MEDIANZ • VOL 14 NO 2 • 2014
DOI: http://dx.doi.org/10.11157/medianz-vol14iss2id97

- ARTICLE -

We Have Never Been Open: Activism and Cryptography in Surveillance Societies

Sy Taffel

Abstract

Whilst there exist a range of contemporaneous discourses surrounding the end of the open Internet, claims that the Internet was until recently 'open' are highly dubious. This paper challenges readings of openness, which derive from the open source movement, but largely ignore the historical specificity of the term's emergence from the free software movement, and consequently equate open to signify better. Indeed, for numerous activist projects, the default position has long been that unencrypted telecommunications present a serious security breach. Recent developments such as the revelations regarding the NSA-run PRISM program, the imprisonment of social media users for making open calls for citizens to engage in direct action, and state-led attempts to curtail online communications during periods of civil unrest, highlight that security measures taken to preserve anonymity and encrypt telecommunications are a useful strategy for contesting the pervasive surveillance apparatus of the state and large corporations within societies of control.

This paper explores a range of such anti-surveillance technologies including TOR, GPG, and FreedomBox. Additionally the paper will highlight the activity of Hacktionlab, a UK-based tech-activist collective in promoting the application of these platforms within wider activist communities. Following Bernard Stiegler's prescriptions surrounding the economy of contribution as an alternative to prevalent pathologies of control, the paper contends that if we are to resist proletarianisation and to contribute towards a sense of communal care through forms of digital literacy—whereby individuals better understand the footprints left by their digital activities—it is pivotal not only to delineate the increasingly pervasive forms of surveillance enacted by state and corporate actors, but to outline various methods by which control over communicative spaces can be contested.

Sy Taffel is currently a Lecturer in Media Studies at Massey University, Aotearoa New Zealand. In 2013 he completed a PhD in Digital Media Ecologies at the University of Bristol, UK. His research interests include political ecologies of digital media, digital media and political activism, pervasive/locative media, software studies, and peer-to-peer production. Sy has also worked as a filmmaker and photographer, and has been involved with media activist projects including Indymedia, Climate Camp, and Hacktionlab.

Introduction

The array of targeted and bulk surveillance programmes conducted by the Five Eyes network (the US, UK, Canada, Australia and New Zealand) revealed by the materials leaked by Edward Snowden has produced rhetoric suggesting that this disclosure marks the end of the 'open' internet (Greenwald 2014; Landau 2013; Schneier 2013). This paper will argue that whilst numerous discourses of openness have long been part of scholarly and vernacular parlance surrounding networked digital telecommunications, scrutinising the singular and totalising notion of an open internet reveals this position to be an overly reductive endeavour which homogenises understandings of openness and occludes an examination of the range of ways in which openness is actively detrimental to particular forms of online communication. In particular, the focus here is upon a range of 'activist'[1] projects whose default position has long been that unencrypted telecommunications present a serious security breach with potentially serious repercussions for those involved. Consequently, a range of Free and Open-Source Software (FOSS) tools have been developed to minimise the effects of governmental surveillance apparatuses which were assumed to exist before the Snowden revelations, and will undoubtedly have evolved since their disclosure. This paper explores a range of such anti-surveillance software including TOR, PGP/GPG, and FreedomBox. Additionally the paper will highlight the activity of tech-activist collectives in promoting these platforms within wider activist communities.

The paper contextualises these practices within a theoretical model informed by Gilles Deleuze's (1992) demarcation of contemporary societies as defined by computational systems of control, and Bernard Stiegler's recent outline of an economy of contribution (Stiegler 2010a, 2010b, 2013) as a potential re-imagining of how societies with advanced information and communications infrastructures could orientate themselves along alternative economic, ethical and political lines, an approach which has recently gained traction within literature pertaining to digital technology and activism (Crogan 2010; Kinsley 2014; Featherstone 2013), and it is this critical context which I turn to next.

Crypto-Activism in Societies of Control

According to Deleuze, the disciplinary societies elaborated by Michel Foucault which were dominated by the relatively fixed vectors of subjectification imposed by institutions such as the prison, the school and the factory were by the early 1990s being deterritorialised by fluid systems predicated on techno-cultural developments emanating from cybernetics, a field defined by Norbet Wiener (1965) as the study of control and communication in the animal and the machine. Deleuze cites the transition from an industrial production to financial and brand-led capitalism as emblematic of these changes; instantaneous globalised flows of capital generate vast sums of wealth largely disconnected from the actual production of commodities in a milieu where marketing and branding frequently require a greater financial investment than the

actual production of the commodity (Klein 2000; Lash and Lury 2007). Deleuze foregrounds the dangers of marketing and perpetual debt within societies of control, but does not posit the emergence of this paradigm as either a positive or negative development; 'There is no need to ask which is the toughest or most tolerable regime, for it's within each of the them that liberating and enslaving forces confront one another' (Deleuze 1992, 4). Deleuze specifies that the future of trade unions will be an important marker within struggles for social liberation, questioning whether institutions tied to resistance against enclosure and disciplinarity will successfully mutate into formations able to provide effective resistance within societies of control.

The notion of societies of control has been productively utilised within the field of surveillance studies (Jones 2001; Simon 2002; Elmer 2003; Best 2010), where the movement from enclosed spaces of panoptical surveillance towards the type of modulating systems of data surveillance dependent upon computational assemblages are frequently identified as a key shift within patterns of surveillance within contemporary society. Writing at the intersection of philosophy, politics and technology, Bernard Stiegler (2009a, 2009b) has similarly used the transition signalled by Deleuze's work on societies of control as a starting point for considering the contemporary techno-cultural and socio-political situation, which he argues are dominated by digital mnemotechnical assemblages (Stiegler 2010b).

Stiegler considers the relative failure of trade unions to successfully confront a globalised and neoliberal capitalism, and consequently turns towards the social formations surrounding commons-led peer production such as FOSS as a potential alternative to neoliberalism, whereby a singular focus upon short-term economic growth has positioned techno-culture racing towards ecological catastrophe(s):

> The software industry and its digital networks will eventually cause associated techno-geographical milieus of a new kind to appear, enabling human geography to interface with the technical system, to make it function and, especially, make it evolve, thanks to this interfacing: collaborative technologies and free license software rest precisely on the valorisation of such associated human milieus, which also constitute techno-geographical spaces for the formation of positive externalities. (Stiegler 2010a, 128).

Stiegler contends that the separation of producer and consumer characteristic of industrial capitalism leads to the formation of dissociated milieus, socio-technical assemblages wherein citizens increasingly lose the knowledge required to construct their own culture as this is exteriorised into technology. This communal loss of knowledge is what Stiegler terms the process of proletarianisation, which follows Marx but not orthodox Marxism, in defining this term through the manner by which the transition from tools to machines saw the transformation of the relationship between living labour and fixed capital:

> The production in enormous mass quantities which is posited with machinery destroys every connection of the product with the direct need of the producer, and hence with direct use value; it is already posited in the form of the product's production and in the relations in which it is produced that it is produced only as a conveyor of value, and its use value only as condition to that end. In machinery, objectified labour itself appears not only in the form of product or of the product employed as means of labour, but in the form of the force of production itself. The development of the means of labour into machinery is not an accidental moment of capital, but is rather the historical reshaping of the traditional, inherited means of labour into a form adequate to capital. The accumulation of knowledge and of skill, of the general productive forces of the social brain, is thus absorbed into capital, as opposed to labour, and hence appears as an attribute of capital, and more specifically of fixed capital. (Marx 1973, 694).

Stiegler argues that this technical absorption of productive forces and communal knowledge urgently requires contestation, and that digital technologies which allow users to become active co-creators of software, artworks and communicative exchanges hold considerable potential in affording the formation of associated milieus by effecting a metamorphosis of the consumer into a contributor and participant. However, far from presenting a straightforward teleology whereby society moves from destructive dissociated milieus towards a collectivised culture of care and 'economy of contribution' (2013, 54-56), Stiegler (2010a, 129) instead posits that the growth of digital technics is 'not necessarily beneficial: it is highly pharmacological, and hence, for example, social networks are clearly also connected to processes of automated traceability… which confer to those who obtain this information a new type of power'.

Indeed, for Stiegler, technics and technologies are always a pharmakon, simultaneously and irreducibly both poison and remedy. Thus the technologies which allow for increasingly sophisticated modes of cryptographically protected, technologically-enabled activism are equally the means by which state and corporate actors institute ever more pervasive apparatus of surveillance and control over techno-cultural milieus. Having briefly laid out the theoretical contexts behind Deleuze's society of control and Stiegler's economy of contribution, which in both cases seek to enact analyses of techno-cultural milieus which go beyond positing straightforward good/bad dualisms, I now turn to the notions of openness which pertain to the Internet.

Beyond the Ideology of Open

There are multiple ways in which the concept of openness is mobilised with regards to the internet. As we shall see, the term 'open' has been fetishized as pointing towards efficiency, fairness, transparency, and other singularly positive traits, however, positioning the internet as entirely open, or that openness is always a desirable characteristic for telecommunications networks is, as Nathaniel Tkaacz (2012) suggests,

overly reductive and empirically dubious. The dominant appropriations of openness in relation to discourses surrounding the internet come from open source software, and the related notion of open protocols. This discussion of openness and the internet commences by revising the genealogy of the term 'open source', and its demarcation from the related trope of free software, as this highlights the manner in which this definition of open was originally intended to present a term removed from the ethical judgements implicit in discourses of the open Internet.

Open source appeared as an offshoot of the free software movement, a project founded by Richard Stallman in 1983 with the development of the GNU (Gnu's not UNIX) operating system. Stallman later launched the non-profit Free Software Foundation in 1985 to maintain the GNU General Public License (GPL)—a software license originally written by Stallman for the GNU project, and which has subsequently been adopted by a wide range of FOSS ventures, with 46% of all open source projects estimated to be using a version of the GPL in 2014 (Black Duck Software 2014) —and the Free Software Definition, a document which outlines the four freedoms associated with free software: the freedom to run programs for any purpose, the freedom to analyse and alter the software (which entails access to source code), the freedom to distribute copies of the software and the freedom to distribute modified versions of the software. The open source movement developed as a breakaway group from the FSF in 1998, led by Bruce Perens and Eric Raymond, who both argued that ambiguities surrounding the term 'free software' engendered suspicion amongst corporate users, for whom the connotations of free as gratis signalled a potential conflict with profitability. Consequently, the term open source was introduced as a preferable label because of its ideological neutrality (Raymond 1998).

Whilst there are striking similarities between the Free Software Definition and the corresponding Open Software Definition, Stallman argues that this practical correlation masks underlying conceptual differences:

> Nearly all open-source software is free software. The two terms describe almost the same category of software, but they stand for views based on fundamentally different values. Open-source is a development methodology; free software is a social movement. For the free software movement, free software is an ethical imperative, because only free software respects the users' freedom. By contrast, the philosophy of open-source considers issues in terms of how to make software 'better'—in a practical sense only… For the free software movement, however, nonfree software is a social problem, and the solution is to stop using it and move to free software. (Stallman 2007).

Situating the historical divergence between open source and free software is worthwhile within this context, as the fetishization of the open internet is partially derived from a position that open source software is inherently better than closed, proprietary code, and thus it becomes useful to highlight that open source itself was

originally an attempt to remove moralistic values from debates surrounding modes of software production and licensing.

Within scholarly debates there exists a homologous spectrum of support for the mode of collectivised production underpinning FOSS, ranging from liberal capitalists to an assortment of anti-capitalist positions. The liberal positions (Lessig 1999; Benkler 2006) identify that within specific material conditions associated with the network society (Castells 1996), commons-based peer production, of which FOSS is a prime example, presents a hyper-efficient mode of production which (at least) for informational assets such as software – whose material instantiation as binary code affords near-instantaneous copies to be transmitted over distributed information networks – entails the capacity to frequently economically outcompete market-based solutions. Under a liberal capitalist ideology, such positions contend that commons-based solutions should primarily be adopted as they present economically efficient solutions which effectively leverage collectivised resources, a process which frequently depends upon the exploitation of 'free labour' (Terranova 2000) and crowdsourcing to generate increased profits, although authors such as Benkler and Lessig additionally note the presence of socio-cultural benefits arising from collectivised modes of production.

By contrast, a range of authors whose political persuasion could broadly be described as anti-capitalist also gesture towards FOSS as emblematic of a potential avenue by which a collectivised mode of production can be envisioned as the basis for an economic mode which could supplant capitalism rather than merely refining it (Hardt and Negri 2000, 2005; Bauwens 2005; Kleiner 2010; Dyer-Witheford 1999). Stiegler (2010a) occupies a position which parallels elements of the political position espoused by Hardt and Negri (2000, 401-403), and Dyer-Witherford (1999, 195-201), insofar as he has publically supported calls for a citizen's income, which does not entirely seek to abolish capitalist wage/labour relations, but significantly alters them by providing a living wage to all citizens, under the auspices that everyone undertakes socially productive work within the context of what Hardt and Negri (2005, 93-95) describe as the contemporary regime of biopolitical production. When the mode of production is not delimited to the economic sphere, but reaches into all facets of life, when every affective and communicative relationship is understood as being itself economically productive, there becomes a strong argument that such work is formally recognised and rewarded. Whilst traditionally formal wage-labour has been the sole mode of labour which is fiscally remunerated, under a citizen's income, other modes of work such as domestic work, familial care or creative work are advanced as equally important to the formation of an economy of contribution where social and ecological care are paramount.

With regard to debates surrounding the open internet, this range of positions effectively highlights the issues with presenting a reductive open/closed binary. There exist a range of positions surrounding openness, freedom and closure, which should preclude simplistic analysis whereby open equates to good. Whilst there are times where open source is economically efficient, this is often predicated on exploiting precarious labour

under the specific material conditions of neoliberalism and post-Fordism (Marazzi 2008; Lazzarato 1996). Indeed, as Jodi Dean (2009, 2013) convincingly argues, digital technologies and open communicative networks have become increasingly integral to the functioning of contemporary capitalism. High profile examples, such as Google leveraging open source software across numerous domains, such as the Android mobile phone operating system and the Chrome web browser, demonstrate that open source has proven to be highly efficient way for multinational corporations to enhance revenues and dominate markets whilst drawing upon cooperative networks of innovation.

Consequently, deterministic proclamations that the open source model itself is sufficient as a condition for ensuring radical social change appear as naïve techno-utopianism, especially when presented through the mode of liberal rhetoric found in Douglas Rushkoff's *Open Source Democracy: How Online Communication is Changing Offline Politics* (Rushkoff 2003). Whilst Hardt and Negri present a far more nuanced political account of contemporary biopolitics, they contend that 'One approach to the multitude, then, is as an open source society, that is, a society whose source code is revealed so that we can work collaboratively to solve bugs and create new, better social programmes' (2005, 340). Such a position reveals a tendency to reductively equate openness with 'new' and 'better,' whilst failing to address pertinent questions surrounding freedom, modification, and circulation, and crucially in the context of social movements, what kind of organisational parallel would equate to the open source process of forking, whereby a divergence of opinion on future direction within a community sees a project fork into two (or more) independent entities. Indeed, the focus within Hardt and Negri's account upon open networks and immaterial labour has led Slavoj Zizek (2006, 263) to argue that their vision of multitude has already been realised within the exploitative practices of corporate entities which leverage open source software and the logic of financial capitalism:

> The organisational forms of today's capitalism – decentralisation of decision making, radical mobility and flexibility, interaction of multiple agents – are perceived as pointing toward the oncoming regime of the multitude. It is as if everything is already here in 'postmodern' capitalism – all that is needed is a purely formal act of conversion. (Zizek 2006).

Whilst such an uncharitable reading ignores some of the nuanced detail drawn out by Hardt and Negri's positions in identifying elements of biopolitical production (such as the reliance upon of forms of commonwealth) as contradictions of contemporary capitalism, Zizek's position does effectively highlight a weakness in their analysis of technological networks and practices of digital networking. A more productive position, following Stiegler, is to understand questions surrounding openness and digital networks within the context of technology as pharmakon. Rather than providing a panacea for the ills of neoliberalism, open source software and the digital informational networks are at once a potential avenue for the types of commons-led social

revitalisation envisaged by Hardt and Negri, and the central plank of communicative capitalism as outlined by Dean and Zizek.

Another usage of the term open with regards to the Internet, which is useful in terms of grasping the differential affordances which exist amongst concrete examples of open culture and technologies refers to the protocols upon which the internet and World Wide Web are built, such as TCP/IP, DNS, HTTP, and FTP (Galloway 2004). The openness of these protocols is paramount, insofar as this is precisely what allows a range of competing platforms such as Windows, OSX, and Linux to access the same network. Whereas closed, proprietary systems entail that only the company responsible for writing the code, or parties who pay for licenses have access, open protocols allow any interested party to create systems compatible with the network. Tim Berners-Lee (1996) describes the historical issues associated with closed systems predating the web thus: 'In 1980, the world still suffered from incompatible networks, incompatible disk formats, incompatible data formats, and incompatible character-encoding schemes. This made any attempt to transfer information between systems daunting and impractical'. Consequently the web was designed by Berners-Lee to be a hardware neutral platform which would allow communications to flow across the divisions created by the incompatibilities associated with closed protocols. In protocological contexts then, openness is pivotal to the evolution of the internet and the web, indeed as Berners-Lee and Galloway note, it is precisely this level of protocological openness which allows the internet to function the way we often assume it must. Contrary to a teleological account of techno-cultural evolution, the internet and the web did not have to exist as cross-platform networks linked by open protocols; this arose as a result of specific decisions surrounding protocological design taken by Berners-Lee and others.

Whereas FOSS and open protocols present broadly positive connotations surrounding openness and the internet, there additionally exist various deployments of the trope of openness which gesture towards ambivalent or predominantly negative outcomes. These include open data (Miller, Styles, and Heath 2008), which refers to allowing universal access to information in a manner analogous to FOSS. Open data has been heralded as allowing citizens to scrutinise the activities of elected representatives (Janssen, Charalabidis, and Zuiderwijk 2012), and affording artists the capacity to mobilize 'the enormous co-creative potential of human discourse captured in the Web,' (Dovey and Rose 2012). However, whilst these cases denote concrete ways that open data can provide positive social impacts, there are obvious and practical limits to the extents to which forms of data ranging from medical records to internet banking details can or should be universally accessible. Indeed, there have been intense debates surrounding privacy in regards to the ethics of utilising user data within social media sites (Papacharissi and Gibson 2011; Beer 2008; Fuchs et al. 2013; Hargittai 2010), with few if any arguments that such data should be universally accessible. Open data, then, presents a case in which openness is often desirable but can present serious breaches of privacy, undermining the association of online openness as an unabated good.

Numerous further examples exist whereby online openness is predominantly an undesirable quality. As a systems administrator, running a platform which is open to spam is tantamount to providing a service where any useful content will be swamped by irrelevant material produced by bots. Similarly, few people would relish the prospect of being open to identity theft, but without privacy, security and cryptography, online shopping and internet banking would present carte blanche for fraud and theft. Whereas libertarian declarations surrounding the independence and freedom of cyberspace (Barlow 1996; Dyson 1996) suggested the internet should be free and open to all forms of communication, child pornography causes revulsion amongst most individuals, and few ethically motivated citizens would support communication systems open to content predicated upon the abuse of minors. As we shall see in the following sections, activist usages of networked telecommunications present further exemplars of scenarios whereby openness is often understood as a serious threat to those involved, whereas anonymity and privacy are desirable features.

Tor and Anonymity

When publically communicating information pertaining to direct actions, or whistleblowing upon the actions of a government or employer, anonymity is usually prized as this effectively prevents retribution being taken against the communicating party. A useful example highlighting this contrasts the legal repercussions pertaining to two internet postings surrounding real or imagined property damage. During the UK riots of 2011, Perry Sutcliffe-Keenan used his Facebook account to create a page entitled the Warrington Riots whilst intoxicated late one evening. In the morning, Sutcliffe-Keenan removed the page, and apologised for what he claimed was a distasteful joke. Using a commercial service entailed that Sutcliffe-Keenan was identifiable as the source of the message, allowing the police to trace and apprehend him, and although his actions did not lead to any criminal activity, Sutcliffe-Keenan was subsequently imprisoned for four years. By contrast, on June 17th 2005 an anonymous report was posted to the Bristol Indymedia website reporting a direct action involving property damage to a freight train in the Bristol area. Attempting to identify the individual responsible for the posting, the British transport arrested an Indymedia volunteer and seized the server used by the group in order to search for the IP address of the computer which had posted the story which the police hoped would reside within the system log file. However, as an activist service which aimed to preserve user anonymity, the Bristol Indymedia website did not record user IP data, and consequently the police were unable to extract any useful information from the server.

These cases, alongside the treatment of high profile whistle-blowers such as Chelsea Manning and Edward Snowden, denote that there are very real consequences for individuals discovered to be involved in telecommunications advocating direct action or whistleblowing. In these cases, activists require anonymity if they wish to avoid incarceration. Whilst Indymedia presents one exemplar of an activist-run service whose

practices are specifically designed to prevent the identification of users as per the global Indymedia principles of unity (Indymedia 2002), commercial websites and social media platforms predominantly function via an economic model predicated upon the collation of various forms of user data which consequently informs the dissemination of highly targeted forms of advertising (Fuchs 2010, 2012). Consequently, such systems are incompatible with maintaining user anonymity, and even had the revelation of the PRISM program not detailed the complicity between large corporate internet actors and governmental agencies, any legal warrant for specific user information would likely be adhered to. Additionally, the platform operator's prerogative is economic output rather than safeguarding user privacy and anonymity, and the dominant economic model of social media—targeted advertising—is inimical to anonymity.

Whilst Indymedia and WikiLeaks are examples of sites which allow anonymous publishing, these sites themselves cannot address issues surrounding data collection and decryption en route from a user's computer to the web server on which the content is to be hosted. One extensively used tool which assists with this and other facets of online anonymity is Tor. An acronym of The Onion Router – a reference to the multi-layered structure of the vegetable – Tor was originally developed by the US Naval Research laboratory as a system for protecting governmental communications in the event of severe disruption to command centres, but has developed into a widely-used FOSS tool for maintaining online anonymity. It functions by connecting users to a distributed peer-to-peer network of Tor nodes, and all internet traffic is dynamically routed via this network. Internet traffic is not traceable to the original computer, as each machine can only see the previous node within the Tor network, so the source of the communication remains anonymous. Although websites do see the final node that the request is routed through (which is known as an exit node), this does not allow the pathway through the Tor network to be traced back to the original user.

Tor was used widely during the uprising against the Mubarak regime in Egypt during the Arab Spring when on January 27th 2011 the government attempted to sever the protesters' channels of digital communication by ordering ISPs to cut off Internet access to Egyptians. This was achieved by ISPs such as Vodaphone, Orange and TE Data enabling IP filters and revoking their Border Gate Protocol (BGP) routes, entailing that their users could not connect to international servers and vice-versa; the physical architecture of the internet remained intact, but software filters prevented Egyptians from communicating online. One response from those inside Egypt registered with Noor and Etisalat ISPs—who enacted IP filters but which did not revoke BGP access—was to utilise the Tor network to anonymize their IP addresses and therefore bypass the filtering restrictions (Ioerror 2011). This led to a huge spike in the traffic within the Tor network in the days following the 27th of January, with Egyptian Tor users increasing by over 500%, resulting in Twitter users tweeting for concerned parties to set up additional Tor relay nodes to accommodate the extra traffic.

Amongst the confidential documents released by Snowden was an NSA presentation from June 2012 entitled *Tor Stinks* (Guardian 2013). In this presentation, the NSA outline that they have effectively been unable to identify the origins of specific messages originating from the Tor network, but that there were a range of alternative techniques used to attempt de-anonymizing Tor users or degrading the performance of the network so that users may consequently use a faster but less secure communication channel. These techniques include using cookies to identify Tor users when they are not using Tor, attempting to route users into a separate private Tor network where all the nodes were run by the NSA, and flooding the network with slow Tor nodes advertised as high bandwidth machines to degrade network performance and stability. What is notable here is primarily that the NSA has effectively been unable to de-anonymize Tor users in response to specific requests, denoting that one of the tools most commonly used by activists to protect anonymity has not been compromised despite the concerted efforts of security agencies.

Pretty Good Privacy?

Whereas Indymedia and Tor present cases whereby anonymity is essential for evading systems of control predicated upon unique identifiers, there additionally exist activist communications in which the transmission of sensitive information requires a different mode of security to anonymity. When members of an affinity group wish to discuss details surrounding direct actions such as shutting down a coal burning power station, setting up a climate camp or preventing a fracking operation, it is imperative that participants can accurately identify other respondents, whilst ensuring that these communications are not openly available, because if the authorities received the contents of these communications, the direct action would result in the arrest of the participants before any operation was conducted.

In order to facilitate this type of secure and private exchange, activists use cryptographic tools such as PGP/GPG. Pretty Good Privacy (PGP) is a standard which uses encryption and decryption to provide the secure exchange of data (primarily emails) based on a web of trust system. Originally designed by Phil Zimmerman in 1991, since 1997 PGP encryption has been developed as OpenPGP by the Internet Engineering Task Force, meaning that the system is available for interested parties to utilise, such as the FSF's GPL licensed Gnu Privacy Guard (GPG). PGP/GPG uses a public key cryptography, a form of cryptography which requires that each user has two keys, one public and one private. The keys are large, random strings of characters produced by a PGP key generating program. The public key can be publically disseminated whereas the private key is kept secure at all times, and if there is suspicion that anyone other than the owner has a copy of the private key, it is strongly recommended that the keys are revoked, and the individual creates a new key pair.

In practice, encrypted email via PGP requires the sender to encrypt the message using the recipient's public key. This message then travels in an encrypted form through the

physical conduits of the internet, before arriving on the recipient's email server, where it can only be decrypted by the recipient's private key. The fact that the message is encrypted whilst travelling across the fibre-optic cables which comprise the physical conduits of the internet is crucial, as this entails that it is not susceptible to man-in-the-middle attacks, whereby a third party is able to intercept or copy the message whilst it travels from sender to recipient. This is particularly important for those interested in secure communications following the revelation that the five eyes network operates bulk data interception and collection programmes such as Boundless Informant and Tempora; if you are sending unencrypted messages with sensitive content they will almost certainly be collated and algorithmically analysed by the bulk surveillance programmes coordinated by state agencies.

One question which this technical system leaves unresolved is that of user authenticity—of knowing that the public key and email address the message belongs to the intended recipient. Indeed, were the details simply pulled from a public key server, sending sensitive information in this way would risk being compromised by faked identities. Consequently, PGP public keys are exchanged in-person at key signing parties which occur at activist-tech events such as Hacklabs and Cryptoparties. Key signing parties sees keyholders present copies of their public key to other PGP users who are personally known to them, or can verify their identities using forms of photographic identification. These keys can then be digitally verified by the individuals present, which extends the web of trust on which PGP is predicated, as other PGP users are subsequently able to see that multiple users have verified that the public key belongs to the individual claiming ownership of the keypair.

As with Tor, there is no evidence that the NSA or other intelligence agencies have been able to break the cryptography which underpins PGP, denoting that the procedures which have long been recommended as necessary for activists to safeguard privacy of digital communications are still believed to be secure from the surveillance programs whose existence was delineated within the material leaked by Snowden. However, the notion of using cryptographic tools to create a sense of security and privacy which is pretty good, but by no means complete and total is useful, especially in the light of the high profile arrests of individuals such as Hector Monsegur. Monsegur, whose online handle was Sabu, was the co-founder and central figure within LulzSec, the hacktivist collective who from 2011 to 2013 perpetrated cyberattacks against high-profile targets including Fox News, Sony, and the CIA. Whilst Monsegur was undoubtedly adept at cryptography and associated online security techniques, he was apprehended after once logging in to an internet relay chat server without using Tor to anonymize his IP address (Leyden 2012). This single mistake, a sole moment of carelessness, was sufficient for the FBI to geo-locate the computer Monsegur was using and subsequently apprehend him.

Whilst utilising cryptographic tools such as Tor and PGP certainly does improve the security of telecommunications, they should not be considered a panacea which implies total security, indeed the notion of total security is a total fantasy, as the eminent

fallibility of the human elements of techno-cultural assemblages entail that there will always be mistakes, compromises and security breaches, even if the cryptographic systems remain secure. Indeed, as the *Tor Stinks* presentation demonstrates, whilst certain elements of computational systems may provide privacy and security which cannot be effectively breached, there are a multitude of alternative avenues through which software and hardware systems may be compromised; running Tor and PGP will do little to enhance security if your computer has a hardware keylogger fitted or is running malware.

The fantasy of total security also fails to acknowledge the dynamism and modulation of cryptoplogical assemblages within societies of control. Security is not a static and unchanging singular state which one occupies, but is itself constantly in a state of flux, changing as various elements within computational ecologies are exploited, patched, hacked, upgraded and otherwise modified. As the serious vulnerability of the open source OpenSSL cryptographic software library known as Heartbleed revealed in 2014, simply having interrogable source code is far from a guarantee that no significant bugs exist within the code, and over time, such flaws present security threats which state and other entities are able to periodically exploit before they are patched. This cyclical, feedback-orientated process, where exploitable code is fixed, leading to the search for new exploits, and so on, is typical of the processes of constant modulation that Deleuze associates with cryptographic systems of control.

Freedomboxes and Hacktionlabs

One of the criticisms frequently levelled at cryptographic tools has been that they tend to require relatively advanced technical competencies, inhibiting the majority of computational users from successfully engaging with them (Whitten and Tygar 1999; Sheng et al. 2006; Furnell 2005). Whereas commercial social media platforms feature intuitive, user-friendly GUIs, tools such as PGP and Tor have in the past required lengthy and relatively complex installation and setup procedures, with text-based guides generally catering for GNU/Linux users adept at using command-line interfaces and editing text-based configuration files. There have been notable attempts to address these concerns through the development of software such as the Tor browser bundle (TBB), a single download available from www.torproject.org with versions available for the GNU/Linux, Windows and OSX operating systems. TBB features a customised version of the open source Mozilla Firefox web browser alongside the Torbutton Firefox plugin, Vidalia (a GUI for controlling Tor), the Tor proxy, and additional privacy-related Firefox plugins such as NoScript and HTTPS Everywhere. Previously, users had to source, install and configure these various components separately, but TBB provides a single package which allows users without command-line interface skills or the knowledge required to locate the correct versions of multiple software elements to access the Tor network.

An additional ongoing project which has significant potential in allowing the proliferation of encrypted telecommunication services is the Freedombox, a venture which aims to collate a stack of existing FOSS privacy tools including Tor and PGP alongside other security-related software such as OwnCloud and PageKite, aiming to provide a one-stop privacy and security solution for users without specialised technical skills. This software stack was originally designed to run on plug servers; low cost miniature computers which require minimal quantities of power, however, the code has recently been integrated into the kernel for Debian, a popular GNU/Linux distribution in order to vastly increase the potential user base by allowing any computer capable of running Debian to become a Freedombox. Furthermore, Freedomboxes form a mesh network, affording users the ability to communicate in a distributed manner which is relatively resilient to the type of centralised shutdown of networked infrastructure seen within Egypt. If any of the Freedomboxes within the mesh can reach beyond national borders, the entire mesh will reroute through that pathway, and even if all BGP routes are severed, the mesh will still be able to communicate internally. By providing a model of cloud computing which involves storing data outside the corporate server farms owned by Amazon, Google and Dropbox, Freedombox provides additional security benefits insofar as there are stronger legal protections for material which is located within a domestic residence than for material which is stored publically.

Whereas Freedombox can be understood as a technologically-orientated way of addressing issues surrounding the level of technical expertise required to engage with cryptographic tools, an alternative approach arises from the Hacktionlab collective, who describe themselves as a:

> UK tech-activist run project that aims to create regular convergence spaces where activists interested and/or working in the areas of alternative media, renewable energy, on-line video distribution, free software or any other form of activism that utilises technology can get together and plan how to better harness the technology (or not) to support grass roots social movements. (Hacktionlab 2014).

Featuring members associated with activist projects including Indymedia, Bristol Wireless, Tachanka, Dissident Island, VisiononTV and Aktivix, Hacktionlab was largely responsible for providing facilities such as internet access and media centres for large-scale direct actions such as the Camp for Climate Action in 2007/8. These centres included computers, radio and video studio facilities, satellite and 3G modems, routers and antennae, solar panels, inverters and other equipment required to allow activists involved in climate camp to create their own visual, audio and text-based media and to publish this material to the internet whilst the protest camp was ongoing. However, there was a feeling expressed on the group's mailing list that adopting this role increasingly saw the division of participants into activist technical service providers and vanilla activists. Such a demarcation is problematic insofar as it recreates the producer/consumer divide characteristic of dissociated milieus within an activist

context. Rather than communally and consensually evolving non-hierarchical ways of living, activist techs were, broadly speaking, expected to adopt the role of corporate telecommunications services, albeit without surveillance or targeted advertising.

Consequently, Hacktionlab moved away from providing infrastructural support, and towards processes of public engagement and outreach, running stalls, workshops and events at conferences, bookfairs, community events and barncamp gatherings, where the ethical and pragmatic rationales for using encryption tools, free software and other elements of tech-activism were discussed and debated. The collective additionally publishes a booklet entitled *Tech Tools for Activism* (n.d.), which outlines the rationale for activists adopting tools such as Tor, PGP, activist email, mobile phone security, open publishing, and non-corporate blogging and microblogging platforms, alongside providing step-by-step instructions for using these services and detailing how and why they work to protect various forms of freedom. Hacktionlab's shift in focus, from providing technical infrastructure, to education and outreach is pertinent to this discussion as it evidences tech-activists attempting to address the dissociated milieu which separates activists into technical platform and infrastructural producers on the one hand and 'regular activists' who act as consumers of both activist-led and commercial telecommunications services on the other. Furthermore, the process of collective education is crucial here, as following Stiegler, this represents the struggle against proletarianisation; by understanding the inner workings of elements of the technical ecologies in which telecommunications circulate, activists are able to undertake communicational practices which enhance privacy and anonymity, whilst engaging with free software systems which correlate with the ethical and political stance of the actions themselves.

Conclusions

Recent developments such as the revelations regarding the NSA-run PRISM program, the imprisonment of social media users for making open calls for citizens to engage in direct action, and state-led attempts to curtail online communications during periods of civil unrest highlight that measures taken to preserve anonymity and encrypt telecommunications are a vital strategy for contesting the pervasive surveillance apparatus of the state and large corporations within societies of control. These examples decisively illustrate that the ideal of an open internet is seriously flawed; communications without encryption and anonymity present a system whereby activists are open to persecution and incarceration.

A common retort has been 'if you've done nothing wrong, you've got nothing to hide,' however, such sentiments barely mask a microfascism which presents the state (in both current and all imaginable future guises) to be an entirely benevolent and just entity to whom social responsibility is delegated, demarcating a dissociation between the 'troublesome' activity of individuals and the ultimate authority and justice of the state. However, even proponents of this argument find it somewhat harder to maintain this

line of reasoning when it is applied to the actions non-Western governments, such as the Mubarak regime's attempt to shut down the Egyptian Internet, demonstrating the cognitive dissonance present in their attitudes towards their own state. Examining the treatment of high profile whistle-blowers such as Manning and Snowden, alongside the exposure that UK police infiltrated peaceful climate protest groups (Lewis and Evans 2013; Loadenthal 2014) reveals the lengths to which notionally democratic societies are willing to go to supress nonviolent dissidents, and consequently, in order to provide telecommunications systems which resist the types of surveillance programmes revealed by Snowden, but which were widely assumed to be in place before this confirmation, activists utilise anonymization and encryption tools, which the Snowden revelations suggest were still broadly effective as of 2013, although the Tor Stinks presentation outlines numerous ways that the NSA and GHCQ are actively seeking to undermine these systems.

One of the key points which emerges from such analysis, is that claims pertaining to the open internet present a partial account of online practices which effectively ignore a broad range of communications, with activist uses of technology proving a pertinent example. The notion of a singular and totally open internet arose in the early utopian days of digital culture, however, these idealised conceptions of online freedom and openness are far removed from the actually existing internet of the past twenty years. Whilst there are certain forms of openness, especially those pertaining to the protocols of the web and internet, which are vital to the evolution of digital culture, these spaces have never been totally open, and neither would this openness be a desirable quality. Indeed, in place of an open/closed dualism which effectively presents openness as an unabated good, this paper has sought to map a range of examples which suggest that issues surrounding openness and the internet are considerably more complex than is often imagined.

Exploring a range of activist cryptography tools and practice additionally foregrounds the importance of collaborative and collectivised modes of education as a means of combatting proletariansation, and seeking to reduce the technical dissociation which is fostered through dependency on technological consumerism. For many activists, relying upon corporate social media platforms not only represents a serious security threat to the continued functioning of affinity groups and collectives, but tends to contradict the stated aims of activist moves to demonstrate that 'another world is possible,' that neoliberal capitalism is not the only possible mode of globalised governance. By further proliferating societal striations, whereby an infrastructural producer/consumer divide renders those communicating information as valued assets within social media revenue generating practices (which themselves are predicated upon surveillance techniques which the existence of PRISM denotes are entangled with state surveillance apparatuses), such activities further concentrate power within digital networks in the hands of global elites, creating the type of deleterious networking practices elaborated by Deleuze and Stiegler.

Consequently, Stiegler has argued for the urgent construction of an economy of contribution which the dissociated milieus of neoliberalism are replaced with architectures of participation which are founded upon eroding the differentiation between end users and systems designers and administrators. Indeed, as we have seen, this separation is predicated upon a consumerist approach to communications infrastructures, and was precisely the issue faced by Hacktionlab, whose consequent shift towards educational events and literature can be understood as the type of move which is required to enact the economy of contribution Stiegler posits. In constructing such an economy, the ability to interrogate the information and communication systems in the manner prescribed by FOSS is vital, however, what is at stake here are questions surrounding freedoms and collective production, closely approximating the founding principles of the Free Software Foundation, rather than the allegedly ideology-free version of openness derived from its open source counterpart.

Notes

1. Whilst the term activist carries general connotations of political activity, as expressed by the notion of 'party activists', and can be understood as referring to the subset of political activists who are engaged in intentional activities 'directed against prevailing authority as domination and exploitation, whether in personal relations of micro-power or in the form of institutional domination,' (Hands 2011, 5), the specific activist projects explored here are those which engage in strategies of direct action (Jordan 2002) and/or whistleblowing aimed specifically at institutional domination.

References

Barlow, John Perry. 'A Declaration of the Independence of Cyberspace'. Last modified May 6 2014. https://projects.eff.org/~barlow/Declaration-Final.html.

Bauwens, Michel. 2005. 'The Political Economy of Peer Production'. CTheory 1. http://www.ctheory.net/articles.aspx?id=499

Beer, David. 2008. 'Social Network(Ing) Sites . . . Revisiting The Story So Far: A Response to danah boyd & Nicole Ellison'. Journal of Computer-Mediated Communication 13 (2): 516-29.

Benkler, Yochai. 2006. *The Wealth of Networks: How Social Production Transforms Markets and Freedom*. New Haven: Yale University Press.

Berners-Lee, Tim. 1996. 'WWW: Past, present, and future'. Computer 29 (10): 69-77.

Best, Kirsty. 2010. 'Living in the control society Surveillance, users and digital screen technologies'. *International Journal of Cultural Studies* 13 (1):5-24.

Black Duck Software. 2014. 'Top 20 Open Source Licenses'. http://www.blackducksoftware.com/resources/data/top-20-open-source-licenses

Boyd, Danah, and Eszter Hargittai. 2010. 'Facebook privacy settings: Who cares?' *First Monday* 15 (8). http://firstmonday.org/ojs/index.php/fm/article/view/3086

Castells, Manuel. 1996. *The Rise of the Network Society: The Information Age: Economy, Society and Culture* Volume I. Massachusetts: Blackwell

Crogan, Patrick. 2010. 'Bernard Stiegler: Philosophy, Technics, and Activism'. *Cultural Politics* 6 (2): 133-56.

Dean, Jodi. 2009. *Democracy and Other Neoliberal Fantasies: Communicative Capitalism and Left Politics*. Durham: Duke University Press.

Dean, Jodi. 2013. *Blog Theory: Feedback and Capture in the Circuits of Drive*. New York: John Wiley & Sons.

Deleuze, Gilles 1992. 'Postscript on the Societies of Control'. *October* 59 (Winter): 3-7.

Dovey, Jon, and Mandy Rose. 2012. 'We're Happy and We Know It: Documentary, Data, Montage'. *Studies in Documentary Film* 6 (2): 159-73.

Dyer-Witheford, Nick. 1999. *Cyber-Marx: Cycles and Circuits of Struggle in High-technology Capitalism*. Chicago: University of Illinois Press.

Dyson, Esther. 1996. 'Cyberspace and the American Dream: A Magna Carta for the Knowledge Age (Release 1.2, August 22, 1994)'. *The Information Society* 12 (3): 295-308. doi: 10.1080/019722496129486.

Elmer, Greg. 2003. 'A Diagram of Panoptic Surveillance'. *New Media & Society* 5 (2): 231-47.

Featherstone, Mark. 2013. 'Einstein's Nightmare: On Bernard Stiegler's Techno-Dystopia'. CTheory. http://www.ctheory.net/articles.aspx?id=728

Fuchs, Christian. 2010. 'Labor in Informational Capitalism and on the Internet'. *The Information Society* 26 (3): 179-96.

Fuchs, Christian. 2012. 'The Political Economy of Privacy on Facebook'. *Television & New Media* 13 (2): 139-59.

Fuchs, Christian, Kees Boersma, Anders Albrechtslund, and Marisol Sandoval. 2013. *Internet and Surveillance: The Challenges of Web 2.0 and Social Media*. London: Routledge.

Furnell, Steven. 2005. 'Why Users Cannot use Security'. *Computers & Security* 24 (4): 274-79.

Galloway, Alexander R. 2004. *Protocol: How Control Exists after Decentralization.* Cambridge, MA: MIT press.

Greenwald, Glenn. 2014. *No Place to Hide: Edward Snowden, the NSA, and the US Surveillance State*. New York: Metropolitan Books.

Hacktionlab. 2014. 'Welcome to Hacktionlab'. https://hacktionlab.org/hacktionlab/index.php/Welcome_to_HacktionLab.

Hacktionlab. n.d. Tech Tools for Activism. https://techtoolsforactivism.org/booklet

Hands, Joss. 2011. *@ is for Activism: Dissent, Resistance and Rebellion in a Digital Culture*. London: Pluto Press.

Hardt, Michael, and Antonio Negri. 2000. *Empire*. Cambridge, MA: Harvard University Press.

Hardt, Michael, and Antonio Negri. 2005. *Multitude: War and Democracy in the Age of Empire*. London: Penguin.

Indymedia. 2002. 'Principles of Unity'. http://docs.indymedia.org/view/Global/PrinciplesOfUnity.

Janssen, Marijn, Yannis Charalabidis, and Anneke Zuiderwijk. 2012. 'Benefits, Adoption Barriers and Myths of Open Data and Open Government'. Information Systems Management 29 (4): 258-68.

Jones, R. 2001. 'Digital Rule: Punishment, Control and Technology'. *Punishment and Society* 2 (1): 5-22.

Jordan, Tim. 2002. *Activism! Direct Action, Hacktivism and the Future of Society.* Clerkenwell, UK: Reaktion books.

Kinsley, Samuel. 2014. 'The Matter of 'Virtual' Geographies'. *Progress in Human Geography* 38 (3): 364-84.

Klein, Naomi. 2000. *No Logo*. London: Flamingo.

Kleiner, Dmytri. 2010. The Telekommunist Manifesto: Institute of Network Cultures.

Landau, Susan. 2013. 'Making Sense from Snowden'. IEEE Security & Privacy Magazine 4: 5463.

Lash, Scott, and Celia Lury. 2007. *Global Culture Industry: The Mediation of Things*. Cambridge: Polity.

Lazzarato, Maurizio. 1996. 'Immaterial Labour'. In *Radical Thought in Italy: A Potential Politics*, edited by Paulo and Hardt Virno, Michael, 133-47. Minneapolis: University of Minnesota Press.

Lessig, Lawrence. 1999. *Code: And Other Laws of Cyberspace*. New York: Basic Books.

Lewis, Paul, and Rob Evans. 2013. *Undercover: The True Story of Britain's Secret Police*. London: Faber & Faber.

Leyden, John. 2012. 'The One Tiny Slip That Put LulzSec Chief Sabu in the FBI's Pocket'. The Register. http://www.theregister.co.uk/2012/03/07/lulzsec_takedown_analysis

Loadenthal, Michael. 2014. 'When Cops 'Go Native': Policing Revolution through Sexual Infiltration and Panopticonism'. *Critical Studies on Terrorism* 7 (1): 24-42.

Marazzi, Christian. 2008. *Capital and Language: From the New Economy to the War Economy*. Los Angeles: Semiotext.

Marx, Karl. 1973. *Grundrisse*. Translated by Martin Nicolaus. London: Penguin.

Miller, Paul, Rob Styles, and Tom Heath. 2008. 'Open Data Commons, a License for Open Data'. LDOW. http://ceur-ws.org/Vol-369/paper08.pdf

Papacharissi, Zizi, and Paige L Gibson. 2011. 'Fifteen Minutes of Privacy: Privacy, Sociality, and Publicity on Social Network Sites'. In *Privacy Online: Perspectives on Privacy and Self-disclosure in the Social Web*, edited by Trepte, Sabine, and Leonard Reinecke, 75-89. Berlin: Springer.

Raymond, Eric. 1998. 'Goodbye, "Free Software"; Hello, "Open Source"'. Eric S. Raymond's Homepage. http://www.catb.org/esr/open-source.html

Rushkoff, Douglas. 2003. 'Open Source Democracy: How Online Communication is Changing Offline Politics'. Demos. www.demos.co.uk/files/OpenSourceDemocracy.pdf.

Schneier, Bruce. 2013. 'The US Government has Betrayed the Internet. We Need to Take it Back'. *The Guardian*, 5 September. http://www.theguardian.com/commentisfree/2013/sep/05/government-betrayed-internet-nsa-spying

Sheng, Steve, Levi Broderick, Colleen Alison Koranda, and Jeremy J Hyland. 2006. 'Why Johnny Still Can't Encrypt: Evaluating the Usability of email Encryption Software'. Paper read at Symposium On Usable Privacy and Security, Pittsburg, Pennsylvania, 12-14 July 2006.

Simon, Bart. 2002. 'The Return of Panopticism: Supervision, Subjection and the New Surveillance'. *Surveillance & Society* 3 (1): 1-20.

Stiegler, Bernard. 2009a. 'Teleologics of the Snail The Errant Self Wired to a WiMax Network'. *Theory, Culture & Society* 26 (2-3): 33-45.

Stiegler, Bernard. 2009b. 'The Theater of Individuation: Phase-Shift and Resolution in Simondon and Heidegger'. *Parrhesia* 7: 46-57.

Stiegler, Bernard. 2010a. *For a New Critique of Political Economy.* Cambridge Malden, MA: Polity.

Stiegler, Bernard. 2010b. 'Memory'. In *Critical Terms for Media Studies*, edited by Mark BN Hansen and William JT Mitchell. Chicago: University of Chicago Press.

Stiegler, Bernard. 2013. *What Makes Life Worth Living: On Pharmacology*. New York: John Wiley & Sons.

Terranova, Tiziana. 2000. 'Free Labor: Producing Culture for the Digital Economy'. *Social Text* 18 (2): 33-58.

The Tor Blog. 2011. 'Recent Events in Egypt'. (page no longer available) https://blog.torproject.org/blog/recent-events-egypt.

Tkacz, Nathaniel. 2012. 'From Open Source to Open Government: A Critique of Open Politics'. *Ephemera: Theory and Politics in Organization* 12 (4):386-405.

'Tor Stinks Presentation: Read the Full Document'. 2013. *The Guardian*, 4 October. http://www.theguardian.com/world/interactive/2013/oct/04/tor-stinks-nsa-presentation-document.

Whitten, Alma, and J Doug Tygar. 1999. 'Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0'. Usenix Security 1999.

Wiener, Norbert. 1965. *Cybernetics or Control and Communication in the Animal and the Machine.* Cambridge, MA: MIT press.

Zizek, Slavoj. 2006. *The Parallax View.* Cambridge, MA: MIT Press.