreement on, much like this very Extropians list. Private law is the only law, as there is no appeal to some higher authority like the Pope or police. (This is why I said in several of my potings on the Hurricane Andrew debate that I am sympathetic to the PPL view.)

And this is the most compelling advantage of "Crypto Libertaria": an arbitrarily large number of separate "nations" can simultaneously exist. This allows for rapid experimentation, self-selection, and evolution. If folks get tired of some virtual community, they can leave. The cryptographic aspects mean their membership in some community is unknown to others (vis-a-vis the physical or outside world, i.e., their "true names") and physical coercion is reduced.

Communalists are free to create a communal environment, Creative Anachronists are free to create their own idea of a space, and so on. I'm not even getting into the virtual reality-photorealistic images-Jaron Lanier sort of thing, as even current text-based systems are demonstrably enough to allow the kind of virtual communities I'm describing here (and described in Vinge's "True Names," in Gibson's Neuromancer, in Sterling's Islands in the Net, and in Stephenson's Snow Crash...though all of them missed out on some of the most exciting aspects...perhaps my novel will hit the mark?).

But will the government allow these sorts of things? Won't they just torpedo it, just as they'd torpedo an offshore oorig data haven?

The key is that distributed systems have no nexus which can be knocked out. Neither Usenet nor FidoNet can be disabled by any single government, as they are worldwide. Shutting them down would mean banning computer-to-computer communication. And despite the talk of mandatory "trap doors" in encryption systems, encryption is fundamentally easy to do and hard to detect. (For those who doubt this, let me describe a simple system I posted to sci.crypt several years ago. An ordinary digital audio tape (DAT) carries more than a gigabyte of data. This means that the least significant bit (LSB) of an audio DAT recording carries about 8 megabytes of data! So Alice is stopped by the Data Police. They ask if she's carrying illegal data. She smiles innocently and say "No. I know you'll search me." They find her Sony DATman and ask about her collection of tapes and live recordings. Alice is carrying 80 MB of data—about 3 entire days worth of Usenet feeds!—on each and every tape. The data are stored in the LSBs, completely indistinguishable from microphone and quantization noise...unless you know the key. Similar methods allow data to be undetectably packed into LSBs of the PICT and GIF pictures now flooding the Net, into sampled sounds, and even into messages like this...the "whitespace" on the right margin of this message carries a hidden message readable only to a few chosen Extropians.)

I've already described using religions and role-playing games as a kind of legal cover for the development and deployment of these techniques. If a church decides to offer "digital confession-

als” for its far-flung members, by what argument will the U.S. government justify insisting that encryption not be used? (I should note that psychiatrists and similar professionals have a responsibility to their clients and to their licensing agencies to ensure the privacy of patient records. Friends of mine are using encryption to protect patient records. This is just one little example of how encryption is getting woven into the fabric of our electronic society. There are many other examples.)

In future discussions, I hope we can hit on some of the many approaches to deploying these methods. I’ve spent several years thinking about this, but I’ve surely missed some good ideas. The “crypto anarchy game” being planned is an attempt to get some of the best hackers in the Bay Area thinking along these lines and thinking of new wrinkles. Several have already offered to help further.

Some have commented that this list is not an appropriate place to discuss these ideas. I think it is. We are not discussing anything that is actually illegal, even under the broad powers of RICO (Racketeer-Influenced and Corrupt Organizations Act, used to go after “conspiracies” of porn dealers and gun dealers, amongst others). What we are discussing are long-range implications of these ideas.

In conclusion, it will be easier to form certain types of libertarian societies in cyberspace than in the real world of nations and physical locations. The electronic world is by no means complete, as we will still live much of our lives in the physical world. But economic activity is sharply increasing in the Net domain and these “crypto anarchy” ideas will further erode the power of physical states to tax and coerce residents.

Libertaria will thrive in cyberspace.

-Tim May

The Anarchist Library (Mirror)
Anti-Copyright



Timothy C. May
Libertaria in Cyberspace
Cyberspace more hospitable to ideas of liberty and crypto anarchy
September 1st, 1992

<https://www.activism.net/cypherpunk/libertaria.html>

usa.anarchistlibraries.net