McMenemy, David (2016) Digital Ethics : A UKeiG White Paper. Other. UKeiG, London. ,

DIGITAL ETHICS

A UKeiG WHITE PAPER

UK eInformation Group

DIGITAL ETHICS

A UKeiG WHITE PAPER

DAVID McMENEMY, UNIVERSITY OF STRATHCLYDE

Published by UKeiG, the UK eInformation Group of CILIP, the Chartered Institute of Library and Information Professionals

www.ukeig.org.uk

Published in November 2016

Series: UKeiG White Paper: 2016/02

ISBN: 978-1-870254-17-5

Abstract

This white paper discusses the topic of digital ethics and considers the topic within the background of theories on ethics and how they apply within the digital realm. It explores the issues of internet governance, net neutrality, freedom of expression, and privacy and considers how they impact on the work of the information profession and wider society.

Issues around internet governance challenge us from the point of view of net neutrality and the tensions between the original ethos of the Internet pioneers and the enhanced role of governemnts and corporations in Interent governance. The concept of “code” as law, introduced by Lawrence Lessig, is explored in terms of how it challenges ethical behaviour.

Freedom of expression is a constant challenge as we are presented with calls to limit acess to certain information types, and are increasingly charged with considering filtering systems to do so. The increasing emergence of online trolls also challenges freedom of expression rights.

Privacy is under challenge via both government and corporate interests in our activities and our data.

Overall the need to be aware of fundamental rights versus how those rights may impact on wider society is the primary concern around digital ethics.

Table of Contents

1. Introduction

The concept of ethics relates to how groups of people in society specify and regulate their behaviour. Thus ethics applies to the behavioural norms of entire societies but also to sub-groups within society, such as citizens, professions, corporations, governments, religious groups and the like. In this white paper, we discuss digital ethics, which applies considerations of ethical behaviour to the realm of information and communications technologies (ICTs).

1.1. What is digital ethics?

Digital ethics relates to how human behaviour is managed and specified as it applies to activities in the digital realm, including online and through our use of software and other technologies. It is an area of ethical study that is growing in societal importance by the day, as new technologies emerge that introduce new challenges to society. A previous UKeiG white paper explored the topic of the *Internet of Things* which is a recent phenomenon but one that raises ethical issues around how we implement these valuable new technologies and the data they produce. As the paper made clear, the "extent to which this is for the common good will depend on who controls this data, how it is used and what safeguards are put in place to protect privacy.[1] This is a classic question of digital ethics and can be applied across the wide range of technologies we use on a daily basis.

A fundamental paradox of new applications of ICTs is that they aim to make life for human beings easier, but at the same time can complicate our lives in ways that are detrimental to us. As Spinello argues with regards to the Internet:

> If it easier to publish and spread truthful and valuable information, it is also easier to spread libel, false-hoods, and pornographic material… And if it is easier to build personal relationships with consumers, it is also easier to monitor consumers' behaviour and invade their personal privacy.[2]

Our discussion in this paper will discuss the ethical issues highlighted by Spinello and more. We will discuss topics such as privacy, freedom of expression and censorship, Internet governance, and how all are being impacted within the digital realm.

1.2. Why does digital ethics matter?

An understanding of digital ethics is a vital area of knowledge for the information professional. As we are bombarded with solutions that appear to solve problems or challenges in our service delivery, we must be aware of the impact those technologies may have on our clients and wider society, but also on our own practice. There are fundamental values that information professionals stand to protect, and the reality is that some digital solutions to service delivery may challenge those values. An awareness of the challenges they pose, then, is of crucial importance in our professional practice. As professionals, we have societal responsibilities that go beyond our responsibility to employer or client, and we must bear this in mind when implementing any new technologies that may potentially harm others.

2. Ethical theories

Since many of the issues we will discuss highlight a dichotomy between opposing ethical viewpoints, it is important to begin with a short summary of those ethical viewpoints and what they say about

[1] De Saulles, Martin. *The Internet of Things: A UKeiG White Paper*. 2016. p.16. http://www.cilip.org.uk/sites/default/files/documents/internet_of_things_white_paper_final.pdf

[2] Spinello, R.A., *Cyberethics: Morality and Law in Cyberspace*. 6th ed. 2017: Jones & Bartlett Learning. p.ix

human behaviour. Readers wishing a more detailed overview are strongly encouraged to read the excellent summary of how ethical theories apply to society provided by Michael Sandel.[3]

When we discuss ethics we often focus on a specific branch, as we are doing in this white paper by discussing digital ethics. We often see discussions of professional ethics, business ethics, or medical ethics, for example. In reality, all micro discussions around branches of *applied* ethics, as all of the above themes would be classified, stem from the same overarching theories.

2.1. The main branches of ethical theory

There are essentially three main branches of ethical theory, complicated by the fact there are several subsets within each. However, an understanding of what the three main branches believe provides a good grounding for our discussion of digital ethics. The three main branches are consequentialist ethics, deontological ethics, and virtue ethics.

2.1.1. Consequentialism

Consequentialism relates to the potential outcomes of an action and the ethical results of that action. What is important for the consequentialist is that the outcome is satisfactory, not necessarily how that outcome has been achieved. The main consequentialist ethical theory is utilitarianism.

The father of modern utilitarianism was Jeremy Bentham whose theories were developed further by John Stuart Mill. The basic formula for utilitarianism is the greatest happiness for the greatest number. Utilitarianism had a significant effect on political philosophy through the Victorian era and well into the late 20th century before it was arguably supplanted by philosophies more focussed around individual freedoms. The emergence of major public services, welfare systems, and institutions like public libraries and museums can be attributed to the emerging utilitarian thinkers of the Victorian era.

As we have stated, utilitarianism relates to the happiness and well-being of the majority – therefore in a utilitarian world, it is acceptable for some in society to lose out if the happiness of the majority is the consequence. This is an important concept since taken to its extreme it could advocate harm being allowed to a small number of people to benefit the majority. Clearly, this raises significant issues of natural justice that have to be addressed by any ethical thinker. In addition, since utilitarianism is focussed on the consequences of an action, the ethics of the motive itself can be questioned.

In terms of digital ethics, we can see utilitarian arguments across many of the areas it is concerned with. For instance, is the monitoring of the online activity of people justifiable if a criminal or terrorist is caught and thus harm does not come to others as a result? A utilitarian might argue that the happiness of the majority is the benefit of online surveillance, as the majority is kept safe at the expense of a small number wishing to do us harm. On the other hand, a utilitarian argument could be made *against* online surveillance, since one could argue that the knowledge we are being surveilled makes the majority unhappy. We will explore some of these ideas further later in the paper.

2.1.2. Deontological ethics

Deontological ethics relate to the concept that there are certain values or actions that are inherently good or bad. Deontological or duty-based, ethics are primarily based on the theories of Immanuel Kant, a German 18th-century philosopher. Kant was not convinced by the concept of utilitarianism,

[3] Sandel, Michael. *Justice: What's the Right Thing to Do?* Penguin. 2009.

believing that it ignored a fundamental point in ethics that some actions were by their very nature good or bad and that this, not the consequences of the actions, were what is important.

Kant's *categorical imperative* is arguably the most important of his theories related to ethics. In his *Groundwork of the Metaphysics of Morals*, published in 1785, he stated two important maxims that underpin his theories. The first of these maxims states that "I ought never to act except in such a way that I could also will that my maxim should become a universal law". Within this oft-quoted line lies the basis of an ethical theory that has been interpreted and re-interpreted to this day. The basis of the imperative is that any action should be morally justifiable by virtue of it being measured against it being a potential universal law of nature. From a normative standpoint, it essentially means that actions that are unjustifiable to a reasonable person are morally unjustifiable. For instance, we would not wish theft or murder to become universal laws of nature, therefore under Kant's imperative, these actions are never justifiable. Conversely for the consequentialist they *can* be if the outcome aids utility.

Kant's final maxim relates to the morality of how we use other human beings. He states "Act in such a way that you treat humanity, whether in your own person or in the person of any other, never merely as a means to an end, but always at the same time as an end". Using a human being as a means relates to using them to further your own interests, and not thinking of their interests. Treating them as an end, on the other hand, means considering their interests in any dealings you may have with them. This essentially means respecting their freedoms to make decisions and to act in their own interests. This part of the categorical imperative is the basis of many of the rights-based philosophies that currently exist.

Deontological ethics apply in the digital realm also. For instance, a deontologist would likely consider the rights of individuals to be more important than the societal impact of an activity. This right to privacy and freedom of expression may be something that a deontologist would guard with care. The issue for a deontologist becomes whose rights should take priority in certain situations.

2.1.2. Virtue ethics

Virtue ethics has its origins in the classical philosophy of Aristotle. A major consideration in classical mythology was what the virtuous life would actually be, and this informed the concept of living the *good life* and being a good person. At the heart of the concept was *eudaimonia* or happiness. The concept of virtue is that it is a mean between excess, on one hand, and deficiency on the other. Importantly, however, it is not about moral absolutes such as anger or pleasure being always automatically right or wrong.

Virtue ethics is arguably of less practical application than either deontological or consequentialist ethics. Since its focus is on the subjective human condition, it is more difficult to apply its theories to discussions of digital ethics. However, as we are seeing increasing calls to the importance of good character in human agents, it seems that virtue ethics are making something of a comeback and are worth being aware of from that standpoint.

3. Internet governance

A vital aspect of digital ethics relates to how the Internet itself is governed. The success of the Internet has been unprecedented in human history. In December 1995 the Internet had 16 million users, and by 2016 the estimate for users was 3.4 billion across the globe. Yet arguably with its explosion in usage and impact the original goals of the medium have been under pressure.

3.1. The Internet manifesto

In 1996 the manifesto that overarched the early days of the Internet was published by John Perry Barlow. You can read the full text via the link below, but some snippets reveal how the early Internet pioneers saw the medium:

> "Governments of the Industrial World, you weary giants of flesh and steel, I come from Cyberspace, the new home of Mind. On behalf of the future, I ask you of the past to leave us alone. You are not welcome among us. You have no sovereignty where we gather." [4]

Importantly the manifesto sought to demarcate the Internet as a new medium that would not be subject to the same mores as the traditional world. As Barlow continues, "You do not know our culture, our ethics, or the unwritten codes that already provide our society more order than could be obtained by any of your impositions." Crucially Barlow is arguing that the Internet is creating a new ethical domain. In terms of digital ethics, the Internet manifesto is of vital importance in understanding the original mission of the medium.

Whether such grand notions for the medium were ever truly real, there was certainly a feeling among early adopters and those who shaped the Internet that this was an entirely new paradigm shift in humanity, and one that would be free of governmental and commercial influences. As Lessig states, "The claim for cyberspace was not just that government would not regulate cyberspace—it was that government could not regulate cyberspace." [5]

3.1.1. The Internet infrastructure

The Internet is governed in a multi-structured way, with several organisations responsible for separate aspects of its operations. These groups include the Internet Engineering Task Force (IETF) and the Internet Architecture Board (IAB), as well as the Internet Society (ISOC). The mission and mandate of the Internet Society are focused on the education, empowerment and awareness of governments, businesses and the users around the world. The ecosystem of the Internet provides a unique governance structure of a type that was originally designed to make the medium as participative and open as is possible.

Timothy Garton Ash highlights that what was essentially the pragmatism of building a network that could still ensure communication after a nuclear war, was also partly inspired by grander notions of openness and cooperation:

> For some of those involved, one reason for developing a 'distributed network', in which packets could reach their destinations via multiple alternative routes, was to increase the chances of information still getting through after a first nuclear strike. But their American libertarian convictions also fed into this notion of free passage irrespective of content: you pass my packets, I'll pass yours. Later, this would be elaborated into the broader principle of 'net neutrality', rejecting any discrimination on grounds of the content of the packet, the identity of its sender or the application used. [6]

We will discuss net neutrality further below.

[4] Barlow, J.P. *A Declaration of the Independence of Cyberspace.* 1996. https://www.eff.org/cyberspace-independence

[5] Lessig, L. *Code version 2.0*. Basic Books. p.3. http://codev2.cc/download+remix/Lessig-Codev2.pdf

[6] Ash, Timothy Garton. *Free Speech: Ten Principles for a Connected World.* Atlantic Books. Kindle Edition. (Kindle Location 465).

3.2. Governance concerns

Cerf et al have observed that despite the desire of many that the Internet remains an open and universal experience "over the last several years more and more governments and companies have been taking action to control the flow of information over the Internet" [7] This focus on the influence of governments and companies forms a significant tranche of the concerns over what has been called, *Internet fragmentation*.

In his testimony on the future of the web to the US House of Representatives, Tim Berners-Lee identified three Internet concepts that he argued were crucial to the foundation of the web:

1. Universal linking
2. An open foundation for information-driven innovation
3. Separation of layers [8]

Hill mirrors this analysis more broadly and argues that:

> early Internet engineers incorporated into the Internet's architecture their belief that connecting people together and enabling them openly to share ideas was an objective that should be encouraged; consistent with that objective, the early designers insisted that governments should have a very limited role in regulating the Internet. [9]

These ideas are potentially under challenge as the Internet evolves, with arguments that both the openness and the freedom from government intervention of the ideal Internet experience are under threat. Although Berners-Lee was talking specifically about the world wide web, as one would expect given his role in its evolution, he is clear that the values that underpin the Internet made the web a reality.

3.2.1. Net neutrality

Net neutrality is an important concept in terms of digital ethics. The idea underpins much of what the Internet has become in terms of being a domain that contains a wide range of traffic that is efficiently distributed without fear or favour. Spinello defines net neutrality as such:

> All ISPs and telecom companies are required to treat every form of data equally, in a way that is consistent with the end-to-end design principle. They cannot discriminate between different packets of data. This means they cannot enhance the performance of some streams of data to create a "fast lane" for that data, nor can they employ "tolls" or any means that slows down the transmission of Internet packets.[10]

Net neutrality is of vital importance in terms of keeping the Internet running smoothly. As French notes, while the Internet has evolved into bandwidth-hungry services that rely on quick and efficient packet switching to ensure the service is provided (i.e. online gambling, Skyping, video streaming), the Internet was not originally designed for this, nor was net neutrality as a concept built around the reality of an Internet that offered such services. Therefore the infrastructure has had to deal with

[7] Cerf, V., P. Ryan, and M. Senges, "Internet Governance Is Our Shared Responsibility". *I/S: A Journal of Law and Policy for the Information Society*, 2014. 10: p.1.

[8] Berners-Lee, T. *The Future of the Web.* Testimony of Sir Timothy Berners-Lee Before the United States House of Representatives Committee on Energy and Commerce Subcommittee on Telecommunications and the Internet. http://dig.csail.mit.edu/2007/03/01-ushouse-future-of-the-web.html

[9] Hill, J.F., *Internet Fragmentation: Highlighting the Major Technical, Governance and Diplomatic Challenges for U.S. Policy Makers*. 2012: Belfer Center, Harvard Kennedy School. p.15.

[10] Spinello, R.A., *Cyberethics: Morality and Law in Cyberspace*. 6th ed. 2017: Jones & Bartlett Learning. p.38.

highly increased capacity and had to undergo essential and expensive improvements in bandwidth capability. [11]

Linked to this is the emergence of telecommunication companies as content providers, something that was not the case when the Internet was designed. Companies whose previous roles were limited to the telecommunications infrastructure and ensuring Internet traffic passed unhindered began to merge with other companies involved in content creation, and thus began to have interests in ensuring their content, or their customers, were privileged. One solution is to more heavily regulate how ISPs offer their services, ensuring they commit to providing a steady service for all. The concerns expressed by those who advocate tighter regulation are highlighted by McCartney, namely the fears that "dominant broadband providers, such as AT&T and Comcast, will use their market power in consumer markets unfairly, favouring Internet content in which they have a financial interest." [12]

French argues that essentially three concepts underpin the net neutrality debate, namely freedom of expression, consumer protection, and innovation and economic growth. [13] Freedom of expression is limited if ISPs are able to throttle content from a service they do not favour. While the intention may not be to censor, the favouring is strictly business, the end result is that legitimate content is not seen by Internet users. A recent example of this was highlighted on BBC News where T-Mobile was argued to be favouring its own video streaming service, *Binge On*, across its US network while throttling content from providers such as YouTube. [14] The *Binge On* service provided content from T Mobile's partner Netflix at the expense of other providers.

The second of French's concepts, consumer protection, is also of vital importance. When a consumer signs up for an ISP account, they are reliant on the service that the ISP provides. They have little way of knowing unless they are informed netizens aware of issues such as net neutrality, whether the reason they cannot access a service is because the service provider is poor, or the ISP is merely throttling bandwidth. Given it is unlikely that a consumer would be able to cite throttling as a reason for getting out of an ISP contract, we have an added element of concern re consumer protection.

Lastly, innovation and economic growth are stifled if ISPs are allowed to favour content from one provider over another. The investment a company may put into providing an excellent service may well be wasted if consumers cannot access it efficiently. If the reason they cannot do so is, again, throttling of content, then a company is having its commercial interests restricted by another with vested interests. This not only goes against the values of the Internet, it is also arguably anti-business generally, and risks stifling innovation and creating monopolies. We can see then that net neutrality does indeed raise important ethical issues with regards Internet fragmentation that we must be aware of.

3.3. Code is law

An important concept around Internet governance and digital ethics is the idea proposed by Lawrence Lessig that *code is law*. A unique aspect of the Internet medium was that it was a system designed around computer code and systems architecture. This meant that those very things could be used to govern interactions with the system. Every act performed on the Internet involves the use of code and a systems architecture to achieve the desired result, and that meant those

[11] French, R.D., "Net Neutrality 101". *University of Ottawa Law & Technology Journal*, 2007. 4(1 & 2). p.115

[12] McCartney, D., "Law and the Open Internet". *Federal Communications Law Journal*, 2011-2012. 64(3). p.494

[13] French. *Op. cit*. p.116

[14] See "T-Mobile 'breaks' net neutrality rules with binge on". http://www.bbc.co.uk/news/technology-35232288

technologies could be used to control the experience. This clearly gives those writing the code and designing and managing the infrastructure, immense power to shape the Internet experience. Lessig argues that:

> “the invisible hand of cyberspace is building an architecture that is quite the opposite of its architecture at its birth. This invisible hand, pushed by government and by commerce, is constructing an architecture that will perfect control and make highly efficient regulation possible. The struggle in that world will not be governments. It will be to assure that essential liberty are preserved in this environment of perfect control. [15]

In terms of code being law, Lessig clarifies his argument and the importance of that idea: “In cyberspace we must understand how a different “code” regulates— how the software and hardware (i.e., the “code” of cyberspace) that make cyberspace what it is, also regulate cyberspace as it is.”[16] The ethical implications of this are clear, and as DeNardis observes, “Technologies of Internet governance increasingly mediate civil liberties such as freedom of expression and individual privacy.”[17] The implications of this will be discussed below when we consider both topics in more detail.

Lessig’s full thesis actually highlighted what he defined as the four modalities of regulation:

1. Law: these are the laws created by governments and other regulatory bodies that govern conduct on the Internet. This mirrors the real world where law governs all.
2. Norms: this relates to the behaviours and the etiquette of the Internet. Norms regulate behaviour because communities in the digital realm specify behaviours they will tolerate and those they will not.
3. Markets: companies provide services that Internet users consume, and the provision of the service also acts as a form of regulation.
4. Code: as we have seen Lessing believes it is the code written by those who build the architecture and services we access on the Internet who are the ultimate regulators. In code being law, all transactions and experiences are subject to regulation by the inbuilt system delivering them. Passwords for website access, filtering systems for limiting certain types of information, and the like.

We will see Lessig’s theory coming up again in several further areas of our discussions below.

4. Freedom of expression and censoring content

Providing access to a wide range of information sources is a *sine qua non* of the information profession. This entails a commitment to and understanding of the debates around freedom of expression. Article 19 of the *Universal Declaration of Human Rights* states that:

> Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers.

The idea is also included in Article 10 of the *Human Rights Act* in the UK. Therefore the notion that access to information should be restricted, clashes with a fundamental core belief in the modern age, and is something that challenges the ethical parameters of information work. Yet there are

[15] Ibid p.4.

[16] Ibid p.5.

[17] DeNardis, Laura. *The Global War for Internet Governance.* 2014. Yale University Press. p.1.

legitimate grounds for restricting access to some kinds of information: "some forms of expression, like pornography, venomous hate speech, or terrorist threats, are offensive." [18]

In the arena of digital ethics Lessig's argument that code can be used to restrict access is again valid here, since, with a system built on code, information can be easily blocked or restricted based on parameters set within the code. This ability is also evident from the point of view of countries being able to apply their own content controls over Internet traffic, which is something that fundamentally goes against the thesis of the Internet pioneers who sought a global medium where governments could not interfere.

As we will find, we can also see this in Internet filtering systems on a daily basis, for instance within public services offering Internet access such as public libraries and schools, where Internet filters on local servers are often utilised to restrict access to information deemed to be inappropriate. As Spinello has argued, "the issue of free speech and content controls in cyberspace has emerged as arguably the most contentious moral problem of the nascent Information age." [19] An overview of the arguments around freedom of expression should provide some context.

4.1. Arguments for and against freedom of expression

The notion of freedom of expression encompasses several important ideas: forming opinions, expressing opinions, and being able to access the information that helps make you informed are inherently related concepts. Immediately then we can also see a direct link to the notion of privacy; privacy allows the freedom for an individual to access information out of the gaze of others and form opinions.

The arguments that are posited for defending and protecting free speech are usually presented as a counter to those who may wish to restrict it for various reasons. The philosophy of free speech could be an entire volume in itself, therefore to neatly summarise the arguments we will focus on and discuss the categorisation put forward in the authoritative summary of the topic in Barendt's peerless text on the subject. Barendt defines some core defences that are often used to justify the protection of free speech, and these can be summarised as:

- Argument from truth
- Argument from autonomy
- Argument from democracy [20]

The *argument from truth* is largely associated with the approach to issues of individual freedom posited by John Stuart Mill in *On Liberty*, although as Barendt observes we can trace similar sentiments in the defences provided much earlier by Milton in *Areopagitica*, and latterly by Judge Oliver Wendell Holmes in the famous *Abrams vs. US 250 US 616* case. Another over-arching term applied to the concept of the argument from truth is that of a *marketplace of ideas*, referencing the notion that people should be presented with the broadest possible range of ideas to select their truth, or in other words: "we cannot deny currency to any expression of opinion without reducing the efficiency of the knowledge market." [21]

As Campbell has also suggested, the argument from truth could be classified as a justification for freedom of speech that is based on a consequentialist rather than a rights-based point of view. In other words, truth matters to society because it ultimately benefits the majority of people by

[18] Spinello. *Op. cit*. p.67

[19] Ibid p.67

[20] Barendt, E. *Freedom of Speech*. 2nd Edition. 2006. Oxford: Oxford University Press.

[21] Campbell, T. *Rights: A Critical Introduction*. 2006. London And New York: Routledge. p.143.

building a better society, rather than truth being fundamentally about any one individual's rights. However, we could contend as Barendt does that truth could also be seen to be "an autonomous and fundamental good" in and of itself. [22] For Mill truth was "justified belief" and this justification was only valid when an idea or viewpoint has been thoroughly tested and critiqued within society through argument and debate. As Campbell summarises with regards to Mill's view, to suppress freedom of expression on a topic "is to make the epistemological mistake of assuming that you know in advance of hearing an opinion that it is false".[23] Therefore, the argument goes that we should not exclude any perspectives because we cannot be certain whether a viewpoint that is being expressed bears some truth to it that can challenge an orthodoxy and make proponents for it justify the truth of that view in the public sphere. By this token, we should also *not* suppress false views we know to be false, as the expression of a falsehood may also have value since it entails the speaker of a truth justifying their truth in the face of said falsehood. As Mill states, no one has "authority to decide the question for all mankind, and exclude every other person from the means of judging." [24]

The *argument from autonomy* is based on the concept that freedom of expression is a fundamental right for individuals if they are to achieve their potential as rational persons. It is one of the most overt justifications of free speech from a liberal standpoint since it is entirely focussed on the rights of individuals rather than any societal benefits that may accrue: it "is an intrinsic, not an instrumental right…It values speech for its own sake, not for the indirect results that flow from it." [25] By the same token, however, it could be seen to be antithetical to consequentialist arguments for free speech, since no consideration is given to the impact of free speech on wider society under this justification.

As Barendt suggests, "restrictions on what we are allowed to say and write, or…to hear and read, inhibit our personality and its growth." [26] Under this justification, we can also see links between it and some other fundamental human rights such as the "rights to freedom of religion, thought and conscience". [27] As he also notes, however, the argument from autonomy also veers into territory that can see a clash between one person's right to express their freedom of speech, versus another's right not to be insulted or defamed. The contemporary problem of online trolling and harassment is an example of the challenges inherent in the argument from autonomy, as we will see below.

Campbell offers that the argument from autonomy is "powerful in its scope, for it can take in all forms and types of speech, and it is powerful in its foundations, for it finds its justification in the flourishing of distinctively human capacities." [28]

The *argument from democracy* relates to the notion that "freedom of speech is a necessary ingredient of the accountability on which the benefits of democracy are posited." [29] This defence focuses on the importance of a free flow of information and viewpoints within a democracy, allowing citizens to be informed and able to hold their elected representatives and the institutions that they manage on our behalf to account. This defence also not only bestows rights to free speech on citizens, it also often focuses on the importance of rights to freedom of information from the point of view of government documents, and many countries have legislated for such rights. In

[22] Barendt. Op. cit. p.7
[23] Campbell. Op. cit. p.143
[24] Mill, J.S. *On Liberty*. London: Walter Scott Publishing Ltd. 1869. pp.11-12.
[25] Campbell. Op. cit. p.147.
[26] Barendt. *Op. cit.* p.13.
[27] Ibid. p.7.
[28] Campbell. *Op. cit* p.147.
[29] Ibid. p.145.

other words, a citizen would have the right to exercise their freedom of speech in asking from the government and getting the information they wish to see to hold them to account.

There are again some key criticisms that can be levelled at this defence: if the focus is primarily on democracy and the institutions and people who are a part of it, free speech could be argued to be defined in a very narrow sense. Unlike other defences which focus on the totality of human experience, the argument from democracy would be in danger of focussing only on speech that supported political decision-making at the expense of artistic, or spiritual expression. As a consequentialist defence of the right, a plausible scenario could be posited that any speech act that harmed democracy could be made illegal. Therefore, it could be deemed wrong "to tolerate the circulation of material advocating its overthrow." [30] Schauer goes further in his analysis: "the very notion of popular sovereignty supporting the argument from democracy argues against any limitation on that sovereignty, and thereby argues against recognition of an independent principle of freedom of speech." [31] As Campbell summarises, the argument from democracy "provides some powerful rationales for increased and different types of freedom of speech, but only within the domain of political assessment and debate." [32]

4.1.1. Free speech restrictions

Challenges to free speech can be identified in several areas. Firstly, we can identify concerns that relate to the dignity of groups, on one hand, whereby hate speech attacks their sense of worth and identity and even possibly places them in physical harm. A second area of concern exists from the point of view of group rights and free speech, largely distilled from a critical feminist perspective, and related to the notion that some voices represent viewpoints that are already over-represented in the public sphere, and therefore more space should be made for voices deemed to be marginal. In this context there is the belief that the privilege of some groups means there is often a case for restricting their access to the public sphere, and therefore by implication their right to speak. In some modern contexts, especially academic settings in both the United States and the United Kingdom under the epithets of *no-platforming*, and *safe spaces*, we see a combination of these two stances combining for effect, and controversy.

At the heart of the debate around hate speech lies the thorny issue of actual harm that can come about as a result of speech acts. For Mill, there was a distinct difference between speech that targeted a group in a general sense, and speech designed to stir up physical harm to someone. In an oft-quoted passage from *On Liberty* he states:

> An opinion that corn-dealers are starvers of the poor, or that private property is robbery, ought to be unmolested when simply circulated through the press, but may justly incur punishment when delivered orally to an excited mob assembled before the house of a corn-dealer, or when handed about among the same mob in the form of a placard. [33]

In the argument from truth, then, there is space for severe speech that challenges individuals, but only when that speech leads to actual harm should it be punished or restricted. This notion forms part of Mill's widely-cited harm principle.

To this end, Post delineates how legislative frameworks have interpreted hate speech from the point of view of passing laws against it. He highlights the fact that in a modern democracy, mere disagreement with an opinion is not enough to constitute a hate crime: thus objecting to a religious

[30] Barendt. Op. cit. p.19.

[31] Schauer, F. (1982) *Free Speech: A Philosophical Enquiry*. Cambridge: Cambridge University Press. p.41.

[32] Campbell. Op. cit. p.145.

[33] Mill. *Op. cit*. p.39.

doctrine and stating that opinion should not be enough to constitute hate speech. He identifies that hate crime normally will only be defined when a speech act expressing abhorrence or dislike is combined with another element "that is thought to identify the unique presence of extreme hate and hence to justify legal intervention." [34] These elements are usually:

1. The manner of the speech act
2. The likelihood of it causing contingent harm, violence or discrimination

In the first category Post explains that the manner of the speech act relates essentially to the style of it; in that vein, it considers speech acts that are "formulated in such a way that insults, offends, or degrades". [35] He acknowledges the difficulty, however, of ascertaining this, and suggests that "ambient societal norms" need to influence the categorisation.

4.2. Free expression and the digital realm

While the technologies used to facilitate free expression may change with each generation, the concerns of unfettered free expression and its impact on society remain the same as those summarised above. What limits should be placed on free expression, and what justifications can be made, if any, have become a major controversy in the digital realm. Two important issues are of immediate concern: filtering of Internet content, and offensive behaviour online.

4.2.1. Filtering of content and managing access to the Internet

Internet filtering is a software-driven process of excluding websites from being able to be accessed is used by many organisations to prevent users from accessing specific categories of website. The process is normally driven by the blocking of words or phrases within the text of a webpage, or via a web address which is on a list of banned sites, or a combination of both. More specifically the two main types of filter have been defined as stand-alone systems or protocol-based systems:

- In a stand-alone system, the filtering software vendors pre-designate which content will be filtered, and the user does not have control.
- Protocol-based systems, on the other hand, do not determine in advance which content will be blocked. Rather, protocol-based systems can locate information on the Internet and, based on established standards interpret the information to determine whether a particular page should be blocked. [36]

While the organisation installing filtering will have some control over the blocking parameters through the initial specification supplied to the vendor, and the administrative settings provided, it remains a fact that the initial design of what the filtering system will block is largely specified by the software creators.

It is certainly true that, as Hauptman puts it, "unfiltered access to the Internet presents some major ethical challenges even to those whose commitment to intellectual freedom is unequivocal," however it is equally true that, "it is not our business to mediate between users and the virtual world." [37] Yet undoubtedly there are occasions when this must be considered.

In terms of digital services, filtering of internet content in publically-funded libraries is ubiquitous in the United Kingdom. The MAIPLE project found that 100% of the respondents to their survey (80

[34] Post, R. (2009) "Hate Speech" In. Hare, I. And Weinstein, J. (Eds) (2009) *Extreme Speech and Democracy*. Oxford: Oxford University Press. p.127.

[35] Ibid. p.127

[36] Sobel, D.L. (2003). Internet filters and public libraries. *First Repor*ts. 4 (2). p.5.

[37] Hauptman, R. *Ethics and Librarianship.* 2002. Jefferson, NC and London: McFarland and Co. p.65.

library authorities) filtered internet content, [38] while a study conducted by Scottish public library services found that 31 of the 32 authorities filtered content. [39] Such filtering has ethical parameters, and there is no public audit of the content that is filtered. Since the process is software-driven, legitimate content can be blocked, and while both of the studies cited above found that some library authorities provided the ability to unblock legitimate sites that are blocked, there remains an issue of equity of access. In the MAIPLE study, it was found that 75% of respondents working for public library services found filtering to be either very useful or somewhat useful. [40] Research earlier this year by the Radical Librarians collective revealed that many public library services have installed off the shelf systems that apply categories of blocking to information which differed between each council, and included categories such as "Abortion", "LGBT", "alternative lifestyles", "questionable", "tasteless", "payday loans", "discrimination", "self-help" and "sex education". [41]

The rationale for filtering is clear from a specific ethical standpoint; it is about the prevention of access to materials deemed to be "inappropriate", such as specific types of pornography, or other materials that be inappropriate for a specific age group or deemed excessively offensive. Yet the basis of Internet filtering is the antithesis of free and open access. This becomes even more of a concern when we consider the nature of the legitimate material blocked, such as material on sexual health, breast cancer, or sexuality, or lifestyle as evidenced above.

Consider how many users may be too embarrassed to ask a teacher or librarian about issues like sexuality, indeed this may be the primary reason why they have chosen the Internet as their information source as it offers relative anonymity and privacy. Being confronted with a screen blocking access to information is unlikely to have such a user politely chatting to the person in charge to have their information provided, regardless of their approachability. It could be argued that many organisations ventured down the filtering route to protect them rather than in a bid to halt intellectual freedom, but this makes the decision even more problematic for an ethical professional. The problem with filtering, as discussed above, is that while it may block material that is offensive or questionable (though the question remains to whom), it has also been found to block material of a legitimate nature, and often this material is of personal or sensitive importance to a user.

It could be argued that it is the clumsiness of filtering software that poses the largest ethical concern. Taking the human out of assessing information for a user is always a bad thing, but to put it in the hands of a software program is clumsy in the extreme. Code may well be law, but code does not understand nuance or subtlety. Code is also not able to understand the urgency or importance, or sensitivity of a piece of information to the person seeking it.

In reality, organisations may be required to manage access to their networks and the content accessed on it for several crucial reasons. Firstly, the accountability of the organisation needs to be considered, as providing access to users will be for a purpose, be it a public access issue, or access for an employee to undertake the business of the organisation. The user of the system is accountable to the organisation, and the organisation is liable to its funders, shareholders or board members.

[38] Spacey, R., Cooke, L., Creaser, C. and Muir, A., 2015. Regulating Internet access and content in UK public libraries: Findings from the MAIPLE project. *Journal of Librarianship and Information Science.* 47 (1). pp.71-84.

[39] Brown, G. and McMenemy, D. (2013) "The implementation of internet filtering in Scottish public libraries", *Aslib Proceedings*. 65 (2) pp.182-202.

[40] Spacey et al. *Op. cit.*

[41] Payne, D. New research maps the extent of web filtering in public libraries. 2016. http://www.cilip.org.uk/blog/new-research-maps-extent-web-filtering-public-libraries

As well as content filtering, developing acceptable use policies (AUPs) that each user would have to agree to before being given Internet access has been a key tool to use. As a general rule, acceptable use policies (AUPs) should include the following considerations:

1. Informing users of their responsibilities;
    a. these include both legal requirements and those defined by the organisation
2. Providing the organisation with legal protection from liability;
    a. it should be made clear to users that the organisation is not responsible for their actions on-line with regard to e-commerce and possible fraud by third parties resulting in losses to the user – for example, all on-line transactions are at the user's risk, and are not the organisation's responsibility
3. Defining a contract between the organisation and the user;
    a. the policy should define the limits of the service, setting out what services are available and what would lead to those services being withdrawn.

The format of an AUP is normally a written document that is presented to a user when they are either requesting access to the network or are being provided with their login details to do so. Other ways of presenting an AUP to users include Log-in Banners, which are agreements presented to a user on the screen of their computer as they seek access. An acknowledgement button normally has to be clicked by the user to confirm that a set of terms have been agreed to by them.

Ethical issues around AUPs are also important to consider. Does the user understand the nature of the document they are signing for? Since the document constitutes a contract between the user and the information organisation, it is important that policies are as understandable as possible. [42]

4.2.2. Freedom of expression online

One of the current concerns of our time relates to what have been dubbed Internet trolls. These are individuals who disrupt online communications or who use social media to harass others, or *"who posts inflammatory, extraneous, or off-topic messages in an online community, such as a forum, chat room, or blog, with the primary intent of provoking readers into an emotional response or of otherwise disrupting normal on-topic discussion."* [43] While traditional online trolling pre-social media may have been aimed at individuals on message boards, special media services like Twitter allow public figures with accounts on the services to become potential targets for the activity.

As Spinello has observed, "offensive and threatening language has become all too common in the infosphere and especially in interactive social media." [44] Even in a country like the USA, with a history of free expression as guaranteed though the First Amendment, behaviour that is threatening towards another crosses a line when it comes to freedom of speech. This could be defined as harm under Mill's principle.

The UK authorities are clearly concerned about what they see as a growing public menace. As Hume informs us, "Guidelines issued by the UK Director of Public Prosecutions in December 2012 make clear that somebody should face prosecution if they post – or repost – a message online that 'clearly

[42] Gallagher, C., McMenemy, D. and Poulter, A. (2015) "Management of acceptable use of computing facilities in the public library: Avoiding a panoptic gaze?", *Journal of Documentation*, 71(3), pp. 572–590. doi: 10.1108/jd-04-2014-0061.

[43] Moreau, E. What Is a Troll, and Internet Trolling? How Internet Trolling Affects Us All. *Lifewire*. 21st September 2016. https://www.lifewire.com/what-is-internet-trolling-3485891

[44] Spinello. Op. cit. p.97.

amounts to a credible threat of violence'."[45] The same guidelines, however, highlight that "online posts deemed 'grossly offensive, indecent, obscene or false' would be much harder to prosecute."[46]

High-profile figures being forced off social media due to harassment seem an ever-present item in the news, but the experiences of US actress Leslie Jones who was racially abused on Twitter highlight how offensive and personal the trolls can be when let loose.[47] The harassment of female UK Members of Parliament such as Stella Creasy has seen trolls convicted and imprisoned, yet the behaviour still occurs.[48]

A large ethical question around online trolling and harassment is how much responsibility social media services themselves should have. Stella Creasy, herself a target of online trolls as cited above, suggests that both the police and the Internet companies need to do more to combat the situation. For Creasy, the issue of online trolls is not one of content, but one of harassment: "I am particularly frustrated with the police and CPS because I still don't think they get it in terms of making it a harassment issue, not a malicious content issue."[49] This is the ethical argument that the trolling behaviour is not one of freedom of expression, then, but one of actual assault on a person. Where harm occurs is an age-old argument that goes back to Mill, and is one that is constantly debated. The ability for numerous individuals to send individuals synchronous online insults and harassing messages is a new problem for that debate, however, as Mill could not have conceived of a medium like the Internet. It is difficult not to accept that Creasy has a point in this regard.

5. Privacy issues

Privacy overarches many of the issues related to digital ethics. The privacy to access and consume materials out of the view of others, the privacy to communicate, and go about our daily lives without hindrance is something many of us have come to expect. The reality is that privacy poses significant ethical issues within the digital realm.

5.1. Defining privacy

Perhaps the most famous definition of privacy was uttered by Supreme Court Justice Louis Brandeis in the case Olmstead v. U.S., 277 U.S. 438 (1928) where he defined privacy as "The right to be left alone—the most comprehensive of rights, and the right most valued by a free people."[50] In more modern times, privacy has been interpreted as a right that we all should be entitled to expect to be defended. For instance, Article 12 of the *Universal Declaration of Human Rights* states that:

[45] Hume, Mick. *Trigger Warning: Is the Fear of Being Offensive Killing Free Speech?* (Kindle Locations 1570-1573). HarperCollins Publishers. Kindle Edition.

[46] Ibid.

[47] Oluo, Ijeomoa. "Leslie Jones' Twitter abuse is a deliberate campaign of hate." *The Guardian*. 19th July 2016. https://www.theguardian.com/commentisfree/2016/jul/19/leslie-jones-twitter-abuse-deliberate-campaign-hate

[48] Twitter troll who targeted Stella Creasy abandons appeal against conviction. *The Guardian.* 7th May 2015. https://www.theguardian.com/uk-news/2015/may/07/twitter-troll-peter-nunn-labour-co-operative-stella-creasy

[49] Creasy, S. Police and tech firms are failing to tackle trolling, says Stella Creasy. *The Guardian.* Friday 15th April 2016. https://www.theguardian.com/technology/2016/apr/15/online-trolling-not-taken-seriously-enough-labour-stella-creasy

[50] American Library Association. *Privacy and confidentiality*. http://www.ala.org/Template.cfm?Section=ifissues&Template=/ContentManagement/ContentDisplay.cfm&ContentID=25304

> No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.

Therefore, privacy is defined as a right that we all should be able to expect to be defended in law. However, the right of the individual to privacy is becoming an ever-increasing concern in the information society, as information about us can easily be exchanged between parties at the click of a mouse, across countries and continents. It is also extremely difficult to know when and if this occurs, and this poses major problems for any legislative body seeking to curb such excesses.

Of course, as we will see, privacy has also to be balanced against other values. As with other rights, there are trade-offs and competing rights and interests which need to be respected. Economic interests may cause consumers to trade privacy for convenience such as occurs in credit card shopping. Efficient government requires personal information for taxation, health care, and the like. Privacy can also conflict with publicly accepted principles of law enforcement and public safety, as it is not desirable for the work of criminals or terrorists to remain private if they break laws and threaten wider society.

It could be argued that privacy is beginning to become a potentially old-fashioned concept. The increasing desire of our governments and the businesses we use to know more about us is impinging more on our day-to-day lives. Registering for many web-based services sees us having to tick boxes to unsubscribe from mailings or to ensure we do not have our data passed on to "selected third parties." Individuals and organisations increasingly have to spend money on spam and junk mail filters to attempt to ensure that their email inbox is not stuffed with inappropriate mails offering dubious services. This is all at the very least an inconvenience, and at the worst offers the potential for personal information to be abused or misused.

5.1.1. Privacy and autonomy

Privacy is also an important element in the autonomy of the individual. Much of what makes us human comes from our interactions with others within a private sphere where we assume no one is observing. Privacy thus relates to what we say, do, and perhaps even feel. If we are not able to trust that we are in a private space, then we may not be completely autonomous, we may hold back crucial elements of ourselves. As Griffin has observed: "frank communication… needs the shield of privacy; it needs the restraint of peeping Toms and eavesdroppers, of phone taps and bugging devices in one's house, of tampering with one's mail or seizure of one's correspondence". [51] Without a right to privacy, then, we are not able to be fully ourselves. Wacks also emphasises this point in considering the issue of electronic monitoring of employees: "the slide towards electronic supervision may fundamentally alter our relationships and our identity. In such a world, employees are arguably less likely to execute their duties effectively. If that occurs, the snooping employer will, in the end, secure the precise opposite of what he hopes to achieve." [52] In summary, "knowledge that our activities are, or even may be, monitored undermines our psychological and emotional autonomy." [53]

Yet undoubtedly privacy can pose significant challenges to security. If an individual is seeking to commit a crime or a terrorist act, then arguably privacy affords him more opportunity to do so.

[51] Griffin, J., *On Human Rights*. 2008: Oxford University Press. p.225.

[52] Wacks, Raymond. (2010) *Privacy: A Very Short Introduction (Very Short Introductions)* Oxford University Press. p.4-5.

[53] Ibid. p.4

This is the heart of the tension between a right to privacy and protecting the legitimate interests of others, and the state.

What is important for us to understand in this context is that privacy is a right *qualified* by other interests. This puts privacy in the same domain as freedom of expression, as other rights can take priority over both. This is a perfectly rational notion since unrestricted privacy could entail individuals undertaking activities that potentially damage the interests of others or society in general. It does, however, reveal that there is a tension between what a person might expect in terms of privacy and what may be deemed to be encroaching on the rights of others in doing so. Whether we recognise it or not, the intricacies of this qualification lie at the heart of the controversies we face in our professional practice. Wacks identifies seven *shortcomings* of privacy that are important to consider:

1. Privacy is often perceived as an old-fashioned value: "an air of injured gentility"
2. It may conceal genuine oppression, especially of women by men, carried out in the private realm of the home.
3. It may weaken the detection and apprehension of criminals
4. It may hamper the free flow of information, impeding transparency and candour
5. It may obstruct business efficiency and increase cost due to the necessity to adhere to standards in the collection of personal information
6. From a communitarian viewpoint, privacy is individualistic and trumps community values
7. Withholding unflattering personal information constitutes a form of deception. [54]

The European Convention on Human Rights (ECHR) states both the right to privacy, and the limits that can be placed on it. Article 8 states that: *"Everyone has the right to respect for private and family life, his home and his correspondence."* Section 8 (2) of the ECHR covers the limits that are allowed to be placed on the right to privacy specified in 8 (1): "There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic wellbeing of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others."

In reality, what does this mean? Firstly, that any restrictions placed on the right to privacy by states must be *lawful*. There must be a legal basis for the intrusion, and it must be justified by existing legislation. Framed as they are we can see here a set of restrictions that advocate invasions of privacy only in terms designed to protect what are deemed to be the legitimate interests of others, whether in the body politic or in their own right.

5.2. Privacy within the digital realm

Within the digital realm, privacy confronts us on two fronts, that of governments monitoring our behaviour, and that of corporations doing likewise. In truth the former can be argued to be about the protection of the realm, while the latter is about commercial advantage, however, both types of surveillance of Internet users raise their own controversies and ethical issues.

A primary concern for EU legislators relates to the ubiquity of cookies, the small files that download to a person's computer when they browse a website in order to track activity and allow the user a more enhanced experience. As much as cookies are essential for e-commerce solutions, they pose significant privacy concerns, as they store user activity while they are using websites, but can also track behaviour across the web. In an analogue world this would be the equivalent of a customer walking into Marks & Spencer's, using their credit card to buy an item, and then being followed

[54] Ibid. p.35-37.

around other stores afterwards by someone who is making notes on their purchases. This is clearly an invasion of privacy and goes against the spirit of data protection in the EU.

EU Directive 2009/136/EC of the European Parliament and of the Council has laid down the parameters of cookie use across the EU, and compels member countries to address its provisions within their own national legislation. The key element that relates to cookies within the Directive states that the placing of cookies on a browser's computer is "only allowed on condition that the subscriber or user concerned has given his or her consent, having been provided with clear and comprehensive information, in accordance with Directive 95/46/EC." [55] The emphasis then is that a user must *opt-in* to receiving a cookie, and in doing so they must have been given access to information as to what that cookie will store about them, and why. In this context, we are dealing with the concept of *informed consent*, which has a history in EU Directives on data protection. [56] In other words, users "must understand the facts and implications of an action to be able to make informed choices, ensuring that they are effectively able to choose freely and voluntarily. [57]

This links to the important point that the "cookie directive", as it is commonly known, builds on pre-existing EU Directives related to data privacy, and thus forms the next link in a chain. *Directive 95/46/EC*, is the backbone of data protection legislation throughout Europe and is an important component in privacy law, and *Directive 2009/136/EC* itself was an update to *Directive 2002/58/EC* which first dealt with the issue of cookies amongst other issues related to electronic privacy and transmission of data. [58] Thus within the EU we can see a natural evolution of data protection law that now encompasses the threats to privacy posed by cookies and the tracking of user behaviour in the online space.

5.2.1. Privacy, customised services, and social media

One of the most contentious areas around privacy online relates to customised services and social media and the voluntary surrender of personal privacy necessary on the part of individuals to take part in them. As online security expert, Bruce Schneier observed: "Surveillance is the business model of the Internet… We build systems that spy on people in exchange for services. Corporations call it marketing." [59] All of this plays into the larger concept of big data, where enormous databases of user data can be mined to predict consumer behaviour for corporate advantage. The elephant in the room, however, is the behaviour of citizens themselves when using online services.

One of the common paradigms of the modern era is the notion of customisation of services to users. In an online environment, the use of cookies for a user could well be a good trade-off with regards their privacy if the experience they receive from the website is more tailored to them. However, this tailoring comes at a cost, the loss of part of their privacy. This is perfectly fine if the informed consent concept we discussed earlier is a part of the process; however, research on the awareness of cookies amongst the population suggests this is far from the case. The Information Commissioner cites a report conducted in the UK for the Department for Culture, Media and Sport that raised some significant issues:

- 41% of respondents were unaware of different types of cookies
- Only 13% indicated they fully understood how cookies work

[55] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:337:0011:0036:en:PDF

[56] Borghi M, Ferretti F and Karapapa S. "Online data processing consent under EU law: a theoretical framework and empirical evidence from the UK" *International Journal of Law and Information Technology* 21. 2013. p.109.

[57] Ibid. p.120.

[58] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0058:en:HTML

[59] Rashid, F.Y. "Surveillance is the Business Model of the Internet: Bruce Schneier." Security Week. April 09, 2014 https://perma.cc/S5AA-299Y

- 37% had heard of cookies, but did not understand how they work
- 37% did not know how to manage cookies on their computer [60]

We can see then a significant issue with regards the actual issue that is being legislated against. If people do not understand the nature of what they are being protected against, how can the legislation be effective?

From an ethical standpoint, we must also consider here the concept of *engineered consent*, which in contrast to informed consent is built around consent being given because the user essentially has no choice, if they wish to receive the service provided. As Borghi et al state, "if data subjects have to give more information than is strictly necessary to buy goods or access services, then it is likely that they will consent to whatever broad uses of their data to obtain the goods or services." [61] If the user *not* accepting cookies on their computer means the service they will receive will be of lesser quality, they may trade off in their mind consent for the service versus their privacy. Such a process has arguably coercive elements to it that we must be wary of. Similar scenarios apply to social media and email accounts: is not having them a worse scenario for a citizen than actually having them?

In terms of social media, how the companies deal with user data is a constant controversy. One example highlights a key issue: in 2007 Facebook launched a new service called Beacon, which sought to provide a peer-based advertising system. Purchases by Facebook members from certain third-party vendors would show up on the pages of friends to alert them to their friend's purchase. This garnered great controversy and was seen by many members as an intrusion into privacy. It does not seem an outlandish concept for someone to wish to keep their purchasing habits secret from others, and the Beacon idea raised a significant issue with regards the usage of user data and how it can be used to invade privacy. Ed Felten sums up the issue perfectly: "We agree that privacy matters, but we don't all agree on its contours. It's hard to offer precise rules for recognising a privacy problem, but we know one when we see it. Or at least we know it *after* we've seen it." [62] Ultimately the Beacon episode is an example of the public recognising a significant privacy problem when they saw it, their autonomy being utilised for the commercial gain of another without their permission, and they acted to stop it.

5.2.2. Privacy, government surveillance

A major controversy with regards to privacy in the digital realm relates to how much power our governments should have with regards to monitoring our behaviour. Governments would argue that since the defence of the realm is a crucial aspect of their role, they have a duty to be able to investigate when people are using online services, etc to cause us harm. Such defences can be argued to include issues around harassment, cybercrime and fraud, and terrorist offences. The arguments around this, as stated earlier, relate to the limits that should be placed on these monitoring activities.

[60] Information Commissioner, *Guidance on the rules on use of cookies and similar technologies*. 2012. https://ico.org.uk/media/1545/cookies_guidance.pdf

[61] Borghi et al. *Op. cit.* p.120.

[62] Felten, E. Lessons from Facebook's Beacon Misstep. 2007. https://freedom-to-tinker.com/blog/felten/lessons-facebooks-beacon-misstep/

In the UK the recent passing of the *Investigatory Powers Bill* into law has raised significant controversies. [63] The provisions that raise most controversies relate to:

- Forcing internet companies to keep user browsing records on users for up to a year
- Forcing companies to hack into products they have built, such as mobile phones, to enable government agencies to monitor them

The government would argue that such powers better enable them to combat crimes since often investigations need to consult records that are old to be able to build a case against perpetrators and to identify the full extent of any others' involvements. On the other hand, campaigners argue that the legislation is unnecessarily invasive and an assault on the citizen's right to privacy.

The topic of government surveillance has become more controversial in recent years after revelations by a former CIA consultant, Edward Snowden, revealed mass surveillance was far more widespread in democratic countries than was ever anticipated. The revelations that the National Security Agency (NSA) were collecting "vast amounts of data regarding the internet use of everyone online" also revealed that the US government was in collusion with large corporations who also collected data on users. [64]

While such surveillance raises issues around privacy and trust in government and those who collect the data, there is also research from the USA that suggests the knowledge of being potentially monitored impacts on freedom of expression, as writers limit what they search for or write about, leading to self-censorship. [65] Therefore, we see here a classic ethical dilemma over whether the utilitarian concern over protecting society as a whole impact on individual rights excessively.

5.2.3. The right to be forgotten

In May 2014 a landmark ruling saw the European Court of Justice support the claim of a Spanish man, Mario Costeja Gonzalez, to block from Internet searches a 1998 newspaper notice that discussed how his home was to be auctioned off to pay off his debts. Gonzalez's argument was that this old information was no longer relevant to his life, and in fact hindered him as it was revealed prominently in searches about him and this saw others make assumptions about him and his ability to manage debt. On the face of it, this seemed like a straightforward argument, and the idea that someone in 2014 should have their life impacted by an out of date aspect of their past seems harsh. The ramifications of the judgement, dubbed the right to be forgotten, have been significant, however.

Essentially the ruling meant that anyone could have removed from Internet searches in Europe any item that was "'inadequate, irrelevant or no longer relevant". [66] Critics argued that it would lead to famous people or criminals seeking to remove embarrassing aspects of their lives. Statistics accidentally revealed by Google, however, suggested that the vast majority of requests came from ordinary citizens seeking to remove embarrassing or irrelevant items related to them: "Less than 5%

[63] Griffin, A. "Investigatory Powers Bill: 'Snoopers Charter 2' to pass into law, giving Government sweeping spying powers" *The Independent.* 17th November 2016. http://www.independent.co.uk/life-style/gadgets-and-tech/news/snoopers-charter-2-investigatory-powers-bill-parliament-lords-what-does-it-mean-a7423866.html

[64] Clark, I. "The digital divide in the postSnowden era" Journal of Radical Librarianship, Vol. 2 (2016) pp.1–32. http://www.journal.radicallibrarianship.org/index.php/journal/article/download/12/26/

[65] Global Chill: *The Impact of Mass Surveillance on International Writers.* US PEN. 2015. https://pen.org/sites/default/files/globalchilling_2015.pdf

[66] Ronson, J..*So You've Been Publicly Shamed* (p. 195). Pan Macmillan. p.195.

of nearly 220,000 individual requests made to Google to selectively remove links to online information concern criminals, politicians and high-profile public figures.” [67]

Nevertheless, the right to be forgotten raises significant digital ethics questions. Does the ability to remove Items from searches impact on freedom of expression? Does the individual’s right to privacy and autonomy for past, and no longer relevant information about them, trump another’s right to know that information? Search engines are relatively new items in terms of our ability to seek out information, and since the right to be forgotten does not remove the actual item, only the ability to find it, there does seem a grey area here from the point of view of ethics. As a relatively new ruling, it is one that must be watched from the point of view of its impact on society.

5.2.4. Privacy and library and information services

A concern for the information profession should be how it handles user data, especially with the expansion of services into the cloud, and the use of third-parties to deliver services. We see such scenarios occurring with the development of software as service platforms, where vendors provide services like library management system (LMS) access via the cloud, as well as the provision of services such as e-book services via vendors.

Caro and Markman urge librarians to be mindful of LMS security and to regularly test their systems for any inadequacies. [68] A recent case saw the Miami-Dade Library Service change their e-book vendor over concerns over third-party access to and data mining of user data. [69] The reality is that the more library services use vendors to store user data, the more valuable datasets on user behaviour that are created. Librarians must be aware of the dangers to that data that are potentially posed by storing it off site and must reassure themselves of the security of the data and that use it will be put to by third parties.

The Library Freedom project provides information for library and information professionals on how to provide more secure services for users and recommendations on software that can be used to protect user anonymity online. [70] Recommended services include advice on encryption software for email services and other online services, as well as advice on how to use secure web services such as https as a standard.

6. Conclusions

Digital ethics presents us with a range of new challenges based on old values and controversies. The arguments around ethical behaviour, freedom of expression, and rights to privacy are not new but transplanted into the digital realm present us with brand new challenges to solve.

The emergence of a new paradigm presented by the Internet, built on an infrastructure and ethos of openness and inclusivity, provides many potentially positive opportunities for access to information and ideas. Nevertheless, it also provides opportunities for enhanced surveillance and usage of citizens’ data that could be potentially detrimental.

[67] Tippmann, s. and Powles, J. Google accidentally reveals data on 'right to be forgotten' requests. *The Guardian*. 14th July 2015. https://www.theguardian.com/technology/2015/jul/14/google-accidentally-reveals-right-to-be-forgotten-requests

[68] Caro, A. and Markman, C. “Measuring Library Vendor Cyber Security: Seven Easy Questions Every Librarian Can Ask.” *Code 4Lib Journal* . 34. 2016-04-25. http://journal.code4lib.org/articles/11413

[69] See Miami-Dade Library Service: press release over use of Overdrive service, http://www.mdpls.org/news/press-releases/2016/overdrive.asp

[70] What is the Library Freedom project? https://libraryfreedomproject.org/

An understanding of digital ethics from the point of view the services provided by information professionals thus necessitates addressing some fundamental ethical theories and applying these to the information domain. We must be cognisant of newly emerging challenges to practice if we are to be able to navigate these challenges.