Cypherpunks

Freedom and the Future of the Internet

Introduction: A Call to Cryptographic Arms

This book is not a manifesto. There is no time for that. This book is a warning. The world is not sliding but galloping into a new transnational dystopia. The Internet, our greatest tool of emancipation, has been transformed into the most dangerous facilitator of totalitarianism we have ever seen (p1).

The Internet is a threat to human civilization. These transformations have come about silently. Within a few years, global civilization willl be a postmodern surveillance dystopia, from which escape for alll b ut the most skilled individuals will be impossible. In fact, we may already be there (p1).

We have met the enemy. We know the new surveillance state from an insider's perspective because we have plumbed its secrets. States are systems through which coercive force flows. A force that can modify historical records, tap phones, separate people, transform complexity into rubble, and erect walls, like an occupying army (p3).

Squatting on fiber optic lines and around satellite ground stations, the state would go on to mass intercept the information flow of our new world. The state would leech into the veins and arteries of our new societies, gobbling up every relationship exprressed or communicated, every web page read, every message sent and every thought googled, and then store this knowledge, billions of interceptions a day, undreamed of power, in vast top secret warehouses, forever (p4).

It is easier to encrypt information than it is to decrypt it. It is possible for individuals or groups of individuals to reliably, automatically encipher something, so that all the resources and all the political will of the strongest power on earth may not decipher it (p5).

In this way, people can oppose their will to that of a fully mobilized superpower and win. Encryption is an embodiment of the laws of physics, and it does not listen to the bluster of states, even transnational surveillance dystopias (p5).

Cryptography is the ultimate form of non-violent direct action. While nuclear weapons states can exert unlimited violence over even millions of individuals, strong cryptography means that a state, even by exercising unlimited violence, cannot violate he intent of individuals to keep secrets from them (p5).

No amount of coercive force will ever solve a math problem. Without cryptography, the Internet will merge global humanity into one giant grid of mass surveillance and control (p6).

Assange, Julian (2012). Cy pherpunks: Freedom and the Future of the Internet. OR books, New York.

The various attempts to persecute Wikileans and the people associated with it

It is WikiLeak's mission to receive information from whistleblowers, release it to the public, and then defend against the inevitable legal and political attacks. It is a routine occurance for powerful states and organizations to attempt to suppress WikiLeaks publications, and as the publisher of last resort this is one of the hardships Wikileaks was built to endure (p11).

In 2010 Wikileaks engaged in its most famous publications to date, revealing systematic abuse of official secrecy within the US military and government. These publications are known as Collateral Murder, the War Logs, and Cablegate. The response has been a concerted and ongoing effort to destroy Wikileaks by the US government and its allies (p11).

As a direct consequence of WikiLeak's publications the US government launched a multi-agency criminal investigation into Julian Assange and WikiLeaks staff, supporters, and alleged associates. In December 2010, in the wake of Cablegate, various active US politicians called for the extrajudicial assasination of Julian Assange, including by drone strike (p12).

US senators labeled Wikileaks a "terrorist organization" and named Assange a "high-tech terrorist" and an "enemy combatant" engaged in "cyber warfare". Employees from the US government warned academic institutions that students hoping to pursue a career in public service should stay clear of material released by WikiLeaks in their research and in their online activity (p13).

WikiLeaks is funded by donations from supporters. In December 2010 major banking and financial institutions, including VISA, MasterCard, PayPal and Bank of America, bowed to unofficial US pressure and began to deny financial services to Wikileaks. They blocked bank transfers and all donations made with major credit cards (p14).

Wikileans has been pursuing major court cases in different jurisdictions across the world in order to break the blockade. The existential threat it poses to Wikileaks exemplifies a new and troubling form of global econonomic censorship (p14).

Assange, Julian (2012). Cy pherpunks: Freedom and the Future of the Internet. OR books, New York.

Increased Communication Versus Increased Surveillance

If we go back to the early 1990s when you had the rise of the cypherpunk movement in response to state bans on cryptography, a lot of people were looking at the power of the Internet to provide free uncensored communications compared with mainstream media (p19).

Surveillance is now being done by every state because of the commercialization of mass surveillance. All these new types of communication that would previously have been private are now being mass intercepted. To declare things secret means you limit the amount of people who have the knowledge and therefore the ability to affect the process (p21).

If you look at the Internet from the perspective of people in power then the last twenty years have been frightening. They see the internet like an illness that affects their ability to define reality, to define what is going on (p21).

The answer is mass surveillance. It is the need to control it totally, to filter, and to know everything people do. And that is what has happened to the inernet in the last twenty years. There was a massive investment in surveillance because people in power feared that the internet would affect their way of governance (p21).

Censorship is a by-product of surveillance generally speaking, whether it's self-censorship or actually technical censorship (p23).

When you build a road it is not a requirement that every inch can be monitored with perfect surveillance that is only avaiable to a secret group of people. But t hat is what is happening on the Internet. But some people build a garden and invite everyone to be naked, as in the case of Facebook (p23).

People were compensated for being in the Stasi but they are compensated in Facebook with social credits. Underpinning the high-tech communications revolution and the liberty we have extracted from that, is the whole neoliberal, transnational, globalized modern market economy (p26).

The Net inteprets censorship as damage and routes around it. The message still spreads through all the people who are not censors. More and more we are building machines that have built-in control, to forbid the user from doing certain things (p28).

That's built-in control to prevent people understanding it and modifying it from the purpose that the manufacturer wanted it for, but we have worse than this now, because it is actually connected up to a network. So it can contain the function to monitor the user and its data. That is why free software is so important for a free society (p28).

Locking things up and keeping them secret is very dangerous on a number of levels not least because humans are imperfect. When we don't understand these systems there's a general trend to defer to authority, to people who do understand them or are able to assert control over them (p30).

Assange, Julian (2012). Cy pherpunks: Freedom and the Future of the Internet. OR books, New York.

The Militarization of Cyberspace

So when we have no control over our technology people in the military and the deep state wish to use it for their ends, for war specifically. There is now a militarization of cyberspace in the sense of a military occupation (p31).

When we communicate over the Internet, when we communicate using mobile phones, which are now meshed to the Internet, our communications are being intercepted by military intelligence organizations. It's like having a tank in your bedroom. It's a soldier between you and your wife as you are smsing (p31).

We are all living under martial law as far as our communications are concerned, we just can't see the tanks – but they are there. To that degree, the Internet, which was supposed to be a civilian space, has become a militarized space. Our private lives have entered into a militarized zone. This is a militarization of civilian life. It's like having a soldier under your bed (p31).

The US government sponsors cyberwarfare meetings to get kids involved in defending the nation from computer hackers and into hacking foreign systems. It's good to be able to know how to keep your system safe and it's good to understand the infrastructure that all o ur lives rely on, but on the other hand, they aren't trying to convince people to understand it, they are trying to whip them up into a sort of fervor in order to make them happy to do this kind of work (p35).

The interest of the United states to keep systems secure is totally limited because they want to make systems vulnerable in order to take control. In relation to mobile phone communications, mass storage is the state of the art as far as government intelligence and bulk surveillance is concerned (p35).

Cyber warriors or mass surveilance are super-cheap compared to just one military aircraft and storage is getting cheaper every year. You get decent voice-quality storage of all German telephone calls in a year for about 30 million including overheads, so the pure storage cost is around 8 million euros (p36).

There has been a shift in the last few years from picking out the particular people you want to spy on and assigning them to human beings, to now intercepting everything and storing it permanently.

The strategic approach is to do it by default, just record everything, and sort it out later using analytic systems (p37).

You never know when someone might become a suspect. The NSA on US soil against US citizens is getting it all. This raises all kinds of constitutional issues because they get to keep it forever. 20 years ago this was seen to be fantasy, as some thing only paranoid people believed but the costs of mass interception have now decreased to the point where even a country like Libya with relatively few resources was doing it with French technology (p38).

Assange, Julian (2012). Cy pherpunks: Freedom and the Future of the Internet. OR books, New York.

FIGHTING TOTAL SURVEILLANCE WITH THE LAWS OF MAN

Now it's a fact that technology enables total surveillance of every communication. We could admit that for what you call tactical surveillance there are some legitimate uses – investigators investigating bad guys and networks of bad guys and so on (p39).

But the question is where do you draw the line for this judicial supervision. That is a policy issue. We as citizens have a role in wading into the political debates that surround the use of those technologies. Democratic states within Europe are massively buying machines that allow them to act outside the law in regard to interception because they don't need a court decision. They can just switch it on and do it, and this technology can't be controlled (p40).

There are two approaches to dealing with mass state surveillance: the laws of physics, and the laws of man. One is to use the laws of physics by actutally building devices that prevent interception. The other is to enact democratic controls though the law to make sure people must have warrents and so on (p40).

But strategic interception is so complex and its use in practice so secret that there cannot be meaning ful democratic oversight (p40). The are excuses the state can use to erect such a system, the four horsemen of the info-pocalypse: child pornography, terrorism, money laundering, and the war on some drugs (p41).

It is too cheap and too easy to get around political accountability and to actually perform interception. The problem is getting worse because of its complexity and secrecy. Hidden by complexity and hidden by secrecy, unaccountability is built-in. It is a feature. It is dangerous by design (p42).

There is a real question of whether or not we should regulate the fact of buying and owning th ese technologies as opposed to regulating the use of them. Like a nuclear weapon: you cannot sell a nuclear weapon easily, and some countries may want to build one but they have problems. When we talk about weapons systems it's the technology that is regulated and not the use that is made of it. The debate might be around whether or not these technologies should be considered instruments of war (p43).

A regulatory movement regarding nuclear weapons has applied controls and so far those controls, and so far those controls have, with the exception of Japan, saved us from nuclear war. But it's easy to t ell when such weapons systems are used and when they are not (p44).

The human populations is doubling every twenty-five years or so but the capacity of surveillance is doubling every eighteen months. The surveillance curve is dominating the population curve. There is no direct escape. We're now at the stage were just $10 million can buy you a unit to permanently store the mass intercepts of a medium sized country (p45).

This is a really big threat to democracy and freedom all around the world that needs a response to try to control it while we still can. Just because it's possible doesn't mean that it's inevitable that we eill go down this path, and it doesn't mean that we have to get all the way to the point of every person being monitored (p46).

Assange, Julian (2012). Cy pherpunks: Freedom and the Future of the Internet. OR books, New York.

PRIVATE SECTOR SPYING

State-sponsored surveillance is indeed a major issue which challenges the very structure of all democracies and the way they function, but there is also private surveillance and potentially private mass collection of data. Just look at Google (p49).

Do you know what you looked for two years, three days and four hours ago? you don't know; Google knows. With Facebook you see the behavior of users who are very happy to hand out any kind of personal data, and can you blame people for not knowing where t he limit is between private and public? When you see teenagers sending pictures of t hemselves drunk or whatever, they may not have this vision that it means the whole of the rest of the world, potentially for a very, very long period of time (p50).

The U.S. spying agencies have access to all of Google's stored data, and all of Facebook's data, so in a way, google and facebook are extensions of these agencies. There's an ongoing legal case about the government's right to keep its tactics secret, not only from the public, but from court records (p52).

The courts have said that on the Internet you have no expectation of privacy, when you willingly reveal information to a third party, and, by the way, everyone on the Internet is a third party, even if the organization like facebook or Twitter says that it will keep the information private (p53).

The NSA and Google have a partnership in Cyber-security for US national defense reasons. They are trying to exempt everything from the freedom of information act and keep it secret (p53). It's absolute madness to imagine that we give up all our personal data to these companies, and then the companies have essentially become privatized secret police (p54).

And instead of being rewarded by the Stasi for giving up information on their friends, we reward them culturally. Facebook don't call their users "subscribers" or "users" they call them "targets". If Facebook know that the government will force it to give up Users' data, maybe they shouldn't build the system in the first place (p56).

So, knowing that's reality, these companies have some serious etehical liability that stems from the fact that they're building these systems and they've made the economic choice to basically sell their users out. They have decided that it's more important to collaborate with the state and to sell out their users than to be resistant to it. So they become part of it; they're complicit and liable (p56).

Assange, Julian (2012). Cy pherpunks: Freedom and the Future of the Internet. OR books, New York.

FIGHTING TOTAL SURVEILLANCE WITH THE LAWS OF PHYSICS

We need to have software that everybody can understand, everybody can modify, and everybody can scrutinize in order to be sure of what it is doing. Free software is one of the bases for a free online society, in order to have the potential to always control the machine and not let the machine control you (p57).

We need to have strong cryptography to be sure that when you want your data to be read only by yourself, nobody else can read it. We need communications tools like Tor to be able to communicate only with people you want to communicate with (p57).

But the power of the state and the power of some companies may always exceed the power of geeks and our ability to build and spread those technologies. Providing secret cryptographic codes that the government can't spy on is in fact munition. We fought this big war in the 1990s to try to make cryptography available to everyone, which we largely won (p58).

The force of nearly all modern authority is derived from violence and the threat of violence. One must acknowledge with cryptography that no amount of violence will ever solve a math problem. That is the thing that is totally non-obvious to people who aren't technical (p59).

Now a couple of individuals with cryptography can stand up to the full might of the strongest power in the world. Unless you're a security expert it's very hard to secure a computer. But cryptography can solve the bulk interceptions problems, and it's the bulk interception problem which is a threat to global civilization. Individual targetting is not a threat (p60).

Nevertheless we are dealing with really big economic and political forces and the likely out come is that the natural efficiencies of surveillance technologies mean that we are slowly moving toward a global totalitarian surveillance society (p60).

Perhaps there will be a few living people who understand how to use cryptography to defend againsts this and stay off-grid. Of course, you can choose not to have a mobile phone but you reduce your influence. It's not a way forward (p61).

Networks are being built up on top of the Internet, virtual private networks, and their privacy comes from cryptography. That is an industrial power base that is stopping cryptography from being banned. Western governments were fine with this until it spread beyond corporations to individuals (p62).

Programs that claim to be secure, that claim to have cryptography in them, are often frauds, because cryptography is complex, and the fraud can be hidden in the complexity. People will either think to themselves "I need to be careful about what I say, I need to conform" or they will think "I need to master little components of this technology and install things that protect me so I'm able to express my thoughts freely and communicate freely with my friends and the people I care about" (p63).

If people don't take that second step then we'll have a universal political correctness, because even when people are communicating with their closest friends they will be self-censors and will remove themselves as political actors from the world (p63).

Assange, Julian (2012). Cy pherpunks: Freedom and the Future of the Internet. OR books, New York.

THE INTERNET AND POLITICS

We may be witnessing the coming of age, the teenage years of the Internet and the way that it can be used by society at large to try to make things change. The four horsemen of the info-pocalypse – money laundering, drugs, terrorism and child pornography are always s brought out and the spectre of them is used to shoot down privacy-preserving technology becaust it is clear we have to defeat these four groups (p68).

There's an awakening in that people thing "oh yeah, I'm a bad person if I speak my mind about something and a person in power doesn't like what I have to say". We can use this work to empower everyday people and change the world (p69).

The Cypherpunk movement really empowered people because they realized they weren't alone anymore and the could write software that could empower millions of people. The people who created google didn't realize that they were creating the greatest surveillance machine that ever existed (p69).

You can have democratic victories that take place in public, on the surface, but underneath things are still done anyway. A win in parliament in relation to legislation doesn't stop this below the surface activity. If everyone understands what is going on and we find it's not something we consent to, then it is very difficult just to pass laws and do it without the consent of the governed (p74).

It's about increasing the political costs of taking those bad decisions , and we can do that collectively with a free internet as long as we have it in our hands. We have Facebook completely centralized, Twitter completely centralized, and google completely centralized. All in the United states, all controllable by whoever controls coercive force (p74).

And we have cloud computing providing an economic incentive for companies to have a cheaper way of processing their data in so-called international data centers run by US corporations, which means brining the data into US jurisdiction (p75).

There is a tendancy within the shift to cloud computing that is quite worrying. There are enormous clusters of servers all in one locations because it is more efficient to standardize control of the enviornment. In economics, the centralized version wins out (p75).

Centralized infrastructures make central control and abuse of power very easy. But there are so many government factions fighting to be big brother that we will be saved from completely centralized abuse of power (p76).

We need something better than saying that we have a poor man's version of Facebook and expect people to use it. Everybody who used Napster back in 1999 became a music fan and then went to concerts and became a descriptor telling everyone else to go to the concert. So you have a practical example of how peer-to-peer technology decentralized the architecture. Napster seeded the idea of decentralized architecture (p79).

The sharing culture is exactly the same when it comes to sharing knowledge (p79). Some members of the European Parliament now understand that when individuals share things, when they share files without a profit, they shouldn't go to jail; they shouldn't be punished (p80).

Assange, Julian (2012). Cy pherpunks: Freedom and the Future of the Internet. OR books, New York.

The printing press taught people how to read; the internet taught people how to write. This is something new, it is a new ability for everyone to be able to write and express themselves. To be able to use this ability to express yourself in public makes you more and more constructed in your way of speaking over time; more and more able to participate in complex discussions (p83).

Assange, Julian (2012). Cy pherpunks: Freedom and the Future of the Internet. OR books, New York.

THE INTERNET AND ECONOMICS

If there's a threat against you for speaking publicly, the only way to safeguard y our right to communicate is to communicate privately. Russia cannot have its own credit card payment system, it has to use american ones like Visa and MasterCard. That means that payments made by Russian citizens in Russian shops will be processed through American data centers. So the US government has jurisdictional control, or at least insight into who is buying what in Russia (p87).

It is a very dangerous thing to have a central place where all payments are stored, because it invites all kinds of usage of that data. So-called "lawful interceptions systems" is just a nice way of saying "spying on people". lawful intercept ion is a euphemism like lawful murder or lawful torture (p88).

You just put the word "lawful" in front of everything and then all of a sudden because the state does it, it is legitimate. The idea is to be able to create anonymous currencies, as opposed to Visa/MasterCard, which is a tracking currency (p89).

Creating an electronic currency is a big deal precisely because if you take away the stat'es monopoly over the means of economic interaction then you take away one of the most important pillars of the state (p90).

Two credit card companies – Visa and MasterCard control most of the credit card payments on the planet. Companies like paypal, which is also governed under US jurisdiction, apply US policies, be it blocking the sale of Cuban cigars from German online retailers or the blockade of payments to Wikileaks in non-US jurisdictions (p90).

The U.S. is currently privatizing prisons and negotiating contracts that guarantee a 90 percent filling rate to the private companies. That is capitalism as absurd as it gets. There are more people in U.S. prisons than there are imprisoned in the Soviet Union (p91).

The freedom of communication has been enhanced incredibly in some ways. In that we are now free to c ommunicate with many more people; on the other hand it is also tremendously degraded because there is no privacy anymore, and so our communications are being spied on and stored and can be used against us (p93).

If you buy something by Visa card from your next door neighbour, they have the data sharing between alll the major western powers, and they all know about it and store it forever. If we want a decentralized way of handling our payments, we need to take the infrastructure into our own hands (p94).

Bitcoin was the most successful attempt to introduce a digital currency in the last twenty years. Several internet service providers, especially in places that can't get easy credit-card services, like the former Soviet Union, are starting to use it (p97).

Cryptography used to be classified as arms trading but one it was in browsers and used for banking there was a powerful enough lobby to prevent it from being banned. If you have a lot of money you can pay a premium to keep your privacy, but if you don't have a lot of money you almost certainly have no privacy. And it's worse with the Internet (p99).

Assange, Julian (2012). Cy pherpunks: Freedom and the Future of the Internet. OR books, New York.

One of the largest political campaign donors in the state of California is the prison guard union. They lobby for stronger laws because they want more people locked up and for longer time (p102). The market has to be regulated to be free because you have to stop monopolies (p106).
Policy should adapt to society, not the other way around. When you enable the most powerful industrial actors to decide what policy should be, you don't make good policy. You can do bad things and generate money with it, and you can generate good things and you will not get a cent (p108).
Commercial data is collected by the U.S. government and they tie it all together (p109).

Assange, Julian (2012). Cy pherpunks: Freedom and the Future of the Internet. OR books, New York.

CENSORSHIP

In China, everything that they read on the internet is being spied upon, and that's true for all of us. That modifies people's behaviour because they become less resolute in compliaing about various kinds of authorities. You can censor google; there are a load of pages that reference Wikileaks that are censored by google.

Censorship is deniable because it takes place out of the light or because there is no instruction to sensor a particular claim. If you behave you will be patted on the head and rewarded, and if you don't behave then you won't (p123).

If you tell people you need to restrict the Internet because of pedophiles then you will be able to do anything. If we are to censor one thing such as child pornography then we need to surveil everything that everyone is doing. We need to build a bulk spyingcensorship system just to censor one thing (p123).

There is a reason a financial blockade was erected against Wikileaks – other organizational components of wikileaks are harder to suppress (p126).

If you are a czar of cyber security, that's no different from a tsar that was in the internal security forces of the Soviet Union fifty years ago. We're building the same kind of authoritarian control structures, which will attract people to abuse them, and that is something we try to pretend is different in the west (p128).

A global universal internet is the only tool we have to address global issues and that is why this fight for a free internet is the central fight that we alll have a responsibility to fight. When we talk about child porography we shouldn't even use the word pornography because it is a representation of crime scenes of child abuse (p131).

One thing we could do is disable the servers and find out who produced the content – who abused the children in the first place and then arrest them. There's a slippy slope though because once you start erasing some content you tend to start erasing other content (p133).

There are probably more abusive cops on the internet than there are child pornographers on the internet. But should we cripple the police's ability to do good policing work? The problem with erasing child pornography from the internet is that people stop lobbying for funds for cops to do the work of finding the perpetrators (p134).

It also removes crime scenes from the historical record. Filtering content should be done in the brain of the User. It shouldn't be done by the government on behalf of the people (p137).

Assange, Julian (2012). Cy pherpunks: Freedom and the Future of the Internet. OR books, New York.

PRIVACY FOR THE WEAK, TRANSPARENCY FOR THE POWERFUL

Germany probably has one of the most well-documented intelligence agencies on the planet. All the handbooks, procedural papers, training documents, internal studies are roughly public. The german government has created an agency to take care of the records so German citizens also have the right to view their own stasi files (p139).

The files are open to the public and take no account of privacy so that you have personal records of your sexual matters, your telecommunications, your money transfers, of everything you have done, which you might not want to have disclosed (p140).

Once records are created and they're in the hands of evil people, it's hard to declare privacy. Powerful groups have such a vast amount of secret material now that it dwarfs the amount of publicly available material. And the operations of wikileaks are just a percentage fraction of this privately held material (p143).

Some people will find this very hard to understand, but if they read their own records, then they will understand. We could argue for full disclosure and I wouldn't be sure if people would oppose it.

Regulation of strategic interception – bulk collection, is completely absurd. It is, by definition, intercepting everyone, so what legislation are we going to apply if your starting premise is to intercept everyone (p145)?

Assange, Julian (2012). Cy pherpunks: Freedom and the Future of the Internet. OR books, New York.

RATS IN THE OPERA HOUSE

We need the right to read and the right to speak freely without exception for every single person. Within that comes the right to anonymous speech, the ability to be able to pay people in a way where there is no interference from third parties, the ability to travel freely, and the ability to correct data about you that is in systems. To have transparency and accountability for any systems where we see any sort of agency (p141).

Governments know that acting in secret these days just means acting for a matter of time in secret, it will be subject to public record sooner or later, and this is a good thing. That means we can make o ur elected representatives more accountable for what they do and when they make bad decisions that affect our fundamental freedoms (p149).

No one anywhere in the world was born with the accomplishments that they later have on their gravestone. We all build alternatives. If you build something, you can give it to a billion people to use. It's about sharing knowledge freely and building communication channels for knowledge to flow freely (p150).

People need to know that they cannot sit idly by, they need to actually take action, and hopefully they will. The Chaos Computer Club is a hacker organization that promotes freedom of information, transparency of technology, and cares about the relationship between human and technological development, so society and development are interacting with each other (p152).

Decentralized thinking and anti-fascistic behavour, like avoiding a totalitarian state, is still taught in German schools because we experienced that at the worst level. The Chaos Computer Club is a German phenomenon. We see this internet censorship, this fight by governments against new technology, as some kind of evolutionary situations which we have to overcome (p154).

There's a generation of politicians coming up who don't see the Internet as the enemy but understand it as part of the solution, and not part of the problem. We still have a world built on weapons, on the power of secret-keeping, on an entire economic framework and so on, but that is changing (p155).

The Chaos Computer Club has managed for a long time to discuss the issues in a controversial way. The most postive trajectory for the future would look like self-knowledge, diversity, and networks of self-determination – a highly educated global population. Not in the way of formal education, but highly educated in their understanding of how human civilization works at the political, industrial, psychological and scientific levels (p155).

With the free exchange of knowledge we stimulate vibrant new cultures and the msximal diversification of individual thought, increased regional self-determination, and the self determination of interest groups that are able to network quickly and exchange value rapidly over geographic boundaries (p155).

That was expressed in the Arab Spring and the pan-Arab activism which was potentiated by the Internet. We saw first-hand the terrific power of the network for moving information to where it is needed, and it was t remendously rewarding to have been in a position to contribute to what was starting to happen there (p156).

Assange, Julian (2012). Cy pherpunks: Freedom and the Future of the Internet. OR books, New York.

Utopian ideals must mean the diversity of systems and models of interaction. The pessimistic scenario is also quite possible with the transnational surveillance state and endless drone wars already upon us. The most probable scenario for the future is an extremely confining, homogenized, postmodern transnational totalitarian structure with incredible complexity, and within that complexity a space where only the smart rats can go (p157).

All communications are being surveilled, permanently recorded, permanently tracked, each individual in all their interactions permanently identified as that individual to this new Establishment, from birth to death. That's a major shift from even ten years ago and we're already there (p158).

it produces a very controlling atmosphere. If all the collected information about the world was public that might rebalance the power dynamic and let us, as a global civilization, shape our destiny. But without dramatic change it will not. Mass surveillance applies disproportionately to all of us (p158).

This system also coincides with a drone arms race that eliminates clearly defined borders as we know them. How can a normal person be free within that system? They simply cannot, it's impossible. The freedoms we have become culturally accustomed to will be entirely eliminated (p158).

The only people who will be able to keep their freedom are those that are highly educated in the internals of the system. So it will only be a high-tech rebel elite that is free – these clever rats running around the opera house (p159).

Assange, Julian (2012). Cy pherpunks: Freedom and the Future of the Internet. OR books, New York.