Cypherpunk rising : WikiLeaks, encryption and the coming surveillance dystopia

R. U. Sirius
7 March 2013

In 1989, when the internet was predominantly ASCII-based and HyperCard had yet to give birth (or at least act as a midwife) to the world wide web, R.U. Sirius launched *Mondo 2000*. "I'd say it was arguably the representative underground magazine of its pre-web day", William Gibson said in a recent interview. "Posterity, looking at this, should also consider *Mondo 2000* as a focus of something that was happening".

Twenty years ago, it was cypherpunk that was happening.

And it's happening again today.

Early cypherpunk in fact and fiction

Flashback : Berkeley, California 1992. I pick up the ringing phone. My writing partner, St. Jude Milhon, is shouting down the line : "I've got it ! Cypherpunk !"

Jude was an excitable girl and she was particularly excitable when there was a new boyfriend involved. She'd been raving about Eric Hughes for days. I paid no attention.

At the time, Jude and I were contracted to write a novel titled *How to Mutate and Take Over the World*. I wanted the fiction to contain the truth. I wanted to tell people how creative hackers could do it - mutate and take over the world - by the end of the decade. Not knowing many of those details ourselves, we threw down a challenge on various hacker boards and in the places where extropians gathered to share their superhuman fantasies. "Take on a character", we said, "and let that character mutate and/or take over". The results were vague and unsatisfying. These early transhumanists didn't actually know how to mutate, and the hackers couldn't actually take over the world. It seemed that we were asking for too much too soon.

And so I wound up there, holding the phone away from my ear as Jude shouted out the solution, at least to the "taking over" part of our problem. Strong encryption, she explained, will sever all the ties binding us to hostile states and other institutions. Encryption will level the playing field, protecting even the least of us from government interference. It will liberate pretty much everything, *toute de suite*. The cypherpunks would make this happen.

For Jude, cypherpunk was both an exciting new vision for social change and a fun subculture dedicated to making it happen. Sure, I was skeptical. But I was also desperate for something to hang the plot of our book on. A few days later I found myself at the feet of Eric Hughes - who, along with John Gilmore and Tim May, is considered one of the founders of the cypherpunk movement - getting the total download.

This was my first exposure to The Crypto Anarchist Manifesto. Written by Tim May, it opens by mimicking *The Communist Manifesto*

: "a specter is haunting the modern world, the specter of crypto anarchy". In a fit of hyperbole that perfectly foreshadowed the mood of tech culture in the 1990s - from my own *Mondo 2000* to the "long boom" of digital capitalism - May declared that encrypted communication and anonymity online would "alter completely the nature of government regulation, the ability to tax and control economic interactions, the ability to keep information secret". The result would be nothing less than "both a social and economic revolution".

> Just as a seemingly minor invention like barbed wire made possible the fencing-off of vast ranches and farms, thus altering forever the concepts of land and property rights in the frontier West, so too will the seemingly minor discovery out of an arcane branch of mathematics come to be the wire clippers which dismantle the barbed wire around intellectual property.

Those words were written way back in 1988. By 1993, a bunch of crypto freaks were gathering fairly regularly in the San Francisco Bay Area. In his lengthy *Wired* cover story, Steven Levy would describe them as mostly "having beards and long hair - like Smith Brothers [cough drops] gone digital". Their antics would become legendary.

John Gilmore set off a firestorm by sharing classified documents on cryptography that a friend of his had found in public libraries (they had previously been declassified). The NSA threatened Gilmore with a charge of violating the Espionage Act, but after he responded with publicity and his own legal threats, the NSA - probably recognizing in Gilmore a well-connected dissident who they couldn't intimidate - backed down and once again declassified the documents.

Phil Zimmermann's PGP (Pretty Good Privacy) software was being circulated largely thanks to cypherpunk enthusiasts. According to Tim May's *Cyphernomicon*, PGP was "the most important crypto tool" available at the time, "having single-handedly spread public key methods around the world". It was available free of charge for non-commercial users, and complete source code was included with all copies. Most importantly, May wrote, "almost no understanding of how PGP works in detail is needed", so anyone could use its encryption to securely send data over the net.

In April 1993, the Clinton administration announced its encryption policy initiative. The Clipper Chip was an NSA-developed encryption chipset for "secure" voice communication (the government would have a key for every chip manufactured). "Not to worry", Phil Zimmermann cuttingly wrote in an essay about PGP. "The government promises that they will use these keys to read your traffic only 'when duly authorized by law". Not that anyone believed the promises. "To make Clipper completely effective", Zimmermann continued, "the next logical step would be to outlaw other forms of cryptography". This threat brought cypherpunks to the oppositional front lines in one of the early struggles over Internet rights, eventually defeating government plans.

John Gilmore summed up the accomplishments of the cypherpunks in a recent email : "we did reshape the world", he wrote. "We broke encryption loose from government control in the commercial and free software world, in a big way. We built solid encryption and both circumvented and changed the corrupt US legal regime so that strong encryption could be developed by anyone worldwide and deployed by anyone worldwide", including WikiLeaks.

As the 1990s rolled forward, many cypherpunks went to work for the man, bringing strong crypto to financial services and banks (on the whole, probably better than the alternative). Still, crypto-activism continued and the cypherpunk mailing list blossomed as an exchange for both practical encryption data and spirited, sometimes-gleeful argumentation, before finally peaking in 1997. This was when cypherpunk's mindshare seemed to recede, possibly in proportion to the utopian effervescence of the early cyberculture. But the cypherpunk meme may now be finding a sort of rebirth in one of the biggest and most important stories in the fledgeling 21st

century.

I am annoyed

Flashback : 1995. Julian Assange's first words on the cypherpunk email list : "I am annoyed".

Of course, Julian Assange has gone on to annoy powerful players all over the world as the legendary fugitive editor-in-chief and spokesperson for WikiLeaks, publisher of secret information, news leaks, and classified media from anonymous sources. And while the mass media world has tracked nearly every aspect of Assange's personal drama, it's done very little to increase people's understanding of WikiLeaks' underlying technologies or the principles those technologies embody.

In the recent book *Cypherpunks: Freedom and the Future of the Internet*, Assange enlists the help of three fellow heroes of free information to set the record straight, aligning those principles with the ideas that Tim May dreamed up in 1989 with "The Crypto Anarchist Manifesto".

The book is based on a series of conversations filmed for the television show *The World Tomorrow* while Assange was on house arrest in Norfolk, England during all of 2011. Attending were Jacob Appelbaum, the American advocate and researcher for the Tor project who has been in the sights of US authorities since substituting as a speaker for Assange at a US hackers conference; Andy Müller-Maguhn, one of the earliest members of the legendary Chaos Computer Club; and Jérémie Zimmerman, a French advocate for internet anonymity and freedom.

The conversation is sobering. If 1990s cypherpunk, like the broader tech culture that it was immersed in, was a little bit giddy with its potential to change the world, contemporary cypherpunk finds itself on the verge of what Assange calls "a postmodern surveillance dystopia, from which escape for all but the most skilled individuals will be impossible".

How did we get here ? The obvious political answer is 9/11. The event provided an opportunity for a vast expansion of national security states both here and abroad, including, of course, a diminution of protections against surveillance. The legalities involved in the US are a confusing and ever-shifting set of rules that are under constant legal contestation in the courts. Whatever the letter of the law, a September 2012 ACLU bulletin gave us the essence of the situation :

> Justice Department documents released today by the ACLU reveal that federal law enforcement agencies are increasingly monitoring Americans' electronic communications, and doing so without warrants, sufficient oversight, or meaningful accountability.
>
> The documents, handed over by the government only after months of litigation, are the attorney general's 2010 and 2011 reports on the use of "pen register" and "trap and trace" surveillance powers. The reports show a dramatic increase in the use of these surveillance tools, which are used to gather information about telephone, email, and other Internet communications. The revelations underscore the importance of regulating and overseeing the government's surveillance power.

"In fact", the report continues, "more people were subjected to pen register and trap and trace surveillance in the past two years than in the entire previous decade".

Beyond the political and legal powers vested in the US intelligence community and in others around the world, there is the very real fact that technology once only accessible to the world's superpowers is now commercially available. One example documented on WikiLeaks (and discussed in *Cypherpunks*) is the Zebra strategic surveillance system sold by VASTech. For $10 million, the South African company will sell you a turnkey system that can intercept all communications in a middle-sized country. A similar system called Eagle was used in Gadhafi's Libya, as first reported by *The Wall Street Journal* in 2011. Sold by the French company Amesys, this is a commercial product, right down to the label on the box : "Nationwide Intercept System". In the face of systems designed to scoop up all electronic communication and store it indefinitely, any showcase civil libertarian exceptions written into the surveillance laws are meaningless. But the threat isn't limited to the surveillance state. There are more than a few self-interested financial players with $10 million lying around, many of whom would love to track all the private data in a several thousand mile radius.

All of this is beginning to sound very much like a dystopian fantasy from *cyber*punk science fiction.

Total surveillance

If, in 1995, some cypherpunks had published a book about the upcoming "postmodern surveillance dystopia", most commentators would have shrugged it off as just a wee bit paranoid and ushered them into the Philip K. Dick Reading Room. Now, it is more likely that people will shrug and say, "that ship has already sailed".

David Brin seems to think so. The author of *The Transparent Society* is well known for his skepticism regarding the likelihood of maintaining most types of privacy as well as his relative cheerfulness in the face of near universal transparency. In an email, I asked him about the cypherpunk ethic, as expressed by Julian Assange : "privacy for the weak and transparency for the powerful".

Brin's response was scathing. The ethic, he says, is "already enshrined in law. A meek normal person can sue for invasion of privacy, a prominent person may not". He's just getting started :

> But at a deeper level it is simply stupid. Any loophole in transparency "to protect the meek" can far better be exploited by the mighty than by the meek. Their shills, lawyers and factotums will (1) ensure that "privacy protections" have big options for the mighty and (2) that those options will be maximally exploited. Moreover (3) as I show in *The Transparent Society*, encryption-based "privacy" is the weakest version of all. The meek can never verify that their bought algorithm and service is working as promised, or isn't a bought-out front for the NSA or a criminal gang.
>
> Above all, protecting the weak or meek with shadows and cutouts and privacy laws is like setting up Potemkin villages, designed to create surface illusions. Anyone who believes they can blind society's elites - of government, commerce, wealth, criminality and tech-geekery - is a fool...

In other words, cypherpunk may be doing a disservice by spreading the illusion of freedom from surveillance.

I posed a similar question to Adrian Lamo, who reported Bradley Manning to federal authorities. Not surprisingly, Lamo is even more cynical.

"Privacy is quite dead", he responded to me in an email. "That people still worship at its corpse doesn't change

that. In [the unreleased documentary] *Hackers Wanted* I gave out my SSN, and I've never had cause to regret that. Anyone could get it trivially. The biggest threat to our privacy is our own limited understanding of how little privacy we truly have".

In *Cypherpunks*, Assange raises an essential point that at least partly refutes this skepticism : "the universe believes in encryption. It is easier to encrypt information than it is to decrypt it". And while Appelbaum admits that even strong encryption can't last forever, saying, "We're probably not using one hundred year (safe) crypto", he implies that pretty good privacy that lasts a pretty long time is far better than no privacy at all.

Assuming that some degree of privacy is still possible, most people don't seem to think it's worth the effort. The cypherpunks and their ilk fought to keep things like the PGP encryption program legal - and we don't use them. We know Facebook and Google leak our personal online habits like a sieve and we don't make much effort to cover our tracks. Perhaps some of us buy the good citizen cliché that if you're not doing anything wrong, you don't have anything to worry about, but most of us are just opting for convenience. We've got enough to deal with day to day without engaging in a privacy regimen. Occasionally, some slacker may lose his job because he posted a photo of himself cradling his bong or the like, but as with civil liberties more generally, as long as the daily outrages against individuals don't reach epic proportions, we rubberneck in horror and then return to our daily activities.

Beneath this complacent surface lies a disquieting and mostly unexamined question. To what degree is the ubiquity of state surveillance a form of intimidation, a way to keep people away from social movements or from directly communicating their views ?

Do you hesitate before liking WikiLeaks on Facebook ?

Throughout its entire history, the FBI has used secret intelligence operations to spy on, disrupt, and otherwise target activists and groups it considered subversive (mostly on the political left). The most notorious incidents occurred between 1956 and 1971, under the umbrella of COINTELPRO (**Co**unter **Intel**ligence **Pro**gram). When the FBI's activities were revealed first in 1971 and later, more fully by the 1976 Church Committee, no politically astute person shrugged it off. It was understood without question that mega surveillance of political activists was an act of suppression period, *full stop*.

Part of the shock of the COINTELPRO revelations was the FBI's engagement in illegal activities to destroy political organizations. The government's violation of its own surveillance laws even trumped the desire to punish the "symbolic bombings" of the Weather Underground. Since the FBI used illegal breaking and entering surveillance in an attempt to destroy the radical group, the leaders received light sentences when they emerged from underground. The same FBI techniques, once illegal, are undoubtedly so legal now under anti-terrorism laws that US Attorney General Holder could conduct the searches personally, dressed like Elvis and surrounded by the *Real Housewives of Orange County* in front of the cameras on a popular reality show.

We have, perhaps, already let the surveillance culture slide too long.

It's not as though the spirit of COINTELPRO has left us. Jacob Appelbaum, who has never been accused of any crime, has been subjected to relentless harassment, starting in the summer of 2010, when he was held up at Newark Airport where he was frisked, his laptop was inspected, and his three mobile phones were taken. He was then passed along to US Army officials for four hours of questioning. One army interrogator told him, menacingly, "You don't look like you're going to do so well in prison". Several contacts found on the confiscated cell phones were then also given a hard time at airports and border crossings. In December of that year he was - along with other WikiLeaks activists - one of the subjects of a court order that compelled Twitter to let the feds snoop inside his account. (He only knows this because Twitter won a petition to be able to inform the subjects.) He has since been continually harassed by airport security and has been detained at the US border

twelve times.

That this harassment is happening to someone who hasn't been charged with a crime is particularly frightening.

"The *Galgenhumor* of our era", Appelbaum told me in an email, "revolves around things that most people simply thought impossible in our lifetime". He lists a number of chilling examples, including indefinite detention under the National Defense Authorization Act of 2012, warrantless wiretaps, drone strikes, state-sponsored malware, and the Patriot Act.

"It isn't a great time to be a dissenting voice of any kind in our American empire", he continues. But it isn't the myriad of ways that civil liberties have been gutted that we'll look back upon. "What we will remember is the absolute silence of so many, when the above things became normalized".