Control society has been discussed in terms of digital, computational and networked machine. Discuss this view of control in relation to theories of biopower. Illustrate your answer by drawing on relevant theories and using specific examples.

Gregory White	Dr. Luciana Parisi
MA Computational Arts	Critical Theory
Student Number:	CU71007A
3316914501	2015-16

Goldsmiths, University of London

Date Submitted:
11 January 2016

During Hong Kong's Umbrella Revolution of 2014, protestors were faced with the threat of network surveillance and censorship from the Chinese government in an attempt to suppress resistance. With photo-sharing websites like Instagram blocked in mainland China due to the widespread distribution of images depicting and documenting the unrest in the streets,[1] the pro-democracy demonstrators anticipated government-enforced Internet outages, and turned instead to the smartphone application FireChat[2] to organise protest activity. FireChat is built on the principle of the distributed or 'mesh' network: it allows users to communicate directly with each other using their phone's Bluetooth or Wi-Fi signals,[3] eliminating the need for a centralised hub which could be monitored or blocked by the government.

This is just one example of the affordances of distributed networks, and how they relate to power, freedom, and control. In this essay I will explore these notions and their complex, intertwined relationships through the work of critics Wendy Hui Kyong Chun and Alexander Galloway. I will select relevant ideas and concepts to discuss them through this lens, leading me towards an analysis of control and freedom, network models and their relationships to power, and how the architecture of the Internet enables the above to function within our society. With this knowledge in place I will return back to the example of FireChat and other recent technologies developed with these very ideas in mind, technologies that Wolfgang Sützl and Theo Hug describe as being "capable of introducing discontinuities in hegemonic discourses, and of surprising and disorienting the strategic system of powerful institutions, be they governmental or corporate."[4]

[1] Lauren C. Williams, 'Damning Photos From Hong Kong Protests Cause China To Block Instagram' in *ThinkProgress* (29 September 2014). Accessed at http://thinkprogress.org/world/2014/09/29/3573251/china-blocks-instagram/. Accessed on 9 January 2016.

[2] Available for iOS and Android: http://opengarden.com/firechat/

[3] Lauren C. Williams, 'The Tech Behind Hong Kong Protesters' Ingenious New Way To Duck Surveillance' in *ThinkProgress* (3 October 2014). Accessed at http://thinkprogress.org/world/2014/10/03/3575225/hong-kong-protesters-use-mesh-networks-to-skirt-censorship/. Accessed on 9 January 2016.

[4] Wolfgang Sützl and Theo Hug (Eds.), *Activist Media and Biopolitics: Critical Media Interventions in the Age of Biopower* (Innsbruck University Press, 2012), 7.

In *Control and Freedom: Power and Paranoia in the Age of Fibre Optics*,[5] Chun examines the etymology of the terms ‘freedom’ and ‘control’, and how they have been conflated into what she refers to as ‘control-freedom’ through the use of information technologies. With this information we will then look at the rhetoric surrounding the Internet, both as a bastion of freedom and a tool for total surveillance, before deconstructing these arguments to reveal how the functioning of the Internet (and indeed, the freedom that it grants) is dependent entirely on methods of control.

The definition of ‘freedom’, as shown by Chun from the very beginning of *Control and Freedom*, is one that has undergone much change in the West, in part due to the recent decades of war and conflict. Freedom has become a goal to fight for and protect — something that requires struggle to defend from the enemy. But Chun argues that this objectification of freedom, conflated with safety and security, diminishes the very term: “If freedom is reduced to a gated community writ large or becomes the ideological watchword of a national security state, then it can turn into nothing more than the partner of, or the alibi for, control”.[6] Freedom in this case has come to refer to freedom of movement (of people or information) within a stringently defined set of rules: it relies on control to operate. This “control-freedom”[7] is exemplified by the protocols that enable the Internet to function, as we will explore later in this essay. Although freedom and control have become conflated here, Chun is keen to point out that they are not the same, that “the linkage is not an identity…their conflation is a response to the failures of both liberty and discipline and marks a significant shift in the apparatuses of power.”[8] This shift has much to do with the emergence of information technologies, particularly the Internet.

[5] Wendy Hui Kyong Chun, *Control and Freedom: Power and Paranoia in the Age of Fibre Optics* (Massachusetts Institute of Technology Press, 2006).

[6] Chun, *Control and Freedom*, vii.

[7] Ibid., 1.

[8] Ibid., viii.

The Internet has long been surrounded by verbose claims that overemphasise its capacity for enabling freedom from governments and corporations alike, and Chun joins critics such as Alexander Galloway and Evgeny Morozov[9] in deconstructing them. Through enabling anonymous communication, the Internet "allegedly freed users from the limitations of their bodies, particularly the limitations stemming from their race, class, and sex."[10] Forums and chat rooms enabled anyone with access to a computer and an Internet connection to discuss and share whatever they wanted without censorship, from Harry Potter fan-fiction to right-wing extremism, without revealing their true identity.[11] Through the use of usernames and avatars, the importance was to be placed on the content, as opposed to who was communicating it. However, anonymity also allowed for widespread 'trolling' and cyberbullying as accountability for our actions was lost behind the protection of our multiple online personas, making online safe-spaces more difficult to maintain. To combat this, corporations who provide social media services like YouTube and Facebook began to force (or at least *heavily persuade*) users to use their real names,[12] thus moving to hold everybody accountable for their actions at the price of anonymity.

These same websites have an interesting relationship with both control and freedom in relation to creative work. Websites like MySpace and YouTube have undoubtably had a dramatic effect on the democratisation of media production, enabling users to share their creations and indeed providing the platform for such successful pop artists as Lily Allen and Justin Bieber to be discovered. These hosting websites and social media platforms have certainly enabled more people,

[9] Some of Alexander Galloway's points will be discussed later in this essay. For Morozov, see *The Net Delusion* (PublicAffairs, 2011).

[10] Chun, *Control and Freedom*, 2.

[11] See Jamie Bartlett's *The Dark Net* (William Heinemann, 21 Aug 2014) for some rather harrowing accounts on the seedier and more extreme uses of the Internet.

[12] After receiving much backlash, Google reversed this policy: Samuel Gibbs, 'The return of the YouTube troll: Google ends its 'real name' commenter policy' in *The Guardian* (16 July 2014). Accessed at http://www.theguardian.com/technology/2014/jul/16/youtube-trolls-google-real-name-commenter-policy. Accessed on 4 January 2015.

from teenage bedroom-vloggers[13] to video-gamers[14] to not only have a voice, and not only make a living off of the content they produce, but become superstars in the process.

But in providing the platforms which allow users to share their work and the work of others, these websites-turned-corporations also hold a lot of power in deciding what, and indeed who, gets heard. In the 2014 documentary *The Internet's Own Boy*, a remarkably young Aaron Swartz deftly summarises the newfound ability for everybody to be heard on the Internet and the corresponding shift in power towards these "gatekeeper" websites:

> In the old system of broadcasting you were fundamentally limited by the amount of space in the airwaves…you could only send out ten channels of television, or even with cable you had 500 channels. On the Internet, everybody can have a channel, everyone can get a blog or a MySpace page, everyone has a way of expressing themselves. And so what you see now is not a question of who gets access to the airwaves, it's a question of who gets control over the ways you find people. You start to see power centralising in sites like Google, these sort of gatekeepers that tell you where on the Internet you want to go — the people who provide you your sources of news and information. So it's not 'only certain people have a license to speak', now everybody has a license to speak: it's a question of who gets heard.[15]

Looking at the top creators promoted by YouTube, both through their website and on billboards across London and New York City, we face the same sorts of problems regarding diversity as in other areas of the media: most are still white and middle class, though typically younger. While this has been a longstanding issue existing even before the Internet, sites like YouTube have the ability to tackle issues of representation through the creators they promote.

[13] Alfie Deyes: https://www.youtube.com/user/PointlessBlog.

[14] Pewdiepie: https://www.youtube.com/user/PewDiePie.

[15] Aaron Swartz, *The Internet's Own Boy: The Story of Aaron Swartz.* Dir. Brian Knappenberger. Luminant Media, 2014. Film.

As described in the introduction of this essay, corporations are not the only bodies to affect the freedoms afforded by the Internet; governments also have an active role, from the 'Great Firewall of China' that prevents Chinese citizens from accessing sites as large as Facebook and Google, to David Cameron's Internet porn ban, proposed in 2013, that forces Internet Service Providers to block anything deemed dubious (including websites providing sex and drug education) by default.[16] In locations where Internet censorship is more prevalent, users may have to use services like Tor, a distributed network that anonymises your identity and location and enables access to blocked content.[17] Furthermore if the government decides to restrict Internet access all together, as anticipated in the aforementioned Umbrella Revolution, then people have to utilise software like FireChat in order to communicate.

Chun is also keen to examine the other side of the coin, stating, "this rhetoric of the Internet as freedom, excessive or not, was also accompanied by Internet rumours of the Internet as a dark machine of control."[18] In her view the idea of an infallible, all-powerful government agency that could store and analyse Internet activity on a national, or indeed international, scale was an overstated one:

> Even the U.S. National Security Agency (NSA) admits this impossibility…Computers crash on a regular basis, portable storage devices become unreadable, and e-mail messages disappear into the netherworld of the global network, and yet many people honestly believe in a worldwide surveillance network in which no piece of data is ever lost.[19]

While Chun may have good cause to be sceptical about the unfailing nature of such intelligence organisations, there is still much reason to scrutinise and critique their behaviour. In the wake of

[16] Laurie Penny, 'David Cameron's internet porn filter is the start of censorship creep' in *The Guardian* (3 January 2014). Accessed at http://www.theguardian.com/commentisfree/2014/jan/03/david-cameron-internet-porn-filter-censorship-creep. Accessed on 4 January 2016.

[17] The Tor project (https://www.torproject.org) will be discussed in more detail towards the end of this essay.

[18] Chun, *Control and Freedom*, 2.

[19] Ibid., 6.

Edward Snowden's leaks on the illegal and overreaching surveillance practises committed by the NSA and Britain's GCHQ, penetrating the very fibre optic cables that Chun refers to in the title of her book, surveillance is in the public consciousness more than ever; which also means that more people are aware that they may be being observed, and, if the effects of Jeremy Bentham's panopticon[20] remain true, are changing their behaviour accordingly.[21]

Debating whether the Internet is an enabler of freedom or control is missing the point, according to Chun, calling these questions and their assumptions "misguided".[22] Instead, she focuses her attention on the control technologies that enable the Internet and the freedoms it affords us to exist, and what it means to link the two together: "Moving from utopian narratives about cyberspace to the underlying hardware the Internet seeks to obscure… [Chun] traces the structuring paradox of information and communications: *without control technologies, no freedom* (of choice or movement)."[23]

Providing the example of what happens beneath the user-interface when we use the Internet, Chun peels back the layers to reveal how much of the activity in browsing a web page is performed without our knowledge or consent, and how user-interfaces merely provide us with an illusion of control over our actions. The passage reads:

> Consider, for instance, what happens when you browse a Web page. Your computer sends information, such as your Internet Protocol (IP) address, browser type, language preference, and userdomain (your userdomain often contains information such as your physical location or username)… the moment you turn on your computer…your Ethernet card participates in

[20] Jeremy Bentham, *The Panopticon Writings* (Verso, 1995).

[21] Lee Rainie and Mary Madden, 'How People are Changing Their Own Behaviour' in *PewResearchCenter*. Accessed at http://www.pewinternet.org/2015/03/16/how-people-are-changing-their-own-behavior/. Accessed on 4 January 2016.

[22] Chun, *Control and Freedom*, 3.

[23] Ibid., viii. Emphasis my own.

> an incessant "dialogue" with other networked machines…Your screen, with its windows and background, suggests that your computer only sends and receives data at your request. It suggests that you are that all-powerful user…Using a packet sniffer, however, you can see that your computer constantly wanders without you. Even when you are not "using," your computer sends and receives, stores and discards—that is, reads—packets, which mostly ask and respond to the question "Can you read me?" These packets are anything but transparent to you, the user: not only must you install a sniffer to see them; you must also translate them from hexadecimal—that is, if your operating system (OS) allows you to install a sniffer, which classic Macs do not.[24]

From this example we can learn several things of importance. First of all, we may feel that we are in control of the information that we share, based on what is displayed on the screen in front of us: perhaps we'd rather keep our physical location or other identifying characteristics to ourselves, so we refrain from adding that information to our Facebook profile or geotagging an Instagram picture. But much of this information is already being shared, just by accessing the webpage. Again, this is why services such as Tor and Virtual Private Networks (VPNs) are useful, particularly to vulnerable people like journalists or activists in politically unstable or dictatorial areas, as they allow the user to reroute their browsing behaviour through servers around the globe in order to protect their physical location.

Also of interest is the knowledge that our computers are engaging in a constant exchange of information, without which "there would be no user interactions, no Internet."[25] Chun challenges the oversimplified idea that the Internet is constructed of 'hosts' and 'servers', describing how (in a literal form of control[26]) our computers are continually reading and reproducing packets to see if

[24] Ibid., 3-4.

[25] Ibid., 5.

[26] "According to the *Oxford English Dictionary*, the English term control is based on the French *contreroule* —a copy of a roll of an account and so on, of the same quality and content as the original." Ibid., 4.

they are addressed to our computer. This behaviour is crucial to the structure of the Internet and the freedoms it affords us, the storage, access, and analysis of data (all heavily associated with organisations like the NSA) inherent in the way that it functions: "the Internet as an unfailing surveillance device is thus the obverse, not the opposite, of the Internet as an agency-enhancing marketplace."[27]

Finally, we become aware that our behaviour is restricted by the way in which the technology we use is designed, preventing us from having the full control we believe we possess. While we may feel like everything is available to us on screen or in a menu, in reality a lot of the more involved technical aspects of our machines are hidden and inaccessible. This is partly why some groups have gravitated towards open source operating systems like Linux, which are not only freely accessible but freely modifiable.

With the understanding that it is the underlying technologies of the Internet and their relationship to these notions of 'freedom' and 'control' that should be inspected, let us move towards a more concrete dissection of how they operate and their relationship with power. For this next section I will draw upon Alexander Galloway's analysis of protocols, specifically TCP/IP and DNS, from his book *Protocol: How Control Exists after Decentralisation.*[28] But before we closely examine these protocols, we need to understand why Galloway argues their importance. Therefore let us first look at the paradox that he, in a similar way to Chun, reveals: how freedom, as afforded to us by the Internet, is built on strict layers of protocological control. This will allow us to see the control that is inherent in the structure of networks, leading to an analysis of how power operates through different types of networks — centralised, decentralised, and distributed — before arriving at TCP/IP and DNS, and the architecture of networked control as it is implemented in our society.

[27] Ibid., 5

[28] Alexander Galloway, *Protocol: How Control Exists after Decentralisation* (Massachusetts Institute of Technology Press, 2004).

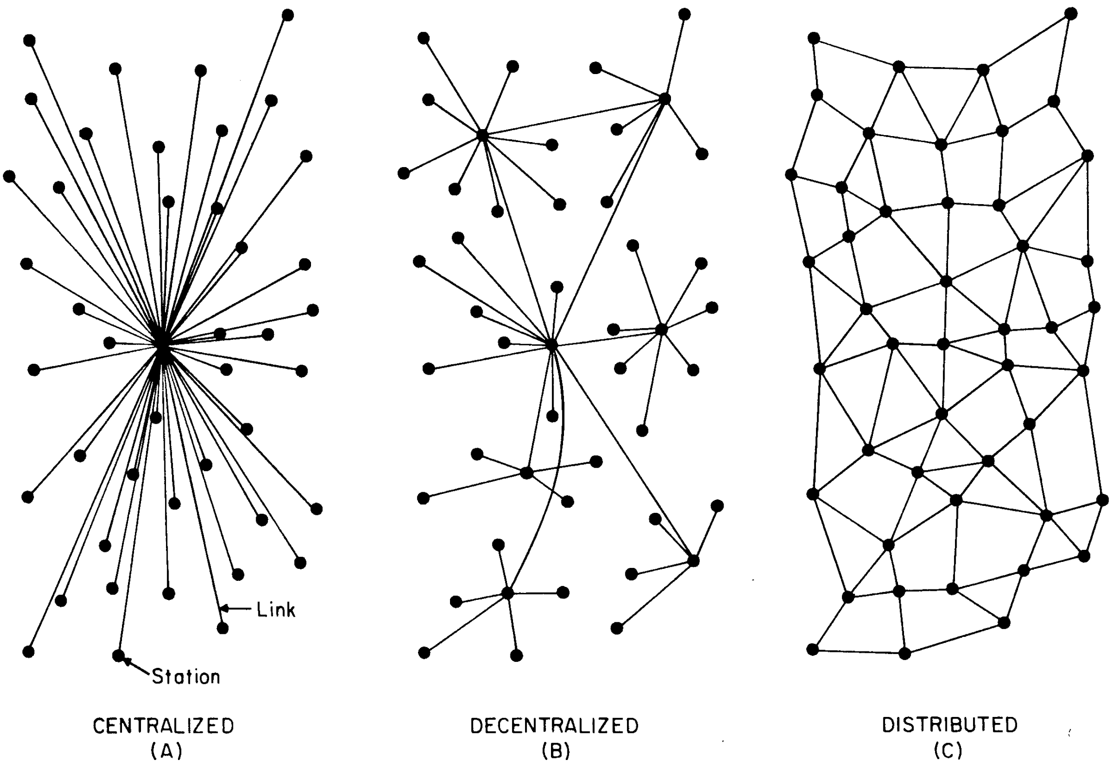


Figure 1: Network diagrams from Paul Baran, *On Distributed Communications: 1. Introduction to Distributed Communications Networks* (RAND, 1964), 2.

In *Protocol: How Control Exists after Decentralisation*, Galloway reveals how fundamentally the Internet is centred around control, not freedom — a protocological control. “Protocols,” Galloway writes, “refer specifically to standards governing the implementation of specific technologies…Computer protocols establish the essential points necessary to enact an agreed-upon standard of action.” But, paradoxically, these layered and hierarchical protocols are what allow the Internet to be so fluid and adaptable, moving away from rigid structures towards a more rhizomatic and distributed form of power. Similar to what Chun argues, these control technologies that form the architecture of Internet networks are key in determining how power operates. Let us now take a deeper look at a variety of network structures to illustrate what this means.

Starting with centralised networks (see figure 1), the most basic diagram, we can see a central hub from which information, power, or whatever else, travels outwards toward the surrounding nodes. Each node is only in contact with the hub, and the flow of information/power is unidirectional, only moving from hub to node. An example of such a network in society could be a king or dictator, from who all laws and orders are given and must be obeyed without chance of appeal. Galloway also indicates that the aforementioned panopticon is an example of a centralised network, with the guard at the centre exercising power from a central (and literally higher-up) position outward towards the peripheral prisoners, each isolated from the others in their own cell. This form of network is therefore a very hierarchical one, with a single body possessing control and power over its subjects. However, this also makes for a particularly vulnerable network: if the main hub is to fall, the whole system breaks down.

Decentralised networks are similar, in that they contain a number of connected centralised networks. Rather than one hub there are several, each with its own set of nodes, but no overarching or all-powerful leader. And again, no node is connected to another, no matter which hub they are bound to. The example that Galloway gives is that of a US airline system: "In it, one must always travel through certain centralised hub cities—generally in the Midwest or central areas of the United States. Direct nonstop service is only possible if one happens to be traveling from one hub to another."[29] This makes for a slightly more flexible network model as there is no central weak point, but failure of a single hub can still have drastic knock-on effects; to continue the airline analogy, delays at a small airport in the south of Spain can have a significant ripple effect on larger international airports like Heathrow.[30]

[29] Ibid., 31-2

[30] This 'power-law', in short the capacity of smaller points in a network to affect larger ones, is discussed in depth by Albert-László Barabási in his book *Linked: The New Science of Networks* (Perseus Publishing, 2002).

For our purposes the most interesting diagram is the third, the distributed network. It differs from the others in that it has no central hub of command, no chokepoints or bottlenecks. Each node has the ability to connect directly to any other node, allowing for highly flexible and adaptable systems; if one path becomes unusable, a multitude of others may be taken in its stead. In this regard distributed networks are similar to the US highway system (interestingly, developed around the same time as the Internet[31]), where many routes may be taken to reach the same destination.[32] Information/power is therefore more free to flow around the network as a whole (it is more *distributed*) than compared to the other two models presented here, potentially leading towards more democratic power structures. Deleuze and Guattari provide a highly effective example of distributed networks in *A Thousand Plateaus*[33] with the rhizome, succinctly summarised here by Galloway:

> Reacting specifically to what they see as the totalitarianism inherent in centralised and even decentralised networks, Deleuze and Guattari instead describe the rhizome, a *horizontal meshwork* derived from botany. The rhizome links many *autonomous* nodes together in a manner that is *neither linear nor hierarchical*. Rhizomes are *heterogeneous and connective*, that is to say, 'any point of a rhizome can be connected to anything other.'[34] They are also *multiple and asymmetrical*: '[a] rhizome may be broken, shattered at a given spot, but it will start up again on one of its old lines, or on new lines.'[35] [36]

Understanding these properties, it is clear that services like FireChat and Tor are built on the very principles of distributed/*mesh* networks. Modelling Internet and communications on distributed

[31] Galloway, *Protocol*, 38.

[32] Ibid., 35.

[33] Gilles Deleuze and Félix Guattari, *A Thousand Plateaus,* trans. Brian Massumi (University of Minnesota Press, 1987).

[34] Ibid., 7.

[35] Ibid., 9.

[36] Galloway, *Protocol*, 33. Emphasis my own.

networks allows users to circumvent government or corporate blocks and censorship that stand in between them and free access to information. As in the example of FireChat, such a network enabled very physical, real-life consequences on the streets of Hong Kong**,** enabling protesters to effectively organise and communicate despite the restrictions imposed on Internet access in an attempt to quell rebellion. Such an example clearly demonstrates the power and effectiveness of distributed networks.

Before we move on, it is worth pausing to note that these three networks do not necessarily constitute a timeline; starting with centralised power before evolving into decentralised, and eventually reaching distributed power today. All three of these structures can be, and indeed are, observed simultaneously within different parts of society. To think that in moving towards distributed networks we have eradicated centralised and decentralised ones is a mistake.

With this knowledge of networks and their relation to power in place, let us make an inspection of the actual technologies that allow the distributed network of the Internet to exist.

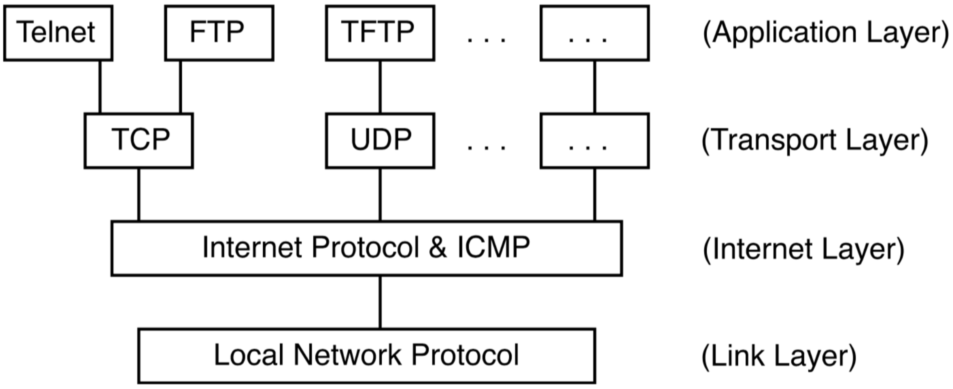


Figure 2: Protocol layers diagram from Alex Galloway, *Protocol: How Control Exists after Decentralisation* (Massachusetts Institute of Technology Press, 2004), 39.

In order for the multitude of connected devices that form ‘the Internet’ to function and pass packets of information between one another, they must adhere to a set of predetermined rules, or *protocols*, outlined in a set of documents called ‘Requests for Comments’ (RFCs).[37] There are numerous layers of these protocols, illustrated in figure 2, each with a very specific function. A detailed description of the intricacies of each layer of protocol is far beyond the scope of this essay; for that information I direct you towards Galloway’s excellent explanation in the *Physical Media* chapter of *Protocol*. Here we will examine TCP, part of the transport layer, and IP, of the Internet layer, since, as Galloway remarks, it is “the division of labour between the transport layer and the Internet layer…[that] *creates the conditions of existence for the distributed network*.”[38]

TCP, or ‘Transmission Control Protocol’, is an example of ‘transport layer’ protocol. This means it has no regard for the actual information being transported, but instead ensures that all of the information comprising the packet arrives to its intended recipient whole. In instances where part of the information is lost, it is simply resent by the transport layer. This is the key advantage that TCP affords, providing a level of flexibility and adaptability that enables the Internet to withstand communication errors and the corruption of information; or, as described in the RFC, “robustness in the presence of communication unreliability and availability in the presence of congestion.”[39]

As seen in figure 2 the transport layer is nested inside of the Internet layer, where IP, or ‘Internet Protocol’, exists. The RFC for Internet IP describes its function as “transmitting blocks of data called datagrams from sources to destinations,”[40] which TCP then ensures has arrived complete. Breaking up data into smaller datagrams allows the information to pass through more limited networks that might hold size restrictions, depending on bandwidth. This is particularly useful in areas where high-speed Internet is hard to access, usually less economically developed

[37] Robert Braden, ‘Requirements for Internet Hosts,' in *RFC 1122* (October 1989).

[38] Galloway, *Protocol*, 41. Emphasis my own.

[39] Jonathan Postel, 'Transmission Control Protocol,' in *RFC 793* (September 1981), 1, as referenced in Galloway, *Protocol,* 44.

[40] Jonathan Postel, 'Internet Protocol,' in *RFC 791* (September 1981), 1, as referenced in Galloway, *Protocol,* 44.

parts of the world. The most interesting part of IP in this context is exactly how it transmits these datagrams, using a flexible routing process that must account for the myriad of possible paths in a distributed network. "Since networks are heterogeneous and ever-changing, the route between point A and point B is never fixed but must be rethought each time material wishes to pass over it," writes Galloway.[41]

> This...is achieved through a "hopping" process whereby data is passed from computer to computer in sequence. None of the computers in the chain of hops knows definitively where the desired destination lies. But they do know in which general direction the destination is. They pass their datagrams to the computer that lies in the "general direction" of the destination.[42]

In the event of a "faulty hop", or if a datagram makes too many hops without reaching its destination, a different route is chosen.[43]

It is this combination of TCP and IP that enables the robustness of communication through a highly-flexible and rhizomatic distributed form of network, able to withstand interruption and corruption alike. As described by Galloway and illustrated above, the implications of such a technology are "enough to distinguish protocol from many previous modes of social and technical organisation [such as centralised and decentralised forms of power]. Together they compose a new, sophisticated system of distributed control."[44]

What really emphasises Galloway's paradox is how TCP/IP, enabling distribution and flexibility, function alongside DNS, a much more hierarchical form of protocol. DNS, the Domain Name System, translates the URL of a website (usually something easy for a human to remember, like www.google.co.uk or en.wikipedia.org) into its actual IP address, a series of numbers separated

[41] Galloway, *Protocol*, 45.

[42] Ibid.

[43] Ibid.

[44] Ibid., 47.

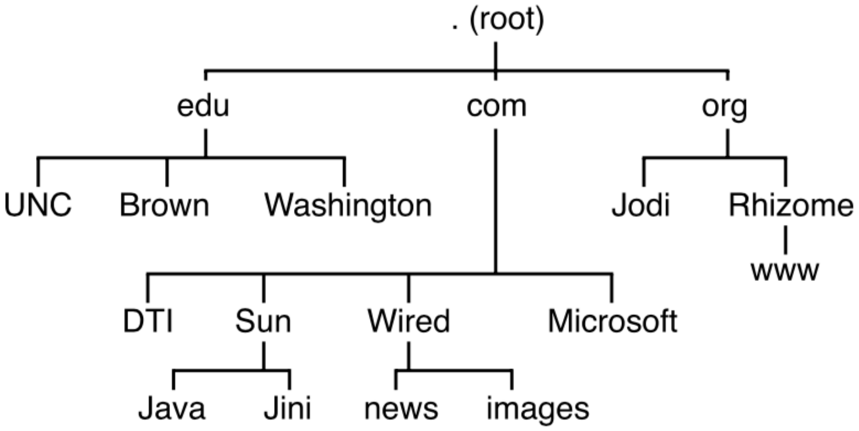


Figure 3: Domain Name System (DNS) diagram from Alex Galloway, *Protocol: How Control Exists after Decentralisation* (Massachusetts Institute of Technology Press, 2004), 49.

by dots.[45] Indeed, websites can be accessed by entering the IP address directly into your browser: typing 74.125.224.72 will take you to Google, for example. Each of the four numbers refers to a specific level of the DNS, which follows a decentralised tree-like structure (figure 3). Starting at the top of the tree with the most general information, like whether the site is commercial or educational, the relevant name server directs to the next step in the chain — but no further. This therefore creates a hierarchical system: "the process starts at the most general point, then follows the chain of delegated authority until the end of the line is reached and the numerical address may be obtained. This is the protocol of a decentralised network."[46] DNS makes for a much more highly organised form of protocol, structuring the Internet through rigid branches that, unlike TCP/IP, resist flexibility. Like Chun's notion of control-freedom, TCP/IP and DNS are two sides of the same coin, locked in a paradoxical relationship: one highly adaptable and rhizomatic, the other highly structured and decentralised. And, as an "exhaustive index" of the Internet, DNS wields a substantial power: "It governs meaning by mandating that anything meaningful must register and appear somewhere in its system. This is the nature of protocol."[47] This notion mirrors that of the

[45] This is according to the common IvP4 protocol; recently the IvP6 protocol has become available, which is comprised of hexadecimal characters separated by colons, and can be significantly longer.

[46] Galloway, *Protocol*, 49.

[47] Ibid., 50.

'gatekeepers', discussed in relation to the democratisation of media production above: chokepoints like those found in hierarchical structures allow certain bodies to control what is accessible, and who gets heard.

Now that we have seen the complex relationship between control and freedom, and how that relationship exists on a material level based on the technologies that enable the Internet, let us continue on to the final section of this essay where we will look at how technology is being used specifically to tackle centralised and decentralised forms of power, utilising distributed models in a fight for greater freedom of information and political resistance.

The first example I will look at, the aforementioned FireChat messaging app for smartphones developed by Open Garden, wasn't actually designed with protest or any form of political activity in mind. In an article with leading technology website *The Verge*, Open Garden's chief marketing officer Christophe Daligault explained that the company had "two use cases in mind: the developing world, where data plans are often prohibitively expensive, and live events or festivals, where cellular networks are usually congested and slow."[48] By bypassing traditional cellular or data networks and instead using Bluetooth and Wi-Fi signals, users connect directly to others within a range of about 70 metres[49] to form a distributed network. Each user acts as a node, thereby increasing the overall size and range of the network, and is able to send both public and encrypted private messages (through a similar 'hopping' process to how IP operates) to other nodes without the need of a centralised hub.[50] Therefore the resulting network is flexible and adaptable: if one or several nodes are removed, communication is still possible between the remaining connected

[48] Amar Toor, 'Why a messaging app meant for festivals became massively popular during Hong Kong protests' in *The Verge* (16 October 2014). Accessed at http://www.theverge.com/2014/10/16/6981127/firechat-messaging-app-accidental-protest-app-hong-kong. Accessed on 9 January 2016.

[49] Williams, *The Tech Behind Hong Kong Protesters' Ingenious New Way to Duck Surveillance.*

[50] A short video explanation of how FireChat works can be viewed here: https://www.youtube.com/watch?v=GogPPT3ePGQ

nodes. The network is also rhizomatic in that it has no fixed size or structure, constantly morphing and asymmetric; to refer back to Deleuze and Guattari, "[it] may be broken, shattered at a given spot, but it will start up again on one of its old lines, or on new lines."[51] These properties have made the app popular amongst protestors from Iraq[52] to Ecuador,[53] who seek to avoid government surveillance and get around Internet outages, as well as attendees of remote festivals like Burning Man[54] in the Nevada desert where Internet access (if available) is limited and overburdened.

The other example I will present is the Tor service. Tor, an acronym for The Onion Router (the metaphor of an onion's layers describing the multiple levels of encryption), utilises a similar node-based model to provide a service which anonymises and protects users' online behaviour. A downloadable Internet browser[55] simplifies the process considerably, so that people can use the Tor network just as if they were using Google Chrome or Firefox to surf the web. But when a user enters a web address or clicks on a hyperlink, their request is funnelled through the Tor network, a collection of relay servers (or *nodes*) run and maintained by volunteers around the globe; as a result the request may finally appear to be coming from a computer in London or Australia or anywhere in-between, protecting the location of the user. Tor is therefore particularly useful for circumventing the blocking or censorship of websites and information based on location. But privacy is the main aim of the service: "Instead of taking a direct route from source to destination, data packets on the

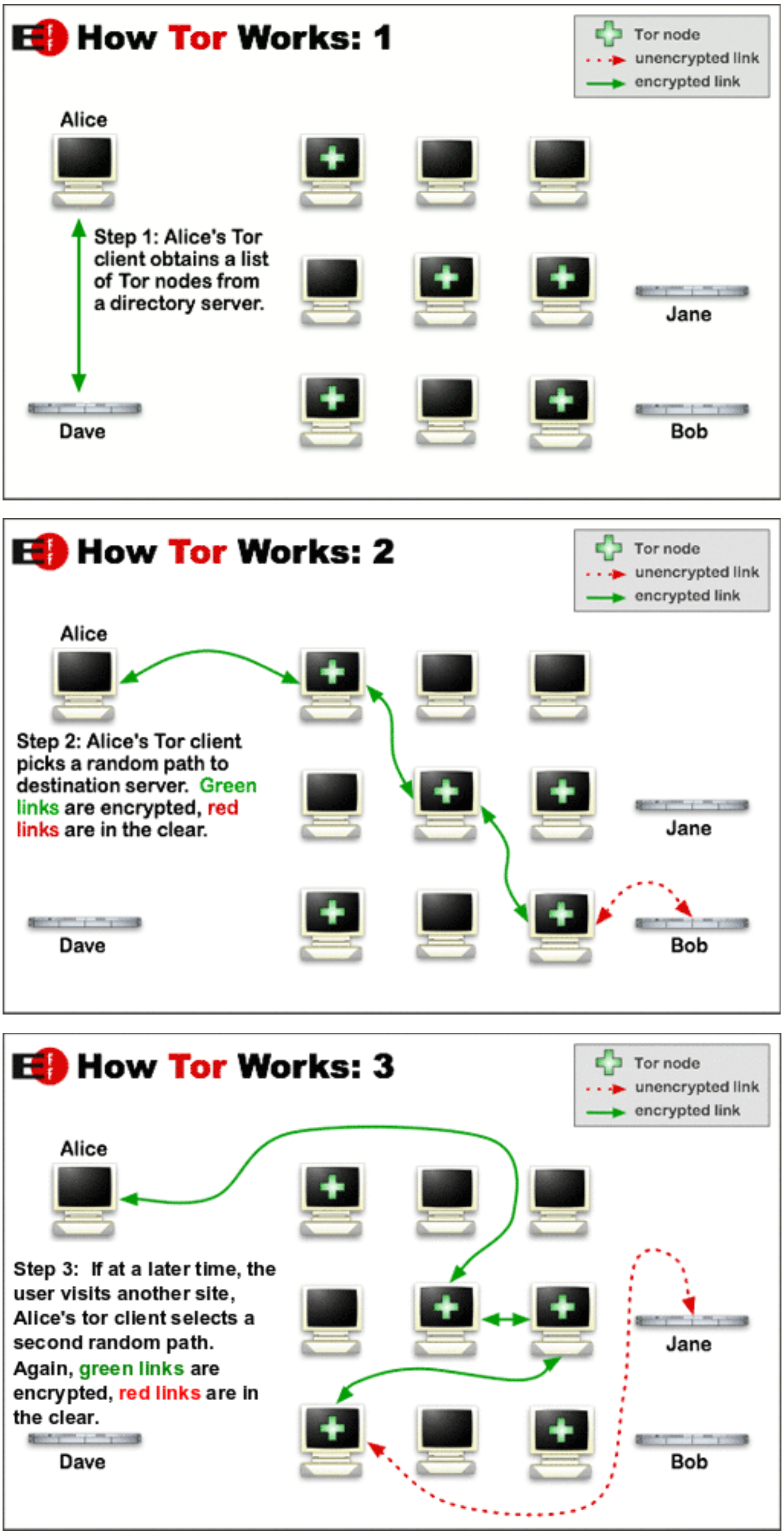
[51] Deleuze and Guattari, *A Thousand Plateaus,* 9.

[52] Mark Milian, 'Iraq Internet Shutdown Is Good News of One App: FireChat' in *Bloomberg* (24 June 2014). Accessed at http://www.bloomberg.com/news/2014-06-24/iraq-internet-shutdown-is-good-news-for-one-app-firechat.html. Accessed on 10 January 2016.

[53] Alfredo Velazco, 'The Internet, a Staging Post for Protests in Ecuador, Is Under Threat' in *GlobalVoices,* trans. Glenn Bower. Accessed at https://globalvoices.org/2015/06/28/the-internet-a-staging-post-for-protests-in-ecuador-is-under-threat/. Accessed on 10 January 2016.

[54] Chris O'Brien, 'FireChat lets Burning Man 2015 attendees create their own wireless network on the playa' in *VentureBeat* (1 September 2015). Accessed at http://venturebeat.com/2015/09/01/firechat-lets-burning-man-2015-attendees-create-their-own-wireless-network-on-the-playa/. Accessed on 10 January 2016.

[55] Download the Tor Browser at: https://www.torproject.org/download/download-easy.html.en.



How Tor Works: 1

Step 1: Alice's Tor client obtains a list of Tor nodes from a directory server.

How Tor Works: 2

Step 2: Alice's Tor client picks a random path to destination server. Green links are encrypted, red links are in the clear.

How Tor Works: 3

Step 3: If at a later time, the user visits another site, Alice's tor client selects a second random path. Again, green links are encrypted, red links are in the clear.

Figure 4: How Tor Works diagrams, EFF. Accessed at https://www.torproject.org/about/overview.html.en. Accessed on 10 January 2016.

Tor network take a random pathway through several relays that cover your tracks so no observer at any single point can tell where the data came from or where it's going."[56] Again, much like IP, each node only knows in which direction the information needs to travel, not the final destination. This anonymity is especially invaluable to journalists and whistleblowers; indeed, the activity of Edward Snowden and consequent documentary *CITIZENFOUR* raised awareness of Tor, with director Laura Poitras acknowledging it and similar encryption software in the closing credits.[57] However, whilst Tor does make users anonymous, it does not make their activity private: signing into accounts tied to your identity, such as Google and Facebook, will nullify these efforts.

Both of these examples show how real-life manifestations of distributed networks can be utilised in order to spread power and autonomy throughout larger bodies of (typically more vulnerable) people, away from centralised hubs of control. Protecting users' identity and enabling secure communications, they have proven to be indispensable communication tools. However, it is important to steer clear of the rhetoric discussed at the beginning of this essay; these networks are not impenetrable, and have gained increased attention from agencies like the NSA.[58] Furthermore, anonymity like that granted by services such as Tor enables much more questionable and dangerous activity like drug trafficking[59] and child pornography.[60] As has become apparent in this essay, there are always two sides to the coin. What's more, Tor is comparatively much slower than a 'standard'

[56] ______, *Tor: Overview*. Accessed at https://www.torproject.org/about/overview.html.en. Accessed on 10 January 2016.

[57] Andy Greenberg, 'Laura Poitras on the crypto tools that made her Snowden film possible' in *Wired* (15 October 2014). Accessed at http://www.wired.com/2014/10/laura-poitras-crypto-tools-made-snowden-film-possible/. Accessed on 10 January 2016.

[58] Jason Koebler, 'How the NSA (or anyone else) can crack Tor's anonymity' in *Motherboard* (19 November, 2014). Accessed at http://motherboard.vice.com/read/how-the-nsa-or-anyone-else-can-crack-tors-anonymity. Accessed on 10 January 2016.

[59] Kim Zetter, 'How the feds took down the Silk Road drug wonderland' in *Wired* (18 November 2013). Accessed at http://www.wired.com/2013/11/silk-road/. Accessed on 10 January 2016.

[60] Jamie Bartlett, *The Dark Net* (William Heinemann, 21 Aug 2014).

Internet connection, since the traffic has to be routed through so many nodes. But interestingly, whereas conventional Internet networks get slower and more unstable as higher numbers of users log on, FireChat and Tor become faster and safer: the more nodes in the network, the greater amount of paths for the information to travel and the easier it is to hide.

To conclude, in this essay I have presented ideas from Wendy Hui Kyong Chun, Alexander Galloway, and other relevant sources, discussed them in terms of how power, freedom, and control operate through networks, and how these networks are enabled through today's technology. Debunking the utopian and dystopian myths that conflate the Internet with absolute freedom and absolute control, I have shown how the underlying protocols of the Internet exist in a contradictory relationship that enables both, simultaneously distributing (TCP/IP) and making hierarchical (DNS). Having analysed centralised, decentralised, and distributed networks and their relationships with power, I related these concepts to existing technologies used by activists and protestors in order to enact change. In closing I would like to revisit Aaron Swartz who, in an interview taken from *The Internet's Own Boy*, manages to succinctly summarise the matter:

> There's sort of these two polarising perspectives: "Everything is great, the Internet has created all this freedom and liberty and everything's going to be fantastic" or "Everything is terrible, the Internet has created all these tools for cracking down and spying and controlling what we say." And the thing is, both are true…and it's up to us which ones we emphasise and which ones we take advantage of.[61]

Word count: 5281 (excluding footnotes)

6302 (including footnotes)

[61] Aaron Swartz, *The Internet's Own Boy*.

Bibliography

Barabási, Albert-László. *Linked: The New Science of Networks.* Perseus Publishing. 2002.

Bartlett, Jamie. *The Dark Net.* William Heinemann. 21 Aug 2014.

Bentham, Jeremy. *The Panopticon Writings.* Verso. 1995.

Braden, Robert. Requirements for Internet Hosts. In *RFC 1122.* October 1989.

Chun, Wendy Hui Kyong. *Control and Freedom: Power and Paranoia in the Age of Fibre Optics*. Massachusetts Institute of Technology Press. 2006.

Critical Art Ensemble. *Electronic Civil Disobedience.* In Electronic Civil Disobedience & Other Unpopular Ideas. Autonomedia. Winter 1995.

Deleuze, Gilles. Postscript on the Societies of Control. In *October*, Vol.59. Massachusetts Institute of Technology Press. Winter 1992.

Deleuze, Gilles and Guattari, Félix. *A Thousand Plateaus.* Trans. Massumi, Brian. University of Minnesota Press. 1987.

Foucault, Michel. *Security, Territory, Population: Lectures at the Collège de France 1977–1978.* St Martins Press. February 2009.

Galloway, Alexander. *Protocol: How Control Exists after Decentralisation.* Massachusetts Institute of Technology Press. 2004.

Gibbs, Samuel. The return of the YouTube troll: Google ends its 'real name' commenter policy. In *The Guardian.* 16 July 2014. Accessed at http://www.theguardian.com/technology/2014/jul/16/youtube-trolls-google-real-name-commenter-policy. Accessed on 4 January 2015.

Greenberg, Andy. Laura Poitras on the crypto tools that made her Snowden film possible. In *Wired.* 15 October 2014. Accessed at http://www.wired.com/2014/10/laura-poitras-crypto-tools-made-snowden-film-possible/. Accessed on 10 January 2016.

Koebler, Jason. How the NSA (or anyone else) can crack Tor's anonymity. In *Motherboard.* 19 November, 2014. Accessed at http://motherboard.vice.com/read/how-the-nsa-or-anyone-else-can-crack-tors-anonymity. Accessed on 10 January 2016.

Milian, Mark. Iraq Internet Shutdown Is Good News of One App: FireChat. In *Bloomberg.* 24 June 2014. Accessed at http://www.bloomberg.com/news/2014-06-24/iraq-internet-shutdown-is-good-news-for-one-app-firechat.html. Accessed on 10 January 2016.

Morozov, Evgeny. *The Net Delusion.* PublicAffairs. 2011.

O'Brien, Chris. FireChat lets Burning Man 2015 attendees create their own wireless network on the playa. In *VentureBeat.* 1 September 2015. Accessed at http://venturebeat.com/2015/09/01/firechat-lets-burning-man-2015-attendees-create-their-own-wireless-network-on-the-playa/. Accessed on 10 January 2016.

Penny, Laurie. David Cameron's internet porn filter is the start of censorship creep. In *The Guardian.* 3 January 2014. Accessed at http://www.theguardian.com/commentisfree/2014/jan/03/david-cameron-internet-porn-filter-censorship-creep. Accessed on 4 January 2016.

Postel, Jonathan. Internet Protocol. In *RFC 791.* September 1981.

Postel, Jonathan. Transmission Control Protocol. In *RFC 793.* September 1981.

Rainie, Lee and Madden, Mary. How People are Changing Their Own Behaviour. In *PewResearchCenter*. Accessed at http://www.pewinternet.org/2015/03/16/how-people-are-changing-their-own-behavior/. Accessed on 4 January 2016.

Sützl, Wolfgang and Hug, Theo (Eds.). *Activist Media and Biopolitics: Critical Media Interventions in the Age of Biopower.* Innsbruck University Press. 2012.

Swartz, Aaron. *The Internet's Own Boy: The Story of Aaron Swartz.* Dir. Brian Knappenberger. Luminant Media. 2014. Film.

Toor, Amar. Why a messaging app meant for festivals became massively popular during Hong Kong protests. In *The Verge.* 16 October 2014. Accessed at http://www.theverge.com/2014/10/16/6981127/firechat-messaging-app-accidental-protest-app-hong-kong. Accessed on 9 January 2016.

Velazco, Alfredo. The Internet, a Staging Post for Protests in Ecuador, Is Under Threat. In *GlobalVoices.* Trans. Bower, Glenn. Accessed at https://globalvoices.org/2015/06/28/the-internet-a-staging-post-for-protests-in-ecuador-is-under-threat/. Accessed on 10 January 2016.

Williams, Lauren C. Damning Photos From Hong Kong Protests Cause China To Block Instagram. In *ThinkProgress.* 29 September 2014. Accessed at http://thinkprogress.org/world/2014/09/29/3573251/china-blocks-instagram/. Accessed on 9 January 2016.

Williams, Lauren C. The Tech Behind Hong Kong Protesters' Ingenious New Way To Duck Surveillance. In *ThinkProgress.* 3 October 2014. Accessed at http://thinkprogress.org/world/2014/10/03/3575225/hong-kong-protesters-use-mesh-networks-to-skirt-censorship/. Accessed on 9 January 2016.

Zetter, Kim. How the feds took down the Silk Road drug wonderland. In *Wired.* 18 November 2013. Accessed at http://www.wired.com/2013/11/silk-road/. Accessed on 10 January 2016.

______. Tor: Overview. Accessed at https://www.torproject.org/about/overview.html.en. Accessed on 10 January 2016.

Figures:

Figure 1: Baran, Paul. *On Distributed Communications: 1. Introduction to Distributed Communications Networks.* RAND. 1964. 2.

Figure 2: Galloway, Alex. *Protocol: How Control Exists after Decentralisation.* Massachusetts Institute of Technology Press. 2004. 39.

Figure 3: Galloway, Alex. *Protocol: How Control Exists after Decentralisation.* Massachusetts Institute of Technology Press. 2004. 49.

Figure 4: EFF. *How Tor Works.* Accessed at https://www.torproject.org/about/overview.html.en.