ONE

Digital Advancements and Threats to Reputation

Introduction

Today it is truly a digital world. Technology both dominates and shapes society and, through its permeation in everyday lives, societal norms and patterns of behaviours are changing in ways which are measurable and susceptible to academic study.[1] It is now commonplace for an individual to use the internet from the moment they wake up until they go to sleep.[2] This chapter argues that the integration of sophisticated technology in daily lives has caused a fundamental societal shift to take place. This shift presents a greater threat to reputation rights than has been seen since the introduction of the printing press in the 15th century.

Rapid technological advancements have changed the global digital landscape. Advancements have come in the form of 'soft' mechanisms or applications, such as 'clouds', which can store vast amounts of information,[3] and 'hard' smart devices,

[1] Maryanne Wolf, 'Skim reading is the new normal: The effect on society is profound' *The Guardian* (25 August 2018) www.theguardian.com/commentisfree/2018/aug/25/skim-reading-new-normal-maryanne-wolf?utm_source=esp&utm_medium=Email&utm_cam%E2%80%A6 accessed 28 November 2022.

[2] One can use an app to 'find my phone' when it is lost, Google Maps to reach a meeting point with a friend and tell Alexa to switch off the lights.

[3] Using its subscription service, Apple offers up to 12 terabytes of storage on the iCloud, which is a vast amount of information, equivalent to up to

which are connected to wireless internet. Socio-economic changes have also had significant impact, in the form of readily affordable internet-enabled devices. It is now possible for many people to own a smartphone, tablet or laptop, easily depositing personal and damaging information about another online and viewing information posted by others. Social media is now intrinsically embodied in daily life. It is the new normal to post commentary about an event on X, to discuss oneself – or others – on LinkedIn and to post all manner of personal information about people we know on Facebook or Instagram. All of these websites are free to use at the most basic level. This personal information is then often backed up online, through the cloud.[4] There have been recent and rapid advancements in artificial intelligence (AI), such that it now seems poised to integrate within multiple aspects of private and public lives: chatbots are now able to have convincing conversations with the living, impersonating those in the 'real world' who are dead or alive.[5] Despite lukewarm early reviews of the 'Metaverse'[6] (financially backed by Facebook co-founder Mark Zuckerberg), parent company Meta appear determined to invest further in the online world and move society to a virtual platform. This online world allows individuals to socialize with one another through digital likenesses and even make speeches

a year of stored TikTok short videos: https://support.apple.com/en-gb/guide/icloud/mm3d17a80e23/icloud#:~:text=When%20you%20set%20up%20iCloud,or%2012%20TB%20of%20storage accessed 2 July 2025.

4 For example the iCloud. See: www.icloud.com/ accessed 2 July 2025.

5 See: 'Google fires software engineer who claims AI chatbot is sentient' *The Guardian* (23 July 2022) www.theguardian.com/technology/2022/jul/23/google-fires-software-engineer-who-claims-ai-chatbot-is-sentient accessed 1 July 2025.

6 Tanya Basu, 'Meta is desperately trying to make the metaverse happen' *MIT Technology Review* (11 October 2022) www.technologyreview.com/2022/10/11/1061144/metaverse-announcements-meta-connect-legs/ accessed 1 July 2025.

and interact with virtual audiences – who represent real people operating through an online avatar.

Such advancements have led to a change in the way individuals view reputational interests and interact with the web, with many now regularly posting information about third parties. This shift to normalizing online disclosures has been compounded by the fact that the 'internet never forgets', as argued by Mayer-Schönberger.[7] This chapter will explain various technological advancements that have galvanized technology usage and led to a plethora of personal and potentially defamatory information deposited online. The chapter then considers specific threats to reputational interests as a result of these.

I. Technological advancements and threats to reputation

a. A beginning: the rise of cloud computing

Cloud computing is the single technological evolution that has shaped most of the digital world as it is now known. The innovation allowed modern advancements in IT,[8] yet experts claim it is still in its 'infancy',[9] with much more capability yet to be seen. Cloud computing is the backbone that supports many digital capabilities, such as the aggregation of personal data, the Internet of Things, AI and social media websites.[10] A working definition of cloud computing is 'on-demand network access to a shared pool of configurable computing resources'.[11] Cloud computing means that 'simple portals'

[7] Viktor Mayer-Schönberger, *Delete: The Virtue of Forgetting in the Digital Age* (Princeton University Press 2009).

[8] Nayan B. Ruparelia, *Cloud Computing* (MIT Press 2016) 3.

[9] Ibid.

[10] Ali Sunyaev, *Internet Computing: Principles of Distributed Systems and Emerging Internet-Based Technologies* (Springer 2020).

[11] Ibid 4. This is a shortened version of the National Institute of Standards and Technology's definition in the US.

can be used to log in to the cloud, a virtual space where data can be stored and shared. This virtual space can be accessed from any number of devices, anywhere.[12] Ruparelia calls this 'ubiquitous computing' and notes that this concept was initially promulgated by universities.[13] Indeed, Facebook initially began as a website called 'Facemash' where a cycle of photographs of two different Harvard attendees were pitted against each other, with a user deciding which of the individuals were more attractive.[14]

The cloud is readily available as it exists in the online space whether users are engaging or not.[15] As such, time and location have lost their previous importance as information can be accessed from any web-enabled place, at any time.[16] Cloud service models are also varied and diverse.[17] Clouds can be personal, social, financial or can be a cloud of 'things'.[18] Oppitz and Tomsu have argued that cloud computing is a 'global service ecosystem' and cannot be explained with reference to the binary understanding of private or public spaces; rather, it is 'a hybrid area where new rules are developed and changed quickly'.[19] The capacity of the cloud to store ever-increasing amounts of information continues to grow,[20]

12 Ibid 5–17.

13 Ruparelia (n 8) 63.

14 Katharine Kaplan, 'Facemash creator survives ad board' *The Crimson.com* (19 November 2003) https://web.archive.org/web/20190504172812/www.thecrimson.com/article/2003/11/19/facemash-creator-survives-ad-board-the/ accessed 28 November 2023.

15 Sunyaev (n 10) 17.

16 Marcus Oppitz and Peter Tomsu, *Inventing the Cloud Century: How Cloudiness Keeps Changing Our Life, Economy and Technology* (Springer 2018) 412.

17 Sunyaev (n 10) 207.

18 Ibid 56 and see Federica Cappelletti, Alessandra Papetti, Marta Rossi and Michele Germani 'Smart strategies for household food waste management' (2022) 200 *Procedia Computer Science* 887.

19 Oppitz and Tomsu (n 16) 411.

20 Ibid 414.

giving users the seemingly endless ability to promulgate true (or false) personal information about others. To add further complexity, the cloud is virtual and therefore 'borderless', going beyond the boundaries of countries or, arguably, social class.[21] It is also possible to create a 'societal cloud' – a service provided to a group that has common purposes or goals. Ruparelia gives the example of a cloud for NATO, as clouds can easily service big data sets due to their ephemeral nature.[22] Posting information or media utilizing such a cloud could reach an unimaginable amount of people. As such, cloud uses can range from mass scale to small scale, with the cloud harbouring material that could reach large or more modest audiences.

i. Cloud computing and threats to reputation

In summary, the cloud makes information sharing on a grand scale possible. Indeed, it makes it easy, fast and convenient to spread misinformation or false and defamatory information.[23] For this key reason, cloud computing has enabled defamation of individuals on a previously unheard-of scale. Defamatory content can be remotely uploaded to the cloud by any user who has login credentials; all one would need is a relatively basic device connected to the internet, such as a smartphone. The cloud could then be used to further share this information to a myriad of other users through its wireless connectivity capability. The cloud's ability to store large amounts of information – be it true or false, accurate or inaccurate – is the reason that social media websites and other such sites (discussed later in this chapter) can function in the way that they do. Cloud computing as a system therefore *enables and allows for*

[21] Ibid 411.
[22] Ruparelia (n 8) 54–5.
[23] Oppitz and Tomsu (n 16) 413.

large-scale defamation of an individual to take place online. This can be seen as the single salient development, much like the printing press, that has changed the global reputational landscape. Before the digital revolution which is currently gripping the world, it would be hard to imagine reputational damage of this scale or magnitude. In the 1980s, when the ruthless UK tabloid press was in its heyday (leading to a new interest in the details of private lives)[24] legal professionals and those wishing to safeguard information rights raised concerns. Despite these issues, impacts on reputations were necessarily limited by the scale of the physical publication of paper copies of newspapers in the 1980s and 1990s. Due to the sheer ease in storing and disseminating false personal information made possible by clouds, the potential for mass libel on a previously unseen scale is now here, dwarfing concerns over the printing press of years past.

A further concern is the power that lies behind cloud computing. As clouds continue to grow and develop, it is likely that the control behind key enterprises will be consolidated into the hands of one or two parent companies.[25] This in turn makes it increasingly easy for such a conglomerate, if they wished, to influence public opinion for a range of nefarious purposes,[26] for example by supplying potentially incorrect information about an individual to a third-party source, such as a government.[27] Extremist groups can also take advantage of the cloud to spread propaganda or hate about an individual, based on false and defamatory information.[28]

[24] See Jacob Rowbottom, 'Kaye v Robertson [1991] FSR 62' in Paul Wragg and Peter Coe (eds), *Landmark Cases in Privacy Law* (Hart 2023) 90ff.
[25] Ruparelia (n 8) 229–30.
[26] Ibid 229–33.
[27] Ibid.
[28] Oppitz and Tomsu (n 16) 418–19.

b. The birth of social media

For the purposes of this book, one of the most significant developments since the early 2000s is the rise of social media. The first widely adopted social media website reaching a world audience was Myspace, which launched in 2003. By 2005, Myspace had 16 million regular users and it was the most successful social media site between 2005 and 2008.[29] It blended social networking with music and hosted personalized landing pages containing a plethora of personal information that was easy to update, such as photo caches, preferred choices of music and a list of 'top friends' who corresponded to real-world individuals who also had accounts on the site. Media such as photographs could be engaged with using comments appearing below an image. In an example of how the digital can impact real-world relationships offline, people were encouraged to rank their on-site 'friends' in what one can only assume was an order of preference for all to see. Myspace could be used to send or post messages containing information about oneself or others. Landing pages were also very customizable, with various themes and wallpapers downloadable from other free sites, while 'arrival music' played when one clicked on a user's profile.

Myspace can be seen as a primary influence or trailblazer for all subsequent developments in social media. Facebook also contained a similar personalized landing page, although with less emphasis on music and more emphasis on posting information about oneself or others through 'wall posts'. Myspace is still credited with beginning the burgeoning rise of social media among young people, by branding itself as an 'edgy' destination people could connect with music artists and friends.[30] After the early success of Myspace,

[29] *Encyclopaedia Britannica*, 'Myspace: Web site' (10 November 2023) www.britannica.com/topic/Myspace accessed 1 July 2025.

[30] Ibid.

social networking sites online have thrived, continuing to grow and expand in popularity. Myspace was eventually deposed by Facebook as the world's most popular social networking site in 2009. Facebook branded itself as a site that predominantly connected friends and family members, with a less fashionable USP than Myspace, which was seen by some as having an element of counterculture. As such, Facebook has been more successful in capturing a broader age range of users. As of 2023, approximately 10 per cent of Facebook users were 65 years old or over. Circa 2025 a further shift occurred and young people (who perhaps would previously have been caught in Myspace's orbit) now predominantly engage with image- or video-based social media websites. This includes YouTube, TikTok, Instagram and Snapchat.[31] All of these sites use short- or long-form video content and images to communicate information to large or small audiences. TikTok, Instagram and Snapchat in particular prioritize short clip sharing as the primary method that information is disseminated on the sites, such as 'stories' on Snapchat.[32] Direct engagement between users happens in public comment sections or private messages, which are available on each of the sites, all of which have 'apps' for ease

[31] See Emily A. Vogels, Risa Gelles-Watnick and Navid Massarat, 'Teens, social media and technology 2022' (*Pew Research Centre*, 10 August 2022) www.pewresearch.org/internet/2022/08/10/teens-social-media-and-technology-2022/#:~:text=YouTube%20stands%20out%20as%20the,%25)%20and%20Snapchat%20(59%25 accessed 8 April 2024. Also see: www.youtube.com/; www.tiktok.com/en/; www.instagram.com/; www.snapchat.com/ accessed 2 July 2025.

[32] See, for example, Aliaksandra Shutsko, 'User-generated short video content in social media: A case study of TikTok' in *Social Computing and Social Media. Participation, User Experience, Consumer Experience, and Applications of Social Computing*, Proceedings of the 12th International Conference (Springer 2020), SCSM 2020, Held as Part of the 22nd HCI International Conference, HCII 2020, Copenhagen, July 2020), Proceedings, Part II, 108.

of use on smartphones. However, purely text-based social media posts are still utilized – for example, YouTube has a 'community' section that acts like a noticeboard where users, using 'channels', can write text comments if they wish. Due to this shift in *type* of social media that is now being widely consumed, claimants may see a rise in potentially defamatory information shared by short video.

ii. Social media and threats to reputation

In the internet age, defamation through social media websites is now not only commonplace but is quickly becoming one of the most prevalent methods by which individuals are defamed in England and Wales. The case of *Stocker v Stocker* reached the Supreme Court in 2019 and argued that the respondent had been defamed through a Facebook exchange stating 'he tried to strangle me'.[33] Three of the most high-profile defamation cases of 2023 and 2024, *Hay v Cresswell*, *Aaronson v Stones* and *Blake v Fox*, concerned defamation through social media.[34] It seems that the transition to the digital era has now been completed and that if one is to be defamed, social media is now a likely form by which this will happen. As will be discussed at length later in this book, this change in medium is causing problems for judges in navigating the complexities of such sites, the extent of audience engagement with the source and whether to take such posts as seriously as those in the traditional print media.[35] English defamation law, with a vast case-law history and roots in the Roman law of *injuria*, is now expected to adapt.

---

[33] [2019] UKSC 17 [1]–[4].

[34] [2023] EWHC 882 (KB); [2023] EWHC 2399 (KB); [2024] EWHC 956 (KB).

[35] For example, which may be considered when evaluating the satisfaction of s 1 Defamation Act 2013.

Long before *Stocker* was decided in 2019, those keenly observing legal developments could see a gradual trend towards defamatory content appearing not only in print, but online – the famous line of decisions in *Flood v Times Newspapers* between 2009 and 2012 drew discussion from the judiciary in the High Court regarding the status of *The Times* website publication,[36] which remained accessible after the print version of the article had gone out of circulation and factual circumstances had changed.[37] Although *Flood* did not specifically concern a *social media* website, herein lies a profound concern for those defamed via social media: the longevity of the post itself. Unless the person who has made the post on social media manually removes it, or the host of the website seeks the post out and deletes it, the defamatory information has the potential to remain on that site forever, cemented into the annals of internet history. This concern has become so widespread that s 5 of the Defamation Act 2013 was enacted to protect operators of websites against a slew of claims that could be potentially actioned against them for defamatory content on their websites, posted by third-party individuals.[38] Aside from the indefinite timeframe that a defamatory post on a social media can be potentially visible, another central factor in the damaging nature of defamation by social media is the global reach of such websites. Facebook has a worldwide audience – statisticians estimate 2.9 billion active users – and if posts are public, there is the potential they can be seen by those who do not even subscribe to the website.[39] This was

[36] *Flood v Times Newspapers* [2009] EWHC 2375 (QB), [2010] EWCA Civ 804, [2012] UKSC 11.

[37] [2009] EWHC 2375 (QB) [H11.6].

[38] This will be discussed in Chapter 3, Part II.

[39] 'Leading countries based on Facebook audience size as of January 2024' *Statista* (2024) www.statista.com/statistics/268136/top-15-countries-based-on-number-of-facebook-users/#:~:text=With%20around%202.9%20billion%20monthly,most%20popular%20social%20media%20worldwide accessed 10 April 2024.

also the case until 2023 for Twitter/X, while YouTube is predominantly public. If one is defamed via a social media website, there is a real potential the statement can go national or 'viral'. A further harming facet of defamation through social media is that engagement with the defamatory post is encouraged. People leave comments and discuss issues on YouTube videos, some videos amassing hundreds of thousands of comments on a single post, with thousands of 'upvotes' and replies. TikTok operates a system where a user can link to a previous video post and respond directly with a video of their own, or respond to a comment using a video.[40] This can lead to further promulgation of the defamatory content and even the generation of new reputationally harmful material.

c. Wide availability of technology

In addition to digital innovations, socio-economic changes have also shaped the modern technological landscape. As such, the ease of access to technology is a significant contributing factor towards increased threats to reputation. In 2025, 95 per cent of the population have a smartphone, a product characterized by internet access.[41] This rapid increase in ownership of internet-enabled devices means that it is quick and convenient to deposit personal information about others on the internet, be it on social media or another type

[40] 'Product tutorial: Reply to comments with video' (*TikTok.com*, 18 June 2020) https://newsroom.tiktok.com/en-us/product-tutorial-reply-to-comments-with-video accessed 10 April 2024.

[41] Catherine Hiley, 'UK mobile phone statistics, 2022' (*Uswitch*, 30 September 2022) www.uswitch.com/mobiles/studies/mobile-statistics/#:~:text=A%20breakdown%20of%20UK%20age,78%25%20aged%2055%20and%20above accessed 28 November 2022. Also see Matthew Boyle and Sophie Barber, 'Mobile phone and internet usage statistics in the UK' (*Finder.com*, 4 July 2025) https://www.finder.com/uk/banking/mobile-internet-statistics accessed 24 July 2025.

of website. Sophisticated technology is also increasingly portable: a smartphone can comfortably sit in a pocket and a laptop or tablet can be easily transported around the country or globe. In the aftermath of the COVID-19 pandemic, many employers have now embraced a 'hybrid' working policy,[42] leading to the workforce having increasing amounts of technological hardware at home and engaging with a wider degree of software which often requires the input of personal information about oneself or others.[43] This normality of access to technology engenders prevalence – technology is now everywhere and seemingly used by everyone, and it is increasingly societally acceptable to discuss others in public settings online.

As alluded to, the affordable price of web-enabled technology has contributed to its wide uptake. As of 2025, certain smartphones in the UK are available to purchase at under £100.[44] A broader social demographic is therefore able to purchase and use such products, while a highly competitive market with a large range of computers, tablets and smartphones acts to drive prices down.[45] This generally accepted – and expected – usage of technology circa 2025 is

[42] The Office for National Statistics (ONS) has reported that even after COVID restrictions were lifted, as of February 2022, eight out of ten workers still planned to work partly from home. See 'Is hybrid working here to stay?' (*ONS*, 23 May 2022) www.ons.gov.uk/employmentandlabourmarket/peopleinwork/employmentandemployeetypes/articles/ishybridworkingheretostay/2022-05-23 accessed 28 November 2022.

[43] For example, Microsoft Teams, providing an online workspace and meeting place. See www.microsoft.com/en-ww/microsoft-teams/teams-for-work accessed 28 November 2022.

[44] See for example Tesco selling the 'moto e14' at under £100: https://www.tesco.com/phones/products/00840023268229 accessed 14 August 2025.

[45] On cursory examination, British electrical retailer Currys has an online offering of nearly 500 laptops and nearly 260 tablets. See

due to changing societal norms in the digital era. The general social response to rapid technological advancements has been to embrace them,[46] as evidenced by the rise in technology usage. It is increasingly common to document life events online to a potentially global audience;[47] uploading a photo or a text-based post to Instagram is a new form of social interaction.[48] Early studies have shown that individuals in Generation Z do not read information in the same way as previous generations: 'skim reading' has become default as information is now primarily consumed online, where data is widely shared through image-based content.[49] As such, the shift looks set to become yet more significant as Gen Z, born into such technology, grow into adulthood.

The role of internet-based technology is now so significant it dominates world affairs of the most crucial kind. A pertinent example is Starlink, a 'satellite Internet constellation' from company Space X.[50] The idea behind Starlink is to provide internet access more readily and efficiently to both areas that do not have coverage and to ones that do; the aim of the scheme is 'providing global Internet access'.[51] It is arguably the most widescale current development in communications

www.currys.co.uk/computing/ipad-tablets-and-ereaders/tablets accessed 28 November 2022.

46 Although this embrace may not always yield positive outcomes. See Shaohai Jiang and Annabel Ngien, 'The effects of Instagram use, social comparison, and self-esteem on social anxiety: A survey study in Singapore' (2020) *Social Media + Society* 1.

47 See picture- (and video)-sharing social media site, Instagram: www.instagram.com/ accessed 2 July 2025.

48 Soo-Hyun Jun, 'Why do people post photos on Instagram?' (2022) 14(12648) *Sustainability* 1.

49 Ibid 2 and Wolf (n 1).

50 Tong Duan and Venkata Dinavahi, 'Starlink space network-enhanced cyber-physical power system' (2021) 12(4) *EEE Transactions on Smart Grid* 3673.

51 Ibid 3673.

technology, and began around 2015.[52] The role of Starlink has already proved impactful on the world stage in the context of the Russian invasion of Ukraine in February 2022. On request from a Ukrainian political official (via Twitter, as it then was), Elon Musk responded that Starlink had unofficially launched over Ukraine, providing the country with satellite internet connection.[53] As of April 2022, Starlink had 10,000 dishes in service, with more expected, and the ability to provide internet access to the most rural of areas.[54] Experts have commented that this has been a 'salvation' – the launch of the project was doubtlessly impressive, despite being a 'mad dash'.[55] This is a further example of how society now ceases to function without internet access, even in wartime. In our homes, it is now a mains service, similar to electricity, gas and water.

iii. Affordable technology and threats to reputation

As explained, the prevalence of technological hardware due to wide affordability means that now most people in the UK have access to an internet-enabled device. The impact of this is that wide-scale communication of defamatory information about another can originate from anyone, at any time, through the medium of the internet. It is now within most people's capabilities to utilize a smartphone to log into a social media website – to which it is free to sign up – and post false and potentially defamatory information about another.

---

52 Ibid.

53 Kevin Collier, 'Starlink internet becomes a lifeline for Ukrainians' (*NBC News*, 29 April 2022) www.nbcnews.com/tech/security/elon-musks-starlink-internet-becomes-lifeline-ukrainians-rcna25360 accessed 2 July 2025.

54 Ibid and Duan and Dinavahi (n 50).

55 Collier (n 53).

This is not the case in the mainstream printed press, such as newspapers: in order that a potentially defamatory story can be run about an individual, the story would have to pass a wide variety of checking points or hurdles, from the person who wrote the story to their line manager, to eventually the editor of the newspaper and the legal team – before the story reached print. This is in contrast to modern technology, which links anyone who can afford a web-enabled device directly to the internet. Everyone now has the ability to publish defamatory content to a potentially wide audience without any form of editorial oversight.[56] This also means that the likely subjects of defamation have changed; in the past, through tabloid press culture, well-known faces were much more likely to be the target subjects of potentially defamatory publications. In 2025 a much wider array of targets are likely, apart from the rich and famous – as people with a myriad of personal and private vendettas are capable of uploading defamatory statements. This links to the concept of posts going viral; noteworthy online posts may generate a wide range interest, far beyond the intended or even expected audience. These instances may well relate to private individuals, rather than celebrities. An example is a recording of a parish council meeting in Handforth, a small civil parish in Cheshire, UK, which went viral in 2021, with videos and clips from the meeting amassing millions of views on YouTube.[57]

---

[56] This is, of course, notwithstanding that many social media and other websites have a terms of service policy. See for example, Facebook's policy, https://en-gb.facebook.com/legal/terms accessed 15 April 2024. Posts can, of course, be taken down by site moderators due to improper usage.

[57] See, for example, this clip of the 'best parts' www.youtube.com/watch?v=zy3Kml-F7J0 and *The Guardian*'s post of the meeting: www.youtube.com/watch?v=l17UIwAFOyk accessed 15 April 2024.

With this increased access to sophisticated technology has come newfound normality in discussing what may have previously been private conversations in public settings on social media websites. It is now the norm to share personal feelings or information about another in a public setting on sites such as Facebook or Twitter/X and, indeed, many defamation cases have arisen pertaining to both sites to date.[58] This shift has led to a situation where posting about another on the internet is not viewed as an unusual thing to do, resulting in yet more potential for defamatory statements to flood the internet. Early studies have shown that a desire to 'belong' can even encourage certain patterns of behaviour on social media sites.[59] Due to the large amount of personal information shared on a daily basis online,[60] it is even possible to foresee unintentional but nevertheless defamatory statements issued on the internet through a post by an individual to their own page, predominantly about themselves – but also containing potentially defamatory content about others. The more one posts on social media, the more incentives there are to continue posting. On YouTube, when an account reaches 1,000 'subscribers' that channel becomes 'monetized' and suitable for companies to place advertisements on. The people behind the YouTube channels then receive monthly 'adsense' payments which correlate to how often the

[58] See Kirsty Horsey and Erika Rackley, *Tort Law* (OUP 2023) ch 17 – websites: (*Godfrey v Demon Internet* [2001] QB 201), tweets: (*McAlpine; Monroe v Hopkins* [2017] EWHC 433 (QB)), blogs: (*Cruddas v Adams* [2013] EWHC 145 (QB)), Facebook (*Stocker v Stocker* [2019] UKSC 17, *Hay v Cresswell* [2023] EWHC 882 (KB)).

[59] Christiane M. Büttner, Fanny Lalot and Selma C. Rudert, 'Showing with whom I belong: The desire to belong publicly on social media' (2023) 139 *Computers in Human Behaviour* 107535.

[60] It was estimated that, worldwide, people spent on average 143 minutes per day on social media in 2024. See 'Daily time spent on social networking by internet users worldwide from 2012 to 2025' (*Statista*, 19 June 2025) www.statista.com/statistics/433871/daily-social-media-usage-worldwide/ accessed 2 July 2025.

video (and therefore advertisements) are viewed. To grow a social media account, advisors argue that there should be an emphasis on creating posts that will be further shared.[61] With this increased traffic of content comes an increased likelihood of defamatory statements as transmitted online. Indeed, the more salacious or controversial the content of a website, the more traffic (and therefore more money) this can drive to a channel and its owners.

Finally, internet-enabled technology also allows an individual to post online *anonymously*. It is straightforward to sign up to a social media website with false details, using an email account that one can easily again obtain with any form of false information. Hiding behind an online pseudonym in order to defame someone is an attractive prospect to potential defamers – as particularly those with malicious intent may feel safe from persecution through an anonymous online persona. As will be discussed later in this book, this in turn makes bringing an action against such an individual difficult, although the annexed statutory instrument to the s 5 defence for operators of websites in the Defamation Act 2013 can be successful at finding a middle ground in such situations.[62]

d. The 'Metaverse' and online worlds

Beyond advancements in hardware and internet access, companies are now striving to take technology one step further

[61] Brendan Kane, 'How I gained one million followers' in *One Million Followers* (BenBella Books 2018).

[62] In such a case, if personal details of the poster are not forthcoming, the website will remove the content within five days to avoid themselves being actioned against in defamation. See The Defamation (Operators of Websites) Regulations 2013, UK Statutory Instruments, 2013 No 3028 www.legislation.gov.uk/uksi/2013/3028/contents/made accessed 26 August 2024.

and develop virtual *worlds*. Facebook parent company Meta has invested a significant amount of money building such a world – the 'Metaverse'.[63] The Metaverse has the aim of creating a fully functioning in-world ecosystem. It hosts digital marketplaces using cryptocurrency and supplemented by the trading of NFTs (non-fungible tokens),[64] but more crucially – as far as this monograph is concerned – builds social spaces for users to interact with one another and allows individuals to embody avatars in an entirely online augmented reality.[65] When users log on, they choose their avatar and then are greeted with a landing page, or a 'safe zone', where people cannot interact with them – however, after a user navigates away from this, they then enter various virtual community spaces where they will interact with others, also embodying avatars. Information can be communicated between avatars in various ways; people can use microphones or text-based comments in order to speak to one another, or make speeches to potentially large audiences of other avatars, all of whom have real people behind them.[66]

---

[63] Reportedly $36 billion dollars. See Jyoti Mann, 'Meta has spent $36 billion building the metaverse but still has little to show for it, while tech sensations such as the iPhone, Xbox, and Amazon Echo cost way less' (*Insider*, 29 October 2022) www.businessinsider.com/meta-lost-30-billion-on-metaverse-rivals-spent-far-less-2022-10?r=US&IR=T#:~:text=Meta%20has%20spent%20%2436%20billion,Amazon%20Echo%20cost%20way%20less accessed 2 July 2025.

[64] Academics have argued that conceptions of property are changing due to the move to 'Web3' and online worlds. See Russell Belk, Mariam Humayun and Myriam Brouard, 'Money, possessions, and ownership in the Metaverse: NFTs, cryptocurrencies, Web3 and wild markets' (2022) 153 *Journal of Business Research* 198.

[65] Peter Weber, 'How Facebook's metaverse could change your life' (*The Week*, 28 November 2021) https://theweek.com/facebook/1007409/how-facebooks-metaverse-could-change-your-life accessed 2 July 2025.

[66] See the video made by RT Game, 'I played Facebook's VR Metaverse so you don't have to' (*YouTube*, 30 October 2022) www.youtube.com/watch?v=UdqrFa6pWLA accessed 16 April 2024.

Access using a virtual reality headset gives users an even more immersive, whole-body experience,[67] where they see the Metaverse as if it appeared directly in front of them and can hold controllers in each hand to give the sensation of physically interacting with both people and things in the virtual world. One can move towards and 'touch' other avatars, while objects in the virtual world can be picked up or otherwise interacted with. While some initial responses to early versions of the Metaverse have been lukewarm,[68] Meta continues to develop the project, particularly as potential for growth has been seen for the product in the gaming industry market.[69] Forbes continues to consider the Metaverse a worthwhile financial investment, partly because it allows advertisers to reach target audiences in new and increasingly diverse ways.[70] Aside from the Metaverse, other virtual worlds have long existed online where individuals can interact and communicate with each other using virtual shared spaces, such as VRChat,[71] which has over 25,000 virtual worlds.[72] Furthermore, virtual reality hardware is not required to engage (opening to the experience to a larger demographic). As such, advancements in digital world building show no signs of stopping.

---

67 See the playthrough in the video (n 66). An example of such a headset is the Oculus Rift: www.oculus.com/rift-s/?locale=en_GB accessed 27 August 2024.

68 Ibid.

69 'Metaverse development complete guide: What you need to know about the Metaverse in 2024' (*TokenMinds*, 21 December 2023) https://tokenminds.co/blog/metaverse-development/metaverse-development accessed 16 April 2024.

70 Andrew Michael and Kevin Pratt, 'How to invest in the Metaverse' *Forbes* (29 November 2022) www.forbes.com/uk/advisor/investing/how-to-invest-in-the-metaverse/ accessed 2 July 2025.

71 See the VRChat website: https://hello.vrchat.com/. The game is accessible through the 'Steam' shop for computer gamers.

72 Ibid.

iv. Online worlds and threats to reputation

Much as in the real world, a virtual world can be used to disseminate defamatory content about another individual, to large or small audiences – as of 2024, it was estimated that there are 400 million active users of the Metaverse.[73] One can foresee the usage of avatars leading to an increase in individuals revealing compromising – and potentially defamatory – information about another in a range of different ways. It is clear that revealing reputationally damaging personal information to a group of other avatars (or people) in a virtual world clearly satisfies the publication requirement for one to be defamed in the eyes of others in English law, although if this would satisfy the serious harm threshold necessary to bring a claim in s 1(1) of the Defamation Act 2013 remains to be seen and would depend, for example, on the potential reach of the information.[74] Information could be delivered in a slanderous capacity through speaking words through a microphone to real-world listeners behind other avatars, or libel could be committed by writing something that would be included in an online world – such as a virtual community noticeboard – in a more permanent form.[75] As one is shielded by an anonymous avatar, this may increase willingness to disseminate spurious, damaging and false information about another, as a user may feel that they would be less likely to experience repercussions.

---

[73] Josh Howarth, '75+ Metaverse statistics (new 2024 data)' (*ExplodingTopics*, 22 November 2023) https://explodingtopics.com/blog/metaverse-stats accessed 16 April 2024.

[74] *Lachaux v Independent Print* [2019] UKSC 27 [21], where Lord Sumption noted, much like Mr Justice Warby before him, that the 'scale of publications' was relevant to whether the s 1 threshold was met.

[75] The importance between the traditional distinction between libel and slander has been eroded due to the introduction of the serious harm threshold in s 1 Defamation Act 2013. Traditionally, libel takes a more

As can be expected, there are a multitude of legal issues with the potential to culminate in the Metaverse (or any other virtual world). Cheong has considered whether a 'veil' should be lifted in certain circumstances to reveal who is behind an avatar,[76] although it is as yet unclear what type of law would apply in an instance whereby one avatar infringed the reputational rights of another, or whether an avatar could have legal responsibility.[77] A veil of an avatar could perhaps be lifted in order that the user be held accountable for civil offences such as defamation – much like legal systems pierce the corporate veil to hold those behind companies responsible, despite companies having separate legal personalities.[78] If an avatar is incorporated, this could lead to an action being brought against the avatar itself,[79] although it is unclear how this would work in practice or if this is desirable from the perspective of legal experts. Short of removing defamatory information from the 'virtual world' (which presumably would be a comparatively achievable fix), a claimant would be unlikely to receive damages – monetary compensation – from an avatar who has no independent financial wealth. The Metaverse will also generate new forms of 'personal' data, specific to an avatar, leading to further questions about the application of supranational data protection instruments such as the General Data Protection Regulation,[80] which could also potentially be used to remove defamatory personal information online, as will be discussed later in this book.

permanent form than slander and is therefore actionable per se. See, for example, *Monson v Tussauds Ltd* [1894] 1 QB 671.

76 Ben Chester Cheong, 'Avatars in the metaverse: Potential legal issues and remedies' (2022) 3 *International Cybersecurity Law Review* 1.

77 Ibid 4.

78 Ibid 15.

79 Ibid 21.

80 Dependant, of course, on this information as classified as personal data. Ibid 25.

Cheong also argues that the potential to hide behind an avatar could lead to people committing acts online that they would not ordinarily commit.[81]

e. Augmented reality

Linked to the Metaverse, another technology trend that has gathered pace is the rise of augmented reality. This is where (for example) a phone application generates a display that represents – in part – the real world, with virtual elements overlaid in order that the display can largely appear real, and where one can interact with it. The reality is 'augmented' because the superimposed parts are 'generated by a computer' and are not real.[82] Despite being a concept first debuted in the 1960s,[83] the trend has only recently begun to dominate the mobile app market, such that Apple have dedicated webpages extoling the virtues of using virtual reality applications on their devices, iPads, iMacs and iPhones.[84] A few of the application examples given by Apple on these webpages include games, but also photography apps and – crucially – social media apps such as 'Snapchat', where the 'reality' of pictures can be superimposed upon. Pokémon GO is an example of an app that was a popular sensation that harnessed real-world locations and user whereabouts as crucial to the game. Pokémon GO uses augmented reality as it blends the real world and the

[81] Ibid 6.

[82] Raffaele Vertucci, Salvatore D'Onofrio, Stefano Ricciardi and Maurizio De Nino, 'History of augmented reality' in Andrew Yeh Ching Nee and Soh Khim Ong (eds), *Springer Handbook of Augmented Reality* (Springer 2023) 35.

[83] Ibid.

[84] 'Augmented reality' (*Apple.com*) www.apple.com/uk/augmented-reality/ accessed 29 November 2023.

digital world.[85] The technology that supports augmented reality programs is 'simple',[86] leading to such apps becoming increasingly commonplace. The technology that supports augmented reality is also relatively low cost, even if one wants a wearable piece of hardware which displays the altered reality, such as Google Glass.[87]

v. Augmented reality and threats to reputation

When one considers reputation rights, augmented reality is a particularly concerning technological advancement as it hinges on the ability to blur lines between what is true and what is false. If someone cannot be certain what they are seeing is real – and if it is in fact only partly real – it is easy to foresee eventualities where, for example, videos of individuals are taken out of context and clipped into other convincing 'realities', changing the nature of what is said or done, to the reputational detriment of those concerned. For example, a pre-existing picture of a person in a compromising position could be overlayed virtually to a real-world environment, implying, for example, moral disrepute. Even if a defamatory imputation was not explicit, defamation by innuendo could potentially mean there was liability for such an augmented picture if a defamatory meaning was implied, for example by 'reading between the lines' or relying on extraneous facts known to an audience.[88] Consider a

---

85 Diana Martinez, 'Counteracting diminished privacy in an augmented reality: Protecting geolocation privacy' (2017) 50(4) *Loyola of Los Angeles Law Review* 713, 715.

86 Ibid 715.

87 Vertucci et al (n 82) 35.

88 See, for example, *Lewis v Daily Telegraph* [1964] AC 234 (false innuendo, reading between the lines to infer the defamatory meaning); *The Lord McAlpine of West Green v Sally Bercow (No 2)* [2013] EWHC 1342 (true innuendo, deduced by knowledge of extraneous facts).

scenario where a computer-generated likeness of an individual could be superimposed virtually over a real-world environment, such as footage of a brothel. As technology progresses, it may become difficult to distinguish which aspects of an image or footage are real and which computer generated, particularly as augmented reality mixes medias (and people may assume that because some of what they are seeing is clearly real, all other aspects are also).

Partly because of its simplicity and the low economic cost of engagement, technology experts have warned that augmented reality is a 'disruptive technology' with the potential to transform the world in a significant way. Vertucci et al observe that 'AR [will] deeply transform the world of work, the way we interact with others, and the society in general.'[89] Laws internationally have been slow to keep up with technological developments in the field,[90] and there are also counter-arguments to strict legal regulation, such as that augmented reality can aid crime prevention.[91]

f. Artificial intelligence

The current technological climate is dominated by developments in AI. The field has been researched in academia and developed in industry since the 1970s and its prevalence has recently gathered pace and media attention.[92] Despite vast amounts of academic discourse on AI, an agreed-upon definition is

[89] Vertucci et al (n 82) 36.

[90] For a discussion of this as the technology became emergent in the US, see Kevin F. King, 'Personal jurisdiction, internet commerce, and privacy: The pervasive legal consequences of modern geolocation technologies' (2011) 21 *Albany Law Journal of Science & Technology* 61, 116.

[91] Elena Militello, 'Geolocation in crime detection and prevention' in Lorena Bachmaier Winter and Stefano Ruggeri (eds), *Investigating and Preventing Crime in the Digital Era* (Springer 2022).

[92] See, for example, Earl B. Hunt, *Artificial Intelligence* (Academic Press 1975).

elusive – Hunt has argued that the term relates to machine problem solving, learning and decision making, among other hallmarks.[93] There is a range of different types and levels of AI: 'strong AI' mimics human levels of intelligence.[94] In 2022, it was reported that Google had dismissed senior software engineer Blake Lemoine who was working on a project concerning AI chatbot LaMDA.[95] Lemoine had expressed to executives at Google (and later the media) that he believed LaMDA was in fact sentient and had the same capacity for interaction as an eight-year-old child due to the nature of the conversations he had conducted with the bot, including ones about personhood.[96] It is not a stretch to imagine individuals cultivating meaningful personal relationships with AI chatbots and revealing private information about themselves, be it true or false, which in turn could be used to publicly humiliate them. Websites which cultivate AI chatbots are thriving. The website 'character.ai' hosts an enormous number of character AI-powered chatbots with whom millions of real people are conversing on a daily basis.[97] The range of characters available to speak with is large; ranging from fictional character Sherlock Holmes, who has 6.7 million 'chats', to bots mimicking *real individuals*, such as a chatbot with a striking resemblance to tech entrepreneur Elon Musk, who has had over 35.1 million 'chats'.[98] These numbers demonstrate the wealth of engagement

[93] Ibid 3.

[94] Konrad Szocik and Agata Jurkowska-Gomułka, 'Ethical, legal and political challenges of artificial intelligence: Law as a response to AI-related threats and hopes' (2021) *World Futures* 1, 2.

[95] 'Google fires software engineer who claims AI chatbot is sentient' *The Guardian* (23 July 2022) www.theguardian.com/technology/2022/jul/23/google-fires-software-engineer-who-claims-ai-chatbot-is-sentient accessed 2 July 2025.

[96] Ibid.

[97] See character.ai: https://character.ai/ accessed 16 April 2024.

[98] Ibid: see the handles @Kapps98 and @elonwhisperer respectively for the relevant Sherlock Holmes and Elon Musk chatbots.

with these programs, and also show that there is a clear interest in individuals communicating with what (at least superficially) appears to be a real, well-known and living person rather than a fictional character. Academics have argued that advancements such as these in AI have led to online life and 'normal life' merging into an 'onlife'.[99] This onlife can increasingly lead to reputationally damaging disclosures of personal information online, as social interaction on the web is the new norm.

Another disturbing advancement powered by AI is the 'deepfake'. Deepfakes are pictures or videos that resemble a real-life individual to such an extent they could be mistaken for them. The developer of the deepfake has control over what is said or done by that likeness of a particular individual. Deepfakes now have the potential to be so convincing that it is extremely difficult to assess whether they are in fact fake, or instead real footage of a person – the developer quite literally can 'put new words into a politician's mouth'.[100] The technology works by running a large amount of pictures of the individual chosen to be impersonated through an AI algorithm, until a convincing image or video of that person can be created and manipulated.[101] The 'synthetic image' is then placed within a set of real images and the result will eventually resemble the person mimicked.[102] Powerful home desktops can now make deepfakes and easily accessible technology that can aid the process is now being developed.[103] As time progresses and AI becomes more

[99] Szocik and Jurkowska-Gomułka (n 92) 2, quoting Luciano Floridi, 'Soft ethics, the governance of the digital and the General Data Protection Regulation' (2008) 376(2133) *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences* 20180081.

[100] Ian Sample, 'What are deepfakes – and how can you spot them?' *The Guardian* (13 January 2020) www.theguardian.com/technology/2020/jan/13/what-are-deepfakes-and-how-can-you-spot-them accessed 4 December 2023.

[101] Ibid.

[102] Ibid.

[103] Ibid.

sophisticated – the more humans feed information to AI, the faster and more accurately it learns – the more difficult it will be to discern which videos or images are real and which fake. The use of AI to impersonate one's image, likeness or voice to commit crime has surged, due to the ever-increasing capabilities of AI making deepfake images and videos more convincing and difficult to determine.[104] Although software exists to help detect deepfakes, many people will not have ready access to such a program and instead rely on other subtle 'tells' with convincing videos, such as strange blinking patterns.[105] The difficulty in recognizing a well-produced deepfake is so significant that MIT launched a 'Detect Fakes' research project and accompanying website in order to train web users to recognize one.[106] The potential for deepfakes to spread false information about individuals is unparalleled. Deepfakes have been used so far to target two particular groups; to defame politicians and women,[107] with the rise of deepfake pornography.[108]

vi. Artificial intelligence and threats to reputation

As will be obvious from the discussion thus far, the most significant reputational threat that AI poses to individuals is the ability to accurately impersonate them. A deepfake

[104] Ben Colman, 'Why detecting dangerous AI is key to keeping trust alive in the deepfake era' (*World Economic Forum*, 7 July 2025) https://www.weforum.org/stories/2025/07/why-detecting-dangerous-ai-is-key-to-keeping-trust-alive/ accessed 24 July 2025.

[105] Sample (n 100).

[106] 'Detect DeepFakes: How to counteract misinformation created by AI' (*MIT Media Lab*) www.media.mit.edu/projects/detect-fakes/overview/ accessed 6 December 2024.

[107] See, for example, Jessica Ice, 'Defamatory political deepfakes and the First Amendment' (2019) 70(2) *Case Western Reserve Law Review* 417.

[108] See, for example, Anne Pechenik Gieseke, '"The new weapon of choice": Law's current inability to properly address deepfake pornography' (2020) 73(5) *Vanderbilt Law Review* 1479.

video or a picture can be manipulated to do, say or show anything, which results in a range of potentially defamatory implications for the individual impersonated. While some deepfake hoax images are clearly satirical, others may not be; or may tread the line so closely it is difficult to tell. Combined with increasingly powerful software and hardware that can generate accurate likenesses, it is easy to see how deepfake content of a real individual engaged in reputational harmful activity could 'go viral' and receive multitudes of views online, engendering serious harm to one's reputation. Even after a successful defamation action is litigated, if such a video was seen by a significant section of the population this damage to reputation is incredibly difficult, if not impossible, to recover from. Although deepfakes have predominantly been used (in high-profile cases) to target public figures,[109] a user could also target a private individual who had incurred their ire if they had access to a suitable photoset and the requisite software and hardware.

Another clear reputational issue raised by AI advancements is if chatbot likenesses say or express views that are potentially defamatory to the 'real' individual mimicked. In addition to this eventuality, if a certain chatbot's algorithm (powered by machine learning) learns to engage in certain types of discussions or behaviour – such as sexist views or a proclivity to engage in sexually explicit or even flirtatious discussions with the user – this could lead to a latent belief in the public that the real-life individual on which a bot is based harbours those same proclivities, leading to potentially defamatory implications or innuendo. There is also the less fanciful possibility that a

[109] Particularly political figures or other public figures of note. This is clearly a widespread concern: see the University of Oxford's Reuters Institute of Journalism, which provided information about how to detect deepfake images in anticipation of the US and UK 2024 elections: https://reutersinstitute.politics.ox.ac.uk/news/spotting-deepfakes-year-elections-how-ai-detection-tools-work-and-where-they-fail accessed 26 August 2024.

text-based AI tool (such as Google's 'Gemini' – a chatbot which Google claims can 'supercharge your ideas')[110] generates results after a text prompt which contains defamatory information about a third party, and in effect publishes these to the human chat recipient or user. Widespread use of AI tools is still largely in its infancy and many users attest to repeated inaccuracies of results generated from text prompts or questions.[111] For example, if one uses an AI tool in order to search for a particular peer-reviewed article on a certain subject, an AI tool may boldly claim one exists and provide a citation – which is entirely false.[112] Many believe this is because, through machine learning, AI tools develop a bias to appear functional to a user and to 'please' by providing a result even when one does not exist. The reputational implications of an AI tool giving the false impression that a real individual has said, done or written something they have not are obvious.

Conclusion for Chapter 1

This chapter has argued that contemporary technological advancements have shaped and changed society such that increased threats to reputation are now widespread. Two types of advancement have been discussed: advancements that are, on the one hand, general and societal and, on the other, advancements of specific technologies presenting new threats to dignity. General developments (that impact not just the UK but

[110] See https://gemini.google.com/?hl=en accessed 26 August 2024.

[111] Readers can easily try this themselves by engaging with an AI tool and prompting it to tell them which article was written by person X on subject Y. What can be found is that, on occasion, the AI tool will entirely fabricate results. It also presents these results 'confidently' – see Thomas Lee, Daniel Campbell, Abhinav Rao, Afif Hossain, Omar Elkattawy, Navid Radfar, Paul Lee and Julius Gardin, 'Evaluating ChatGPT responses on atrial fibrillation for patient education' (2024) 16(6) *Cureus* e61680.

[112] Ibid.

many populations throughout the world) include the birth of social media and the increasing prevalence of internet-enabled devices. As handheld technology becomes more affordable, it also becomes increasingly commonplace in society and therefore more frequently used and ingrained into daily ways of life. This in turn changes patterns of human behaviour. Wider engagement with the internet in professional and private lives leads to the increasing likelihood that someone may upload potentially defamatory information about another to the web, as disclosures online are normalized. The advent of social media in the early 2000s shows no signs of stopping; although the *type* of social media site has altered in popularity,[113] engagement with social media continues to thrive. Posting personal and (potentially) defamatory information about another using a social media website is a convenient dissemination tool, able to be accessed more readily than print newspapers. There is now the additional concern of posts 'going viral' and amassing millions of views, and further difficulties of removing the online information that are not faced in the same way by purely print publications. The other type of advancement that this chapter has evaluated is the purely technological. Cloud computing powers websites and makes social media possible, storing vast data sets virtually – accessed using log-in credentials from anywhere. Virtual worlds, augmented reality and AI present unique threats to reputation. Virtual worlds can allow individuals to hide behind avatars but engage with other real people, and use a virtual world system to defame others by using voice or text. Augmented reality disrupts what we understand to be 'real' or 'fake' and can use false images overlaid onto real-life backgrounds to distort reality and engender a defamatory meaning. Advancements in AI can lead to a wide range of defamatory implications: chatbots could give misleading impressions about individuals they represent and

[113] Websites such as Snapchat or TikTok.

disclose false and damaging personal information about others (or their users), deepfakes can be used to spread likenesses of real people engaged in reputationally damaging activities, and AI tools can create and spread false personal information via their search results.