Journal of Media Critiques [JMC]
doi: 10.17349/jmc117204 P-ISSN: 2056-9785 E-ISSN: 2056 9793
http://www.mediacritiques.net jmc@mediacritiques.net

PRIVACY AS A CULTURAL PHENOMENON

GARFIELD BENJAMIN*

ABSTRACT

Privacy remains both contentious and ever more pertinent in contemporary society. Yet it persists as an ill-defined term, not only within specific fields but in its various uses and implications between and across technical, legal and political contexts. This article offers a new critical review of the history of privacy in terms of two dominant strands of thinking: freedom and property. These two conceptions of privacy can be seen as successive historical epochs brought together under digital technologies, yielding increasingly complex socio-technical dilemmas. By simplifying the taxonomy to its socio-cultural function, the article provides a generalisable, interdisciplinary approach to privacy. Drawing on new technologies, historical trends, sociological studies and political philosophy, the article presents a discussion of the value of privacy as a term, before proposing a defense of the term cyber security as a mode of scalable cognitive privacy that integrates the relative needs of individuals, governments and corporations.

Keywords: Privacy, information technology, digital culture, social media, communications.

INTRODUCTION

Privacy has become a convoluted, murky, and often contradictory term in the information age. The complexities and counterarguments to any position on privacy in contemporary society hark back to a divided history of the term and herald the potential for even greater confusion and exploitation in the future. New modes of using technology to organise society often run counter to privacy on both technical and social levels. For example, Tapscott and Tapscott's (2016) proposition that 'the Internet of Everything needs a Ledger of Everything' leads to pseudonymity at best and a buzzword-laden trap for the uninformed and the unwary. Similarly, the burden of privacy falling on users themselves can create unusual and seemingly paradoxical results. One study (Mamonov and Koufaris, 2016) found that with the 'spectre of government' on their minds, participants were actually less likely to create a secure password. The scale at which people presume their privacy is infringed has led to a culture of helplessness in which it does not seem worth bothering with personal security online. The failure of governments to foster a positive culture has instigated an existential crisis of privacy, thereby exposing citizens to criminal as well as state

* PhD. University of Birmingham. g.8enjamin@gmail.com

threats. The media too participates in this culture of fear, feeding us the image that this situation will only get worse and there is nothing we can do about it. Indeed, key influential cyberculture figures such as Cory Doctorow (2016; 2007) paint a bleak picture of the future in the context of the Internet of Things and the new pervasive role of the server log, supported by an almost constant stream of news articles reporting botnets, vulnerabilities, information leaks, and hacks of digital devices and infrastructure at all levels. And yet, in such a cultural and technological environment defined by the economic context of big data, privacy becomes ever more important both socially and existentially. When the CIA are willing to 'kill people based on metadata' (Johns Hopkins University, 2014), the need for privacy extends far beyond the scope of any individual or any specific technology. A systemic shift is required in the culture of privacy for a more informed and more secure digital future for everyone.

The current state of research on privacy has yielded both broad and deep discussions across technical and social contexts. Yet there is a tendency to remain rooted in one field and, consequently, a proliferation of increasingly complex taxonomies, examples and specific applications of the term. Thus, the concept of privacy remains muddled and, particularly for the average layperson whose awareness of privacy is ever more mediated by a fear-mongering and sensationalist press, often obfuscates many of the underlying antagonisms and importance of the issue(s) at stake. This article presents a higher-level analysis of privacy in terms of its functional effect on human behaviour and subsequent systemisation and inclusion in broader political and technical instances. Rather than a detailed taxonomy, privacy will be redefined into two overarching interdisciplinary categories: freedom, corresponding to the influence of fear on techno culture, and property, underpinning the relations between humans and their digital selves. These terms will be traced through the history of privacy to inform the specifically digital context of the culture of privacy both today and in the future.

The article will ask: How long a culture of privacy last? What will replace it? And how can we ensure that the positive values it protects continue to remain an essential component of future collective culture in an ever more technologically mediated world?

BACKGROUND

The current debate over privacy has proliferated between academic and public disciplines, resulting in often conflated and/or contradictory conceptions of the concept and its impact. As a term, privacy has perhaps received most attention in the study of law, as well as politics, with scholars such as Daniel Solove (2006; 2008) and others (Scholz, 2016; Bambauer, 2013; Halbert, 2016). The necessary precision required for legal debates - the need for detailed definitions that can be applied to niche circumstances in order to provide clarity in situations of great complexity - has tended towards ever more elaborate taxonomies focusing on specific legal applications, or the application of existing legal and political systems to issues of digital privacy. While providing incrementally greater accuracy, these definitions are not necessarily related to the actual available digital technologies, nor to how they are used in practice, but rather to an abstract system of potential use in the context of public and civil legal processes and frameworks. Progress in this area has entailed reducing the argument to a basis in fundamental rights in order to penetrate the web of intricate layers of legal structures that impede a rapid response to evolving digital technologies (Ojanen, 2016). This is, however, reliant on a clear system of rights that are not always present

amidst national and international constitutions, treaties and other directives. Such studies still fail to overcome the problem of current laws being ill-equipped to deal with the architectures and behaviours of cyberspace, not least due to the fundamental dilemma of laws being rooted in nation states and thus unable to respond to the global structures and activities of digital networks. A cultural perspective thus offers a broader and more widely applicable mode of viewing behaviours beyond the traditional geographical-legal boundaries with which law as a field must concern itself.

Computer science approaches generate similar terminological problems when discussing privacy. The exponentiation of taxonomies is here derived largely from different attacker models that require specific technical responses. There has historically been a tendency to simply oppose privacy and security (Liu, Ryan and Chen, 2014; van Schoonhoven, Roosendaal and Huijboom, 2013), although others have been involved in attempts to move past this dichotomy (Kwecka, Buchanan, Schafer and Rauhofer, 2014). The confrontational model of privacy and security exemplifies the technical constructions that are commonly at odds when defending the interests of the individual citizen versus the interests of the nation state. As will be discussed below, this problem of scale risks conflating issues of freedom and property, cascading into a series of potential inconsistencies and personal or ideological biases. One such example is that of Bruce Schneier who - along with many other technologists known for promoting the advancement of the scientific method and progress towards an increasingly digital society - counterintuitively objects to online voting at both the practical and conceptual levels. Despite his famous critique of fear-based decision-making (2003), Bruce Schneier's vehement opposition to electronic voting (2016) demonstrates the limit that plagues even the hardest techno-utopian: a loss of control when scaling from the individual to society as a whole. A decade after Beyond Fear, Schneier's focus on trust, risk and uncertainty risks closing avenues of research based on current fears and a nostalgic reliance on a lost sense of security rather than developing new approaches to improved privacy for all levels of technology and society. For example, the overemphasis on trust risks limiting the development of 'trustless' systems that could bypass many privacy issues and provide individuals with greater freedom, anonymity and control over their data. While he acknowledges that technological and societal issues do not necessarily coincide (Schneier, 2012), a regressive attitude towards the familiarity and apparent certainty of the paper ballot is echoed in further examples of archaic models of physical security, such as bemoaning the decline of handwriting in an age of typing (or tapping) and standardised testing that could lead to more easily forged signatures rather than pushing for new modes of proving identity that harness ubiquitous computing technologies. Further fear-based texts (Schneier, 2015) aimed at a broader and interdisciplinary readership feed off a culture of privacy that has already been subsumed by that of security. Such approaches not only risk closing off the individual as a self-protecting isolationist but actively harm future technological development that might arise from collective activities and a more socially aware approach (let us not forget that a large proportion of research conducted today is collaborative). The all-or-nothing approach espoused by technologists such as Schneier when they reach perceived technical limits closes off a productive connection with actual social problems. While technology cannot necessarily produce a positive culture of privacy, it can at least strive not to harm it.

Despite this need for socio-cultural interventions in the development of privacy, the field of cultural and media studies has tended to limit its focus to very specific instances or issues of privacy rather than the trends and cultures as a whole. This is in part due to the complexity of the issue and its many contradictory arguments, such as the dilemma of privacy for feminism that will be discussed below, in which privacy itself can be both positive and negative for women's rights. It is also in part due to the inherent bias when discussing social and cultural phenomena, such as the paper by Fuchs (2011). On the one hand, this work broadens the privacy debate into critical political economy. On the other hand, however, the use of a Habermasian methodology projects its explicitly socialist ulterior motives with a Marxian reduction of the entire issue to economic forces of capitalist systems, denying the anti-statist and anti-corporate possibilities within the libertarian (broadly conceived) and 'liberal' (capitalist and post-capitalist) conceptions of privacy that played an actual role in defining the early development of the internet. It is not only ideological perspectives that can limit a cultural approach. Media/cultural studies allow for an acknowledgement and discussion of international issues, beyond the legal structures of individual nations. Studies undertaken in this area (Millhan and Atkin, 2016; Liang, Shen and Fu, 2016) have made great progress in demonstrating the intricacies of cultural shifts in privacy. However, a focus on the impact of specific existing cultures on privacy, rather than a discussion of global (cyberspace) trends and a culture of privacy itself, creates a tendency towards emphasising cultural differences. While individual cultural issues must be taken into account, this difference-based approach risks limiting the development of broader positive attitudes towards privacy by entrenching traditional socio-economic identities and divisions within a micro-political agenda.

Despite this, it is the socio-cultural impact of privacy that has the most profound effects, influencing not only public opinion but the formation and definition of the future of privacy, a collective psychology that will guide the development (or not) of positive attitudes and the demand for change across technology, law and other fields. In the psycho-social sphere, the privacy versus security antagonism can be translated into a dilemma of anonymity and responsibility. It is the behaviour (that is, individually, the psychology or, collectively, the culture) of companies, governments and individuals - indeed any and all can be at fault - that is under scrutiny or not as the case may be. For example, a company may sell user data or block disclosure of vulnerabilities, a government may conduct illegal surveillance or interfere with the democratic process of another state, or individuals may be engaged in online trolling including even children being responsible for online bullying. The implications of all these can lead to the ruin of the victim, whether it be undermined sovereignty, damaged reputation, financial loss, contravention of human right, or being driven to suicide. While there has been work undertaken on the impact of specific culture(s) on privacy (Li, Kobsa, Knijnenburg and Nguyen, 2017), there remains the need for a discussion of the underlying culture of privacy. Furthermore, this study uses, for example, demographic cultural data points that risk falling into the trap of being privacy-invasive. The use of data collection and analytics to predict users' privacy views is inherently problematic in promoting privacy awareness and an open debate. The interdisciplinary approaches available to contemporary researchers, combining social, legal and technical perspectives, must also take a more self-reflexive view in which systemic biases are taken into account. Indeed, historically it has been the pre-existence of physical world

ideologies, attitudes and biases that have led to the fear-based privacy culture in which many individuals now live.

To illuminate the root of the term, and in order to strip back its increasingly complicated applications that often too quickly become too specific for any overarching cultural analysis, it is first necessary to discuss the history of privacy. Privacy is a recent invention. When humans lived in settlements no larger than a village, everybody knew everybody and there was no need for or conception of privacy. Indeed, this is the historical background to and social truth of McLuhan's global village (2001 [1964]): at all times, your activities are known to all. But where in contemporary 'village' models of global networks the constant observation is seen as a threat to privacy, in the primitive village or tribal society such notions as privacy and even individualism did not enter into the collective culture. Demonstrating the lack of clear cut shifts from one cultural epoch to another, this attitude persisted until at least the 19th Century CE, where urban working class living in large industrial cities such as Birmingham, UK, included shared gardens and access, close proximity, and a class-based identity based on locality and familiarity. Often the tensions between communities (whether geographical, national, class or ethnicity) devolve out of a fear of the unknown, while a lack of privacy is to a certain extent inherent to the culture of a close-knit community. This stems from a scaling of subjectivity from the individual to the group onto which it displaces its identity. The interactions with external entities therefore follow the logic of the Lacanian big Other (Lacan, 1977). This concept is the psychological function of radical alterity beyond identification. It is simultaneously the fundamental 'otherness' of our experience of the world and yet also the position from which we view ourselves and our desires. It is no wonder, then that an encounter with perceived outsiders, the threat of an often-illusory adversary, is the cause of decisions based on fear. These psychoanalytical structures are inherently bound to the role of the symbolic order, to the structures of language and semantic codings that give meaning to human consciousness. Thus, language as the externalisation of memory places the individual in a position of vulnerability as their internal thoughts become at risk of being revealed and/or used by the Other.

The invention of writing, followed by the printing press and mass literacy, therefore acted as an enabler of the shift towards a concept of privacy. This externalisation of memory that supported greater powers of communication over both space and time is not without its own 'side channel attacks'. Indeed, the first call for a legal protection of privacy in 1890 (Warren and Brandeis) was a direct call for the law to adapt to the pressures and social implications of new communication technologies, emphasising the need to protect both people and their (material and intellectual) property. Since then, theft of important or secretive documents has given rise to a multitude of issues concerning persistence, data loss (or collection), censorship, copying or plagiarism, and security. These forms of personal and political espionage underpin the need for privacy, for when our innermost thoughts are recorded (whether by our own hand or others) we have something to fear from their being revealed, and a culture of privacy develops. From the seemingly petty accusation of 'hands off my diary' between siblings, through to high-stakes classified documents between nation states, the permanence of writing was the first step on the road to privacy.

The history of privacy, even before it became concrete as a specific term, can be generally defined as the relative impact of two pre-existing behaviours that span

politics, economics, society and technology: a gradual shift from freedom to property. The following discussion will present this history and its relation to the cultural functions of fear and exploitation. In its present state, and the context of digital technologies, our culture displays a conflation of both aspects of privacy. Indeed, it is this relation between two different definitions that gives rise to many of the persistent issues and lack of clarity in discussing the term, particularly between disciplines. Yet the two forms of privacy are not necessarily counterposed. Rather, their increasingly complex interaction has had a profound impact on the contemporary culture of privacy and the particular emphases of different actors and perspectives. Thus, the conflict is a product of the specific uses of the term, a cultural phenomenon that defines its interpretation and the attitudes it engenders, rather than a quality inherent to its technological or legal framework. Between freedom and property rests the basis of privacy as a cultural phenomenon, as well as the key to understanding its potential future(s).

FREEDOM

Privacy as freedom is the basis for the historical antagonism with security, the perpetuation of Hobbes's dilemma of the contract between individual and state, liberty and authority, risk and safety. Freedom is also thus linked directly to fear, and indeed privacy was originally the necessary requirement of those deemed outcasts, deviants and traitors. Until the long transition was complete from tribal or village mentality into individualism, metropolitanism and enlightenment, privacy remained the domain of criminals, assassins and usurpers, as well as a defence against persecution and fear of the establishment or the regressive masses. Followers of dark or marginal gods, adherents of upstart religions such as Christians under the Roman Empire, practitioners of witchcraft or alchemy, all had need for clandestine behaviours to keep their shunned activities secret. Even homosexuals historically needed to hide their identity, and when talking of security and privacy one cannot but think of the tragic impact of this situation for Alan Turing. Indeed, the history of computing and encryption has become inextricably bound to this outsider status and violation of human dignity, even as it developed to assist surveillance and code-breaking in the state military agenda and in the name of 'freedom'.

This alterity, a binding of privacy to fear as the threatening Other, aligns with the history of writing in its use by the state to collect data on its citizens. Long before big data, the census enabled records of individuals that could be used for control and to assert homogeneity upon a conquered or subjugated population. In Mediaeval Britain, the very name of the great census of 1086 - the Domesday [Doomsday] book, also known as the Book of Judgement - conjured up apocalyptic connotations of location tracking, the inescapability of the state and the reduction of a conquered nation to a collection of data for manipulation and exploitation. This great ledger represented the inevitability of death and taxes rolled into one. Similarly, the Biblical Roman census that formed a backdrop to the nativity myth represented an obligatory upheaval followed by a period of restricted movement in order that the populous be counted for tax purposes. The earliest census can be traced even further back to at least ancient Egypt in the fourth millennium BCE, and the roots of data collection stems from the origins of written language - a technology that enabled record-keeping for the economic or legal control of expanding settlements. Yet the economic argument always belies a function of control, a fixing of the individual to limit their freedom

through increasingly constant monitoring. Indeed, the contemporary state census, and even data collected and held by supranational bodies such as the World Health Organisation, ostensibly for positive purposes, is always at risk of transforming into an authoritarian regime in which knowledge of each and every individual is a source of great power. The US government, for example, has stated its intention to use the Internet of Things to track people, spreading the reach of state collection of data beyond the official census into commercial and private domains. Technology has enabled a universal panopticon, full state surveillance on the assumption that all citizens are potential criminals mitigated by the fear that any individual could be being monitored at any given time, an inherent discipline within surveillance (Foucault, 1991). Even the genesis of the contemporary digital computer - such as Colossus at Bletchley Park, arguably the first programmable computer - was entwined with state-based surveillance, espionage and the application of military might.

However, the internet has its basis not only in defense contracts but in openness, a countercultural phenomenon committed to sharing and the pursuit of knowledge. The roots of connectivity in building research networks gave rise to the view of cyberspace as a separate dimension with its own rules and governance, and early internet utopians making declarations as such (Barlow, 1996). But opposition to state limits on freedom and the desire to create an alternative model for society predates the information age. The following passage by Pierre Joseph Proudhon demonstrates this counter-surveillance tendency and critique of government as an information-collecting entity at least as far back as the industrial revolution:

You know it, and you permit it. To be GOVERNED is to be kept in sight, inspected, spied upon, directed, law-driven, numbered, enrolled, indoctrinated, preached at, controlled, estimated, valued, censured, commanded, by creatures who have neither the right, nor the wisdom, nor the virtue to do so.... To be GOVERNED is to be at every operation, at every transaction, noted, registered, enrolled, taxed, stamped, measured, numbered, assessed, licensed, authorized, admonished, forbidden, reformed, corrected, punished. It is, under the pretext of public utility, and in the name of the general interest, to be placed under contribution, trained, ransomed, exploited, monopolized, extorted, squeezed, mystified, robbed; then, at the slightest resistance, the first word of complaint, to be repressed, fined, despised, harassed, tracked, abused, clubbed, disarmed, choked, imprisoned, judged, condemned, shot, deported, sacrificed, sold, betrayed; and, to crown all, mocked, ridiculed, outraged, dishonored. That is government; that is its justice; that is its morality. (Proudhon, 2007 [1851])

Today, the anarchist critique takes on new relevance, with the Investigatory Powers Bill in the UK and Rule 43 in the US demonstrating the state's continued need for a "monopoly on the legitimated use of physical force" (Weber, 2004 [1919]) in the cyber realm. Whereas conventionally the state functioned according to such a monopoly over a given geographical area, in a globalised world with an internet that stretches both across and beyond physical locations this concept breaks down. Overly restrictive and increasingly authoritarian cyber legislation can therefore be seen as an incredibly problematic and worrying, yet perhaps predictable and understandable response to the global digital medium by the archaic psychopathologies of the state. It is a one-sided arms race, a cold war against an imaginary adversary, the ultimate non-linear warfare. It is also a strategy that is ineffective on two counts. Firstly, its negative impact on

culture, stemming from a sense of overwhelming helplessness in the general population, propagates an insufficient culture of privacy that also serves to enable criminal and state actors. Secondly, it gives rise to stronger counter-cultures embodied in privacy campaigners such as the EFF and companies such as Mozilla, Opera or Apple, whose promotion of accessible privacy would impede and eventually undermine the systems of legislation that seldom keep pace with technological and social developments.

The issue(s) of digital freedom itself has a problematic history. The counter-cultural background of the outsider status of early computer scientists and programmers has become entrenched in the technologies and their further cultural development. As Kwecke et al. (2014) state, "Most approaches to PET reflect the individualistic, libertarian origins of privacy law as an individual right". Freedom is, as far as possible, built into both the technical architectures and their cultural tropes. The very basis of the internet is an open network, yet openness and freedom is at odds with true privacy as the secrecy within which to conduct free behaviour. How can one's own freedom be compatible with the freedom of a malicious Other? The ideal of privacy as freedom, in relation to the potential state control of overarching structures such as telecommunications networks or specific technologies such as the constant threat (or prominent illusion) of NSA or GCHQ backdoors, thus reveals an internal dilemma in privacy culture, a technophobic kernel of libertarian techno-utopianism. This underlying fear of technology even by those who are responsible for its creation is disseminated throughout society, borne by the apocalyptic warnings of Schneier and others before mutating through different ideological positions into nostalgia, analogue fetishism and reactionary conservatism. At this point misinformation runs amok with the technically ignorant and privacy takes on an air of white male privilege - a boon for the l33t hax0rz that form the elusive technocrats who mysteriously control technologies beyond the grasp of the layman. The trust required of this outsider community places technologists and other privacy experts as the big Other of a global anonymous computer network striking fear into the hearts of average citizens and the existing establishment. The fear of technology becomes therefore a fear of loss of status and control, a fear of Otherness embodied in both the networks of digital devices and those seen to be controlling them. This Otherness works in both directions, as the traditionally alter group of technologists loses its own controlling, outsider in the gradual diversity of the technology industry. While the industry itself may purport to embrace diversification and inclusion of, for example, women, the culture it propagates is not always so progressive or adaptive. The gamergate situation demonstrates the broader impact of the technocratic community for, while it is not necessarily technologists themselves who engaged in the abusive hateful activities, the white male privilege combined with a prized outsider status led to an aggressively defensive cultural identity for a select group of gamers who feared their own loss of status amid the changing culture of technology as a whole. While not explicitly a privacy issue, the anonymity prized by this culture provided an apparently safe space from which to launch attacks stemming from trolling to death threats, and the unmasking of those involved appeared as an affront to their sensibilities. It revealed the negative aspects of privacy culture, with abusers having latched onto a perceived identity emboldened by a sense of power derived from anonymity. They are a far cry from the original members of the outsider groups involved in generating the technologies and their

cultures and certainly diametrically opposed to groups such as the EFF which place great emphasis on diversity and inclusion in privacy technologies.

The gamergate scandal highlights a further dilemma in the freedom debate for privacy - that of women's rights and gender equality more generally. As far back as Aristotle there has been a division between public and private life, where private life concerns the internal affairs of the family. This suggests a strong argument for privacy in feminism, allowing women freedom over their own bodies and sexuality without the invasion of social pressures or governmental regulation. However, this assumption of privacy that tends towards a social system in which the private family life remains free from scrutiny works to protect not only the otherwise oppressed but also their oppressors. Historically, the family unit has supported the perpetuation of overarching patriarchal structures, concealing oppression in this system of the privacy of family affairs (MacKinnon, 1989). There is here a "darker side of privacy" that becomes "a shield to cover up domination, degradation and abuse of women and others" (DeCew, 2013). . Between these two extremes, instances such as gamergate and the more general persistence of male privilege in technology demonstrate that digital forms of privacy often serve only to amplify pre-existing societal issues. The issue of freedom for online privacy, as for society in general, is far from resolved, but it remains a defining feature of the culture of privacy and a core value for those who seek to promote both the technologies for and awareness of digital privacy throughout society.

PROPERTY

Where the freedom aspect of privacy has developed slowly over the long history of philosophy and indeed human society, the rapid rise of widespread privacy as an explicit concept, and the assumption of rights thereof, has been an effect of the invention and cultural development of literacy, capitalism, electrical media and then finally into the digital or information age. This link to techno-economic developments is derived from the term 'private property'. In this sense, privacy takes on the role of ownership. The exclusion of outsiders (thieves, etc.) from prime farmland or a factory in order to ensure the economic viability of the asset as a means of production finds its fulfilment via writing as the development of intellectual property through the printing press through to computational media. Control of one's informational assets has gradually overtaken the more concrete ownership of material capital to the point where immaterial or cultural capital has become a dominant force in contemporary economics and culture. Thus, finally, copyright and intellectual privacy have become the new form of private property (Bard and Söderqvist, 2012), no longer protected by moats, fences and physical force but by cryptography. While secret information has always held the potential for economic benefit - from blackmail to shorting the market or simply getting an edge over one's competitors - the contemporary economy involves personal, conventionally private information as a key business model. This engages with privacy not just of property but as property, and as inherently linked to exploitation. Just as the factory owner exploited their workers in the industrial revolution or stolen information has been used throughout the ages to blackmail those in positions of power, today private information is itself a means of production. What was once the purview of illegal business dealings or political corruption have now become the basis for multi-billion-dollar industries with companies such as Google or Facebook. It is their cultural impact in particular that has given these technology giants

their social power, to the point where the oppressed masses even consent to their own exploitation. The socio-cultural obligation to post to twitter or facebook, and the pressure from all sectors to conform to common digital tools that collect ever more data, has rendered the populous of the entire world a new self-sustaining means of production. The maxim "property is theft" (Proudhon, 2014 [1840]) takes on new meaning where it is control over one's own personal identity that is being taken, exploited and repackaged as a marketable commodity. The totalising (or even totalitarian) nature of this socio-economic shift is a fulfilment of cyberculture as a"romance of finance capital" (Jameson, 2005).

Indeed, the cultural paradigms of the internet have their origins bound with privacy not only as freedom but also as property - from Neuromancer onwards the cyberpunk battle against (states and) corporations has raged across the real world in line with its expression by William Gibson and Neal Stephenson through to Cory Doctorow and Ernest Cline, along with many other writers and thinkers. Perhaps paradoxically, in its valorisation of the "heroic pirates of cyberspace" (Jameson, 2005), this culture is often opposed to private property, particularly that held by corporations - hacker culture, cypherpunks, anti-DRM, through to outright piracy - while at the same time asserting the privacy of the individual. This is due to a binding together of freedom and property: for example, personal data is both the property of the individual and a mark of freedom. Thus, the underlying trends that instigated many facets of contemporary privacy culture are pro-freedom and anti-property. This displays an expression of anarchic, or at least libertarian undertones, with ideologies such as Proudhon's mutualism forming an unspoken founding principal. The resolution of the antagonism therefore attempts to emerge in this culture through an opposition to the exploitation inherent to property in the Marxist/Anarchist sense of the term as the means of production, rather than opposing the notion of individually owned items/information. It aims for structures that should be open in order for freedom, yet need measures in place to restrict exploitation. This is the technical dilemma of privacy as property. If privacy were only concerned with freedom, then it would be comparatively simple at the systemic or ideal level (although of course the notion of negative rights - freedom from external constraint - generates tension between opposing interests). It is when property is added that the situation becomes contradictory and a complex set of interactions must be enabled to allow for freedom without exploitation. For example, companies own any data that they legally and legitimately collect, just as individuals own their own memories. Short of anonymity to the point of solipsism - or the technocratic use of VPNs, onion routers and so forth - it is perhaps neither practical nor desirable to achieve an absolute level of privacy, insofar as it undermines the very connectedness that the internet enables and upon which it is founded. Radical accessibility of complete digital freedom leaves users open to direct exploitation by any and all attackers, reinforcing the inequalities embedded in cypherpunk culture whereby the privacy aware and technically competent can achieve their ideal of privacy at the expense, or regardless, of the average user.

The problem of freedom in the context of property and competing claims to ownership thus becomes an issue of 'security', expressing for the individual an attack akin to national security 'leaks'. New approaches are now being sought to designing privacy enhancing technology in the context of a radically different cultural context - promoting a system of social relations whereby privacy is considered a common good and its protection an essential collective endeavour (Kwecka et al., 2014). While such

models call for a breaking down of divisions towards a collective defense of anonymity - producing strength through a (distributed, obfuscated) unity - it must be wary of being reversed into a fear of unknown forces by those who are slower to adopt such technologies. Perhaps a less divisive term can in fact be found already in one that is often used specifically for issues of national defense and protecting corporate interests: the oft-maligned phrase 'cyber security'. The separated origins of this hybrid term suggest not only security within (or from! to a conventional state actor) cyberspace, but in cybernetics as the act of 'steersmanship'. Thus, cyber security becomes taking control of one's own security and one's own informational property, emphasising the need for everyone to be aware of their own privacy concerns and equip themselves accordingly. While this too risks fuelling an individualised society based on fear of Otherness, rather than collective technological development, it does offer a scalable conception of the need for privacy between the interests of states, companies and individuals. Privacy thus is security, even if it must be understood in terms of psychology (including paranoia and 'in-security'), ethics (the moral status of data) and intellectual property (ownership of the data that constitutes selfhood in a digital age). The balance between - and relative importance, emphasis or priority of - scales therefore becomes an ideological matter, reflecting broader cultures of technology and beyond. For example, a liberal cyber security would emphasise individuals followed by corporations, a socialist model would emphasise the state as protector of the individual, a capitalist cyber security would emphasise corporations and other 'property owners' (which could include the individual), nationalism would of course emphasise the state, and an anarchist conception would de-emphasise the state in favour of either the individual or society as a whole. The relative neutrality of the term cyber security in itself can therefore be reappropriated to emphasise any particular group, and indeed when privacy technologies themselves become property to be exploited this becomes a further aspect of the business model. While this term is scalable and adaptable over time to adjust to prevailing concerns, it is unsuitable as a universal framework, remaining caught between the needs of freedom and privacy.

The role of property in privacy adds economic complications to political and social concerns, intruding further on issues of freedom as state and corporate interests become increasingly entwined in the broader cultural logic of late or digital capitalism. The outsourcing of security and data collection by nation states to private firms (even here the term private property returns to signal the closing off of our own data from such protections as Freedom of Information that enforce a degree of accountability for many state actors) can be seen in such extreme circumstances as counter-terrorism surveillance (de Londras, 2014) to the extent that property wins out not only over freedom but even over un-freedom as corporate interests outway both individuals and states. This bypassing of the state in an increasingly globalised world drives property to control freedom, not only by corporations but also by other transnational organisations, even those originally aimed at tackling these issues. WikiLeaks, while beginning from a noble cause has seen increasing problems in its execution, to the point where it has elevated certain individuals (Julian Assange, for example, but also Chelsea Manning, Edward Snowden or the journalists to whom they disclose the 'private' information) to the status of 'global actor' on a level with states and corporations while entrenching the majority of people in their perpetual role as the fearful herd. WikiLeaks reinforces the flawed mentality often used by states when

developing stricter security and privacy legislation that having nothing to hide means you have nothing to fear. Anyone who stands out can be subjected to exposure, with an ideological inconsistency that is echoed in the work of Anonymous (or, at least, those claiming use of the label). The average citizen, who is not a security or even technology expert, sees only a series of attacks at the structure of society. A legitimate mission towards equality and freedom of information thus becomes another form of control through intimidation. Despite its best intentions and original vision, WikiLeaks is therefore, at base, simply a new mode of asserting power: a totalitarian technocracy ruled by fear replacing one damaged and corrupted system with another.

PRIVACY TODAY

In the context of WikiLeaks, increasing surveillance legislation, the possibility of state attacks on other countries' democratic processes, and the new crypto-wars, privacy maintains a continued surge as a topical issue. Indeed, Andy Grove, Chairman of Intel, stated in an interview that "privacy is one of the biggest problems in this new electronic age. At the heart of the Internet culture is a force that wants to find out everything about you" (Sager, 2007). And yet this anti-privacy momentum is the same force that drives increasing openness of information - such as WikiLeaks (on both sides of the coin), open access publishing, or increased VPN usage to enable file sharing (using anonymity for openness) - and indeed allows the internet itself to function. The digital society is based on the antagonism of privacy with openness as well as the tensions within privacy between freedom and property.

A politics of privacy

In an age described as 'post-truth', the value, veracity and manipulation of information has reached new depths of defining culture. Today, privacy culture is political culture as the digital world takes precedence over the physical and the conflicted inscriptions of privacy and its inverse in the technical architectures of the modern world are played out in all spheres of human activity. Returning to WikiLeaks, Julian Assange (2006) provided an ideological basis for an effective critique of privacy as power in the formulation of conspiracy as government , and the WikiLeaks project offered the tools by which the anonymous collective of the people (here the parallel to the increasingly politicised and decreasingly neutral hacker group Anonymous must be drawn) might assert control and hold those in power to account. However, as discussed, the execution has proven to be flawed and WikiLeaks is now merely another form of technocracy ruled by 'cypherpunks'. There has been a split between the medium and its original culture or purpose, a corruption of intent, for if all power corrupts then organisations such as WikiLeaks that exert a radically different form of power are still not immune to its seductive call for greater power and its use for ideological or personal gain. This failure can be pinned in part to the persistent assumption that tech is 'neutral' until it is used by humans. Indeed, commentators continue to worryingly assert that "WikiLeaks' initial self-presentation was as merely a conduit, simply neutral, like any technology...The problem is, WikiLeaks is not just a technology. It's humans too" (Fenster in Ellis, 2016). Against this prevailing naivety is the structure by which technology is always a mediator, always redefining the message it carries (McLuhan, 2001 [1964]). If by no other reason than the fact that technology is built both by and for humans, the apparent 'human factors' and non-neutrality will always-already exist with any technological system. Even the apparent neutrality of the

internet is a constructed quality, for openness and even free speech are still ideological points of view even if they are widely held and accepted. Indeed it was WikiLeaks' ideological commitment to a warped form of openness that contravened the privacy many of its creators and supporters would hail as an essential right in cyberspace. This same issue can be seen further in the racial bias that plagues facial recognition software based on the ethnicity of face samples given to the algorithms, or the machine learning techniques that amplify existing human prejudices in search engines. Technology is a defining characteristic of humanity, yet is also a product of it, and will always be tainted by pre-existing cultures and their antagonisms.

A digital generation

If the transition to a fully digitised society has transferred prior cultural problems, both of privacy and more generally, what then of the new generation of those raised more completely within the grasp of ubiquitous devices and radical data collection? The contemporary youth have been described as a "new privacy paradox" (Blank, Bolsover and Dubois, 2014) in their seemingly contradictory behaviours and attitudes, yet their responses to technology can perhaps be traced to the culture of privacy within which they have developed. There is a persistent public image of young people as flagrantly ignoring the perils of a lack of privacy. It often appears as though young people simply do not expect privacy in the information age, fatalistically accepting that they will be monitored at all times, and indeed there is some truth to that notion. This is demonstrated culturally by a shift from the relative privacy of blogs, by default viewed only by the technorati engaged in a privacy through lack of either interest or access to technology, towards the potential for limited privacy settings on facebook and then to the mass publishing of twitter and instagram. It can seem as though contemporary attitudes to privacy in an age of hopelessness concerning total government surveillance relies on being a needle in a stack of needles (anonymity through sheer quantity of data) or through the often false assumption of superior capability and/or interest (versus parents or schools). This technocratic, or netocratic (Bard and Söderqvist, 2012) assumption is false, for while the attentional economy might drive media sales there remains the possibility of technologically superior actors, such as organised criminals or nation states, coopting one's personal data for illicit and exploitative purposes. The apparent laissez-faire attitude of the youth backs up the prevailing concerns of older (possibly outdated and certainly fear-based) digital migrants supported by the appearance of younger people in casual surveys as less security or privacy aware.

However, counter behaviours are developing. For example, social media in teens can be as much about ignoring others as it is about collecting information on them, for when it is possible to stalk all of one's friends at any given moment a new social capital is given to those who appear aloof, rising above what has apparently become not a vicarious new experience but rather a mundane part of everyday existence (Choi, 2016). Similarly, there are new cultures of privacy that adeptly manipulate the various platforms available. For example, many young people use facebook only as their most outwardly facing, public persona, with the more private instagram reserved for friends and the even more private 'finstagram' (face instagram) reserved for close trusted friends with whom one might share photos of parties involving socially frowned upon or illegal behaviours (Safronova, 2015). There is here a fluid negotiation of public and

private identities that, while superficially appearing as a willing desire to show all to all at all times in fact belies a shrewd use of technology to achieve a variegated privacy structure and complex online identity. It could also be that in at a time when traditional authority figures such as presidential candidates are developing tactical approaches to 'post-truth media, the lack of concern for a more fundamental privacy is genuine. With increasingly ironic postmodern culture, teenagers may well be more worried about privacy in relation to their teachers and parents than they are in relation to Russia undermining a constitution they have never been convinced to believe in. New cultures of privacy are certainly developing, and it may be impossible for those not at its forefront to penetrate the layers of outwardly contradictory attitudes that make up this potentially increasingly self-aware collection of innate technology users. In a society that is completely mediatised, and in which the expected level of interactivity necessarily contradicts privacy for the computer to see what you are doing, it is not only other humans that are actors defining the culture of privacy.

Privacy from the machine

Felix Guattari (2013 [1989]) has hailed the age of planetary computerisation as the development of new machinic subjectivities. While his conception of abstract machines has developed over decades of philosophical enquiry in collaboration with Gilles Deleuze, outlining the role of machinic thinking within human subjects and society, it is increasingly a literal machine that is producing new forms of subjectivity. David Gunkel (2009) highlights that humans most commonly see digital media as a tool to communicate through, whereas the computer is also a tool to communicate with. Indeed, the majority of traffic on the internet, particularly in the context of Industrial Control Systems, the Internet of Things and Artificial Intelligence, is either human to machine or between two or more machines. It is thus not only new human cultures that are of concern to privacy but also machinic cultures as well as the impact on human culture of machines as actors. The fulfillment of the big Other of computer systems is now occurring as machine learning challenges all limits of privacy. Facebook, for example, are using machine learning to determine the contents of images, and combining their AI with satellite imagery to build the most accurate map to date of population density in rural and conventionally closed off (private) countries and areas. With AI cartography, even existence can never be private, no matter what physical separation one might seek. Humans will need to adapt to such further shifts and reorganise their privacy culture accordingly. Both Luciano Floridi's (1999) information ethics and David Gunkel's (2009) machine ethics are founded on the principle that ethical consideration should be afforded to any entity that exists as "a coherent body of information" (Gunkel, 2009). This acknowledgement of the socio-political power and necessary legal consideration of machines as both actors and an equal part of privacy culture will become increasingly important in the wake of neural networks that can teach themselves encryption that lies beyond human technical capabilities (Abadi and Anderson, 2016). Perhaps the future for privacy is indeed bright, but it may not belong to humanity.

CONCLUSION: THE FUTURE

This article has presented a new model for privacy as freedom and property that enables a broader, interdisciplinary theorisation of the concept. It thus overcomes many of the complexities of specific legal, technical or social taxonomies by

emphasising the role of privacy as a culture in and of itself. While the model is, as with all such socially orientated research, not free from its own ideological biases (such as: a tendency towards an anarchist critique of the state in relation of freedom; and a left-leaning or post-capitalist economic perspective in relation to property) the aim has been to utilise these perspectives as conceptual tools for their critique of the present situation of privacy without imposing an explicit agenda for the future. But a conceptual method is only as good as its ability to predict, or at least set out guidelines for, the future. What, then, of the future of privacy? The need to relive, relearn and readdress 90s PC privacy issues in the plethora of insecure IoT devices currently on the market suggests that the future perhaps holds an inevitable lack of privacy. Should we then simply adopt some form of denialist, nihilistic, or voyeuristic acceptance? Perhaps AI will overcome the current technological and epistemological limits of big data rendering privacy moot in the face of the machine, yet relevant in its exploitation by other humans? Perhaps a culture will develop whereby data itself is viewed as a 'victim' to be protected, giving new meaning to the term 'information security'? Or, as argued here, new cultures will form that adapt to the complexities of perpetually unresolved issues and competing concerns.

Post-digital subjectivity

Guattari (2013 [1989]) states that the act of enunciation is based on the perpetuation of the individual as a subjective position from which one speaks, and that "one cannot connect it and disconnect it as one would a computer". Indeed, one always retains the option to unplug or turn off the device. However, there are increasing socio-cultural and economic costs involved in such detachment, and as shown, there are methods being developed such as Facebook's population density map, or the new image recognition cameras and advertising screens in London's Piccadilly Circus that will track our activities regardless. We no longer have the option to unplug, surveillance is everywhere. We have finally reached a full state of constant digital subjectification, inherent to data collection and now enabled through cyber-physical systems, big data and machine learning. We are forced to continually speak to the big Other of computer networks. And yet, young people are showing the ability to effectively manage their disconnections, using a mix of digital and physical methods of communication to adapt to the specific contextual privacy needs, a less black-and-white and more subconscious negotiation of privacy throughout the various aspects of their lives (Livingstone and Sefton-Green, 2016). It is not that young people are unconcerned, but differently concerned, and are developing new modes of thinking and new cultures of privacy. If the rest of the world is to keep up, it must negotiate not only the traditional issues of privacy but develop new cultures across society that support positive attitudes towards both freedom and property that might allow us to negotiate an ever more digitised future. In an age of increasingly invasive government surveillance laws, cheap and rushed to market consumer devices, and corporate interest in big data, the need for privacy enhancing technologies and an effective privacy culture will only increase. But like the touchscreen and augmented reality interfaces that are permeating our mediated lives, new forms of privacy must function seamlessly and become functionally invisible. Like the inherent integration of the Signal protocol to messaging tools such as WhatsApp or the Signal app itself, privacy must become an expected necessity for any user, a standard marketing strategy for

any successful company, and an essential component of an ethical technoculture. Technology and culture must develop hand in hand not only to protect the value of privacy but to ensure that it adapts to the changing landscape of information as a driving force in human and computer society.

REFERENCES

Abadi, M. & Andersen, D. 2016. Learning to Protect Communications with Adversarial Neural Cryptography. Arxiv (Under review as a conference paper at ICLR 2017), 1-15. 21 October 2016. https://arxiv.org/abs/1610.06918

Assange, J. 2006. Conspiracy as Governance. Iq 3 December 2006. http://web.archive.org/web/20070129125831/http://iq.org:80/conspiracies.pdf

Bambauer, D. 2013. Privacy versus security. The Journal of Criminal Law & Criminology 103(3), 667-683.

Blank, G., Bolsover, G. & Dubois, E. 2014. A New Privacy Paradox: Young people and privacy on social network sites. Global Cyber Security Capacity Centre: Draft Working Paper, 1-33.

Bard, A. & Söderqvist, J. 2012. The Futurica Trilogy: The Netocrats. Stockholm: Stockholm Text.

Barlow, J.P. 1996. A Declaration of the Independence of Cyberspace. 9 February 1996. https://w2.eff.org/Censorship/Internet_censorship_bills/barlow_0296.declaration

Choi, M.H.K. 2016. Like. Flirt. Ghost: A Journey into the Social Media Lives of Teens. 25 August 2016. https://www.wired.com/2016/08/how-teens-use-social-media/

DeCew, J. 2013. Privacy. Stanford Encyclopedia of Philosophy. 9 August 2013. http://plato.stanford.edu/entries/privacy

de Londras, F. 2014. Privatized counter---terrorist surveillance. Constitutionalism undermined. In F. Davis, N. McGarrity and G. Williams, (eds.), Surveillance, Counter---Terrorism and Comparative Constitutionalism. Abingdon: Routledge, 59–72.

Doctorow, C. 2007. Scroogled. Craphound (Radar October 2007) http://craphound.com/scroogled.html

Doctorow, C.. 2016. The Privacy Wars Are About to Get a Whole Lot Worse. Locus Online 4 September 2016. http://www.locusmag.com/Perspectives/2016/09/cory-doctorowthe-privacy-wars-are-about-to-get-a-whole-lot-worse/

Fenster, M. in Ellis, E.G. 2016. WikiLeaks Has Officially Lost the Moral High Ground. Wired. 27 July 2016. https://www.wired.com/2016/07/wikileaks-officially-lost-moral-high-ground/?mbid=social_twitter

Floridi, L. 1999. Information ethics: On the philosophical foundation of computer ethics. Ethics and Information Technology 1(1), 37-56.

Foucault, M. 1991. Discipline and Punish. London: Penguin

Fuchs, C. 2011. Towards an Alternative Concept of Privacy. Journal of Information, Communication & Ethics in Society 9(4), 220-237.

Guattari, F. 2013 [1989]. Schizoanalytic Cartographies. London: Bloomsbury.

Gunkel, D. 2009. Beyond mediation: thinking the computer otherwise. Interactions: Studies in Communication and Culture 1(1), 53-70.

Gunkel, D. 2012. The Machine Question: Critical Perspectives on AI, RObots, and Ethics. Cambridge, MA: MIT Press.

Halbert, D. 2016. Intellectual property theft and national security: Agendas and assumptions. The Information Society: An International Journal 32(4), 256-268.

Jameson, F. 2005. Archaeologies of the Future: The Desire Called Utopia and Other Science Fictions. London: Verso.

Johns Hopkins University. 2014. The Johns Hopkins Foreign Affairs Symposium Presents: The Price of Privacy: Re-Evaluating the NSA. youtube 7 April 2014. https://www.youtube.com/watch?v=kV2HDM86XgI

Kwecka, Z., Buchanan, W., Schafer, B. and Rauhofer, J. 2014. "I am Spartacus": privacy enhancing technologies, collaborative obfuscation and privacy as a public good. Artificial Intelligence Law 22, 113-139.

Lacan, J. 1977. The Four Fundamental Concepts of Psycho-Analysis. London: Hogarth.

Li, Y., Kobsa, A., Knijnenburg, B. & Nguyen, M.C. 2017. Cross-Cultural Privacy Prediction. Proceedings on Privacy Enhancing Technologies 2, 93-112.

Liang, H., Shen, F., & Fu, K. 2016. Privacy protection and self-disclosure across societies: A study of global Twitter users. New Media & Society, 1-22.

Liu, J., Ryan, M.D. & Chen, L. 2014. Balancing Societal Security and Individual Privacy: Accountable Escrow System. IEEE 27th Computer Security Foundations Symposium, 427-440.

Livingstone, S. & Sefton-Green, J. 2016. The Class: Living and Learning in the Digital Age. New York: NYU Press.

MacKinnon, C. 1989. Toward a Feminist Theory of the State. Cambridge: Harvard University Press.

Mamonov, S. & Koufaris, M. 2016. The impact of exposure to news about electronic government surveillance on concerns about government intrusion, privacy self-efficacy, and privacy protective behavior. Journal of Information Privacy and Security 12(2), 56-67.

McLuhan, M. 2001 [1964]. Understanding Media. Abingdon: Routledge.

Millham, M.H., & Atkin, D. 2016. Managing the virtual boundaries: Online social networks, disclosure, and privacy behaviors. New Media & Society, 1-18.

Ojanen, T. 2016. Rights-Based Review of Electronic Surveillance after Digital Rights Ireland and Schrems in the European Union. In D. Cole, F. Fabbrini and S. Schulhofer (eds.). Surveillance, Privacy and Trans-Atlantic Relations. Oxford: Hart, 13-30.

Proudhon, P.J. 2007 [1851]. The General Idea of the Revolution in the Nineteenth Century. New York: Cosimo.

Proudhon, P.J. 2014 [1840]. What is Property? An Inquiry into the Principle of Right and of Government. Createspace.

Safronova, V. 2015. On Fake Instagram, a Chance to Be Real. New York Times. 18 November 2015. http://www.nytimes.com/2015/11/19/fashion/instagram-finstagram-fake-account.html?smid=pl-share&_r=0

Sager, M. 2007. Andy Grove: What I've Learned. Esquire. 29 January 2007. http://www.esquire.com/entertainment/interviews/a1449/learned-andy-grove-0500/

Schneier, B. 2003. Beyond Fear: Thinking Sensibly About Security in an Uncertain World. New York: Copernicus.

Schneier, B. 2012. Liars and Outliers: Enabling the Trust that Society Needs to Thrive. Oxford: John Wiley & Sons.

Schneier, B. 2015. Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World. New York: W.W. Norton.

Schneier, B. 2016. By November, Russian hackers could target voting machines. Washington Post 27 July 2016. https://www.washingtonpost.com/posteverything/wp/2016/07/27/by-november-russian-hackers-could-target-voting-machines/?utm_term=.471a6a2c3dc1

Scholz, L.H.. 2016. Privacy as Quasi-Property. Iowa Law Review 101, 1113-1141.

Solove, D. 2006. A Taxonomy of Privacy. University of Pennsylvania Law Review 154(3), 477-564,

Solove, D. 2008. Understanding Privacy. Cambridge, MA: Harvard University Press.

Tapscott, D. & Tapscott, A. 2016. The Impact of the Blockchain Goes Beyond Financial Services. Harvard Business Review 10 May 2016. https://hbr.org/2016/05/the-impact-of-the-blockchain-goes-beyond-financial-services

van Schoonhoven, B., Roosendaal, A. & Huijboom, N. 2013. Privacy Versus Collective Security - Drivers and Barriers Behind a Trade-off. IFIP Advances in Information and Communication Technology 421 Privacy and Identity Management, 93-101.

Warren, S. & Brandeis, L. 1890. The Right to Privacy. Harvard Law Review IV(5).

Weber, M. 2004 [1919]. The Vocation Lectures: Politics as a Vocation. Indianapolis: Hackett.