Ross Chalmers, R.A.

S2076365

MA International Relations W/Global Political Economy

The Politics Of Cryptography: How Has Cryptography Transformed Power Relations Between Citizens And The State Through Privacy & Finance?

Supervisor: Roshni Sengupta

Word Count: 15,637

Contents

Abstract

This research examines the role of Cryptography in altering the power relations between the State and its citizens in relation to both privacy and economics. As Cryptography has become stronger with the rise of the computer age the ability to hide oneself has accompanied it, however, this has also allowed for stronger surveillance techniques from the State as well. The debate between the privacy of citizens against the security of the State and its peoples have accompanied this debate since the rise of advanced Cryptology since the 1960's. The Crypto Anarchist ideology has also grown with these advances and their battle against the State has been key in disseminating the ideas of privacy for oneself. In recent years, Crypto Anarchist's have achieved their goal of a Peer-To-Peer decentralised currency by the name of Bitcoin. This has revitalised the movement and is another example of Crypto Anarchists attempting to wrestle back individual citizen's control against that of the State. This paper will examine this understudied ideology and examine the battle that continues to this day between Crypto Anarchist's, the State and its citizens.

Introduction

The issue of privacy in the online space has entered the public, offline consciousness in a new way. The Cambridge Analytica scandal, whereby the company is accused of harvesting data from Facebook to influence political elections throughout the world, has once again brought the issue of personal data and how it is used to the forefront of discussion. This is only the most recent privacy related scandal. However, since 2004 the list of corporate and government hacks has been massive, from Sony, to Uber, to Facebook, to the US military (Information Is Beautiful, 2018). These hacks commonly hand the private details of people to criminals. Currently, citizen's privacies are under threat from their own government as evidenced by the Snowden leaks (Guardian, 2017). Coupled with this we live in uncertain economic times. The crisis of 2008 has led to dramatic changes in the world order. We have seen the rise of populism, culminating with the Brexit referendum and the election of Trump in the West. In the Global South, the Arab Spring revolutionised the region. All the while, as inequality is on the rise with no solution in sight, there has been a counter-culture that has been discussing these issues since the 1990's. One group has been philosophising, posing and tackling these very problems, through the lens and medium of the Internet. When looking at the problems of the direction of the Internet, solving technical obstacles to privacy, and conspiring against the "owners" of the Internet, one under-analysed group has contributed immensely to the Battle for the Internet. The CypherPunks, the practisers of the Crypto Anarchy ideology.

In 1991, a small group of computer coders met in California to discuss the best ways to use new advances in Cryptography. They were to self-label themselves "CypherPunks" and their philosophy was Crypto Anarchism. The basis for their newfound hope of society was through Cryptography, a process of keeping messages secret through techniques of encryption.[1]

[1] Encryption is the process of encoding a message so that only an authorised party can read it.

Cryptography was not a new notion; indeed, examples of Cryptography can be traced throughout history usually in the form of ciphers and codes to keep messages secret. The use of computers for Cryptography has allowed for new techniques to be created enhancing encryption of messages to previously unseen levels. This process of encrypting messages and breaking them via the use of the new technologies that computers enabled continues to this day. However, there have been notable consequences that have arisen with the rise of this technology.

Crypto Anarchy finds its popularity amongst the fringes of the online community. Dismissed by the mainstream as a form of extremism, the influence of the philosophy should not be underestimated within the online space. Despite its modest beginnings being that of an online mailing list, there have been remarkable accomplishments achieved so far, whether they be positive or negative. The rise of WikiLeaks and Julian Assange, one of the earliest CypherPunks and Crypto Anarchists has thrust State secrets into the public discourse, particularly the Iraqi war leaks by Chelsea Manning. The movement has been further invigorated since the Financial Crash of 2008 with the rise of Bitcoin and other "CryptoCurrencies" fulfilling one of the earliest aims of the Crypto Anarchist movement of an online digital currency with untraceable elements (May, 1992). The tools and ideas released by Crypto Anarchists are left for the individual to choose how to use them. Cryptography can play hugely positive role for citizens in suppressive regimes yet at the same time they can be used for nefarious means such as the purchase of illegal goods and terrorism. In the same way that previous communication innovations such as the telegraph, radio and television revolutionised modern society, so has the Internet through cyberspace. One key difference between the former and the latter, however, is that the Internet has allowed for a greater control for both the individual and similarly the State. Encryption technologies and surveillance are key discourses within current society, which is why a closer examination of Crypto Anarchy is necessary. The debate regarding Crypto Anarchy has been crucial in defining and revealing parallels with wider debates over the rise of the information technology society we live in. This paper will seek to analyse:

How has Cryptography, through Crypto Anarchy, changed the power relations between the State and its citizens?[2]

The new technological advances in Cryptography has allowed individuals to retain their privacy by hiding their messages and identity online as well as avoiding State-controlled currencies with the rise of CryptoCurrencies. It could be argued that through these new techniques, State control over their citizens should be diminishing. Surveillance of citizens online should have become extremely difficult and new CryptoCurrencies could offer the capabilities to not only give financial freedom devoid of the State but also the possibility of damaging the current neoliberal financial system. However, this paper will show that, similar to how the Internet was seen as a decentralising force of democracy in its birth but ultimately became the new corporate playground of Silicon Valley, the rise of new techniques of Cryptography has in fact led to more surveillance, less privacy and greater control through the State in retaliation. Whilst the technology is still prevalent and available to the majority of citizens through an Internet connection, the State has retained and increased its power over its citizens.

The paper tracks the Crypto Anarchists that pioneered the technical, social and political use of encryption from a position of below State actors. A tech we now use – and have used against us - every day. This paper explores the Global Political Economy implications of encryption. It has released a political Pandora's Box, with neither side in control. The political and social ramifications, of which can be best understood through the lens of the computer scientists that first saw it coming and decided to act: The Crypto Anarchists. Understanding CryptoCurrencies from this perspective allows us to see past the sort-termism of current public discourse. By viewing it as the long-fought struggle for privacy, initially by a small, immeasurably intelligent group of programmers trying to accomplish an encrypted digital payment system, we can see just how long before the actual

[2] The paper will be focusing on the Western States, most notably the USA and its Western allies whereby notions of freedom and privacy are portrayed an inherent rights of the citizen.

invention of Bitcoin this project has been under construction. It also is proof of how much further it has to go.

This paper will be split into four sections. The first section will compare the competing theories of Anarchy relevant to Crypto Anarchy to place it within the current theoretical background. Through this, the paper will show that within Anarchy there has been competing notions of how best to harness technology, or whether to harness it at all. Coupled with this, through analysing these theories we shall see that Crypto Anarchy is composite of previous individualist theories prevalent in the United States from the 19th and 20th century. The second section will cover the recent history of Cryptography, beginning in the 1960's to the crystallisation of the Crypto Anarchist manifesto. In doing so we will see that the debates regarding one's privacy in relation to the State has long been fought by advocates of freedom and by States fearful of losing control of the spying techniques. The idea of a digital currency that came into fruition with Bitcoin is also evidenced as a long-term goal of the Crypto Anarchists. The relationship between security agencies, big business and the academic world will also be explored. The third section will analyse the how Crypto Anarchists use privacy as the key tenant of their ideology and analyse the discourse of government agencies from Western States. In doing so, terrorism and the security of citizens can be seen as the vital elements in promoting surveillance of one's own citizens. In retaliation, Crypto Anarchists highlight privacy as an inherent right, fearing total State control. The fourth section will analyse how Crypto Anarchy has become intertwined with the economics of today's world. Their economic ambitions were revitalised in 2008 thanks to the global financial crash and the Crypto Anarchists coup de *grâce*, the digital currency Bitcoin. For Crypto Anarchists, the ultimate goal through encryption was to create a digital currency that could be spent without knowing the payee or the recipient. After many failed attempts, this was realised in 2008 and allowed for further Crypto Anarchist ideas to be implemented. In the creation of a non-State backed currency, Crypto Anarchists have attempted to subvert the power of one of the key powers of the State, their economic and financial hegemony.

Through this paper, the effects of the advances of cryptology will be analysed and how individuals as well as States attempt to use these techniques to gain competing versions of power.

Methodology

This paper will bring in examples of historical, qualitative content analysis to support the goals of this study. Through a historiographical, the paper will show how the discussion over the role of Cryptography has evolved as new technologies bring about evolutionary advancements within the paper. In doing so the paper will show how these debates have mirrored the discourse still occurring today. By using qualitative content analysis in the second and third chapters, the paper will analyse the discourse that the State has created surrounding encryption techniques. The dangers that encryption poses to the State, namely fearing a loss of control, is disseminated to its citizens under the guise of protecting their security. One of the main catalysts for such discourse have been the numerous terror attacks that have taken place within the Western world since 9/11. The State then furthers these discussions by incorporating the notions of criminality and highlights the necessity for protecting its citizens through surveillance in an attempt to stop such crimes from occurring. By combining these two analytical methods, we will be able to see the changes in power relations between these Western States, the supposed bastions of freedom, incorporating further elements of totalitarianism and those who are and have been leading the fight to protect citizens' individual rights. The two cases that will be examined regarding the changes of power relations between the State and its citizens are within the Privacy and Economics sections. These have been the two bulwarks of Crypto Anarchist thinking, whereby they view Cryptography as the technological advance that can embolden citizens. With Cryptography, particularly in relation to Crypto Anarchy, an understudied field, there is a lack of debate about the possibilities and limitations of such technologies. Therefore, academic sources are limited; however, this has not stopped debate

between politicians and those Crypto Anarchist philosophers in pushing their views into the public domain. This paper looks to contribute to the debate surrounding the politics of encryption.

Literature Review

The Theory Of Crypto Anarchy

Perhaps the initial comprehensive and prophetic illustration of the development, and transformative potential, of the politics of encryption, was first laid out in Timothy May's ground-breaking (within the circles 'in the know', at least) Crypto Anarchist Manifesto in 1992:

> *"Computer technology is on the verge of providing the ability for individuals and groups to communicate and interact with each other in a totally anonymous manner. Two persons may exchange messages, conduct business, and negotiate electronic contracts without ever knowing the True Name, or legal identity, of the other. Interactions over networks will be untraceable, via extensive re- routing of encrypted packets and tamper-proof boxes which implement cryptographic protocols with nearly perfect assurance against any tampering. Reputations will be of central importance, far more important in dealings than even the credit ratings of today. These developments will alter completely the nature of government regulation, the ability to tax and control economic interactions, the ability to keep information secret, and will even alter the nature of trust and reputation.*
>
> *The technology for this revolution--and it surely will be both a social and economic revolution--has existed in theory for the past decade. The methods are based upon public-key encryption, zero-knowledge interactive proof systems, and various software protocols for interaction, authentication, and verification."*

Timothy May wrote the Crypto Anarchist manifesto in 1992 as the basis for the beginnings of a loose group of computer coders that would become to be collectively known as the CypherPunks (May, 1992). The keys to unlock this ideology had recently been invented by various computer coders that had advanced the art of Cryptography and encryption to allow for one of the key elements of Crypto Anarchy, privacy. Using encryption, the CypherPunks aim to remain anonymous

from the State and subvert the rule of law if they so desired. The Anarchist aspect of the ideology was not merely to cause disruption for governments however. Since George Orwell's *1984*, the idea of a Big Brother State has been lurking within the consciousness of many an activist fearful of the power that the State can accumulate. The Internet as we know it was created with a truly Anarchist sentiment. There was a lack of central power structure and was viewed as a great equalising force for good, taking power from the top and redistributing it to the people. This is despite the Internet stemming from the military technology of the US. No nation, company or person was meant to be able to control what the Internet was. This is what CypherPunks mean when they see Anarchy. May has described the "Crypto" aspect to refer to as hidden, the ability for a person to hide one selves' activities from others and in particular the State. The ability to hide oneself coupled with the lack of leadership and the rise of Internet lacking national borders led May to view this culmination as a form of a virtual community separate to the nation State. The transnational communication that the Internet provided diminishes the ability of the rule of law of nation States. When communicating from one State to another and if illegal in one nation, whose law applies?

The Anarchy within "Crypto Anarchy" is far removed from such thinkers as Bakunin or Kropotkin where their elements of Anarchism are closely linked to Marxist thought. Rather, the history of Crypto Anarchy bases itself within the American realm of Anarchism. American Anarchism can be traced back to such thinkers as Bill Tucker and his theories of individualistic Anarchism. The basis for such thinking stems from the founding fathers of America who Tucker saw as having inherent Anarchist individualism within their political thinking. Minimising the government and promoting individual liberty is key to Anarchists such as Tucker. Coupled with this is the notion of basing decisions on "rational considerations of evidence" rather than emotion (Shone, 2013). Kropotkin argued that Tucker's ideas were only relevant to those within the middle class, not those suffering daily such as ordinary people. For many early Crypto Anarchists this fact was true, they were not poor working-class Americans but successful in the realms of computer science allowing them the luxury to pursue their whims. By having the fortunate position of not having the fear of

monetary worries, early Crypto Anarchists were able to expend the majority of their energy on their passions, most notably enhanced encryption techniques. Tucker saw that Kropotkin's Anarcho-Communism would merely lead to replacing exploitation with bureaucracy. Whilst Kropotkin argued with Tucker regarding the ultimate end stage, he was not averse to the use of technology. Rather, he envisioned a different outcome. Instead, he saw that technology would result in a form of no government socialism, where new technologies could be an equalising force for the working classes (Gordon, 2008, p.113). Crypto Anarchists are certainly individualist in their nature but, like Tucker, their processes show that they can see the benefits of the community process that is prevalent within Libertarian thought.

Writing computer code is difficult therefore, sharing your code and discussing it with your friends might help one to finally crack the problem that has been causing the issue. We can see the benefits of this sharing nature within the Free Software Movement. Software such as Linux is based upon the free sharing of code for anyone to view and upgrade so long as they then share their improved code. This has allowed Linux to be one of the most widely used Operating Systems in the world today (TedX, 2013). For coders, sharing is caring. This notion of free sharing appears at odds with the capitalist nature of Crypto Anarchy. However, at its core software is viewed as to be beneficial to society. Perhaps more than any other group – they have an understanding of maxim of "If I have an idea and share it with you, we both have the idea. But I can't share a dollar with you". If it is beneficial to society, it is therefore beneficial to the individual and vice versa. By harnessing free sharing techniques, not only does better code arise but also for Crypto Anarchists, it removes the possibility that the State can become involved. If enough people share the code, the State is unable to shut it down.

The further similarity between the two philosophies is in basing their thoughts within rational considerations of evidence. Crypto Anarchists work in a binary fashion. Their computer code will both work and run smoothly or it will not. No amount of philosophy will alter erroneous

mathematics. Their process is solely based upon numbers and science ultimately. The advantage that this provides Crypto Anarchists is that it directs their motivations to provide tangible goods rather than becoming bogged down by philosophical arguments.

The Relationship Between Crypto Anarchism, Libertarianism And Silicon Valley

The Libertarian nature of many in Silicon Valley has been termed the Californian Ideology (Barbrook, 1996). With its basis within the 1960's social revolution it has been described as a melting pot of hippies and yuppies coming together to reform "Jeffersonian democracy", whereby individuals can express themselves freely within cyberspace. These ideas are based off the writings of Marshall McLuhan, an English Professor who noted the possibility of technological advances to empower individuals (Barbrook & Cameron 1996, p. 3). Crypto Anarchy borrows much from this form of thinking whereby encryption allows for privacy, which in turn not only allows individuals to express themselves freely but also empowers the individual to the detriment of the State. Yet this focus on the individual also means that larger social issues are widely ignored be they racism or social strife. With their focus on Thomas Jefferson as their forefather, members of the Californian Ideology ignore that much of his success and theirs is built on the backs of others, in Jefferson's case slavery and in the modern day, cheap labour provided by the global south. The Californian Ideology whilst similar in its technological optimism for improving individual lives is less extreme than those who would call themselves Crypto Anarchists. Whilst both are capitalistic and favour free markets the Crypto Anarchist anti-statist approach is much more extreme in that they want the removal of the State whereby the Californian Ideologists favour a more limited government approach. This form of Anarchism is the opposite to the technologically fervent and individually based Crypto Anarchists. Technology within Anarchist thinking rarely appears as a neutral force due its ability to reshape activity and meaning which is why such battles within Anarchist thinking are apparent.

The relationship between technology and Anarchists has long been complicated with some viewing the advances of technology with a sense of distrust whilst others viewing it as the path to a glorious future. The Internet was initially seen as a great equalising form of decentralisation. Yet other technologies such as genetically modified crops have been met with severe opposition from many Anarchists. This dichotomy is to be expected. Whilst the initial industrial revolution changed the way our economies work, for many people on the lower rungs of the social ladder, life got worse before it improved. Modernisation of warfare also led to great suffering of the world. This distrust from Anarchist results in what has been called Anarcho-Primitivism. This form of Anarchy is based upon ecological and spiritual concerns with a reassessment of the hunter-gatherer societies praising them, as they were "egalitarian, peaceable, leisurely, ecstatic and connected to natural lifestyles" (Gordon, 2008). While technologies have been seen as liberating, there is also the undeniable argument that they have splintered classes associations, further divided races, alienated individuals and thus made them easier to "control". This is one of the main motivations of the Crypto-Anarchists: to use this tech to at least temper the operation of the ownership class and, at most, to over throw it.

Crypto Anarchism Research

Whilst research on Crypto Anarchy has been limited within the academic space the origins of the movement have been covered within two books, the first being *Crypto* by Steven Levy charts the history of encryption from the 1960's. Based upon research and interviews spanning from 1992 to 2000 Levy (2001) is able to point to the key figures behind the movement of Cryptography. Rather than discuss the virtues of encryption, be they positive or negative, Levy expands on the story of how academics from US universities stumbled upon the methods to secure communications via information technology. Despite this, Levy can be seen within the writings to admire the capabilities and innovative nature of the cryptographers in their battle against the State in allowing the encryption technology to be used more than by just the government itself. Written in 2001, *Crypto* is

a key text in outlining the historical nature of the debate that is prevalent when discussing privacy versus security. However, there is a lack of theoretical basis within, therefore harming the ability to open up a wider debate on the topic. Due to the nature of information technology and the notion of Moore's Law[3], the work has already become slightly dated as Crypto Anarchy continues to progress with enhanced computing power.

More recent work on Crypto Anarchy can be found within *This Machine Kills Secrets* by Greenberg (2012). Again, another historical overview but this time focussed on the harbingers of Crypto Anarchy, the CypherPunks. Greenberg charts the rise of the CypherPunk movement and is particularly interested in the works of Julian Assange and the role of WikiLeaks. Rather than focus on individual privacy that encryption allows the texts shows how encryption has reversed the power structures in that individuals can now remove the cover of privacy that guards the State through the same techniques that enhance the privacy of the individual. Greenberg has a long history of covering the outer rims of technological movements and is limited in questioning the ethical nature of the methods used by those he discusses. Rather, much like Levy there is certain bias towards portraying the CypherPunks as romanticised rebellions. Further to this, the structure is formulated in such a way as that of a glorified storytelling, although the piece is relevantly sourced. As an evolution upon Levy's work, the text is useful in bringing certain aspects of the Crypto Anarchy movement up to the point in which it was released.

From a more balanced perspective, Peter Ludlow's *Crypto Anarchy, Cyberstates & Pirate Utopias* (2001) blends a discussion from various thinkers on the prospects of Crypto Anarchy. As a collection of various essays, the benefits of this text is that rather than focus solely upon the Crypto Anarchist perspective, Ludlow includes those who see no future for such a kind of ideology within the online or real world space. Within though it contains the clearest determination behind Crypto

[3]The observation that the number of transistors in a densely integrated circuit doubles every two years, therefore exponentially increasing computing power

Anarchist thinkers and their expansion of their thoughts. Rather than focus upon the bold predictions of how Crypto Anarchy may change the world many of the chapters include arguments against such a thesis. Bold predictions are made by both sides making the piece even more relevant than when it was published in 2001 as we can view their work with the benefit of hindsight. Much of the debate highlighted remains relevant to the debates that we see today. Indeed, this is the case for many of the works based within Crypto Anarchy. Because of Moore's Law, the consistent evolution of computers allows new and unforeseen ways to adapt and enhance technology by both the State and the individuals using it. This however highlights the limitation of such work, or most work based within the information technology sphere in that not only can the basis of your argument be irrelevant due to technological advances but also that also predictions on how they will evolve can prove extremely difficult. With this being the case, it is perhaps unsurprising as to why there is limited work by social scholars on the impact of the Internet due to their work becoming outdated at a much faster rate than other areas of International Relations discourse. Unlike Levy and Greenberg's work, the contributors are unafraid on combating difficult theoretical strands of Crypto Anarchism and their relevance as well as progression through modern history.

Julian Assange, as one of the most prominent and famous members of the CypherPunk movement, is a well-known Crypto Anarchist. His *CypherPunks: Freedom and the Future of the Internet* (2012) is an interesting discussion that allows for one to get a closer understanding of their issues not only with the privacy of the individual, but also the increasing questions aim at the Neoliberal world order. However, within this strength it also belies its own weakness. The discussion disregards many of the issues that can arise through Crypto Anarchy and instead focusses on what they see as the issues of the State leading to a one-sided view of the movement. Whilst the participants (of which there are four) in the discussion may not agree on each issue, all of them come from a background that has elements of Crypto Anarchistic ideals to some extent. This inherent bias is a limiting factor.

Chapter 1 - History Of Encryption And Crypto Anarchy

Advances In Cryptography: The Academics And The NSA

Whilst the Crypto Anarchy as an ideology began in earnest by 1992, it was during the 1960's where the discussion and tools for encryption began to be explored by a wider audience. Up until this point, much of the encryption knowledge was exclusively held within the security agencies of the superpowers of the world. For those interested in Cryptography, generally their career would lead them to working as a part of this system within government as to allow them to continue focusing on their passion without fear of reprieve (Bauer, 2013, p.346). Encryption techniques were considered akin to munitions which meant exporting this technology outside of the US was equivalent to dealing weapons. With encryption techniques held largely within the domain of security services coupled with the strict export controls, gaining and sharing knowledge of the processes was extremely difficult. Despite this, within the academic scene of the United States, mathematicians, physicists and early computer scientists began to explore the long-standing issues of how encryption works and new techniques that the computer had made possible.

The catalyst for research into Cryptography was David Kahn's book *The Codebreakers* released in 1967. Kahn, a historian by nature charted the history of cryptography in relation to the military and diplomatic consequences it had. Whilst lacking the technical knowhow of experts Kahn included enough detail within the text for NSA to try to prevent its release (Kahn, 1996) The NSA failed with their attempt and Kahn's work inspired a new generation of cryptographers. Codebreakers was the first time information of modern cryptology escaped from the clutches of the security agencies and became public knowledge. The relationship between the NSA, early technology companies and the academics varied between cooperation and antagonism during the latter half the 20th Century (Bauer, 2013, p.353). At some points, partnerships were formed with each piece of work and knowledge helping the other. However, at the same time strained

relationships were also apparent with the NSA enforcing strict controls on the nature and the release of works. The NSA's fear of losing control would lead them to attempt to supress new revelations that weakened their hegemony over Cryptography. Yet at the same time, new advances within Cryptography could be incorporated within the techniques that the NSA used thereby helping improve the NSA's ability. Throughout the NSA was trying to balance their approach between seeking new and improved techniques that the US can use through the new techniques revealed by academics and the technology companies versus the fear of encryption techniques becoming widely available. Similar debates regarding Cryptography and the right to privacy are present to this day. The relationship between the security agencies, large technology corporations and individuals within cyberspace portrays a dichotomy of cooperation and antagonism.

The creation of the National Security Agency of America had its roots within the conflict of World War 2. Soon after the end, Truman created the NSA in its full form unbeknownst to the American public as well as Congress. Indeed, for many academics involved in the field during the 1960's and 1970's the NSA remained so secretive that they were unaware that the agency existed. As cryptologic knowledge began to disperse knowledge of the NSA likewise spread. Their cover was ultimately blown truly when a in a forebear to the Snowden leaks the US Intelligence Agencies were accused of spying on US citizens. In 1975, the Church Committee was set up to investigate these claims. Whilst the FBI and the CIA took the brunt of the fallout from the scandal, the NSA soon became more public and vocal about its aims. The Church Committee findings highlighted the dangers that can occur when the State has the monopoly of encryption technology (Bauer, 2013, p.351). Abuse of power, whilst not actively sought by the States agencies becomes extremely easy to pursue. The results of the investigation, much like the recent Snowden leaks, brought the concept of privacy into the public discourse and acts as encouragement to privacy and anti-State egalitarians.

For the early academics involved with Cryptography the motivation for such was not based upon Crypto Anarchist leanings or protection of the rights of citizens. Rather the motivations

stemmed from the pursuit of knowledge for most. The puzzles that encryption techniques created were the kind that mathematicians loved to solve. Early innovators within computer science soon realised that as computers become more interconnected with data flowing that major issues would arise though. Similar to the rise of the telegraph whereby transmitting messages would be subject to eavesdropping, so would messages sent via computers be vulnerable to similar issues. As computers become interconnected, the issue would be amplified. Similarly, as ATM's would become more popular, Cryptography would be key in preventing malicious actors from altering the system to allow peoples to steal from the machine. By using encryption, they could protect the consumer and business to prevent such events from occurring. IBM was one such company that began to invest heavily in Cryptography realising that as computers evolved cryptographic techniques would become valuable assets for companies around the world. Through the 1960's they worked with Lloyds bank in providing the underlying techniques for automatic teller machines (ATM's) to be used in and around London. IBM's own creation is directly linked to NSA work. The NSA is credited with providing the necessary funding for their development. Such examples are evidence of how encryption is not just important to an individual but can also enhance business and the economy. However, IBM's most important contribution to encryption was not in providing Lloyds Bank the ability to safely create ATM's. Rather their creation of what became known as the Data Encryption Standard (DES) is their key work. The NSA's influence on DES is notable as well. For the DES system to work a key of "bits" is necessary to make the algorithm secure from Brute Force Attacks.[4] The NSA was involved in the key size debate. Initially DES was implemented with a 128-bit key, which at the time would have been practically, technically and financially impossible to crack. However, it is now known that, thanks to the NSA interference, the key chosen was a 56-bit key thereby reducing the security of DES, the larger the bit key the harder the encryption is to crack. IBM argue that this was due to the ability to fit this on a computer chip. Yet many have questioned this, instead, they argue

[4] A brute force attack involves having a computer repeatedly attempt to guess the key. The longer the key the more difficult it becomes for a computer to guess, therefore a shorter key is easier to "Brute Force Attack".

the 56-bit key was chosen due to the NSA having the ability to complete a Brute Force Attack on this strength. Further to this, some have argued that the relationship between IBM and the NSA goes further, with the NSA placing a back door on DES (Levy, 2002, p.38).[5] Whilst neither of these accusations have been proven as of yet DES would go on to become the standard of encryption for many. Having a State run security agency heavily involved in the creation of an encryption standard can be viewed from both positive and negative perspectives. At the time, the NSA was at the forefront of encryption technology so their expertise would be invaluable to a new company such as IBM. However, the NSA's involvement also raises important questions. Questions are raised as to the NSA's motives particularly in their involvement to the key size debate. By limiting the key size, the NSA is thereby rendering DES susceptible to attack by both international and domestic State and non-State actors (Levy, 2002, p.59). Retaining control of encryption technology is a theme that runs throughout the 20th century for the US State.

Whilst DES became the encryption standard, the revolutionary moment in Cryptography arrived with the creation of Public Key Cryptography. Initially one of the biggest issues that arose within the field was that if, hypothetically, Alice wanted to send Bob a message then they would have to meet or discuss beforehand to share their private keys. The private keys allowed encrypted messages to pass from to another, but if someone in the middle of the transaction gained access to those private keys, they could intercept the message. This could prove both problematic and inconvenient. By creating algorithms that could work whereby both a public key and private key were used simultaneously, this issue with dissipate. One could share the public key as much as they like without fear of reproach. The process began thanks to Walt Diffie and Martin Hellman. Diffie was a long-standing libertarian whilst Hellman was well known for his anti-war protests. Both were anti-government. In 1976, they released their paper suggesting the possibility of such a system, a revolutionary moment in encryption techniques. Three MIT professors who came up with the

[5] A back door is the ability to bypass the encryption method thereby allowing instant access to the encrypted material.

solution then expanded upon this. Their names were Ron Rivest, Adi Shamir and Len Adlemen. The algorithm became known as RSA and became vital to the future structure of the Internet (Holden, 2017, p.220). Such advances in cryptology though came with the attention of the NSA. Attempts to limit the spread this research were enacted. In 1977 a conference was scheduled to take place to discuss the findings. Beforehand however the NSA stated that such publications needed to be approved by the NSA beforehand, they based this claim upon the law that encryption was equal to munitions. Despite the threats, the conference went ahead as planned. The uneasy relationship between academics and the NSA continued however (Levy 2002). The National Science Foundation, one of the key funders of academic work became aligned with the NSA. Funding for new research would not be allowed without NSA approval. Whilst the NSA might have preferred to stop all cryptology research, the Pandora's Box had been irrevocably opened by Diffie and Hellman's landmark paper. Despite this, the NSA's back up tactic of collaborating with the NSF proved shrewd. They would be able to choose what does and does not get funding. They would have easy access to the research material. In doing so, they would have the first glimpse of new cryptographic techniques in an attempt to stay ahead of the curve.

Cryptography Without The State

As Diffie and Hellman's ideas spread along with the RSA algorithm, further study of encryption within American colleges continued to spread as computers became widely available, the ability of the NSA to prevent further research became more difficult. David Chaum's (1985) "Security Without Identification: Transaction Systems To Make Big Brother Obsolete" proved to be another ground-breaking moment that served as another catalyst for what was to become. In an eerie prediction of the future, Chaum opened the article suggesting:

"*The foundation is being laid for a dossier society, in which computers could be used to infer individuals' life-styles, habits, whereabouts, and associations from data collected in ordinary*

consumer transactions. Uncertainty about whether data will remain secure against abuse by those maintaining or tapping it can have a "chilling effect "causing people to alter their observable activities. As computerization becomes more pervasive, the potential for these problems grows dramatically".

Chaum also had the belief of some that with the birth of the Internet and the data that would be prevalent online mass surveillance by the State or others would become possible. To combat this Chaum (1983) suggests on using what was termed "blind signatures" to make payments online. The process involved using Cryptography to hide the sender or recipient of money in a hypothetical case, yet this was just one example. Chaum takes the idea further implying that through these techniques encryption of all data could be possible to stop snooping of any kind. Chaum had long been writing about the possibility of anonymity online, four years previous he wrote a paper suggesting ways to create anonymous emails. The ideas that there were dangers lying within the possibility of an interconnected society via computers was becoming more prominent. Yet much of the philosophical nature of the debate and scientific coding to counteract this was left to individuals. Slowly as these ideas spread from one to another the idea that one could protect themselves from snooping of any kind, be that by the State or by an individual became more prominent.

It wasn't until Phil Zimmerman's (1991) creation of "Pretty Good Privacy" (PGP) that an encryption program was created that permitted the individual to fully protect themselves as long as they had the technical knowledge to incorporate it. PGP was a program that allowed users to encrypt their emails as well as the files that they stored upon their computer. Zimmermann saw the need for PGP as an essential tool of freedom for citizens under severe control of their State such as those in China or anti-nuclear activists in the USA. Zimmerman was not as radical as many of the other CypherPunks but still saw privacy as an essential and unalienable asset of a citizen, he had been arrested at protests criticising the US government and their nuclear capability. With the creeping possibility of government surveillance Zimmerman believed "if privacy is outlawed, then

only outlaws will have privacy" (Zimmerman, 1999). These arguments for encryption are countered by the State as one would expect. Whilst dissidents in China can use encryption to fight totalitarianism of the State so too do western States lose their oversight of criminals within their territory as well as terrorists outside. After sending a copy of the software to a friend, Zimmermann soon found that PGP was being shared online as freeware. PGP was a success from its release. Unfortunately, for Zimmermann this created issues in that encryption techniques had long been solely used by governments, in particular the US government. The Crypto Wars as it was termed was the battle between the US State and individuals such as Zimmerman. The fear for the USA was that if these encryption techniques became widely available they would lose their control over the Internet, its citizens and the wider world. Two attempts were made by the US to combat this. Firstly, Zimmerman was put under investigation by the US State. Not only had elements of PGP that Zimmerman used been patented by RSA Data Security Inc., the company based upon the RSA algorithm, but cryptographic software was viewed as munitions by the government. With the release of subsequent sharing of PGP, Zimmerman became the equivalent of an arms dealer in the eyes of the government. The second attempt to combat the use of encryption techniques by the US State was through the creation of "the Chipper Clip" under the Presidency of Bill Clinton. Senator Joe Biden announced the Clipper Chip in 1993 and it was to allow the US government access to encrypted messages when given authorisation. If the Clipper Chip had been able to pass through Congress then ''backdoors'' would have been a necessity on any encryption technology (Pedneker-Magal & Shields, 2003). This would allow the US State to be privileged to view all data and transactions. Yet, both attempts by the US State ended with failure.[6] The Clipper Chip proposal also failed. Lack of support from the public coupled with that of Silicon Valley did not help the process but a major vulnerability within the program that made the Clipper Chip easy to crack also ended its prospects. The Crypto Wars as they would become to be known within the 1990's have remerged in

[6] Attempts to indict Zimmerman collapsed in part thanks to clever manoeuvring from other coders sympathetic to Zimmerman.

recent years with the issue of encryption within smart phones as well as their apps. The San Bernardino attacks of 2015 in California once again put the US State in combat albeit this time with one of its largest corporations, Apple. One of the perpetrators of the attack was the owner of an iPhone that Apple were instructed by a federal judge to decrypt but Apple held its ground. Apple could not decrypt the iPhone unless it handed over the password of the phone to the FBI. Their motives for refusing were summed up by CEO Tim Cook "The 'key' to an encrypted system is a piece of information that unlocks the data, and it is only as secure as the protections around it". Thus, Apple ceded to the FBI's demands than there would be no point in using encryption in the first place (McLaughlin, 2016 p.371-372). The debate over encryption has a long history, one that is continuing today under the same arguments.

The Birth Of The CypherPunks

With strong encryption now within the hands of the public, albeit ones with extemporary computer skills some began to examine how these techniques could restructure society. Timothy May, Eric Hughes and John Gilmore were three of these. Both May and Gilmore had early careers within the information technology industry. Together, these three created a small band of anarchist thinkers known as the CypherPunks and through using Hughes's remailer created an online community of likeminded Crypto Anarchists with May writing their manifesto (Greenberg, 2012). Through Crypto Anarchy, May proposes that a social and economic revolution is possible thanks to encryption techniques that have been born. State secrets and stolen goods will now be freely traded and the State will be unable to stop it. Evading taxes and drug dealing are two other outcomes that are possibly easier thanks to the rise of Crypto Anarchy (May, 1994). The manifesto, written as a call to arms in a similar vein to Marx's original is a call to arms for likeminded anarchists to embrace this new technology and subvert the State's power. Another important facet of the Crypto Anarchists and the CypherPunks is that they "write code". Indeed this is their motto, "CypherPunks write code" (Hughes, 1993). Rather than being a loose group of anarchists spread over the Internet discussing

various ways to incorporate this technology on a philosophical level, Crypto Anarchists pride themselves on their ability to put their words into practice in the form of computer code to see whether their ideas are actually viable.

Their communication was in the form of rare meetings on the west coast of America but mainly through their mailing list. Each member could message one another with various ideas and debates. Some key ideas that were to happen and that shall be discussed later were the creation of a Dark Net, an Internet-based browser where the user could not be tracked. Anonymous Internet money that could be transferred between peoples online. Notable early CypherPunks include Julian Assange, Nick Szabo and Adam Beck. Within the next two sections this paper will show how these early Crypto Anarchists ideas continue to battle with the balance between anonymity online versus the possibility of mass surveillance as well as further evolution into the realm of economics.

The history of encryption and the rise of Crypto Anarchists continues to have parallels to the present. The battle over new technology verves between an embracement from the so that they themselves can harness the techniques but whilst also fearful of this technology spreading not only to individuals but also rival States. Initially attempts to improve Cryptography or even widening the knowledge of techniques was prevented by the NSA. Yet their attempts failed and currently attempting to remain ahead of the curve proves problematic for security agencies around the world with the ability of cyberspace to remove borders allowing for collaboration throughout the world so long as an Internet connection remains. Much of advancement within information technology did though arise through investment from the State itself and this continues to this day. Through the history of Cryptography we see how the advances in new techniques not only provided possibilities for greater individualism but also how the State incorporated these new techniques to improve their own abilities. Not only has the rise of information technology made Bentham's Panopticon possible it has also allowed for a greater level of privacy for the individual. However, the benefits of encryption and privacy appear to have not caught the public imagination despite evidence of State

surveillance. Consumers are willing to provide vast amounts of personal data for the use of free social media which had altered capitalism as we know it. Orwell's 1984 dystopia is closer than ever yet further than before.

Chapter 2 - The Battle Between Privacy And Surveillance States

Privacy And Anonymity

The debate surrounding privacy and anonymity was very much within the public discourse during the 1990s as encryption techniques became widely available. The debate regarding the Clipper Chip, which would allow the US government a backdoor to encrypted protocols, served as the catalyst for this discussion (Pedneker-Magal & Shields, 2003). Yet within recent years, the debate has sparked into life again. Rather than fearing the government, which is still evident, citizens are also wary of the threat that arises from large corporations harvesting data. Yet despite the discourse of privacy prevalent since the Snowden leaks people continue to permit access to their own through their use of social media where sharing details of one and another's life is extremely common. If one is not hiding their footprints online then companies are able to view a person's like, dislikes and even secrets without their knowledge. Yet before we further examine these issues, we first must examine what is the difference between the notion of privacy and its differences with anonymity. Privacy as a concept has been difficult for many to define. The limits and scope of what contends to be privacy prove difficult from State to State, as each one has their own culture and normative ideas therefore to create a fully cohesive definition for all is difficult. Parent (1983) has defined privacy succinctly within philosophical terms pertaining as to three key elements. These include, privacy allows for one to be left alone, allows for autonomy over personal matters and that it is limitation on access to the self. Pressing ''ACCEPT'' to privacy terms and conditions is quite literally the biggest rewriting of the Social Contract since the Magna Carta. Despite Snowden's leaks, people seem happier to forgo their privacy beyond for ease. This may be down to the lack of structural and technical support and understanding citizens have of the digital realm. Even so, the simplicity in which the public have already given up their rights to privacy was beyond what the Crypto Anarchists could predict.

Anonymity is an extreme form of privacy and could be considered as a separate idea. Whereas privacy can be the protection of your informational data, anonymity can remove any doubt of invasion as to yourself. Anonymity has been common in cyberspace, sometimes in the case of pseudononmity, particularly within the online realms of certain social media spaces or in online virtual reality spaces such as Second Life where you can become someone else altogether. The issue that arises with anonymity is that one can perform acts that are illegal and immoral. This safety net has in some cases allowed citizens to become the polar opposite of how they represent themselves in the real world. Yet, such is the ability and pervasiveness of online collaboration techniques that allow personal data to be mined that anonymity has become one of the most secure ways to protect your privacy online. The debate surrounding anonymity shares parallels with that of privacy with academics, activists and governments unable to formulate a cohesive prognosis. Whilst some view the idea as the bastion of trolls and hate speeches, others see the value of anonymity as an essential human right. Throughout this chapter, we will see how the issues of privacy and anonymity have evolved. Anonymity techniques are not only used by citizens however as we shall see. As States try to prevent their spread, they themselves are not only great users of such techniques, essential in transmitting top secret messages without being spied upon by other nefarious States or terrorists but also the creators themselves that allow for the possibility of civilians to use it.

The debate has its seeds in the late 1990's as computers began to be common household accessories for many in the west. The Crypto Anarchists were painted as extremists by the government and central academics. Etzioni argues amongst a Communitarian line that the needs for privacy need to be balanced with the safety of the citizens. He argues that Crypto Anarchists have no need for total anonymity and that governments should be allowed the keys necessary to reveal encrypted messages. To secure citizens against undue surveillance these keys could only be used with permission of the courts. Further to this, he argues that the Crypto Anarchist view that governments will want to snoop on citizens is unlikely, therefore, their fears are misplaced (Etzioni 1999). Two caveats should be noted regarding Etzioni's arguments however. Firstly, he has had a

history of working with government as a senior adviser in the late 1970's so his trust of government is unsurprising. The second issue, and to criticise Etzioni for this is harsh as hindsight can be 20/20 is that the present day is rather different to when Etzioni was writing. His viewpoints constructed in 1999 are fair and balanced, however his trust in government to not abuse their power has been shown to be misplaced with the extensive snooping techniques that were to be employed by the NSA. The Crypto Anarchists predictions have turned out to be more persuasive with the hindsight of history. Yet Etzioni's ideas of finding a right balance between privacy and the safety of citizens is not without merit. The dangers that are posed by Crypto Anarchy are real, yet as this chapter will show, so are the dangers of refusing Crypto Anarchy.

The Influence Of 9/11

One event that was to change the course of government rhetoric as well as the publics was the events of 9/11. The rhetoric built upon similar ideas mentioned by Etzioni of freedom of the individual versus the safety of the collective society. The debate then evolves into not whether the government should have access to encrypted messages but to what extent? Should they focus on possible suspects or should the Patriot Act allow for blanket coverage rendering everyone a possible subject? Section 215 of the Patriot Act allowed the U.S State to have businesses hand over records of an individual who may be involved in terrorism. Section 215 was also the legal basis used to defend the NSA's harvesting of data from US phone companies that led to ordinary Americans to be tracked as revealed by the Snowden leaks (Brennan Centre For Justice, 2013). Section 206 allowed the government to tap a person's phone, laptop or mobile phone with approval from the Foreign Intelligence Service Court (Ibid). Rather than the Internet being a democratising tool for the masses, this evidence would suggest that it has enhanced the capabilities of the government itself.

The clearest example of this dichotomy is seen within the Arab Spring. Circulation of anti-government sentiment was common which led to the governments of Egypt and Tunisia to restrict

Internet access. More resources were used on surveillance and censorship of their citizens in the build up to the Arab Spring (Howard, Hussain, 2013, p.2). Whilst the argument can be made, that encryption allows terrorists to communicate without the eye of governments being able to see, at the same time, encryption can protect civilians trying to overthrow corrupt and authoritarian governments.

For the Western States, the events of 9/11 and subsequent terrorist attacks have proven key in their arguments for their arguments in requiring further surveillance, this is not just limited to the US but their allies as well. The devastation events that occur from terrorist attacks and the subsequent loss of life encourage government to further cast their surveillance net in attempts to stop them. The UK's Investigatory Power's Bill passed in 2016, also known as the Snoopers Charter greatly extended the surveillance power of the British government. Having been no stranger to events of terrorism on its own soil, the same arguments made by the American State are relevant to the UK. Questions can be raised yet over whether the extent of what bill allows is necessary or even helpful in their tasks. UK security agency GCHQ already had deep ties to the NSA of America through their five eyes program which encouraged data sharing between agencies (Lyon 2015, p.58-59). Their relationship, however, was not just one sharing intelligence in order to stop terrorist attacks but also to spy on politicians in G8 and G20 meetings (Ibid). Arguments from the State suggest that these intrusions into people's privacy are used to prevent crime or terrorism but that the technology can also be abused to spy on innocent civilians as well as foreign diplomats are generally ignored by portraying government agencies as friendly watchdogs. They have no reason to spy on their own citizens who do nothing wrong, yet when digging deeper when the capabilities are possible it proves hard to resist. Therein lies a further issue for many of the spy agencies however, with data collection so widespread analysing and making sense of the data can prove difficult, a point noted by MI5 of the UK (The Intercept/MI5, 2016). Whilst criticism has been strong from civil libertarians, the Investigatory Powers Bill has also faced harsh words from the Human Rights Council of the UN who saw the bill as disproportionate, which would lead to negative ramifications (Cannataci, 2016).

Similarly, Snowden accused the UK government of copying China's strict Internet laws (Snowden, 2016). This issue has been further exacerbated with the recent High Court ruling that the bill is incompatible with current European Law and therefore requires rewriting (Guardian, 2018).

State Vs Crypto Anarchist Discourse

Post Snowden, there was clear evidence that the Crypto Anarchists prophecies had already become true. Whilst the philosophies of Crypto Anarchy were still outside of mainstream discourse, their ideas were now being discussed more fervently. The reaction of the US State was one of defence. Former Director of the CIA Michael Hayden argues from a variety of standpoints defending the US security agencies and their policies as one might expect from a former employee. The leaks and subsequent media coverage are "hyperbole" in that they have exaggerated the extent of surveillance (Hayden, 2014, p.17). Further to this, Hayden's key argument is that under the Fourth Amendment of the Constitution American citizens are protected from undue surveillance, non-Americans are not. This argument defends the NSA from international espionage (Hayden, 2014, p.21). Yet in the same piece, Hayden notes that international terrorists as evidenced by 9/11 are "already inside the gates, and even when not physically in the country, terrorists made use of e-mail accounts whose servers were here" (Hayden, 2014, p.14). This issue complicates matters for the US narrative they are attempting to construct. Obama continues this in a speech discussing the Snowden revelations. Firstly, the impact of 9/11 is mentioned to show why security is important. He follows up Hayden's constitutional argument regarding overseas espionage. Obama as President though is targeting a much larger and different audience than the writings of Hayden. The emotional appeal to the people, arguing the members working for the NSA are Americans with family much like themselves (Washington Post, 2014). By taking a patriarchal view over their citizens, the State is effectively implying that Big Brother is necessary to preserve your freedoms by taking a some of them away. Whilst some of the arguments raised by the US State are plausible, they remain deflective. Whilst the option to remove the conditions to allow the surveillance from the NSA was

under threat, Congress approved the bill to continue it soon after the Snowden revelation. Trump himself has just extended it for another six years (Reuters, 2018). Despite the Crypto Anarchists warning of this possibility and providing the tools in an effort to prevent it the general populous continue to allow this surveillance.

Without managing to achieve encryption for all through the use of tools such as PGP there have been notable success (in the Crypto Anarchist viewpoint) from individuals. Julian Assange is one of the key proponents of the Crypto Anarchist philosophy, being an early member of the CypherPunk mailing list under the pseudonym Proff (Assange, 1995). His creation of WikiLeaks ultimately turned the battle of encryption back around to the State itself, rather than the State snooping on the people, people began to reveal State secrets. Their most famous trove of classified data was the Chelsea Manning leaks highlighting the accused war crimes of the US army in Iraq. Much like the defence regarding the Snowden leaks, the attack from the US State against Assange has been strong. Recently, Secretary of State and former CIA Director Mike Pompeo has portrayed WikiLeaks as a "non-state hostile intelligence service" coupling this with an affiliation to Russia and their State broadcaster Russia Today inferring that they are partners (Pompeo, 2017). Safety of the American people is also key to their discourse over the problem WikiLeaks has caused, coupled with the morale of employees of intelligence service employees. When providing this speech Pompeo was still head of CIA, so boosting employee morale would be key in the face of attacks from the media and members of civil liberties groups (Pompeo, 2017).

The argument that Assange outs forward stems from his early CypherPunk days when the battle over encryption between the US government and Crypto Anarchist still continues, however now the forms of communication have massively expanded. With increased communication, increased surveillance is possible. Rather than this surveillance stemming from major powers such as the US or Russia he argues nearly every State is snooping on its citizens. During the revolution within Egypt, protestors were informed not to use Facebook or Twitter as they could be found yet many did

and suffered the consequences. Further to this, the hypothetical question of what would happen to these websites if an organised revolution occurred in the US is prominent. Being large US corporations, the ability of these companies, due to the information they have on potential dissidents, means their ability to crackdown is almost total. Similar to the Apple San Bernardino case, it would be up to the higher brass as to whether they cave. This Assange argues is why the ability of the individual to use encryption software that is open source is hugely important. By relying on a third party to encrypt for oneself you are at risk if that third party becomes under pressure. By decentralising the software through open source techniques citizens can achieve greater anonymity (Assange, 2012, p.21-22). Assange has become one of the foremost Crypto Anarchists in modern times, especially in relation to issues of surveillance. However, as he admits himself he struggles to explain his viewpoint from "the common perspective". It is clear from the CypherPunk mailing list that Assange's ego is apparent, and this issue proves problematic when attempting to convince the populous of his ideas. This has not been helped further by the allegations of sexual assault which has seen Assange in the Ecuadorian embassy for six years at the time of writing.

When viewing the CypherPunk mailing list the anarchic ideas proposed by some are extreme. As Anarchists themselves, they were a loose group with no moderator allowing for both moderate and extreme suggestions. One of the most extreme was made by CypherPunk mailing list member Jim Bell that he titled Assassination Politics (Bell, 1995). The premise was that through using encryption technologies coupled with a form of anonymous digital cash marketplaces could be set up whereby money can be provided to kill politicians. The idea can be extended further however, as under Bell's argument there is no reason why the assassination of members of the general public could take place if one had reason to suggest it. The basis for this radical idea was that if a politician knew that this marketplace existed, then they would therefore behave for fear of death. The reaction from the Crypto Anarchists were mixed. Whilst some agreed with the radical notion, most

members flamed[7] Bell or the idiocy of his suggestions (CypherPunk Mailing List, 1996). Whilst Crypto Anarchists had strong arguments for the protection of privacy in the 1990's, Bell's idea shows the extreme nature of some of these Anarchists. Not only does Bell show the dangers of the possibility of encryption techniques he also helps in keeping the group firmly on the fringes of society, thereby inadvertently helping governments maintain the more persuasive narrative over the dangers of encryption. Bell's ideas and beliefs are but one of the issues that face the Crypto Anarchist community. Under their ideas of a lawless Internet without any central power structure, humanities own free will has proved to have severe and unpleasant consequences. Within the depths of the Dark Web, there are examples of paedophilia, extremist thought, and the freedom of speech allows for death threats even on popular platforms such as Twitter. However, even today as surveillance is prominent these issues are still prevalent. Within Crypto Anarchist thought, such bad actors are thought of as an unfortunate side effect and ultimately unstoppable unless every single byte of data is monitored. In the Crypto Anarchist whilst drug markets are acceptable, episodes of paedophilia are certainly not. Yet if the choice had to be made between illegal activities being possible compared to a mass surveillance system most Crypto Anarchists would side with the former. Such a radical discourse is hard to swallow for many. Drug markets in the mind of many are immoral; never mind some of the more extremist elements that can be found in the depths of the Internet. This extreme discourse pushed by Crypto Anarchists eventually plays into the State's hands in that it provides ammunition for a more regulated Internet; the illegal market argument is an easy win for government officials and waters down the debate. Whilst encryption and privacy are a tool for freedom, especially those in strict regimes, the technology also provides tools for bad actors to abuse. Nevertheless, Bell's idea and subsequent enacting of such within the Dark Web is perhaps the clearest example of how Crypto Anarchy has attempted to provide power to the people. The arguments raised above have been long argued from law professionals to social scientists, but these

[7] Flamed or flaming is a term that is an early precursor to what would become now known as trolling. In the early days of Internet mailing lists, flaming was as common as trolling is today. However, whereas trolling is commonly for the "lolz" flaming was also an attempt to encourage discussion through harsh criticism.

have largely ignored the Crypto Anarchist viewpoints who have been key in improving encryption systems since the late 1980's. In between messages of philosophy, cryptographic techniques and flaming/trolling each other on the CypherPunk mailing list the issue of paedophilia is also discussed in relevance to some UK cases at the time in 1995.

One of the greatest ironies in the debate over privacy versus surveillance is that the greatest weapon provided to Anarchists and terrorists alike was not actually created by the CypherPunks but by the US Department of Defence that now exists as of non-profit organisations partly funded by the US State and partly by civil libertarians (Bartlett, 2015, p.2). The Onion Router as it is known, or TOR for short, is a web browser similar to that of Microsoft Edge or Google Chrome yet there is one major difference. By routing the navigation of webpages through numerous computer routers (imagine each router provides another layer, like that of an onion) it allows people to surf the web anonymously and see what has become known as the Dark Web. The Dark Web was another hypothetical notion first thought of by Crypto Anarchists yet they never managed to create one, nor needed to in the end (May, 1995). The Dark Web contain websites that are not found on standard browsers and commonly used for illegal purposes. The creation and usage of TOR is essential for the US military in protecting their communications when overseas but since the program was released to the public, Crypto Anarchists have not only improved the source code but also expanded its usage worldwide. Tor has become the go to web browser for people who are fearful of State surveillance and criminals. Much easier to use and to set up than previous encryption methods such as PGP, Tor has increased the difficult job of security agencies in their attempts to view and control what takes place in cyberspace. The creation of TOR has enhanced the privacy of States between themselves but with its public release has enhanced the privacy of the individual at the detriment to the State's ability to reign over their citizens.

Whilst the discussion over privacy has become a common theme within the media and within government in recent years, it is perhaps surprising that the actual desire from the general

population remains limited to embrace the software available to them. The arguments put forward by governments of the western world coupled with various terrorist attacks has made the “if you have nothing to hide you have nothing to fear” mantra a winning one. The cultural and structural argument has been won by the forces of surveillance. This in turn has meant that despite restructuring power relations away from government and towards citizens has become easier, the opposite has happened. Instead, western governments have enacted one of the largest surveillance regimes in modern times. Despite this knowledge becoming public thanks to Snowden, appetite for privacy has remained limited at best. Crypto Anarchist discourse on the importance of privacy has failed to reach the public, in part due to apathy from the public and in part due to the extremist ideas purported by some on the side of the Crypto Anarchists. Yet, it is in the Economic realm, however, where Crypto Anarchists have provided the greatest contest of their philosophy. Through the technologies afforded by Cryptography, namely Bitcoin.

Chapter 3 - Power To The People - Decentralising Economics

The Crypto Anarchists Coup De Grâce: Bitcoin And CryptoCurrencies

Whilst the Crypto Anarchist movement forewarned of the dangers of a surveillance State, which subsequently happened, the revitalisation of the movement in the past ten years is not due to this unheeded prediction. Instead, economics is how Crypto Anarchy has been updated for the 21st Century. Within the CypherPunk mailing list, the idea of a digital currency was mentioned very early by one of the founding members, Timothy C May, and the possibilities it could encourage (May, 1992). Ideas such as ''Assassination Politics'' required not only anonymity online but also the ability to send money anonymously over long distances removing and solving the tyranny of space. During the 1990's and early 2000's there were many iterations of such an idea from prominent Crypto Anarchists such as Adam Beck, Nick Szabo and Wei B. Another early example came from the expert cryptographer David Chaum, initially discussed in 1982 but coming to fruition with his business "E-Cash" in the 1990's (Chaum, 1983). Every iteration, however, suffered from flaws of centralisation or technical issues. It was not until the midst of the 2008 Financial Crisis that a man/woman or group under the pseudonym Satoshi Nakamoto wrote on a later version of the CypherPunk mailing list of his project called Bitcoin (Nakamoto, 2008). The reaction to the announcement amongst Crypto Anarchists was minimal with only Hal Finney, a member of the CypherPunk mailing list from 1992 showing any interest (Finney, 2013). On the 12th January 2009, Nakamoto sent the first Bitcoin transaction to Finney and the network went truly live (Popper, 2015). Initially valued at nothing, a single Bitcoin is now ranging between $7000-$8000 (although infamously the digital currency is known for its volatile swings), the current market cap is touching $119,000,000,000 with the various other CryptoCurrencies as they are known reaching a total market cap of $252,000,000,000 (CoinMarketCap, 2018). This has been achieved in the space of nine years. The rise of digital currencies has created a buzz on both sides of the debate.

Bitcoin's First Use Case: The Silk Road

Whilst the early days of Bitcoin generally consisted of the CypherPunks playing with and improving the technology, it was the idea of an American college student Ross Ulbricht to mix the digital currency with the anonymous web, the Tor Network. He created the website The Silk Road, an online marketplace for narcotics and other nefarious products. The benefits of The Silk Road to consumers is that not only could they remain anonymous through Tor; they could also purchase drugs anonymously as well. The Silk Road was the Crypto Anarchist dream in reality. The idea was not new with the early CypherPunks, discussing such a marketplace in 1992 on their mailing list in relation to digital currencies. However, it was not until Ulbricht put these two new technologies together that it came to fruition. Within the online marketplace, one could purchase close to any drug they chose as well as various illegal items such as weaponry (Vinga & Caset, 2015, p.84)

The website exploded in popularity when Gawker ran an article on their website in June 2011 (Gawker, 2011). Ulbricht was still unknown to the authorities and went by the pseudonym Dread Pirate Roberts. By 2013, the website had 10,000 products for sale and after Ulbricht's arrest, the FBI were able to secure 144,000 Bitcoins. At the time, this was equivalent to $28.5 million; it is now worth over $1 billion. Whilst The Silk Road was extremely popular, the technology of Bitcoin was still relatively new. The importance of The Silk Road in Bitcoin's evolution should not be underestimated. Ulbricht's website provided the first use case of the currency, enhancing not only its value but also its profile at the same time. The Silk Road proved that there was a market for digital currencies and that they were viable as well as useable. For the most part, law enforcement agencies are consistently attempting to play catch up to cyber criminals in their efforts to stop law breaking online. So far, they are losing the battle. The arrest of Ulbricht led to a significant drop in the value of Bitcoin, but the Silk Road survived with version 2.0 then 3.0 appeared under different ownership. Bell's Assassination Politics also became a reality with a website being set up on CryptoCurrency Augur, with President Trump one of the targets (Independent, 2018). The Silk Road

ultimately provided real Libertarian freedom for the consumer in a capitalist system. Whilst practically all the items for sale were illegal, using Tor and Bitcoin, consumers could operate beyond the laws of State, reducing their States power and emboldening their own. Whilst drug purchasing is obviously possible within society, never before had it been as easy and as safe for the consumer in terms of avoiding the law.

Since the events of the Silk Road, Bitcoin has attempted to become a more legitimate form of currency. Whilst still being used for many illegal purchases, many of the exchanges where Bitcoins are purchased have implemented "Know Your Customer" protocols to assuage the regulators from further inspection. This would seemingly go against the Crypto Anarchist persuasion of anonymity. Yet their solution has been to create various alternative coins that can be traded for Bitcoin. Coins such as Monero provide further anonymity features that prevent anyone from knowing who sent or even who received the coins (Noether, 2015). Users therefore can circumvent regulatory pressure, by changing their Bitcoin to Monero and then back again to Bitcoin, they can adhere to the current regulatory rules. Their argument for this level of privacy is based upon a long held idea that economies in developed nations are turning towards a cashless society (Warwick, 2002, Papadopoulos 2007). As debit and credit cards transactions begin to overtake cash, and then much like snooping on the Internet, banks and financial institutions can trace your location, your purchases and therefore your preferences. It gives them a near total understanding of yourself, beyond even your own understanding of self. Attempts by the State to combat the use of CryptoCurrencies mirror those of the initial combative measures taken when other encryption techniques arose such as Zimmerman's PGP. With the boundary of cyberspace being minimal new technologies can spread without friction. The Silk Road showed that Bitcoin and other CryptoCurrencies have value and can act much like money. As we head towards a cashless society, whereby your transactions can be closely monitored, CryptoCurrencies can retain the privacy element of cash, where by one can engage in the cash nexus without authorities knowing what you bought from who.

The Network Effect Of Peer To Peer Technology

Encryption techniques have been almost impossible for the State to stop once Zimmerman's PGP came out in the 1990's, despite this the State has increased control over surveillance due to a lack of appetite for this technology from the majority of citizens. In attempting to take on the economic sector through CryptoCurrencies, the Crypto Anarchists have yet to seriously suffer from the State. Rather the State has watched from the side-lines. An attempt to ban them would prove fruitless as not only could a person remain anonymous away from government eyes through Cryptography it is highly likely people would continue to use them for illicit activities. Added to this, the network remains impervious to outside influence thanks to its decentralised nature whereby no one, but everyone can verify it (Nakamoto, 2008). With the Proof Of Work algorithm underlying Bitcoin, for mining, the larger the chain of blocks becomes, the harder it becomes to attack it. Therefore, even at a market cap of $35 Billion, there were no supercomputers that were capable of breaking the Bitcoin protocol (Antonopoulos, 2017, p.4). The episode of Ulbricht's Silk Road showed that there is clearly a market for CryptoCurrencies even when their price is relatively cheap. So whilst a ban could have a severe effect on the price of one Bitcoin, it would be expected that people would still use it to transact with one another.

There have been previous Peer-To-Peer networks that have upset the apple cart in a similar way to the Silk Road and Bitcoin. The most notable of these was the rise of Torrent websites such as The Pirate Bay. Their system is not too dissimilar to that of Bitcoin. Rather than using a central intermediary such as Amazon to buy a DVD or CD of music, Torrent website created a decentralised network to share such files between people. Torrent websites proved that there was a demand for a new way to disseminate media. The influence of The Pirate Bay should not be underestimated with, The Pirate Party of Sweden a direct relation to the Pirate Bay's ideological thinking (Miaoran, 2009). Rather than sharing files, however, people are now sharing an economic network in Bitcoin. They are, consciously or unconsciously, removing the power from the 1% and return it to the people. Like

the early Torrent websites, Bitcoin has changed the narrative from breaking the rules to creating their own rules outside of the State.

A Currency Outside Of State Control

Bitcoin has been the saving grace of Julian Assange and WikiLeaks. In 2010, after one of their biggest leaks the large financing companies including Visa, MasterCard, PayPal and Western Union all shut of their services to WikiLeaks. This reduced their revenue by 95%. Without having the financial support through donations from people, it is likely that WikiLeaks would cease to exist. To solve the issue of funding, WikiLeaks decided to accept donations in Bitcoin instead in the year of 2011 (Popper, 2015, p.56-58). Since Bitcoin is not under any form of government control, there was very little that could be done to stop this happening. Assange has since claimed that this switch has allowed WikiLeaks to make a 50,000% return after Bitcoin's considerable price rise in the intervening years (Assange, 2017). The use of Bitcoin to support WikiLeaks highlights one of the key use cases for the digital currency and Crypto Anarchists. Without the State control that is provided through fiat currencies, WikiLeaks was able to attack the power of the State and continue to function through the use of this digital currency. Abstractly, it allows for the further funding/support of agencies and entities that the government does not agree with. Of course, there is a broad spectrum of who these actors are. However, the decentralized support for agencies considered beneficial to society will, in theory, receive more financial support. The survival of WikiLeaks has shown that although still in its early days CryptoCurrencies can remove the necessity of elements of the current financial system. This debate mirrors that of encryption. The greater encryption techniques one State or individual has over the other the greater power they retain. Yet unlike encryption and privacy, the State has been slow to react to the rise of Bitcoin and CryptoCurrencies.

Minimal government and currency control outside of Central Banking hegemony is key for Crypto Anarchists. If Bitcoin continues to advance in technology and more importantly in popularity,

then it could pose a greater problem for the hegemonic power of the USA through the US Dollar as the reserve currency of the world as the borderless nature allows US Dollars to be immaterial. International economic sanctions could become avoided by a nation harnessing CryptoCurrencies. Preventing finance going into the hands of unwanted actors becomes much more difficult, as evidenced by WikiLeaks. This possibility highlights that even power relations between States could be transformed. Russia and Venezuela have been investigating the potential of CryptoCurrencies diminishing the effects of sanctions placed upon both countries by the international community (Washington Examiner, 2018, Al Jazeera, 2018). Added to this as an open source project, anyone with the technical knowledge and desire can add to the technology. The open source movement has proven extremely powerful in creating some of the biggest advances in computer technology so far. Linux is the most popular Operating System in the world, above Apple's Mac operating system and above Microsoft Windows (TedX, 2013). Further to this, there are more benefits for those in the developing world to harness the use of Bitcoin and CryptoCurrencies. Globally 1.7 billion people still lack access to traditional bank accounts with the most common reason being that they lack the funds to open an account (Demirguc-Kunt, Asli, et al, 2017, p.5). With no permission needed from a central intermediary to purchase a Bitcoin, or even a fraction, this large market of people could enter a new economic model without the restrictions currently placed upon them.

State Disapproval But Finance Sector Intrigue

Despite the events of The Silk Road epitomising the Crypto Anarchists dream of a lawless Internet, the reaction from States has been remarkably subdued when compared to the debates over encryption. Not only have they been unable to form a cohesive message over what Bitcoin is, i.e. whether they should class it as money or something completely different, they are unable to decide whether they approve of the technology or not. Research from the University of Sydney has shown that around 44% of Bitcoin transactions are related to illegal activities with 25% of those using Bitcoin do so for illegality (Foley, Karlson, Putniņš, 2018). Currently around $5 billion worth of

Bitcoin are transacted each day (CoinMarketCap 2018). Not only can this illegality include drug trafficking but also the many scourges that politicians use as their reasons for stronger surveillance, including terrorism and money laundering. The difference in approach from government agencies towards the issue of encryption and CryptoCurrencies is partially due to the lack of knowledge on CryptoCurrencies being a new technology. Whilst encryption was largely in the hands of security agencies of the world throughout the 20th Century, CryptoCurrencies were never on their radar. This has led to the wide definition made by most government agencies.

In 2014, James Clapper acknowledged the use of Bitcoin by criminals in relation to money laundering for the Senate Select Committee on Intelligence but failed to mention anything more. This is despite the clear evidence they had from the Silk Road of further illegality in its use (Clapper, 2014). The Centre for a New American Security, a Washington based think-tank researched the use of virtual currencies such as Bitcoin in their relation to terrorist financing, however they only found anecdotal evidence suggesting that terrorists were still using more common methods of traditional finance (Goldman, Zachary K., et al, 2017). Yet there are still many worries that terrorism financing through CryptoCurrencies is a very real risk that needs to be monitored carefully. There have been calls from certain members of government to ban the use of CryptoCurrencies, but these tend to be from a single member of the elected government and rarely comes to fruition (Forbes, 2014). Despite the criticism of CryptoCurrencies, the unrivalled currency used for criminal activity is the US Dollar as noted by Jennifer Fowler, Deputy Assistant Secretary for the U.S Department of the Treasury (Fowler, 2017). Fowler hereby highlights the key issue that faces governments in arguments against such CryptoCurrencies. With the US dollar being the world reserve currency, much of it, like Bitcoin, is used on illegal activities. This is another reason why the push towards a cashless, traceable money society is a popular focus. As shown, within the privacy discussion, surveillance of online activity is constant. If citizens continue to use electronic payments, then another bow will be added to the string of the security agencies in their ability to analyse its citizen's lives.

The reaction from the Central Banks has been quite different however. One key aim of the Crypto Anarchist movements and Bitcoin is to subvert the power that these entities have over the economy. Whilst the Central Banks struggle to agree on how to define CryptoCurrencies, whether they are investments like gold or similar to actual currencies, they all show an interest in the underlying technology. Many companies and banks are permitting their own research into Blockchain technology, or distributed ledger technology as they sometimes refer to it (Ramsden, 2018). Rather than have a decentralised blockchain akin to Bitcoin, they are looking at centralised versions that will reduce the costs and rigidity of their business whilst maintaining their own control. Indeed, Central Banks of some nations are also researching such an idea. The initial interest, not only from Central Banks but also commercial banks, highlights that Blockchain technology has piqued their interest, much like the early advances in encryption of the RSA algorithm, DES or PGP. However, whilst these techniques were eventually overcome by the State, it remains to be seen whether the mainstream society of economics can provide superior versions of CryptoCurrencies that are centralised and at the same time convincing its citizens of their benefit.

With CryptoCurrencies making the Crypto Anarchist dream a reality, the discourse of government agencies between encryption and Bitcoin are stark. Whilst encryption is still seen as a danger, as it was throughout the 20th Century and surveillance key for "security" for civilian against the threat of crime and terrorism, Bitcoin has been allowed to continue to flourish relatively unscathed from criticism. Whilst leaders such as Theresa May or Attorney General Jeff Sessions stating they need to keep a close eye on Bitcoin, the reaction has been far more positive when compared to encryption (The Independent, 2018, CoinDesk, 2017). Encryption techniques have proven extremely valuable to the economy; they have enhanced the banking system through security and allowed governments to hide their messages. Despite this encryption for the public is still seen as a danger. The possible benefits of blockchain technology appears to have overridden such concerns for the government. The situation is not helped by States having to play catch up on

what Bitcoin is or how it works. By analysing the theory of Crypto Anarchy, they would be able to gain a clearer picture what the currency is aiming to achieve.

Whilst surveillance has been on the increase, it is through Bitcoin and CryptoCurrencies that the Crypto Anarchists could achieve greater disruption of power relations. Discussions over the benefits of new technologies often prove to be a double-edged sword. The future is notoriously hard to predict and advances in new technologies are faster than ever. This is why it is important to note the potential effect Bitcoin could have in disrupting the traditional financial sector, whilst remaining rational in noting the long way Crypto Anarchists have yet to go through CryptoCurrencies. The potential for CryptoCurrencies is evident though. However, much like the advances in encryption, the potential is limited in that of the citizens. Unless the articulation of what CryptoCurrencies and Bitcoin are capable of can be disseminated by the zealots of Bitcoin, then they could follow a similar path as to that of privacy whereby the technological advances are incorporated into the current economic system thereby nulling the benefits that the Crypto Anarchists seek. The ability of Bitcoin to subvert the current economic paradigm is possible not only for the individual but also for those States who are unhappy with the current neoliberal American hegemonic order. The developments of Crypto Anarchists and the intelligence agencies have been used for each other's benefit in combating one another. The dialectical outcome of this reality has been a political, social and technological double helix progression. One that neither side has complete control of. All the while, the contest for the hegemony of encryption takes place hidden in plain sight of the general population, thanks to the very nature of encryption.

Conclusion

Having published *1984* weeks before his deathbed, like a final prophetic warning to decedents of the Orwellian state, Orwell provided a bleak picture of the future: "If you want a picture of the future, imagine a boot stamping on a human face – for ever" (Orwell, 2013, p.337). The Crypto Anarchists can be seen as the premier group of intellectuals who, regardless of common sense, thought or opinion, have been the guardians against totalitarianism in all its guises. They are the citizens who, are, at the very least, trying to do something about Orwell's metaphorical stomping boot. The possibilities highlighted by the CypherPunks of Crypto Anarchy in the early 1990's have largely come true. Not only has the interconnected world through cyberspace led to higher levels of surveillance, but cryptology has also allowed for the creation of digital cash, the dark web and illegal markets that prove extremely difficult to stop. However, despite the powers of government attempting to prevent the spread of encryption, the cryptology of digital cash has yet to suffer such an attempt. Whilst the debate over encryption and privacy will continue throughout the coming decades as surveillance programs become total, the state will struggle to snoop on their citizens if those citizens choose to fight back. The technology that allows for anonymity, whether that be through encrypted applications or individual programs of code means that anonymity is possible even with the high levels of surveillance.

By analysing the philosophy and history of Crypto Anarchy, academics to activists, governments to citizens can better understand the crucial fight of our times – that for the right of the individual's privacy. If the popularity of CryptoCurrencies continues to advance, then the arguments used to dissuade people from encryption will likely be used to discourage citizens using CryptoCurrencies. By using CryptoCurrencies, States will attempt to show how, in so doing, citizens are supporting criminals and terrorists and ultimately making the world less secure. The effects of 9/11 cannot be underestimated on the encryption debate. Likewise, the popularity of Bitcoin cannot be delinked from 2008 Financial Crisis. Attempting to achieve Bitcoin's lofty goals of removing the

State from public life appears unlikely, though it does provide a sanctuary. A modern Pirate Utopia upon the open waters of the Internet. Yet with the technology now in the open, much like when Zimmerman's PGP became public, it is unlikely to go away. For governments to ban either encryption or CryptoCurrencies would prove problematic as well. The anonymous capabilities of both means that banning them might harm their popularity but the government would not be able to stop their use completely. Indeed, it may inspire the more ardent Crypto Anarchists to maximize the potential utility of Cryptography to engage in full-blown cyberwarfare (Bartlett, 2017). For many in oppressive regimes, this is fortunate. Both encryption and CryptoCurrencies prove their value in these circumstances. For those under control in China, TOR allows for access to materials that are banned by the State. Similarly, in Venezuela Bitcoin has proven an effective hedge against the hyperinflation of the Bolivar.

The citizens of the West have never possessed such an ability to regain individual power. We see this manifesting itself within the democratic systems with the election of Trump and the referendum of Brexit. There remains an underlying dissatisfaction, sparked by the Financial Crisis of 2008, combined with austerity programs and a lack of economic growth. This has been expressed in the form of anti-immigration sentiment in both countries. As this unhappiness continues to manifest itself, the State will look for protection. The easiest way to do so is gain more control through further surveillance and removing the ability to debate. Encryption techniques and privacy could prove to be essential. Freedom of speech is under threat from both the Left and Right as they attempt to use it to shut down one another. With this being the case, the ability to hide oneself online becomes ever more apparent in protecting one's rights. The partisan arguments of the day, Identity politics on the Left, and the Xenophobia of the Right, has nothing to say on the privacy debate. In fact, it makes the incursion of the State on individual's privacy simpler. It is akin to a self-imposed divide and conquer.

Under Crypto Anarchist thinking the rise of new encryption techniques were meant to revert power back towards the people. The fear of a surveillance state was correct, but the Crypto

Anarchists failed to predict the lack of appetite from citizens to protect themselves online. Therefore, instead of people increasing the power over the state the opposite happened whereby citizens can be closely monitored. The revitalisation of the Crypto Anarchist movement through Bitcoin and CryptoCurrencies has provided a second attempt at this reversal of power relations. However, this second attempt not only attempts to enhance the power of citizens but to remove the State totally through the destruction of the economic system. With the failure of the first movement through encryption, the likelihood of Bitcoin and its variants succeeding appear slim. Yet, at the same time, dissatisfaction with the status quo is growing around the world. Rather than tackle this dissatisfaction on a Nation State level, citizens of the world now have an opportunity to unite through the world first global digital currency, Bitcoin. Further financial woe coupled with the prospect of rising tensions throughout the world means that the possibility of a peaceful revolution under the guise of economic freedom is, for the first time, an actual possibility. However, potential for change within the hierarchy becomes much more challenging when those in power have a total overview and control of all the transactions. This is fundamentally what the Crypto Anarchists aim to remain free from. However, for now, the power of the State looks odds on to continue to dominate within the world of Cryptography. Unless a coherent network of positive Crypto Anarchism can form, expect more of Orwell's stomping boot on the human face.

Bibliography

Al Jazeera /. 2018. *What is Venezuela's new petro cryptocurrency?*. [ONLINE] Available at: https://www.aljazeera.com/news/2018/02/venezuela-petro-cryptocurrency-180219065112440.html. [Accessed 7 July 2018].

Antonopoulos, Andreas M. 2014 *Mastering Bitcoin: unlocking digital cryptocurrencies*. " O'Reilly Media, Inc.",.

Assange, Julian, 1995, *The Cypherpunk Mailing List,* Archive Available: https://github.com/Famicoman/cypherpunks-mailing-list-archives/tree/master/cryptome.org

Assange, Julian, et al. 2013, *Cypherpunks*. OR books,.

Barbrook, Richard & Cameron, Andy. 1996. *The Californian Ideology.* Science As Culture. 6. 44-72.

Bartlett, Jamie. 2015, *The dark net: Inside the digital underworld*. Melville House,.

Bauer, Craig P. *Secret history: The story of cryptology*. Chapman and Hall/CRC, 2013

Bell, Jim, 1995, *The Cypherpunk Mailing List,* Archive Available: https://github.com/Famicoman/cypherpunks-mailing-list-archives/tree/master/cryptome.org

BitcoinTalk.org / Hal Finney. 2013. *Bitcoin And me*. [ONLINE] Available at: https://bitcointalk.org/index.php?topic=155054.0. [Accessed 31 July 2018].

Brennan Center For Justice. 2013. *Are They Allowed to Do That? A Breakdown of Selected Government Surveillance Programs*. [ONLINE] Available at: https://www.brennancenter.org/analysis/are-they-allowed-do-breakdown-selected-government-surveillance-programs. [Accessed 1 July 2018].

Cannataci, Joseph A. 2016, "Report of the Special Rapporteur on the right to privacy." *Human Rights Council* .

Central Intelligence Agency. 2017. *Director Pompeo Delivers Remarks at CSIS*. [ONLINE] Available at: https://www.cia.gov/news-information/speeches-testimony/2017-speeches-testimony/pompeo-delivers-remarks-at-csis.html. [Accessed 20 June 2018].

Chaum, David. 1985. Security without identification: Transaction systems to make big brother obsolete. *Communications of the ACM, 28*(10), 1030-1044.

Chaum, David. 1983. Blind signatures for untraceable payments. *Advances in cryptology* (pp.). Springer, Boston, MA. 199-203

Clapper, James R. "*Worldwide Threat Assessment*," Testimony to the House Permanent Select Committee on Intelligence, 29th January 2014, Available: https://www.dni.gov/files/documents/Intelligence%20Reports/2014%20WWTA%20%20SFR_SSCI_29_Jan.pdf

CoinMarketCap. 2018. *Top 100 Cryptocurrencies by Market Capitalization*. [ONLINE] Available at: https://coinmarketcap.com/. [Accessed 6 August 2018].

CoinDesk / Nikhilesh De. 2017. *Attorney General Jeff Sessions: Bitcoin on Dark Web 'Is a Big Problem'*. [ONLINE] Available at: https://www.coindesk.com/jeff-sessions-bitcoin-use-is-a-big-problem/. [Accessed 2 July 2018].

Demirguc-Kunt, Asli, et al. 2018, *The Global Findex Database 2017: Measuring Financial Inclusion and the Fintech Revolution*. The World Bank,.

Etzioni, Amitai. 1999. *The limits of privacy*. New York: Basic Books.

Foley, Sean and Karlsen, Jonathan R. and Putniņš, Tālis J., Sex, Drugs, and Bitcoin: How Much Illegal Activity Is Financed Through Cryptocurrencies? (January 15, 2018). Available at SSRN: https://ssrn.com/abstract=3102645

Forbes / Andy Greenberg. 2014. *Senator Calls For Ban In Bitcoin Letter To Financial Regulators*. [ONLINE] Available at: https://www.forbes.com/consent/?toURL=https://www.forbes.com/sites/andygreenberg/2014/02/26/senator-calls-for-bitcoin-ban-in-letter-to-financial-regulators/. [Accessed 3 July 2018].

Fowler, Jennifer, *Deputy Assistant Secretary, Office of Terrorist Financing and Financial Crimes,* Testimony to the Senate Judiciary Committee Hearing, 28th November 2017, Available: https://www.judiciary.senate.gov/imo/media/doc/Fowler%20Testimony.pdf

Gawker / Adrian Chan. 2011. *The Underground Website Where You Can Buy Any Drug Imaginable*. [ONLINE] Available at: http://gawker.com/the-underground-website-where-you-can-buy-any-drug-imag-30818160. [Accessed 8 July 2018].

Goldman, Zachary K., et al. 2017, "Terrorist Use of Virtual Currencies." *Washington DC: Center for a New American Security, May* 3

Greenberg, Andy. 2012, *This Machine Kills Secrets: How WikiLeakers, Hacktivists, and Cypherpunks Are Freeing the World's Information*. Random House,.

Gordon, Uri. 2008. *Anarchy alive! : Anti-authoritarian politics from practice to theory*. London. Pluto Press

Hayden, Michael V. 2014, "Beyond Snowden: an NSA reality check." *World Affairs* 176.5 : 13-23.

Holden, Joshua. 2017. *The mathematics of secrets : Cryptography from Caesar ciphers to digital encryption*.

Howard, Philip N., and Muzammil M. Hussain. 2013, *Democracy's fourth wave?: digital media and the Arab Spring*. Oxford University Press,.

Hughes, Eric, 1993, A Cyperpunk's Manifesto, In: Ludlow, P. (2001). *Crypto Anarchy, Cyberstates, and Pirate Utopias* (1st ed.). London: The MIT Press.

Information Is Beautiful. 2018. *World's Biggest Data Breaches*. [ONLINE] Available at: http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/.

[Accessed 17 July 2018].

Kahn, David. 1966. *The codebreakers : The story of secret writing*. London: Weidenfeld and Nicolson.

Levy, Steven. 2001 *Crypto: How the code rebels beat the government--saving privacy in the digital age*. Penguin

Li, Miaoran. 2009, "The pirate party and the pirate bay: How the pirate bay influences Sweden and international copyright relations." *Pace Int'l L. Rev.* 21 : 281.

London Real. 2017. *Jamie Bartlett - Radicals- PART 1/2 | London Real*. [Online Video]. 9 July 2017. Available from: https://www.youtube.com/watch?v=85zOpnrfum8. [Accessed: 1 August 2018].

Lyon, David. 2015, *Surveillance after Snowden*. John Wiley & Sons,.

May, Timothy, 1992, *CypherPunk Mailing List,* [Online] Archive Available: https://github.com/Famicoman/cypherpunks-mailing-list-archives/tree/master/cryptome.org

May, Timothy, 1994, Crypto Anarchy and Virtual Communities In: Ludlow, P. (2001). *Crypto Anarchy, Cyberstates, and Pirate Utopias* (1st ed.). London: The MIT Press.

May, Timothy, 2001, The Crypto Anarchist Manifesto, Communities In: Ludlow, P. (2001). *Crypto Anarchy, Cyberstates, and Pirate Utopias* (1st ed.). London: The MIT Press.

McLaughlin, Paul. 2016, "Crypto Wars 2.0: Why Listening to Apple on Encryption Will Make America More Secure." *Temp. Int'l & Comp. LJ* 30, 353

Nakamoto, Satoshi. 2008, "Bitcoin: A peer-to-peer electronic cash system." .

Noether, Shen. 2015, "Ring SIgnature Confidential Transactions for Monero." *IACR Cryptology ePrint Archive,* 1098.

Orwell, George, 2013. *1984*. 4th ed. London: Arcturus Publishing Ltd.

Papadopoulos, Georgios. 2007 "Chapter 4: Electronic money and the possibility of a cashless society." *Survey of Electronic Money Developments* .

Parent, William A. 2017, "Privacy, morality, and the law." *Privacy*. Routledge, 105-124.

Pednekar-Magal, Vandana, and Peter Shields. "The State and Telecom Surveillance Policy: The Clipper Chip Initiative." *Communication Law and Policy* 8.4 (2003): 429-464.

Popper, Nathaniel. 2015, *Digital gold: Bitcoin and the inside story of the misfits and millionaires trying to reinvent money*. New York: Harper,

Ramsden, David 2018, *The Bank Of England – Open To Fintech,* 22nd March 2018, Available: https://www.bis.org/review/r180327a.pdf

Reuters / Dustin Volz. 2018. *Trump signs bill renewing NSA's internet surveillance program*. [ONLINE] Available at: https://www.reuters.com/article/us-usa-trump-cyber-surveillance/trump-signs-bill-renewing-nsas-internet-surveillance-program-idUSKBN1F82MK. [Accessed 3 July 2018].

Shone, Steve. 2013. *American anarchism* (Studies in critical social sciences). Leiden: Brill.

TedX Talks. 2013. *What the Tech Industry Has Learned from Linus Torvalds: Jim Zemlin at TEDxConcordiaUPortland*. [Online Video]. 15 April 2013. Available from: https://www.youtube.com/watch?v=7XTHdcmjenI. [Accessed: 23 July 2018].

The Guardian. 2013-2017. *The Snowden Files*. [ONLINE] Available at: https://www.theguardian.com/world/series/the-snowden-files. [Accessed 31 July 2018].

The Guardian. 2018. *The Cambridge Analytica Files*. [ONLINE] Available at: https://www.theguardian.com/news/series/cambridge-analytica-files. [Accessed 11 July 2018].

The Guardian / Ian Cobain. 2018. *UK has six months to rewrite snooper's charter, high court rules*. [ONLINE] Available at: https://www.theguardian.com/technology/2018/apr/27/snoopers-charter-investigatory-powers-act-rewrite-high-court-rules. [Accessed 9 July 2018].

The Independent / Aatif Sulleyman. 2018. *Bitcoin Latest: Theresa May '' Very Seriously'' Considering Taking Action Against Digital Currencies*. [ONLINE] Available at: https://www.independent.co.uk/life-style/gadgets-and-tech/news/bitcoin-latest-updates-uk-regulation-theresa-may-control-ban-digital-currencies-cryptocurrencies-a8177631.html. [Accessed 21 July 2018].

The Independent / Anthony Cuthbertson. 2018. *Donald Trump Assassination Market Appears On Blockchain Platform Augur*. [ONLINE] Available at: https://www.independent.co.uk/life-style/gadgets-and-tech/news/donald-trump-assassination-market-blockchain-augur-a8464516.html. [Accessed 4 August 2018].

The Intercept / MI5. 2016. *The Digint Narrative*. [ONLINE] Available at: https://theintercept.com/document/2016/06/07/digint-narrative/. [Accessed 4 July 2018].

The Washington Post. 2014. *Transcript of President Obama's Jan. 17 speech on NSA reforms*. [ONLINE] Available at: https://www.washingtonpost.com/politics/full-text-of-president-obamas-jan-17-speech-on-nsa-reforms/2014/01/17/fa33590a-7f8c-11e3-9556-4a4bf7bcbd84_story.html?noredirect=on&utm_term=.1e3feef030cd. [Accessed 28 June 2018].

Zimmerman, Phillip. 1999. *Why I Wrote PGP*. [ONLINE] Available at: https://www.philzimmermann.com/EN/essays/WhyIWrotePGP.html. [Accessed 26 July 2018].

Zimmerman, Phillip 1997. *Beware Of Snake oil*. [ONLINE] Available at: https://philzimmermann.com/EN/essays/SnakeOil.html. [Accessed 19 June 2018].

Twitter / Edward Snowden. 2016. *The UK has just legalized the most extreme surveillance in the history of western democracy. It goes farther than many autocracies.*. [ONLINE] Available at: https://twitter.com/snowden/status/799371508808302596?lang=en. [Accessed 28 June 2018].

Twitter / Julian Assange. 2017. *My deepest thanks to the US government, Senator McCain and Senator Lieberman for pushing Visa, MasterCard, Payal, AmEx, Mooneybookers, et al, into erecting an illegal banking blockade against @WikiLeaks starting in 2010. It caused us to invest in Bitcoin -- with > 50000% return.*. [ONLINE] Available at: https://twitter.com/JulianAssange/status/919247873648283653/photo/1?ref_src=twsrc%5Etfw%7Ctwcamp%5Etweetembed%7Ctwterm%5E919247873648283653&ref_url=https%3A%2F%2Fwww.cnbc.com%2F2017%2F10%2F16%2Fwikileaks-julian-assange-bitcoin-50000-percent-return-thanks-to-us-government.html. [Accessed 20 July 2018].

Vigna, Paul, Casey, Michael 2015. *The Age Of CryptoCurrency*. 1st ed. New York: St. Martins Press.

Warwick, David R. 1992, "The cash-free society." *The Futurist* 26.6 : 19.

Washington Examiner / Travis Tritten. 2018. *The dark side of bitcoin: Terror financing and sanctions evasion*. [ONLINE] Available at: https://www.washingtonexaminer.com/the-dark-side-of-bitcoin-terror-financing-and-sanctions-evasion. [Accessed 1 August 2018].