1 The Internet, Warts and All

> Invention, it must be humbly admitted, does not consist in creating out of void, but out of chaos . . .
>
> Mary Wollstonecraft Shelley, Introduction to *Frankenstein*

1.1 Warts and All

When Oliver Cromwell went to Samuel Cooper to ask for his portrait to be painted, he was the most powerful man in the country: Lord Protector of England. He had effectively deposed King Charles I: the king was executed in 1649, the same year that Cromwell invaded Ireland and perpetrated the massacres that make him one of the worst of all villains in the eyes of the Irish. He was a driven man, a 'great' man, but still a man almost obsessed with humility and what he saw as the truth. As John Morrill put it: 'He was called to overthrow tyranny and pride and replace it with humility and a common concern to share the fragments of truth that so many men of goodwill had been granted.'[1] This obsession with humility and with truth presumably lay behind his answer to Cooper's question about whether to include his prominent and disfiguring warts in his portrait. It would have been easy to have the portrait exclude them – indeed, the most prominent portraits of Cromwell, from an initial portrait by Cooper himself in earlier years to the later much-copied full-sized portrait by Sir Peter Lely, seemingly based on Cooper's 'warts and all' miniature, have the warts blurred, minimised or removed.

For the crucial Cooper miniature Cromwell was clear. He wanted the portrait to show him 'warts and all'. He wanted as truthful a picture as possible. He wanted to be remembered as he was, not in some false, idealised form. This is how the term 'warts and all' entered the English language – to see a thing as a whole, including all the unappealing features. If we are to understand something properly and truthfully, we

[1] Morrill 2007, p. 121.

https://doi.org/10.1017/9781108381161.002 Published online by Cambridge University Press

need to see, understand and accept its unappealing features as well as those features that we find attractive.

This story about Samuel Cooper, recounted above as though it were fact, may actually not be true. Some attribute it to another artist entirely – the aforementioned Sir Peter Lely – based in part on Horace Walpole's famous book of anecdotes collected more than 100 years later.[2] The whole story may be apocryphal. It may be 'fake news' invented after the events in order to portray Cromwell in a favourable light. It is all but impossible, more than 350 years after the event, to be absolutely sure what actually happened or what was said. Expert opinion based on other historical evidence and a detailed analysis of the paintings themselves strongly suggests that it was Cooper to whom the 'warts and all' comment was made, but it is not absolutely certain.[3] That is generally the nature not just of history but of much more. Certainty is rare. That is equally true of much concerning the internet.

1.1.1 The Internet We Have

If we are to get closer to the kind of internet we want, we need a better understanding of the internet that we have. We have to look at the Internet, warts and all, and not be seduced by the illusions of how the internet *seems* to be, or how others would like us to see the internet for their own purposes.

The internet is not a permanent, perfect archive of historical information, indexed by neutral and purely algorithmic services such as Google or accessed through neutral and apolitical platforms such as Facebook. It is messy, dynamic and constantly changing. Things are being deleted, modified and blocked all the time. Search engines, social media platforms and other services are not neutral public services but money-making self-serving businesses. Their algorithms are neither neutral nor 'organic', but created by humans and with biases, assumptions and faults. Intervention with those services and platforms, and with the algorithms and indexes

[2] In Horace Walpole's *Anecdotes of Painting in England, with Some Account of the Principal Artists*, p. 226 of the 6th edition, Walpole records an indirect anecdote: 'Captain Winde told Sheffield, Duke of Buckingham, that Oliver certainly sat to him, and, while sitting, said to him, "Mr Lely, I desire you would use all your skill to paint my picture truly like me, and not flatter me at all; but remark all these roughnesses, pimples, warts, and everything as you see me, otherwise I will never pay a farthing for it".'

[3] See, for example, the catalogue of Phillip Mould's exhibition, 'The Portrait Miniatures of Samuel Cooper (1607/8–1672)'. The Cromwell portraits by both Cooper and Lely are Cat. 21–23, with detailed commentary by art historian Dr Bendor Grosvenor, pp. 70–74: http://philipmould.com/application/files/3114/4708/8432/Warts_and_All_catalogue_v12.pdf.

created by them, is not a fundamental and wholly inappropriate interference with freedom of expression, but part of a regular, important and potentially positive process that can help keep a more appropriate balance between the rights and interests of people and corporations.

The internet is neither an ungoverned and ungovernable realm of criminals and terrorists that needs to be reined in to protect us nor a massive surveillance engine that has brought us to the brink of an Orwellian dystopia. There are criminals and terrorists – and paedophiles and drug dealers – on the internet, but most of the time, for most of the people, it is a place to find information, socialise, do business, and generally live, and do so in relative safeness and simplicity. There is a great deal of surveillance – most of people's web activity is monitored in a wide variety of ways – but the surveillance is neither as effective nor as malicious as some might suggest. Understanding the context, the complexity, the nuance, the dynamism and the relationships between the various issues – and, in particular, understanding the messiness of the whole situation – can help us to take a more balanced view of each of the issues in turn.

1.1.2 Free Speech, Privacy and Truth

Free speech, privacy and truth are the central themes of this book. There are specific chapters devoted to each of them – Chapter 5 on Free Speech, Chapter 6 on Privacy and Chapter 9 on Truth – but none of these is an idea about which it is easy to be precise. Neither free speech nor privacy can be easily defined or pinned down. Some scholars contend that attempting to define privacy in particular can be counterproductive or a distraction from addressing the very real problems.[4] Whatever definition is taken can end up either missing something crucial or covering areas that are really not about what people understand by privacy at all.[5] Pinning down free speech may be just as difficult. What counts as 'speech' and what constitutes 'freedom' is not as simple as it seems. Freedom to do what? Freedom from what? Truth may look as though it is easier to understand and deal with, but even here there are difficulties. Perspectives matter. Interpretations matter. Context matters. All these things are

[4] For example, Helen Nissenbaum: '[b]elieving that one must define or provide an account of privacy before one can systematically address critical challenges can thwart further progress'. Nissenbaum 2010, p. 2.

[5] Daniel Solove, notes that '[p]rivacy is too complex a concept to be reduced to a singular essence. It is a plurality of different things that do not share one element in common but that nevertheless bear a resemblance to each other'. Solove 2011, p. 24.

discussed in more depth in the relevant chapters, both in general and in the specific topical examples that are examined – social networking, trolling, fake news, surveillance and so forth. It is a central contention of this book that the three central issues of free speech, privacy and truth are intrinsically and inextricably linked, in a way that is often surprisingly complex and nuanced.

1.1.3 Taking a Broad Look

This is a book about law. It is also a book about technology, about politics, about psychology, about society, about history, about philosophy. A great deal is covered here, by design. We need to take a broader, more multifaceted approach to the way we deal with the internet. This means, amongst other things, that we need to consider all these aspects. Decisions in relation to the internet that may *seem* to be about law have political implications, technological implications, societal implications and more.

Legal and technological measures that impact upon one of the three key issues – free speech, privacy and truth – will generally have an impact upon another – or more likely on *all* – of them, and often not in the way that appears immediately obvious. For example, a policy such as requiring real names on social media,[6] whilst ostensibly about authenticity – and hence truth, will mean invasions of privacy and will chill freedom of speech for many. Sometimes it will reduce truthfulness as people unable to gain the privacy-related protections of anonymity or pseudonymity will be more likely to omit some of the truth or to lie. As the many examples presented in this book will demonstrate, 'real names' is not the exception but the rule: free speech, privacy and truth cannot be easily separated.

Other examples show the same patterns. Invasions of privacy are used to identify websites to censors. Trolls 'dox' people, invading their privacy and revealing true details of their lives in order to scare them into silence. The advertising industry argues that ad-blockers – installed by some specifically to protect themselves against the invasions of privacy that are inherent in behavioural targeting systems now commonly used by advertisers – are an infringement on their freedom of speech.[7] The same pattern is repeated again and again. Whichever of the issues we are trying to 'deal with', we need to consider each of the others.

[6] See Chapter 8, pp. 220–223. [7] See Chapter 9, p. 257.

https://doi.org/10.1017/9781108381161.002 Published online by Cambridge University Press

1.2 Perspectives on the Internet

We are confused about what the internet is, but we are also confused about what we want the internet to be. The two confusions interact to produce even more confusion: it is that interaction that makes the regulation of the internet especially difficult and particularly troublesome.

1.2.1 The Internet as an Information Resource

The ability to find information is a critical but often misunderstood and underestimated part of freedom of expression: in most formulations, the right to freedom of expression includes the freedom to both impart *and receive* information.[8] The internet can help this freedom to be realised perhaps better than anything else in history – both in theory and in practice. If you want to find something out, the first thing that you do is look on the internet. Almost any kind of information can be found – anything that can be digitised, from the text that formed the early web to images, sound, video, 3D imagery and much more. You are most likely to *search* for the information – and most often to use Google for that search.[9] You may instead go through a social media platform – more than two billion people are on Facebook.[10] You might use an online encyclopaedia – most likely Wikipedia, which has more than 43 million pages of regularly checked and updated information on almost everything.[11] You might look at specific and specialised websites for particular subjects, at forums that you know about, or ask people that you know (either online or in 'real' life) and trust to recommend places to visit.

There are conflicting needs when using the internet as an information resource. For the purposes of historical research, an archive should be keep as pristine as possible, with records as complete as possible and as they were when they were laid down. Records should not be deleted, and any modifications made should be recorded, together with the reasons for them – and only certain kinds of modifications should be possible: adding newly discovered resources, for example, or correcting clear errors. History, in these terms, should not be 'rewritten'. In principle, this sounds nice and clear, but even a little thought shows that it is not as simple as that. What kinds of errors should be corrected? Who should determine

[8] E.g. in Article 10 of the European Convention on Human Rights and in Article 19 of the Universal Declaration of Human Rights. See Chapter 5, p. 104.

[9] Google has dominated the search market for some years – around 90 per cent worldwide. See e.g. http://gs.statcounter.com/search-engine-market-share.

[10] Mark Zuckerberg celebrated Facebook passing the two billion people mark on 27th June 2017. See www.facebook.com/zuck/posts/10103831654565331.

[11] See https://en.wikipedia.org/wiki/Wikipedia:Size_of_Wikipedia.

whether an error has been made and how to correct for it? If an error is discovered, how can the repercussions of that error be addressed as well as the error itself? If it is determined that it was definitely Samuel Cooper rather than Peter Lely to whom Cromwell gave the instruction to paint him warts and all, how can all those records (dating back to 1764 at least) that suggest it was Lely be corrected? If they are not corrected, people will continue to be misled. They will not find the truth. If they are corrected, changes will have to be made in the historical archive itself. Should Horace Walpole's seminal piece of work on English painting be marked down as including an error everywhere it is mentioned?

There are no easy answers here, primarily because the idea of an accurate and complete archive is based on a misunderstanding of the nature of history and the nature of factual information. Not only do new facts emerge but our understanding of existing facts and interpretation of them changes. As J. S. Mill put it, '[v]ery few facts are able to tell their own story, without comments to bring out their meaning'.[12]

All this means is that a historical archive – or, to be more precise, an information resource useful for historical research – can often be complex, with notes, qualifications, references and cross-references. It can need time, attention and expertise to understand and to navigate through – but the complexity is necessary for the archive to be useful. That is fine for those with the requisite time and expertise, but it makes the archive very much less useful for those without it – and the vast majority of users of the internet have neither the time nor the expertise. They need a very different kind of information resource: they want information quickly and easily, in a form that can be understood without specialist knowledge or expertise.

For these people – most people – if the required information exists but is hard to find, or if would take too long to find, or if it is obscured by a morass of other information, or if verifying that it is the right information is too difficult, then for most practical purposes it might as well not exist. People trying to find the information without sufficient time, energy and expertise will not find it. This is one of the reasons that internet tools like search engines have become so popular: they make it easy and fast to find things for everyone. People want to find the most relevant information quickly, and don't want to be bothered with detailed fact checking – or even know how to do proper fact- or source-checking, one of the reasons behind the fake news problems.[13] They aren't likely to want to have to go through information in detail before finding the pertinent facts – they may

[12] Mill 1859, p. 22. [13] See Chapter 9.

https://doi.org/10.1017/9781108381161.002 Published online by Cambridge University Press

well only look at headlines on search results without even visiting the relevant pages, for example.

People in this scenario want their search engines, social media platforms or online encyclopaedias to help them to find the information they need. They want those engines, platforms and encyclopaedias to be *neutral*. At this point they do not seem to be aware that these engines, platforms and encyclopaedias are not, and *cannot* be, neutral: the crucial neutrality myth is the subject of Chapter 4. They don't want to be distracted by irrelevant information. They don't want old or irrelevant information to clutter up their timelines or search results: having complete and accurate information, as required for historical archives, could be a distraction and a disadvantage. It could stop them finding what they want to find.

The search engines and social media platforms know this. This is why Google constantly tweaks its algorithm and has been 'personalising' search results based on what it 'knows' about individuals since 2009,[14] and why Facebook has been algorithmically curating its news feed since it was introduced in 2006.[15] Twitter, whose nature until that time had been much more about a pure, unaltered, chronological timeline, began experimenting with algorithmic curation of timelines in 2015, and has tried a number of different versions, including 'while you're away' (a curated selection of tweets since you last logged on) in January 2015,[16] 'Moments' (thematically curated tweets) in October 2015[17] and 'Best Tweets' (tweets you're most likely to care about) in February 2016.[18] These have been as options rather than the default timeline, but they emphasise that the need to select or curate, to help people to have a route through the mass of information to what they need, is seen as vital for the mass audience. The needs of most people for speed, convenience and ease of use are quite different from the needs of specialists – journalists, academics, researchers – for a complete, accurate and historical archive that can be trawled through exhaustively and logically. When both groups want access to the same information and use the same tools – search engines, social media platforms and so forth – that naturally brings tension, confusion and problems.

[14] https://googleblog.blogspot.co.uk/2009/12/personalized-search-for-everyone.html.
[15] See the official launch notification of Facebook's News Feed and Mini Feed: www.facebook.com/notes/facebook/facebook-gets-a-facelift/2207967130.
[16] https://blog.twitter.com/official/en_us/a/2015/while-you-were-away-0.html.
[17] https://blog.twitter.com/official/en_us/a/2015/moments-the-best-of-twitter-in-an-instant-0.html.
[18] https://blog.twitter.com/official/en_us/a/2016/never-miss-important-tweets-from-people-you-follow.html.

When looked at from the perspective of those wanting 'their' information to be known rather than those seeking information, a whole set of other potential issues arises. First of all, which people are concerned – those who create or want to disseminate information, or those who the information is about? Others who might be impacted upon if the information is known? Still more who just have an interest in a subject or an agenda? Some people will want particular information to be found by everyone. Some would prefer this information not to be found at all. Others would like it to be found by some and not by others. When information concerns more than one person, their desires may be in tension or in conflict.

The internet's role as an information resource also brings in the need for privacy. For an information resource to function well it not only has to exist and be relatively 'user-friendly', it has to actually be used – and that means that people need to be willing to use it. They need to know that their use of the information resource will not in itself be used against them. A victim of spousal abuse will not search for information about refuges if they believe their abuser could discover they were searching for them and even discover which refuges they have been investigating. A whistle-blower would be wary of putting information about their employer's misdeeds on the internet if they thought their employer might easily be able to discover who they are. A teenager might not seek out information about sexual health if they thought their conservative parents would immediately know it. A dissident would not want their oppressive government to know that they were accessing opposition websites or information that showed that government in a bad light. One of the most notable results of intrusive surveillance is a drive towards conformity and an unwillingness of people to take risks.[19]

There are others whose interests come into play here: groups, most importantly governments and other authorities, who wish to prevent people having access to information for various reasons. Access to offensive material such as child abuse imagery,[20] material deemed to promote terrorism or encourage extremism, material which breaches copyright, material that should only be accessed by adults, or material that is deemed defamatory, blasphemous or offensive to others. The variety of different reasons that material might be deemed objectionable by one government or another, or by one interest group or another, is extensive.[21] Sometimes

[19] See Chapter 7, particularly pp.135–136.

[20] Historically (and in places such as the USA) referred to as 'child pornography' – the term 'child abuse imagery' is generally preferred in the UK as it makes clear that even the making of this material involves child abuse.

[21] Discussed in Chapter 5, and in some specific areas in Chapters 8 (on trolling) and 9 (on fake news).

the issues and reasons behind the blocking are political, sometimes moral or religious, sometime economic, sometimes pragmatic or instrumental. Some of the reasons are positive and valid – most formulations of freedom of expression include caveats such as for the protection of people or of their rights – but some are distinctly less convincing. The balancing of rights and interests in conflict is often complex and nuanced.

At the moment, maintaining that balance is largely in the hands of the internet giants who control so much of the access to the information – Facebook, Google, Twitter and, in a rather different way, Wikipedia. In whose interests do these organisations operate? That of their 'customers'? Of their advertisers? Of their shareholders? Facebook, Google and Twitter are businesses and the bottom line is the bottom line, which sometimes means that people's rights and needs do not exactly take centre stage.

How regulators could or should respond to that is complex. Lawmakers can tend to take the rights of the third group – those who wish to block access to material of various kinds – more seriously than others, primarily because they themselves are often in that position, and – as shall be demonstrated by many of the examples in this book – because they have a limited understanding of both the issues and the technology. It is important to be fair to the lawmakers, however: this is not easy. The balances are very difficult to find even when the issues and technology are understood, but it is of critical importance and could often be done much better.

1.2.2 The Internet as a Communications Medium

At its beginning, the internet was primarily a communications medium, and that aspect has remained and dramatically expanded over the years. Electronic mail (email) was one of the first applications for the internet and remains one of the most important and trusted.

Some communication is effectively instant and ephemeral: Internet Relay Chat ('IRC'), the first system in common use, was developed in 1988.[22] Others, from email onwards, are intended to form part of a permanent record. Official and legal correspondence is often done by email – and is expected to be part of official records. Emails are subject to freedom of information law:[23] there is a good reason why Hillary Clinton got into so much trouble for seeming to hide and then delete a significant

[22] A summary of the history of IRC is online at https://daniel.haxx.se/irchistory.html.
[23] In the UK under the Freedom of Information Act 2000. There are similar laws in many states.

amount of email correspondence. In the current internet, a vast variety of forms of communication are possible, from the equivalent of telephone calls (Voice over Internet Protocol – 'VoIP' – has been in relatively common use since 2003) and video calls (Skype launched its video calling system for Windows in 2006)[24] to experimentation in 3D virtual reality communications.[25]

The requirements of the internet as a communications medium are qualitatively different from that as an information resource. Someone communicating directly with another person needs to know that their information has gone safely and securely to the right place, fast enough and reliably enough for the particular kind of message. Instant and interactive communication puts the emphasis on speed – bandwidth was the key limitation for early adopters of online video communication – and reliability of connection.

Communication also brings privacy into play. Different kinds of communication require different kinds of privacy. Some are highly confidential – the use of encryption for communications has a history far older than the internet – whilst others might be readily shared within various different groups who hold the requisite trust. Privacy in law has generally considered privacy of correspondence a key element. It is included in both the Universal Declaration of Human Rights[26] and the European Convention on Human Rights,[27] and the US Supreme Court ruled it was constitutionally protected as early as 1877.[28] Opening letters, tapping phone lines and their equivalents are not things that can be done as a matter of course in a democratic state.

1.2.3 The Internet as a Business Platform

Though the internet was initially a communications platform for the military, scholars and geeks,[29] the opportunities that it presented for business became apparent relatively quickly. The rapid growth and development of the internet over more recent years could be argued to have taken place to a great extent because businesses have grasped those opportunities. There is a reason why many of the biggest companies in the world are primarily internet-based companies. In 2017, according to Forbes, the top four companies in the world in terms of market

[24] See https://blogs.skype.com/wp-content/uploads/2012/08/skype-timeline-v5-2.pdf.
[25] E.g. Facebook Spaces; see www.oculus.com/experiences/rift/1036793313023466.
[26] Article 12. [27] Article 8.
[28] In *Ex parte Jackson* 96 US 727 (1878), online at https://supreme.justia.com/cases/federal/us/96/727/case.html.
[29] See e.g. Naughton 2000.

capitalisation were Apple, Alphabet (Google's holding company), Microsoft and Amazon, with Facebook in sixth and Alibaba (the biggest Chinese e-commerce company) just outside the top ten.[30]

It is not just the internet-based companies that have taken advantage of the internet. It is a very rare business that does not at least try to use the opportunities presented by the combination of provision of information, instant interactive reliable communications, electronic payments, electronic contracts, global reach and much more. Websites are the public faces of businesses as much as their corporate headquarters or high street shops ever were. Digital goods can be sold and distributed directly and automatically. Services can be provided online. Physical goods can be ordered, online support provided and much more. The internet starts off by being a marketing opportunity but ends up underpinning an entire business, just as for individuals the internet started as a communications opportunity and an information resource but now underpins almost every aspect of their lives.

The requirements of business are qualitatively different from those of an information resource and a communications medium. Businesses do, of course, need both of these, but they also require reliable and secure payments systems, legal frameworks that work with these systems to provide certainty, and so forth.[31] As their websites are their public faces, they also have to keep these up to date, which means being able to delete or amend old information, remove discontinued products, change prices and more. In general, they would like only the current information to be easily found. They might specifically want old information to be unavailable: the opposite of the demands for a historical archive.

Many online businesses need to ensure that the internet infrastructure provides sufficient speed and reliability for their services to operate: streaming video, for example, high definition games, or almost any form of virtual reality system require fast, reliable and uninterrupted connections. Some want to be able to prioritise their data over that of their

[30] See www.forbes.com/global2000/list#header:marketValue_sortreverse:true. These are rankings by market capitalisation – an assessment of future value rather than current sales and assets. In its 2017 rankings, Forbes places Apple 9th, Microsoft 19th, Alphabet 24th and Amazon 83rd.

[31] Contracts concluded electronically have to be enforceable, money has to be transferrable easily and quickly and so forth. There have been national, regional and international laws, conventions and agreements to ensure that this is possible. In the EU, for example, this includes the E-Commerce Directive (2000/31/EC), an Electronic Signatures Directive (1999/93/EC) and the e-IDAS 'identification and trust services' regulation that replaced it (910/2014/EU), as well as two Electronic Money Directives (2000/46/EC) and (2009/110/EC).

competitors, an aspect of the net neutrality debate that can put them at odds with freedom of speech advocates and others.

Businesses also want influence over the information put out by others on the internet. They want to be able to protect their brand by shutting down websites purporting to be theirs or confusing customers and potential customers. They want to be able to prevent the sale of counterfeits or 'grey' imports, blocking or shutting down websites offering them. They want to stop businesses that compete against them illegally or unfairly. They want to ensure that where they are restricted by local rules on advertising etc. that competitors are similarly restricted. They want to control which regional versions of websites people can access so that they can control local pricing and prevent access to products before they are properly introduced in a particular market. They want to stop the spread of 'pirate' copies of their digital products. They want to build 'digital rights management' systems into the infrastructure of the internet.[32] They want to stop people spreading disinformation about their businesses, damaging their reputations. They want to be able to control the information available about them on the internet. All of this puts their wishes in potential conflict with the freedom of expression and access to information of others.

Security and privacy are also paramount for businesses. Confidentiality of communications – the ability to keep trade secrets, to negotiate contracts and other business arrangements – as well as the ability to perform transactions with certainty is crucial. Privacy for their customers and potential customers is quite another matter: businesses know that the more they know about their customers, the better they might be able to serve them. They can tailor goods and services, develop new services, discover better marketing opportunities and find new customers – and the internet provides unparalleled opportunities to do so. It is not just the advertising industry that wants to be able to monitor and scrutinise the people who visit their websites and to use 'big data' analysis to profile them. The potential is enormous – and so is the desire of businesses to try to take advantage of it. Many in the advertising industry in particular see protecting privacy from advertisers as potentially destroying much of the internet. Randall Rothenberg, CEO of the Interactive Advertising Bureau, the US advertising industry body, said in August 2017 that the EU's latest proposal for reforming their 'e-Privacy Directive' would

[32] The drive to include DRM into the web browser ecosystem has been running since 2013. In 2017 it caused the Electronic Frontier Foundation, one of the leading civil society internet organisations, to resign from the World Wide Web Consortium ('W3C') – the main international standards organisation for the World Wide Web. See www.eff.org/deeplinks/2017/09/open-letter-w3c-director-ceo-team-and-membership.

'eviscerat[e] the basic business model that has supported journalism for more than 200 years' by allowing people to protect their privacy through the use of ad-blockers and still get access to content.[33] Rothenberg uses journalism as his weapon in this conflict: freedom of speech is a more 'acceptable' argument than the right to make money, particularly if that money is made through the exploitation of people's personal data and the invasion of their privacy.[34]

All this analysis is of course very general and different businesses have very different priorities. Some of the key conflicts over internet regulation have ultimately been about the conflicts between different business sectors and their related lobby groups. Whether Google, Facebook and other intermediaries should be shielded from responsibility for material available through their services where that material *might* breach copyright pitches Silicon Valley against Hollywood, with individual internet users little more than bystanders. What businesses have in common is that their priority – both legally and in practice – is their bottom line. That should not be forgotten, but neither should it be dismissed as mere corporate greed. The internet has grown through economic success as well as technological innovation and people's embrace of the online world. All three elements matter and are intrinsically interlinked. Economic success both drives and is driven by technological innovation – and that innovation is only economically successful if it meets people's needs and desires. For people to get the internet they want, there has to be economic success: shutting out all opportunities to make money will stifle the development of the internet.

1.2.4 The Internet as a Political Platform

In its initial form, the internet was seen as separate from the mundane world of politics – indeed, that separateness was proclaimed boldly. John Perry Barlow's 1996 'Declaration of the Independence of Cyberspace' said:

> We have no elected government, nor are we likely to have one, so I address you with no greater authority than that with which liberty itself always speaks. I declare the global social space we are building to be naturally independent of the tyrannies you seek to impose on us. You have no moral right to rule us, nor do you possess any methods of enforcement we have true reason to fear.[35]

[33] In August 2017. See http://uk.businessinsider.com/european-regulators-are-about-to-kill-the-digital-media-industry-2017-8.
[34] See Chapter 10, p. 257.
[35] The Declaration of Independence of Cyberspace was originally in an email but is now available online in a number of places, including www.eff.org/cyberspace-independence.

As the 'separateness' of the internet from 'real' life has been melting away in so many other ways, so it has with 'real world' politics. Politics has pervaded almost every aspect of the internet, so it is no coincidence that many of the case studies examined in this book are either directly political or have a significant political aspect: the Conservative Party speeches story in Chapter 2, political censorship in Chapter 5, many of the surveillance issues covered in Chapter 7, the trolling of MPs in Chapter 8 and the fake news phenomenon discussed in Chapter 9. Chapter 4, on the myth of neutrality, is deeply political. One of the key conclusions of the book is that the political implications of *everything* we do on and with the internet needs to be considered.

Though they took their time in understanding the possibilities offered by the internet, politicians have now grasped them with both hands. The internet gives them a chance to connect directly with their voters without the interference of the media, avoiding the questioning of journalists, the selectiveness of editors, and any impartiality requirements specified by law. In the UK, the Ofcom Broadcasting Code[36] requires that news is reported with due accuracy and presented with due impartiality.[37] The internet can also enable them to sidestep other laws that might be in place controlling advertising or elections. The Communications Act 2003 S 321 forbids political advertising on broadcast television, replacing it with carefully apportioned 'party political broadcasts' at agreed times. Using social media can allow political material to be made available to millions, targeted much more effectively than traditional media can ever manage.

This latter point is particularly important. All the targeting methods and big data analyses that can be used by businesses are also available and ideally suited for political uses. The kinds of profiling used to identify the potential market for a product can be used to target potential voters. The extent to which this kind of work has already had a significant effect on politics in the UK (and, in particular, on the referendum on leaving the European Union – the Brexit referendum) and in the USA (and, in particular, on the election of Donald Trump) was the subject of considerable analysis at the time of writing, and it is difficult to be certain at this stage. What is clear is that the potential for its influence is immense and that very significant efforts are being put into its use by many people across the political spectrum.

[36] As required by the Communications Act 2003 (as amended) and the Broadcasting Act 1996 (as amended).

[37] The Broadcasting Code is online at www.ofcom.org.uk/tv-radio-and-on-demand/broadcast-codes/broadcast-code.

Social media has many other effects on politics: its potential is only just beginning to be tapped. It can save on costs: it costs nothing to tweet, even if you have millions of followers, whilst advertising in the conventional media is very expensive. It allows people who are not part of the political mainstream to be directly involved in politics. This can be a double-edged sword, as politicians who have become the victims of trolls have discovered. The trolling of female politicians, in particular, discussed in Chapter 8, continues to be especially vile.

Social media allows politicians to work both on a large scale – broadcasting their views to a mass audience directly – and on an intimate scale, having direct conversations with 'ordinary' people, seemingly breaking down the barriers between themselves and their voters. Social media can also provide a counterbalance to an antagonistic and often less than accountable press. As Labour former Deputy Prime Minister John Prescott put it in 2012, 'Twitter has created an important and speedy check on our newspapers – a role the Press Complaints Commission (PCC) failed miserably to fulfil – and finally made press barons accountable to the people.'[38] Prescott had used Twitter this way himself in 2011, after the *Sunday Times* included a quote purportedly by him criticising the then Labour leader Ed Miliband, he was able to extract, via a tweet, a correction and apology from the newspaper within an hour.[39]

Use of social media can work to the advantage of politicians: Donald Trump is the most dramatic example but he is far from alone. It can also have disadvantages beyond that of becoming the victims of trolls. In 2014 Labour Shadow Cabinet member Emily Thornberry resigned after tweeting the picture of a home bedecked with St George's flags and with a white van parked outside. She was accused of snobbery and insulting the people of Rochester, where a by-election was taking place, as well as looking down on patriotism.[40] It is not perhaps coincidental that Emily Thornberry, a woman, was attacked so vehemently. Female MPs are subject to a great deal of attention on social media, much of it highly unpleasant or worse.[41]

As well as the ability to have direct interactions with potential voters, politicians are beginning to take advantage of the analytical and targeting capabilities of social media. The depth and significance of the work of

[38] From May 2012 www.theguardian.com/politics/2012/may/15/life-is-tweet-john-prescott.
[39] See e.g. www.theguardian.com/media/2011/jun/12/sunday-times-apologises-prescott-quote?CMP=Share_iOSApp_Other.
[40] See e.g. www.theguardian.com/politics/2014/nov/20/emily-thornberry-resigns-rochester-tweet-labour-shadow-cabinet?CMP=Share_iOSApp_Other.
[41] See Chapter 8, p. 216.

companies like Cambridge Analytica is yet to be fully evaluated but that they worked with Donald Trump's campaign,[42] with the 'Leave' campaign in the Brexit referendum,[43] and had some involvement in the overturned Kenyan presidential election[44] in 2017 should give pause for thought. The combination of analysis of Facebook data and the delivery and dissemination systems that Facebook, Twitter and the rest of the social media provides is very powerful. The potential for its use for political purposes is clear: how this pans out in reality and whether it is good for democracy is quite another.[45]

Politicians have also become aware of the potential use of social media to invade individuals' privacy. In 2015, when the Labour Party was concerned about people who were not really Labour supporters joining the party in order to participate in their leadership election, they chose to scour the social media postings of members in order to check what might loosely be described as their loyalty. As discussed in Chapter 6, this shows a fundamental misunderstanding of privacy – people do have an expectation of privacy even in what might generally be called 'public' spaces on the internet – as well as a distinctly creepy feeling. It was labelled by some as the 'Labour Purge' with echoes of Stalinism that were distinctly uncomfortable for those on the left in politics.[46] Those feelings of creepiness, though easily dismissed by some as unimportant as they cannot be pinned down as clearly 'wrong', let alone actually illegal, do matter.

As the section above illustrates, what is needed for the internet as a political platform is highly complex. At present, it is only clear that politicians and those behind them are using the potential that the internet provides in a wide variety of ways – and that is without even going into the contentious issue of 'fake news' and the highly controversial story of the Russian use of troll farms and 'troll-bots' on Twitter to influence elections in both the USA and the UK.[47]

[42] The exact nature of the work that Cambridge Analytica did with the Donald Trump campaign was still the subject of discussion and investigation at the time of writing.

[43] The role of Cambridge Analytica in the Brexit campaign has been the subject of an extensive piece of investigative journalism by the Guardian's Carole Cadwalladr. See www.theguardian.com/technology/2017/may/07/the-great-british-brexit-robbery-hijacked-democracy. At the time of writing, this was also subject to legal action by Cambridge Analytica and SCL Elections Limited. See also the work of James Patrick, in Patrick 2017, particularly Chapters 9–11.

[44] For Cambridge Analytica's involvement, see www.bbc.co.uk/news/blogs-trending-40792078. The election was overturned by the Kenyan Supreme Court. See, for example, www.independent.co.uk/news/world/africa/kenya-uhuru-kenyatta-supreme-court-election-win-nullified-president-electoral-irregularities-a7923656.html.

[45] See also Chapter 9, p. 243 and Chapter 10, p. 265.

[46] See e.g. https://paulbernal.wordpress.com/2015/08/27/the-labour-purge-and-social-media-privacy/.

[47] See Chapter 9, pp. 212–213.

That the internet offers opportunities for a better form of democracy has been apparent for a long time. That it is a potential *threat* to democracy has been equally apparent to those who have studied the subject: Morozov about the potential use by authoritarians,[48] Sunstein and Pariser (as well as this author) on the fracturing and polarisation effects and exacerbation of extremism[49] amongst others. The extent to which it might have already undermined democracy remains under both question and investigation. It would be distinctly naïve not to take these issues very seriously. The internet is now a political space and is being used as a political platform: how it should be regulated from a political perspective is critical.

What we as people want from the internet as a political space is neither simple nor easily deliverable. We want freedom of speech – and we want to avoid being bullied or attacked for our own opinions – which means the needs of the internet as a communication medium are paramount. So is privacy, so that we cannot be located and persecuted for our political beliefs or for researching political information. We want access to politically relevant information through as neutral and objective means as possible. We want not to be misled or manipulated by those who seek to influence our opinions or votes, which, as shall be shown, is very hard indeed given our embrace of social networks. We do not want to have the internet 'reined in' by governments which we neither should nor do trust. It is a tall order.

1.2.5 The Internet as a Public Space

One of the issues raised when considering the internet as a political platform is the extent to which it can or should be considered a 'public' space. This underlies many of the other questions discussed in this book. The rights covered here – privacy and free speech in particular – are qualitatively different in a public space than in a private one, though not as simply or baldly as is sometimes thought. People do have both an expectation and a right to *some* privacy in public spaces, for example, but not to the extent that we do in places that we consider to be private. We have more freedom of speech in public in one way (private actors cannot silence us so easily in public) but less in another, as we have to abide by laws on public order, incitement and so forth. In private spaces,

[48] Morozov's *The Net Delusion: How Not to Liberate the World* from 2012 made one aspect of the argument – that the internet was not a force for freedom in relation to authoritarian (or formerly authoritarian) states – very strongly. The evidence in relation to its undermining existing democracies is growing all the time.

[49] See Sunstein 2007, Bernal 2010 and Pariser 2011.

we will generally be expected to abide by the rules of those who own or control them, rules that can vary significantly from place to place.

The problem with the internet is that the boundaries between what is public and what is private have been more than just blurred; they have been all but obliterated. Facebook has more than two billion members and is used as a primary source of news and social interaction, and you can choose whether things are private or not. Twitter's privacy policy says that a tweet 'is public by default'.[50] People appear to treat both Twitter and much of Facebook as essentially public spaces – including for political debate – and yet they are privately owned and run, according to their own rules and standards.[51]

Moreover, social media such as Facebook and Twitter are international and the 'spaces' that people spend time in are not geographically constrained: a discussion on Twitter may well involve people from many states at the same time. The extent to which the laws of any particular state apply to that discussion can be an area of contention, not just in terms of whether they can apply but whether they should apply, and whether and how they could or should be enforced if they do. This is not a new discussion: how to regulate a seemingly borderless internet has been central to the theoretical arguments amongst academics and others almost since the inception of the internet. The growth of the social media and the increasing use of the internet as a business platform and, in particular, a political platform has given these theoretical discussions much more pertinence. Governments are now both more conscious of the issues and bolder in their attempts to apply their laws and standards to the internet. The pushes to rein in the social media (and the internet in general) that come from governments all over the world, from the most authoritarian to the most seemingly liberal and democratic, are regular and powerful. Given the key role that the internet now plays in politics, the motivations behind those pushes need to be examined very carefully.

How internet companies in general, and social media companies in particular, respond to these moves from governments is one of the key questions in relation to the regulation of the internet in the current era, and the internet companies know it. Sometimes they portray themselves as serving the public good – as champions of free speech, as guardians of people's privacy, as providers of public services – but when the regulation that would usually accompany their being providers of public services is suggested, they remain staunchly private businesses. The methods and

[50] www.twitter.com/en/privacy.
[51] Facebook's 'community standards' (https://en-gb.facebook.com/communitystandards) and Twitter's 'rules' (https://support.twitter.com/articles/18311).

algorithms they use are claimed to be 'trade secrets' that should not be subject to detailed scrutiny.

The way that various internet intermediaries (both search engines and social networks) have been involved in the fake news furore has added to the pressure. Are they helping to undermine democracy itself? What they could or should do about it is the subject of analysis in Chapter 9. Whether they can do anything about it at all without fundamentally changing both their technology and their business models is a question that has not to date been satisfactorily answered. In the last two chapters of this book, suggestions will be made as to how things could be improved – but this, like so much that is dealt with here, is not something that can be easily solved.

1.2.6 The Internet as Integral to Society

So, the internet is an information resource, a communications medium, a business platform, a political platform and a public space – and all at the same time, using the same services and systems, even within the same conversations and interactions. It is where people converse and socialise, where they organise their 'offline' lives, where they find jobs and romance, where they shop, where they find entertainment. Government services are increasingly available only through the internet, and businesses give you better prices and better services if you access them online. More and more people watch television and listen to the radio through the internet. Their televisions are themselves connected to the internet. Cars are connected to the internet. Heating systems, coffee machines, fridges and even fish tanks[52] are connected to the internet. The number and variety of devices in the so-called 'Internet of things' is growing all the time.

The internet is now integral to the way our society operates. Almost every activity has an online element, whether it is that events are organised through Facebook or that support is provided via online chat. A plethora of specialist communities exist primarily online, from football teams' fan clubs to those who keep particular species of tortoise. To exclude yourself from the internet is to put yourself at a massive disadvantage in all kinds of ways. In most rich countries, this means that few people do exclude themselves, notwithstanding the issue of access for the old and for disabled people and people living in remote areas. It is no longer credible to treat the internet as an optional extra or as separate from the 'real' world.

[52] In July 2017 a casino was hacked through its 'smart' internet-connected fish tank. http://money.cnn.com/2017/07/19/technology/fish-tank-hack-darktrace/index.html.

1.3 The Internet and Law

That in turn has important implications for how law applies on the internet. If the internet is integral to how society works then laws that apply to how society works have to apply somehow online. Conduct that is considered unacceptable offline should be unacceptable online and conduct that is *illegal* offline should be *illegal* online. Though that might appear to be obvious, it goes against some of the history of law on the internet. To see how, it is necessary to understand at least some of the early history of internet legal theory.

1.3.1 Cyberpaternalism and Cyberlibertarianism

John Perry Barlow brought the question of internet regulation into focus with his Declaration of Independence of Cyberspace in 1996, as mentioned above. It was a bold statement that effectively represented the thoughts of many of the people who spent significant amounts of time online. The internet in 1996 was very different from the internet two decades later. The population of what Barlow called Cyberspace was a much more homogeneous group than today: largely white, largely male, young(ish), geeky and predominantly American and with a strong libertarian and free-speech background, Barlow's declaration struck a chord that resonated for many years. To some degree it resonates still. A school of thought followed from it: the cyberlibertarians. The essence of the argument was that 'earth-bound' laws should not apply in cyberspace – and could not work in cyberspace. Both the moral and the practical arguments mattered. As Barlow put it: 'You have no moral right to rule us nor do you possess any methods of enforcement we have true reason to fear.'[53] At the time, it seemed a bold statement but not entirely unsustainable. Two US law professors, David Johnson and David Post, turned it from polemic into scholarship with an influential paper, 'Law and Borders: The Rise of Law in Cyberspace',[54] effectively arguing that the ability of people 'in' cyberspace to move freely over borders and between different jurisdictions, effective regulation was impossible – people could choose which regime to operate in, a form of regulatory arbitrage.[55] Johnson and Post (and many others) were arguing for a new form of law for the new internet community, independent and separate from the material world.

Attractive as it seemed, and well-argued as the case was, there were fundamental flaws in the cyberlibertarian argument. As Reed pointed out,

[53] www.eff.org/cyberspace-independence. [54] Johnson and Post 1996.
[55] See also Froomkin 1997.

https://doi.org/10.1017/9781108381161.002 Published online by Cambridge University Press

setting out what he called the 'cyberspace fallacy',[56] though a person's online identity may operate outside borders, their physical body exists in a physical place where a real-world government holds power. Even if enforcement online were impossible, governments could take hold of the physical person. Further, as Sunstein noted, even in 1996 there was no single coherent and cohesive 'internet community' with common standards and beliefs, but a series of very different communities with a wide range of different beliefs – the nature of online activity was, in Sunstein's view, likely to isolate, divide and polarise.[57] Events in more recent years made this observation particularly poignant.

These fairly fundamental flaws notwithstanding, cyberlibertarianism still has many adherents. There are many more who support at least some of the overall philosophy and who want to resist the continued attempts by governments of all flavours to take more control over the internet. It is not necessary to be an extreme cyberlibertarian to see the dangers to free speech presented by governmental censorship of the internet (see Chapter 5) or surveillance (see Chapter 7). Conversely, some of the activities that have developed on the internet, from the distribution of child abuse imagery to networks of extremist material, cyberbullying, hate speech and much more – and the integration of the internet into almost all elements of our life – make it impossible for governments not to become involved. If the internet is riven with lawlessness, so is our society: the two cannot be treated separately.

The school of cyberpaternalism arose in direct response to the cyberlibertarians, in part using this kind of logic. Just as the cyberlibertarian argument had both a moral and a practical aspect, so did the cyberpaternalist. Essentially, the argument was not only that lawmakers could apply their laws online but that they *should* apply their laws online. The 'could' part of the argument was, in the eyes of cyberpaternalist scholars Joel Reidenberg (in *Lex Informatica*[58]) and Laurence Lessig (in his seminal text, *Code and Other Laws of Cyberspace*[59]), one that could be solved technologically. The 'architecture' of the internet could be, should be – and *was* – a tool of regulation, not a barrier to it. For the cyberpaternalists, the key was who should take control of those tools and to what end. This was, for Lessig in particular, critical: 'We can build, or architect, or code cyberspace to protect values that we believe are fundamental. Or we can build, or architect, or code cyberspace to allow these values to disappear. There is no middle ground.'[60] Governments should,

[56] Reed 2004, pp. 174–175. [57] In Sunstein 2001, further developed in Sunstein 2007.
[58] Reidenberg 1998.
[59] Originally in Lessig 1999, developed extensively in Lessig 2006. [60] Lessig 2006, p. 6.

according to this logic, intervene at the code level – effectively ordering those who create and run the internet to build-in their 'values'. As shall be seen, particularly when looking at both censorship and surveillance in Chapters 5 and 7, governments have taken this idea on board in recent years very strongly. The results have not been uniformly good, to say the least. Governments around the world have tried to impose their laws on the internet, paying almost no attention to the arguments of the cyberlibertarians. Some have chosen to embrace code as their way to do so, with website blocking and filter-based censorship and a wide variety of technical methods for surveillance. The problems lie in a number of directions, starting from the idea that it is a government's job to impose values at all. Which values? Whose values? The idea itself has a distinct air of authoritarianism to it – which is part of the reason that working at this level and in this way has proved distinctly attractive to the more authoritarian of governments. The so-called 'Great Firewall of China' is just one example amongst many.[61] There is a burgeoning worldwide market in surveillance technology, whilst 'content filtering' and other methods of what amount to code-based censorship is being implemented for many different reasons from fighting extremism and piracy to 'protecting' children from 'adult' content.[62]

Even more important is the question of the objective of the regulation. What kind of an internet are the regulators trying to create? As has already been discussed there are many ways of looking at it. Do regulators want the internet to work perfectly as an information resource? As a communications medium? As a business platform? As a place for political debate? As a public space? The needs of each are both theoretically and practically different. Make the internet work perfectly for business, and individuals' privacy and freedom of speech are stifled. Prioritise free speech and the net will work far less effectively as a reliable information resource. Optimise it for honest and informative political debate and business freedom is restricted. Governments have very different priorities and often those are directly at odds with the needs of either their citizens or the businesses that operate in their territories, let alone those of others around the world. For businesses that wish to operate globally, operating according to all the standards of all the countries they operate in means applying vastly different standards around the world and being accused of hypocrisy and cynicism by those with different standards – perhaps fairly, when

[61] See Chapters 5 and 7 on free speech and surveillance respectively for a discussion of the use of censorship and surveillance by authoritarian states.
[62] See Chapter 5, particularly pp. 128–133.

they claim to be champions of freedom of speech in the USA but block blasphemy in Pakistan.[63]

There are very few issues that do manage to provide a consensus – abhorrence of child abuse imagery is perhaps the best example, though even that does not quite manage to generate unanimity.[64] For almost everything else there are varying degrees of disagreement between states – and between governments and those within their states. Attitudes to such things as hate speech and blasphemy, or the extent to which police forces should have access to people's private information, are not generally agreed upon at all. Nor are seemingly simpler questions such as what 'net neutrality' means, what would constitute 'fair use' for copyrighted material or how to deal with obscenity.

1.3.2 Symbiotic Regulation and Network Communitarianism

From a regulatory standpoint, another school of regulation seems much more appropriate than the two extremes of cyberlibertarianism and cyberpaternalism: the less well-known but more nuanced idea of network communitarianism, and the mechanism through which it works: symbiotic regulation. Rather than viewing people online as a coherent self-governing community (as in cyberlibertarianism) or as a group of pathetic dots[65] to be governed through code by wise governments (as in cyberpaternalism), network communitarianism views the online community as a complex, dynamic and constantly changing group. Regulating this community is similarly complex but largely best done through relatively small 'tweaks' to existing relationships, and constantly monitoring the reactions. As Andrew Murray, the developer of the theory, puts it:

> Regulation is a process of discourse and dialogue between the individual and society. Sometimes society, either directly through the application of norms, or indirectly by distilling its opinions, norms or standards down to laws, wishes to force a change in behaviour of the individual. But, sometimes it is the regulatory settlement itself which is challenged by society when there is no longer any support for it.[66]

[63] In March 2017, for example, after meeting with Pakistani government officials, Facebook blocked 85 per cent of supposedly blasphemous content in Pakistan (see e.g. www.dailymail.co.uk/sciencetech/article-4357694/Pakistan-says-Facebook-vows-tackle-concerns-blasphemous-content.html).

[64] See pp. 128–133 in Chapter 5. The USA stands apart from most of the world in that it allows child abuse pseudo-imagery, for example.

[65] Lessig's term for the individual on the internet, a pathetic dot being worked on by four modalities of regulation: law, markets, norms and architecture.

[66] Murray 2016, p. 74.

The regulated can push back against the regulation and against the regulators. This understanding of regulation fits the messy, unruly, complex, interlinked and dynamic environment that is the internet. It fits with the way that when something is done that has an effect upon privacy, it also has an effect on freedom of expression and truth, and that there are often unforeseen and unpredicted consequences that need to be adjusted for, or even that are so significant that they overwhelm the intended consequences. This can be seen in the examples throughout this book, from 'porn-filtering' to the disaster that was the Samaritans Radar.[67]

This subtler and more nuanced form of regulation does not fit so easily with the simpler ideas that are common in politics and the media. That may be the biggest problem of all. Complexity does not go down well in politics. Nuanced messages and ideas that are counterintuitive are difficult to sell. The simplistic approaches to regulation and law that are put forward often by those who do not understand either the technology or the internet communities which would be subjected to them, on the other hand, work well in the media and in politics.[68]

1.4 An Unruly Internet

What works for the media or the cut and thrust of politics is often highly unsuitable for the internet or for people, businesses and others for whom the internet has become crucial. As the case studies throughout this book demonstrate, sound-bite approaches to regulation often either do not work or have such serious side effects or unforeseen consequences that whether they work or not does not really matter.

Poorly conceived laws fail to produce the results they intend. Supposedly anti-troll laws get a few convictions but fail to slow, let alone reverse, the trend in trolling, whilst being used inappropriately for cases that make the prosecutors look foolish or the country look authoritarian.[69] Business models designed without understanding the complexity of issues and rights can fail, sometimes dramatically: the Samaritans Radar case study in Chapter 6 is just one example. Surveillance laws created without a proper understanding either of the technology or of the relevant rights get thrown out by the courts when challenged by small but savvy individuals and groups. The Data

[67] The central case study in Chapter 6.

[68] The Dunning–Kruger effect comes into play here: the tendency for those who don't understand something to underestimate their lack of understanding and to be unwilling to admit to their lack of understanding, even to themselves. See Dunning 2005.

[69] The Twitter Joke Trial (Chambers vs DPP [2012] EWHC 2157) is perhaps the most direct example. See Chapter 8, p. 216.

Retention Directive was invalidated after intervention from a small Irish NGO;[70] Digital Rights Ireland and the Safe Harbour agreement was thrown out after the action of Max Schrems,[71] an Austrian student and activist. A significant change in the operation of Google's search was forced by an obscure Spanish businessman through the controversial 'Google Spain' case[72] – primarily because individuals' privacy rights were not taken sufficiently seriously. The ongoing 'war on encryption'[73] is doomed to failure one way or another, regardless of how aggressively governments pursue it: it is a Canute-like fight against reality based on a simplistic misunderstanding of how the technology works. Much of this could be avoidable if those involved cared sufficiently about the actual results rather than how they appear in the media and political spheres.

A more nuanced understanding is required if these kinds of problems are to be avoided. The starting point is to face up to the real nature of the internet and of our desires for it. Not all of the conflicting desires for the internet can be met at the same time: many of the conflicts are not resolvable. There are always unforeseen consequences and side effects. The three key issues of this book, free speech, privacy and truth, are linked in such a way that measures to address problems in one will have implications for the others. The internet really is a mess, and that needs to be faced up to and accepted. There is no simple, clean and perfect future that can be reached – just a constantly changing mess. The best that can be hoped for is to find a messy way through, finding balances and compromises in a flexible and dynamic way, adapting and changing as technology develops, as the uses of the technology develops and as our understanding of the technology changes. That is why the regulatory approach suggested above – community-based symbiotic regulation – is the best way to go about it.

The starting point for all of this is to have a more honest examination of the internet itself – a more *warts and all* examination. So much of our regulatory action has been based on misunderstanding and myth that even if it had been better-intentioned and better-performed it would have failed to achieve its objectives. The next chapters of this book look at three of the biggest of the myths and illusions held about the internet. They are

[70] At the CJEU in Joined Cases C-293/12 and 594/12 Digital Rights Ireland Ltd and Seitlinger and others – see p. 188.

[71] At the CJEU in Case C-362/14 Maximillian Schrems v Data Protection Commissioner – see Chapter 7, p. 181.

[72] At the CJEU in Case C-131/12 Google Spain SL, Google Inc. v Agencia Española de Protección de Datos, Mario Costeja González. Costeja González at least wanted *some* obscurity. See Chapter 2, pp. 36–43, for a full discussion of this distinctly controversial case.

[73] See Chapter 7, pp. 165–167.

not really separate myths but are interlinked not just in practice but in theory, and based directly on the way that the internet has grown over the years – on both the technology and the business models of the big companies and others that have come to dominate the internet in recent years. None of the myths is necessarily believed directly – as the chapters will show, they do not survive close scrutiny – but people and businesses often seem to act as though they believe them.

The first, in Chapter 2 is the myth of permanence – that once something is on the internet, it is there forever. The normative version of this is that once something is on the internet it *should* be there forever – based on the idea of the net as a historical archive, that deletion (or forcing deletion) of something from the internet is tantamount to Stalinesque removal of non-persons from the historical record. The second, in Chapter 3, is the myth of perfection – which we all know is not true really, but is still in our thoughts when we object to the alteration of records to correct for errors or misconceptions, or the alteration of search results to reduce access to old or irrelevant material. If we do not see the record as perfect, why do we object so vehemently to its manipulation? The third, in Chapter 4, is the myth of neutrality – that it is possible and desirable for both people and algorithms to act from a neutral, objective point of view. Many claim to be neutral – from Wikipedia editors' 'five pillars' to Google's 'organic' search algorithms – and from that claim a kind of moral high ground or immunity from legal or other scrutiny. None of it is true: people are always biased, and algorithms embed the biases of those who create them, either consciously or subconsciously.

These three chapters take on the myths one by one, but they need to be considered together as well. In many ways, they are parts of the same myth – the same illusion about the nature of the internet. It is an illusion related to the original dreams of the cyberlibertarians of some kind of a perfect 'space' without the flaws and the problems of our messy earthbound world. The internet is not like that – it is more like the child in poet Philip Larkin's *This Be The Verse*.[74] The internet has our human flaws – our *warts*, from misunderstandings, anger, hate, greed and selfishness to terrorism and extremism – and has added some more of its own.

The problems that we need to deal with are not so much the visible warts but what lies beneath the surface and causes those warts to erupt.

[74] *They fuck you up, your mum and dad.*
They may not mean to, but they do.
They fill you with the faults they had
And add some extra, just for you.

Many of those warts – trolling and fake news in particular – are in practice the inevitable results of the business models and practices of the internet giants and, in particular, Facebook, Google and Twitter. Unless we at least start to understand and address this, all of our efforts will be in vain.

Others of the warts – terrorism and extremism are the most dramatic examples – are in essence societal issues of which the internet activity is just a manifestation and, in relation to the underlying issues, to some extent a distraction. Whilst it may be true that Facebook and Google 'don't do enough' to address their role in it, once again that role is misunderstood and the focus is on the surface warts rather than the underlying malaise. It is not that they do not do enough to deal with issues like extremism, but that they do far too much: as shall be seen in Chapters 8 and 9 in particular, their business models and data practices can encourage and exacerbate extremism – and that is without even considering the growing spectre of political interference through the internet. The problem is that it is sometimes difficult to distinguish between different kinds of wart. Some are ugly. Some are cancerous. Some are both. Some need to be removed – whilst for others, attempting removal will cause great damage and leave awful scars. Some cannot ever be removed at all.

That does not mean that the internet is irredeemably disastrous but that it has to be accepted for what it is, and not for what we dream that it might be. The messiness of the internet – its unruly nature – is something that, rather than trying to completely iron out, we could embrace. The unruly nature is the strength of the internet and something to be harnessed rather than feared. Embracing the creative chaos is hard both theoretically and practically – lawyers and businesses in particular tend to prefer certainty and predictability – but it is also necessary. Trying to achieve more certainty and clarity can often produce exactly the opposite. Accepting the mess may ultimately make things less messy.

Accepting the mess does not mean accepting the unacceptable, and there are many things that happen on the internet that really are unacceptable. Advocates of privacy need to understand, for example, that the problems of terrorism, child abuse and other serious crime do need to be addressed. Similarly, advocates of freedom of speech need to understand that the abuse on some online forums reach unacceptable levels – and that a 'shout-'em-down' free-for-all does not constitute the perfect marketplace of ideas – whilst political debate is better served if it is at least partially possible to tell truth from falsehood. Free speech, privacy and truth are all important ideas – and though it must be accepted that there are no perfect versions of any of them, striving to do our best to support them is something worth aiming for.