1

Internet privacy rights

1 Introduction

Privacy on the internet has gone from being a subject of interest only to what might loosely be described as 'geeks' and 'nerds' to something that is of relevance to almost everyone. The internet is huge business. Facebook has more than a billion users worldwide.[1] Apple, whose products are almost all internet based – the 'i' in 'iMac', which led to the 'i' in iPod, iPhone and iPad, originally stood for 'internet'[2] – and Google are two of the world's three biggest corporations.[3] For all of these organisations, privacy has become increasingly important. Data breaches have started to become front-page news. Privacy policies and practices are now taken far more seriously; whenever Mark Zuckerberg announces a new product or service for Facebook, he makes privacy one of the key things that he talks about.[4] The authorities, too, are taking privacy more seriously: in the United States, for example, Google and Facebook have been made subject to Federal Trade Commission (FTC) privacy audits for twenty years, and Twitter for ten.[5]

Why has privacy become such a big issue? Do we need a new approach to understanding it? These are questions that have been coming more and more to the fore. Amongst other things, this book attempts to explain

[1] Facebook passed 1 billion active users in October 2012: see their press release at http://newsroom.fb.com/News/457/One-Billion-People-on-Facebook.

[2] When Steve Jobs first introduced the iMac in 1998, he said 'iMac comes from the marriage of the excitement of the Internet with the simplicity of Macintosh'.

[3] See for example http://online.wsj.com/article/SB10001424127887323539804578264024260588396.html. In January 2013, in terms of market capitalisation Apple was the second largest and Google the third largest corporation in the world.

[4] When launching Graph Search in January 2013, Zuckerberg said 'We've built Graph Search from the start with privacy in mind, and it respects the privacy and audience of each piece of content on Facebook.' See http://newsroom.fb.com/News/562/Introducing-Graph-Search-Beta.

[5] For Facebook see www.ftc.gov/opa/2011/11/privacysettlement.shtm, for Google see www.ftc.gov/opa/2011/10/buzz.shtm, for Twitter see www.ftc.gov/opa/2011/03/twitter.shtm.

why and to suggest a way forward. The key to that approach is an understanding that the key reason that privacy has become important is that privacy matters to people, at least in part, because people care about their autonomy, and privacy is a crucial protector of autonomy.

When people care about something, ultimately that finds its way into how businesses react, and how governments react. That is why both businesses and governments are beginning to take privacy seriously. As the case studies in this book reveal, however, that process is taking a long time, and there has been a lot of pain and misunderstanding along the way. The ideas presented in this book are intended to help to reduce that time, and to minimise the pain and misunderstanding. The starting point to that is to have a better understanding of the role that the internet plays in people's lives. From there we can start to understand what people expect from the internet, and what they believe their *rights* should be while they operate on the internet.

1.1 The internet in contemporary life

For most people in what might loosely be described as the developed world the internet can no longer be considered an optional extra, but an intrinsic part of life in a modern, developed society. Significant aspects of life take place on the internet. Interactions with government, for example, are becoming increasingly electronic, not only in terms of access to information but more directly and interactively: the completion of tax returns, access to health services,[6] interaction with local government, and much more. Indeed, the UK government is moving to a 'digital by default' policy.[7] The digital economy has already become a significant part of the economy as a whole, and this is increasing all the time. In the UK, it is predicted that by 2016, 23 per cent of all purchases in this country will be made online.[8] It is increasingly the case that people who are not able to access products and services online are at a significant disadvantage, being unable to take advantages of discounts for insurance,[9] better interest rates

[6] See www.nhsdirect.nhs.uk/. NHS Direct is suggested as the first port of call for health problems in the UK.

[7] See http://digital.cabinetoffice.gov.uk/about/ – Digital by Default is central to the UK government digital strategy.

[8] See www.bcgperspectives.com/content/articles/media_entertainment_strategic_planning_4_2_trillion_opportunity_internet_economy_g20/.

[9] Aviva insurance, for example, in February 2012, was offering a 20 per cent discount for online applications for car insurance. See www.aviva.co.uk/car-insurance/.

on savings,[10] and having tighter deadlines for the submission of information, for example.[11] Moreover, there are some very useful services that are only available online, such as price comparison sites for insurance and other financial services.[12] Shopping has been revolutionised, from specialised online services such as Amazon and auction sites such as eBay to the online versions of existing supermarkets, allowing ordering online and delivery to your home.[13]

All this is without considering the most direct, 'traditional' uses of the internet, as an unparalleled source of information, for educational or recreational purposes, as an increasingly important news source,[14] or simply to discover practical information such as the location and opening hours of shops, events and so forth.

Perhaps even more important is not the extent to which a capacity to use the internet is now required but the reality of how much it is used in practice. The numerous sites and services noted above are only a small part of what has become a significant element of life. There are many others that have become part of the social fabric for a large section of society. Social networking sites are just one example. They cannot generally be said to be either practically necessary or economically advantageous but they are used, extensively and increasingly, and not just by young people. The same can be said of a whole range of other services, from message boards and blogs to media services such as YouTube.

Further, the internet is no longer something that is only to be accessed through computers. More and more devices can and do use or provide a connection to the internet, from smartphones and tablet devices to Blu-ray players, TV receivers, game machines and digital cameras. This trend appears certain to increase, and increase rapidly,

[10] Most UK banks offer 'e-savings' accounts or equivalents, only accessible online, offering better interest rates or other advantages.

[11] UK tax returns submitted on paper, for example, are required to be submitted by 31 October each year, while online submissions are allowed until 31 January the following year. See www.hmrc.gov.uk/sa/deadlines-penalties.htm.

[12] E.g. www.gocompare.com/, www.confused.com/, www.comparethemarket.com/.

[13] See www.amazon.com or www.amazon.co.uk, www.ebay.com and, for example, www.sainsburys.co.uk/home or www.tesco.com/ for online stores of supermarkets.

[14] In the 2008 US election, for example, the Internet was one of the most important sources of news for voters, particularly for young people. Pew Internet Research reported that '42% of those ages 18 to 29 say they regularly learn about the campaign from the internet, the highest percentage for any news source'. See http://people-press.org/report/384/internets-broader-role-in-campaign-2008.

as the advantages of using internet connections for all kinds of devices become more apparent, and more innovative ideas such as Google's Glass[15] are developed.

The ultimate implication of this is that living without using the internet places people at a significant disadvantage in many different ways, including socially, culturally, democratically and financially. The concept of a 'digital divide', or more accurately 'digital divides',[16] between those who have the skills and opportunities to take advantage of digital services and those who don't, has been discussed since the 1990s – see for example the work of Norris (2001) and Mossberger (Mossberger *et al*., 2003). The nature of the relevant divides has changed considerably over the last decade, as the role that the internet plays in society has become more significant, as outlined above, and access to it has become the norm rather than the exception. The disadvantages to those who do not have internet access are continuing to grow both in scale and breadth, which is one of the reasons why there are increasing calls to consider access to the internet a 'right'.

The idea of internet access as a basic human right has been put forward by many, and according to a large survey by the BBC World Service, nearly 80 per cent of people around the world believe that it should be.[17] In Estonia,[18] France[19] and Greece,[20] for example, internet access has already been made a constitutional right, while in Finland this right has become

[15] Google Glass is a headset designed to be worn like glasses, 'reading' what you see and providing a 'heads-up display' of relevant data before your eyes. See www.google.com/glass/start/.

[16] Divides between rich and poor nations, between the rich and the poor within nations, between the better and worse educated, between the urban and the rural, divides based on gender, disability, race and more – there are many possible reasons for what might be termed digital disadvantage. Mossberger also identifies different aspects of the divides – what she terms the 'access divide', the 'skills divide', the 'economic opportunity divide' and the 'democratic divide', paralleling some of the discussion in this chapter. See Mossberger, Tolbert and Stansbury (2003, particularly p. 9).

[17] http://news.bbc.co.uk/1/shared/bsp/hi/pdfs/08_03_10_BBC_internet_poll.pdf. The survey included more than 27,000 people in twenty-six countries.

[18] See http://news.bbc.co.uk/1/hi/world/europe/3603943.stm.

[19] See for example www.dailymail.co.uk/news/worldnews/article-1192359/Internet-access-fundamental-human-right-rules-French-court.html?ITO=1490.

[20] Article 5A, paragraph 2 of the Constitution of Greece states that 'All persons are entitled to participate in the Information Society. Facilitation of access to electronically handled information, as well as of the production, exchange and diffusion thereof constitutes an obligation of the State.' See for example www.unhcr.org/refworld/docid/4c52794f2.html.

legally enforceable.[21] The EU Telecoms Reform Package agreed in 2009 supports high-speed access for 'all citizens' throughout the EU.[22]

In the UK, surveys suggest the same. In 2009, a survey for the Communications Consumer Panel showed that '84 per cent of people agreed that it should be possible for everyone in the UK to have broadband at home, regardless of where they live. Many people already see broadband as essential and even more believe that soon it will be essential for everyone.' As Communications Consumer Panel Chair Anna Bradley put it:

> The tipping point will be when broadband does not just provide an advantage to people who have it, but disadvantages people who do not. Interestingly some people already feel disadvantaged: those who live in not-spots and those who have school-age children but do not have broadband at home.[23]

The idea that internet access could be a human right is debatable. Vint Cerf, for example, one of the 'fathers of the internet', has suggested that it is not.[24] The nature and scale of the discussion over this issue, however, and the reality of the way that the internet is used in practice do suggest that at the very least an inability to access the internet puts people at a significant disadvantage. To be able to participate fully in contemporary life, people need internet access, and so to participate freely in that life, people need the opportunity to act freely on the internet.

1.2 Data and the internet

The internet offers hitherto unheard-of opportunities to gather, analyse, use and store personal data, and it has become the focus of efforts to do all of this.[25] The case studies in Chapters 5 to 7 reveal just some of the ways in which this is already happening, and give at least some idea of how this could develop into the future.

[21] See for example www.bbc.co.uk/news/10461048. Finland not only made internet access a legal right, but specified a minimum speed of access of 1Mbps.

[22] See http://europa.eu/rapid/pressReleasesAction.do?reference=MEMO/09/491.

[23] www.communicationsconsumerpanel.org.uk/press-releases/press-releases/post/173-soon-it-will-be-essential-for-everyone-to-have-broadband.

[24] See for example www.nytimes.com/2012/01/05/opinion/internet-access-is-not-a-human-right.html?_r=0.

[25] Each of Cate's four principles for data growth, set out in Cate (1997, pp. 13–16), applies directly to the Internet. His fourth principle in particular refers to the impact of computer networks.

The nature of the internet makes manipulation of the lives of individuals through the use of personal data particularly easy. The ways in which this can work are analysed throughout the book and specifically in Chapter 3, where a model describing the current functions of the internet is set out, and its implications explored, including some of the direct and indirect ways that individuals' autonomy can be threatened. This model, the Symbiotic Web, suggests that there is a symbiotic relationship between the individuals who use the internet, and are reliant on 'free' sites and services, and the businesses that provide those services and which have built business models dependent on their ability to gather and process personal data from those individuals.

It is becoming increasingly difficult to separate 'online' and 'offline' data. As the internet becomes more and more integrated into 'real' life, online and offline data become commixed. To take one example, one of the largest types of data gathered in the 'real' world is that gathered by supermarkets for their loyalty schemes, such as the Tesco Clubcard and the Nectar service operated by Sainsbury's, BP and others. Though initially this data is gathered and used in relation to 'real-world' shopping, it now includes the shopping done online, and it is held in such a way that it can be accessed online and used online. The data itself has become online data.

Even data held by corporations or government departments on 'private' computers or networks is also becoming part of the 'online' world, as those networks are using 'public' infrastructure or running on 'virtual private networks' on the internet, with the same computers being used to gather, hold and access the data that are also used to access the internet. Separation and isolation of computers from the internet is increasingly uncommon and likely to become more so. Added to that, data gathered offline may be (and is likely to increasingly be) integrated and aggregated with other data, much of which is gathered online, and the results are then stored and used online.

The concepts of an 'internet of things' and 'augmented reality' take the integration between the online and offline worlds further steps forward. The 'internet of things' refers to the way that more and more 'real' objects have an online 'presence' through chips (and particularly RFID chips) built into them, allowing them to be mapped, tracked, inventoried and so forth,[26]

[26] The term 'internet of things' may have been coined by Kevin Ashton in 1999, though it is now of common usage. See Ashton's article in *RFID Journal* in 2009 'That "Internet of Things" Thing', accessible at www.rfidjournal.com/article/view/4986.

while 'augmented reality' refers to the use of digital information to supplement 'real' information in heads-up displays in aeroplanes and cars, providing assistance for pilots and drivers, or in mapping applications for smartphones, for example. The use of augmented reality in smartphones in particular – taking advantage of the geo-location systems built into such phones – is already relatively widespread.[27] With the increasing prevalence of smartphones, augmented reality might be expected to become more common. Google Glass takes this to the next logical stage, with the possibility of an always-on camera, always-on geo-location and a constant stream of data in both directions, integrating pretty much your entire life with the internet.

Finally, the internet introduces new levels of vulnerability and new ways in which private data, once it has been gathered, stolen or otherwise acquired, appropriately or inappropriately, may be loosed upon the world. The most graphic examples of this involve leaks such as those performed by WikiLeaks, but there are many more insidious and less dramatic ways in which this happens. This is an issue that is not going to disappear: quite the opposite, it can only be expected to grow.

1.3 Underlying questions and a paradigm shift

One of the underlying questions in this book is how 'public' is the internet? Should the internet, or some significant part of it, be considered a 'public space' and if so, what does that imply? If the answer to this question is 'yes', as this book contends, then the implications are considerable, not just for the rights of individuals as they browse the web or use internet-based services, but for the obligations of those providing or hosting websites or offering internet-based services.

How 'public' the internet should be considered is a complex question, and one that cannot easily be answered using what might be termed 'old-style' rules. It raises numerous issues: what is cyberspace, and what is the internet? Is it simply a collection of connected private spaces, each owned and governed by the people who run the websites concerned? In practice, the vast majority of the internet is owned and run privately. So should the web be considered something effectively private, with browsers having to follow whatever rules the web owner sets, particularly in terms of privacy? Or is it a public space, and governed by public rules, public

[27] By June 2013 the number of augmented reality apps available through the iTunes Store was in the thousands.

norms and so forth, with people having an expectation that they should have certain rights, and that those rights will be respected as they browse the internet?

The implication of the suggestion that the internet is now an intrinsic part of contemporary life is that it should, in certain ways, be considered public, and that people who use it should be able to rely on their rights being respected. This is already true to an extent in terms of commerce – commercial law including contract law applies to commercial transactions that take place over the internet – and issues such as copyright, defamation, pornography and so forth. Though there are complications, jurisdictional issues and so forth, the principles in all these areas are clear. Despite the declarations of independence of cyberspace from Barlow onwards,[28] law has been applied to online life, with varying degrees of success, in many different ways.

This leads to the conclusion that we must consider the internet to be to a significant extent a public space and that rights are applied to the internet as a consequence. If we as people have the *need* to use the internet, and the *right* to use the internet, we should have appropriate protections and rights *when* we use the internet.

This brings up the question of which parts of the internet should be considered public and which private, and hence what kinds of right (and in particular what degree of privacy) someone using those parts can reasonably expect. The principle answer, this book suggests, is that the default position, the assumption, should be that everywhere on the internet should be considered public unless there is a compelling reason to the contrary.

A second underlying question concerns the personal data itself: to what extent is personal data 'ours'? And, behind that question is the question of what actually counts as 'personal' data. Opinion, law and practice produce a wide variety of potential answers to both of these questions. In countries such as the United States few forms of data are considered personal enough that an individual has any rights over them at all, while the data protection regimes in Europe effectively consider any data that can be directly linked to an individual as 'personal'. The issue of what rights an individual has concerning data held 'about' them is another central

[28] Barlow's famous 'Declaration of the Independence of Cyberspace', found at https://projects.eff.org/~barlow/Declaration-Final.html, was made in 1996, but there have been similar claims made subsequently over the years, right up to the claims by the hacker group Anonymous in 2010. See www.youtube.com/watch?v=gbqC8BnvVHQ.

theme, and one of the conclusions drawn is that more rights are needed in order to give individuals more control, and hence more autonomy.

If the answers to these underlying questions are as suggested, what is required is a paradigm shift in attitudes to privacy on the internet, and to data privacy in general. In a private place, individuals control their own 'privacy settings', while in a public place individuals do not, and hence require protection through privacy rights.[29] The default position needs to shift from one where privacy is the exception to one where privacy is the general rule. Surveillance on the net should not be *assumed* to be acceptable, and neither should the gathering, processing or holding of personal data. At present, unless an objection is made, it appears that surveillance can and does happen, without the knowledge or consent of the individual, and that data can be and is gathered, processed and held, similarly without the knowledge or consent of the individual. The opposite needs to become the case: those who want to monitor people and those who desire to gather, use or hold data about people should need to justify that monitoring, that data gathering, use or holding. If they cannot justify it, or if their justification is inadequate or inappropriate, they should not be able to perform that monitoring or data gathering, and they should not be able to use or hold that data. The privacy rights suggested here are designed to support and enable that paradigm shift.

1.4 Autonomy as the prime concern

This book takes an essentially liberal perspective that takes autonomy as its prime concern. What is meant by autonomy in the context of this book is examined in depth in Chapter 2, but the essence is relatively simple. The approach is drawn primarily from Raz's conception of autonomy, describing an autonomous person as one who 'is a (part) author of his own life' (Raz, 1986, p. 369). It is an approach that sees autonomy as a 'constituent element of the good life' (Raz, 1986, p. 408). The rights set out flow directly from this idea of autonomy: they arise from autonomy and if brought into play they support, protect and help preserve autonomy.

Though the issue of privacy is central, it is privacy as a protector of autonomy rather than privacy per se that is of prime concern. As already

[29] Cases such as *Campbell* v. *Mirror Group Newspapers Ltd* [2004] UKHL 22, *Von Hannover* v. *Germany* [2004] ECHR 294 and *Mosley* v. *News Group Newspapers* [2008] EWHC 1777 (QB) have centred around what expectations of privacy are appropriate in private or public spaces.

noted, it is particularly true that in the digital world privacy is crucial to protect autonomy. As Nissenbaum puts it:

> Widespread surveillance and the aggregation and analysis of information enhance the range of influence that powerful actors, such as government agencies, marketers, and potential employees, can have in shaping people's choices and actions. (Nissenbaum, 2010, p. 83)

Nissenbaum's analysis categorises the relationship between privacy and autonomy in the digital context in three ways. Firstly, that privacy can itself be considered an aspect of autonomy: autonomy over one's personal information. Secondly, that as privacy frees us from the 'stultifying effects of scrutiny and approbation (or disapprobation)', it contributes to an environment that supports the 'development and exercise of autonomy and freedom in thought and action' (Nissenbaum, 2010, p. 83). This can be looked on as a converse to the panopticon effect: if we don't feel ourselves to be under the constant risk of observation we will feel more able to think and act freely. Thirdly, and most directly for the purposes of this book, that without privacy our ability both to make effective choices and crucially to follow them through can be curtailed (Nissenbaum, 2010, pp. 82–3). The nature of the manipulations possible can be both in terms of the choices suggested and offered, and the information provided in order to aid in making those choices.

1.5 Privacy per se?

The existence and nature of any 'right to privacy' is a subject that is much discussed, and as the digital world becomes more significant it is likely to be discussed even more. The difficulties in pinning down the definition of privacy are discussed in Chapter 2, but they are not of a key, central concern here. Nonetheless, the conclusions and suggestions of this book could, indeed *would*, have a significant effect on privacy in many ways, as well as providing more autonomy for individuals, but these can be considered as side effects or peripheral benefits rather than the main intention.

Privacy and autonomy go hand in hand in protecting and supporting many 'human rights', as we currently consider them. Most directly, such rights are often called 'civil liberties' – freedom of association, freedom of expression, freedom of assembly, freedom of religion and so forth – but they also embrace other important rights including social, cultural and economic rights. The last of these is one that demonstrates some of the most insidious problems on the internet: without appropriate privacy