Thank you for choosing Cyberpunk dystopia

Totient
8 July 2013

June has been a pretty surreal month. As the *Guardian* and the *Washington Post* continue to publish internal NSA documents in what has become a torrential TOP SECRET/NOFORN early Christmas bonanza, many of us in hacker and activist communities have now seen what we long suspected confirmed : that the government is indiscriminately collecting and storing massive quantities of data, and that the distinction between the "law enforcement" and foreign intelligence use of this data has become increasingly blurred. For people who have family ties in Pakistan or regularly attend Mosque, for those who were a part of Occupy Wall Street, or have participated in the blockade of the KXL Pipeline, the fact that the national security apparatus conducts domestic operations on a racial and political basis is no surprise; it has often been a daily fact of life for years.

Yet, being right is obviously not reassuring, and how to turn these revelations into substantive change is far from clear. Unlike in 1976, when the Church Committee was formed to address the abuses of the Nixon era, there is now a broad spectrum of established legal precedent and business practices which make widespread surveillance both legal and profitable. The courts have consistently ruled that when we turn our data over to a third party, we have no reasonable expectation of privacy. Never mind that it is pretty much impossible to communicate online today without handing your information to a third party, whether that is Apple, Facebook, Google, Dropbox, or any email server, for that matter. At the same time, the dominant business model for online services has come to be based on user data exploitation and targeted advertisements. Companies that can't access their users' data because it is encrypted deny themselves revenue from targeted ads. Users who have become accustomed to not having to pay to access online services are less likely to buy into a fee-for service business model that might offer them greater privacy. These two aspects of the world we now find ourselves in, the legal architecture supporting surveillance and the profit motive driving private data exploitation, together compose a mutually re-enforcing bulwark defending the state's panopticon from both passive individual resistance and organized direct attack. All of this is happening in a world where the real-time location tracking of millions of people has become trivial, where commercial facial recognition is becoming ubiquitous, and in which the president reserves the right to murder anyone, at any time, with a flying killer robot. If there are prophets of our time, they are Kafka, Alan Moore and Phillip K. Dick.

The failed Cypherpunk insurgency

That to defy the surveillance state should be harder today than it was twenty years ago is tragically ironic, since today there are publicly available cryptographic tools that can effectively shield individuals' communications from interception. Free software such as LUKS, GnuPG and OTR theoretically allow anyone to secure their hard drive, their email and their conversations online. For much of the 1990s, there was a fight to make these tools publicly available. Many of the most secure crypto algorithms, such as RSA, were patented and couldn't be used without first paying a hefty license fee. Cryptography was legally considered to be a type of "munition" by the US government and anyone who developed software that employed crypto risked being prosecuted in the US for unlawfully trafficking in ordinance. The cypherpunks of the 1990s were committed to spreading cryptography through any means necessary. Phil Zimmermann, who wrote PGP, the free software for encrypting email, successfully circumvented the legal blockade on the export of cryptography by publishing his source code as a book, *PGP Source Code and Internals*. The text was written in machine readable format, so that anyone who purchased a copy of the book would be able to scan in the software, then use it or distribute it themselves. Although he was charged with violating the ban on munitions exports, Zimmermann was able to successfully argue that his book was not software, but first amendment protected speech. The 90s are littered with similar cypherpunk battles; some hackers set off to countries with laws favorable to exporting cryptography, so that they could safely write code and share it with the world. They believed that if encryption was widely available, government surveillance would be impossible, censorship would become a historical relic, and untraceable digital currency would become ubiquitous. Without the ability to monitor citizens or collect tax revenue, governments would fall and the people of the world would build a new society on the ashes of the old. If this sounds grandiose or naive, that's because it was.

The cypherpunks believed that with cryptography, the internet could exist as a platonic space, free from the coercive influence of organized violence. Since no amount of force can solve a math problem, and since individuals online become place-less avatars of their physical selves, then theoretically a cryptographic net could become the ultimate state-proof reality. They failed, though, to anticipate that the hegemonic forces of organized capital would exert the same disproportionate influence over people online as in the physical world, and that these new internet capitalists would be just as welcoming to the coercive influence of the state as their predecessors had been.

Today, the cypherpunk mindset lives on among technically inclined people who have fallen in love with cryptography. I know because I'm one of them. I think the way the Diffie-Hellman exchange appears to defy logic is utterly fascinating. I make one time pads for fun, I occasionally tune into shortwave number stations based out of Russia, and if you get me drunk I will explain public key cryptography in detail to anyone present regardless of their expressed level of interest in the subject. That people would freely choose to use cryptography and become enthralled with its mathematical simplicity seems natural to me. However, if I'm honest, I have to admit that I go well out of my way to use crypto tools on a daily basis. The online spaces most of us frequent aren't designed to protect our data from the people who built them, because if they were, those same people would very quickly be out of business.

Free choice isn't free

All of us express our agency within a given set of restrictions. If I live in a neighborhood without stores that sell fresh fruits and vegetables, then my "choice" to eat healthy food comes with higher costs in travel time and money that I may not have. When all of my friends use cell phones to make plans and meet up, then my choice not to carry an insecure tracking device expands to include the choice not to spend as much time with my friends. If most all of my friends are planning parties on Facebook, then my choice not to use Facebook expands to include the choice not to go to most parties. These are choices that aren't really free choices; they are all weighted by the influence of dominant players who define the shape of the terrain in which I make my choice.

The terrain of online communication is similarly shaped and defined by hegemonic players : companies that profit off of user data exploitation and seek to keep users within their internally coherent fiefdoms. Once a company achieves a certain critical mass of users, it is no longer in their interest to be compatible with other platforms and technologies; since their users have already become dependent upon them, it is now in that company's interest to force a choice away from their competitors, rather than offer users more choice. Google, for example, recently decided to stop supporting XMPP, an open chat protocol that allows GTalk users to chat with a wide variety of other platforms, including Facebook, Outlook, and free software applications such as Pidgin that support true end-to-end encryption. Since GTalk is tied to GMail, Hangouts, and Google+, users who are upset at losing the freedom of XMPP will have to decide if they are mad enough to forgo the benefits of those other Google products. Even if a user were to leave Google, in order for them to be able to chat with all of their friends, they would have to convince them all to use Jabber instead of GTalk. Their choice then, is not really a free choice.

This effect of choices that aren't choices applies to anyone trying to secure their online communications with cryptography as well. Since any end-to-end crypto tool requires that both people are using the tool to communicate, an individual who wants to use crypto has to convince other members of her social network to adopt the same tool she is using. This means that anyone designing a crypto tool today, no matter how easy to use, is swimming upstream against the closed networks of the established players.

This network effect inherent to successful platform adoption means that secure communication is a social phenomenon as much as a technical one; whenever there is a large community of people using a particular technology, that network is healthy and there is an incentive for other people to join it. A technology with a small network faces large barriers to widespread use. Generally, we can say that successful technologies are (a) easy to use and (b) have large networks. It's clear that these two qualities are mutually re-enforcing and together encourage widespread adoption of a platform. What's not clear is whether an easy to use tool naturally leads to widespread adoption.

Some cryptographers are attempting to address the user adoption friction caused by difficult to use software like PGP by making elegant, easy crypto tools that work where users already are : their phone and the browser. Moxie Marlinspike and Nadim Kobeissi are two of the most prominent developers doing this kind of work. Moxie founded Whisper Systems, and brought encrypted VoIP and texts to smart phones with Red Phone and Text Secure. Nadim built Crypto Cat, the first in-browser encrypted chat platform (note : Crypto Cat has apparently just been hit with the discovery of another major security flaw). Both have simple interfaces that are pleasant to use. Whether they will be widely adopted largely depends on the hope that good design leads to a larger user base, which by way of the network effect will accelerate user adoption.

There is some reason to believe that this may not be the case. A software tool's ease of use is not just a function of design, but interoperability with other existing stuff that people are already using. Red Phone and Text Secure are deliberately grafted into existing users' habits by seamlessly replacing the default phone and texting applications in Android. However, because Google defines the state of play by controlling the platform on which both of these programs run, Red Phone and Text Secure function more or less at the mercy of Google. What happens to Red Phone if Google tries to force out competitors and make Hangouts, their video chat and VoIP client, the replacement for standard calls on Android ? That might be back to the drawing board for Whisper Systems. Crypto Cat, on the other hand, runs as a Chrome and Firefox plugin, so while it seems unlikely that it would be swept off of either of those platforms, people still have to go out of their way to use Crypto Cat; people go there for secure communication, but it isn't built into any of the increasingly closed online worlds they inhabit. Companies that are able to generate mass revenue through user data exploitation are able to construct a constellation of interdependent services whose convenience is primarily derived not from their user design in and of itself, but from the fact that they are part of a large, internally coherent ecosystem. This is the "sandbox effect" of monopolistic design. Without the ability to derive revenue from user data, most user friendly encryption applications are either run out of pocket like Whisper Systems and Crypto Cat, or are fee-for-service, like Silent Circle.

User choice isn't just restricted by the coercive effect of the rent seeking and anti-competitive behavior of hegemonic companies like Google; their entire business model is based on undermining privacy. No major internet company is interested in offering true end-to-end encryption, because this would mean that they would no longer have access to the user's plaintext data : the lifeblood of their ad-based business model. These companies effectively offer what Bruce Schneier has dubbed "feudal security". Google promises to keep your inbox free of competitors' spam in exchange for discretely offering you some of its own. Data exploiting companies effectively secure their users' against their competitors and against malicious exploitation, but they horde users' plaintext data for themselves. Which, since almost all of these companies are US based and subject to US law (whatever that may happen to be these days), means that Google, Facebook, Skype, etc. also horde users' data for the NSA.

Cyberspace isn't space : trouble with the law

Quite obviously, when the fourth amendment was written, there was no internet. Personal papers were largely kept at home or at an office, and the protection against "unreasonable searches and seizures" referred to trespass by government officials. This has created problems when the deterritorializing effect of technology confuses the nature of private space. However, much of this apparent confusion in the courts is fairly recent, and there is a strong historical precedent of US courts adapting to new technologies while upholding the intent of the fourth amendment.

In a 1928 case before the Supreme Court, *Olmstead v. United States*, the defendant argued that the evidence gathered against him by a phone wiretap should not be admissible in court, since the government hadn't bothered to obtain a warrant to do so. The federal government argued that no such warrant was necessary, since no "search or seizure" of the defendant's home had taken place. The court ruled with the defendant, arguing that :

> Applying to the Fourth and Fifth Amendments the established rule of construction, the defendants' objections to the evidence obtained by wiretapping must, in my opinion, be sustained. It is, of course, immaterial where the physical connection with the telephone wires leading into the defendants' premises was made. And it is also immaterial that the intrusion was in aid of law enforcement. Experience should teach us to be most on our guard to protect liberty when the Government's purposes are beneficent. Men born to freedom are naturally alert to repel invasion of their liberty by evil-minded rulers. The greatest dangers to liberty lurk in insidious encroachment by men of zeal, well meaning but without understanding.

The court went on to conclude that :

> By the laws of Washington, wiretapping is a crime, Pierce's Code, 1921, § 8976(18). To prove its case, the Government was obliged to lay bare the crimes committed by its officers on its behalf. A federal court should not permit such a prosecution to continue.

You would think that such an astounding instance of common sense would equally apply to the protection of email from warrantless seizure, but you'd be wrong. In *United States v. Miller* (1976) and other similar recent cases, the court has repeatedly bought the argument that since sending an email involves "voluntarily disclosing information to a third party" the person sending that email therefore has no valid expectation of privacy in their communications. If there were no precedent analogous to email upon which to base their decision, it might make sense that the court was just confused, but that's not the case. As far back as 1876, in *Ex parte Jackson - 96 U.S. 727*, the government has previously argued that the fourth amendment does not protect against the interception of mail, since the sender has entrusted it to a third party, the US Postal Service. The court rejected that line of argument, declaring that :

> Letters and sealed packages of this kind in the mail are as fully guarded from examination and inspection, except as to their outward form and weight, as if they were retained by the parties forwarding them in their own domiciles. The constitutional guaranty of the right of the people to be secure in their papers against unreasonable searches and seizures extends to their papers, thus closed against inspection, wherever they may be. Whilst in the mail, they can only be opened and examined under like warrant, issued upon similar oath or affirmation, particularly describing the thing to be seized, as is required when papers are subjected to search in one's own household.

Unfortunately, the effect of recent decisions in line with *United States v. Miller*, which perpetuate the notion that privacy is obviated if a third party is involved, has not just undermined our online privacy, it has also produced a myriad of insidious structural changes in how the judicial review of executive power operates, often in ways which are not immediately apparent.

One of the virtues of the post-feudal common law legal tradition is the principle of equality before the law. Individuals are all theoretically subjected to the same set of laws via the same legal process, whether they are a part of the state power structure, are wealthy "private" parties, or are ordinary persons. Of course, people with more access to societal privilege or with connections to people of influence almost always fair far better than those who don't have such access, but this sort of corruption of the judicial process is quite different from its structural abrogation, which is what we are seeing now between the state and internet companies, a relationship which has come to resemble more a series of feudal fiefdoms negotiating their position with a ruling state than it does the functioning of a healthy judicial system in a democratic society.

In the physical world, if the government wants to search my house, then they (theoretically) get a warrant to do so. I would have the opportunity to fight over the legitimacy of that warrant in court. Today, my data is stored with a few very large companies, and so the government instead goes straight to them, via an administrative subpoena or similar rubber-stamp instrument to get my data. While a warrant to search my house might be issued on an *ex parte* basis, meaning that I am not notified of the warrant hearing and do not have the opportunity to object beforehand, I would nonetheless be able to argue that the warrant was issued illegitimately afterwards, and get any evidence associated with the improper warrant tossed out of court as well. This isn't the case with National Security Letters, which are served to ISPs and internet companies and include a gag order, effectively banning the company that receives them from ever notifying the customer being targeted that they have received such an order. ISPs and companies like Google and Twitter which receive these orders can fight them in court, but unlike the actual defendants, they lack a strong incentive to do so; resisting these types of requests is a civic service that private companies have little reason to pursue. Beyond maintaining their reputation with their customers, Google or Facebook have a weak incentive to spend thousands of dollars in legal fees just to stick up for any individual user.

As a result of the courts' ongoing habit of upholding the notion that we somehow forfeit our expectation of privacy when storing information with a third party, the conversation in the court system has contracted from a very broad based series of diffuse opinions written in many courts by judges hearing objections from many defendants' attorneys to a very narrowly based series of secret conflicts between large internet companies and the government, most often before the secret and unaccountable FISA court. Effectively this has bypassed any thoroughgoing legal examination of the legitimacy of the government's broad surveillance practices by transforming common law judicial review into a series negotiations between internet companies and the government over how much information they are willing to share about their users. This isn't equality before the law, since individuals are powerless to question the legitimacy of the surveillance directed at them. Instead, the companies that "own" the data choose whether they want to resist government requests at their own expense.

All of this is to say that the situation we now find ourselves in is quite complex; a series of interdependent and mutually re-enforcing edifices which support mass state surveillance have metastasized over the past decade : in the legal sphere, through the ad-based services we use, and due to a deficit of viable, easy to use online tools that incorporate true end-to-end crypto. Without a business model that can support end-to-end crypto and a robust court challenge to the current widespread (mis)interpretation of the fourth amendment by the judiciary, the future looks very bleak. Think Blade Runner meets Minority Report.