FREE SPEECH ONLINE:

Regulating the internet without impeding free speech.

Louis Stuart Eastwood Fairweather (LLB Hons, MSc).

Submitted in fulfilment of the requirements of the Degree of Master of Laws by Research.

School of Law,

College of Social Sciences,

University of Glasgow.

May 2024

Abstract

This thesis considers the free speech implications of applying a harms-based approach to internet regulation. The Online Safety Act 2023, which was enacted in the United Kingdom in October 2023, aims to regulate content and activity online based on its capacity to cause harm. In doing so, it imposes new duties on providers of online services and grants OFCOM new powers to hold these providers accountable for any failure to carry out their duties under the Act. Similarly, proposals have been put forward by the Law Commission of England and Wales to reform the current criminal law concerning communications sent over public electronic communications networks (section 127(1) of the Communications Act 2003), and to replace this with a harms-based offence. This thesis seeks to identify which type of speech (if any) causes harm and will examine the extent to which legislation that targets speech based on its capacity to cause harm risks impeding our right to free speech.

Table of Contents

INTRODUCTION

"Online safety is one of the most complex and most fundamental policy issues of our age."

- Joint Committee on the Draft Online Safety Bill.[1]

This thesis was inspired by the discourse surrounding the Online Safety Bill, prior to the bill receiving royal assent and becoming the Online Safety Act 2023[2] in October 2023. The Act came into being more than three years after it was first proposed by the government,[3] and a further one year after the government consultation on online harms began in April 2019.[4] The passage of the bill was subject to several external challenges, including the frequent changes of government that took place in the United Kingdom over this time, which undoubtedly contributed to the delay. However, much of the delay can be attributed to the time required by members of parliament to duly consider the most complex issues within the bill – not least how the bill might impact upon free speech. As such, the bill was subject to substantial changes as it progressed through parliament – the original approach within the bill, which sought to tackle content and activity online solely on the basis that it caused harm to adults, was completely abandoned on 28th November 2022[5] (leading to further delay as the bill had to be recommitted to the Public Bill Committee to allow debate on the amendments).[6]

The Online Safety Bill also originally contained provisions intended to resolve wider concerns about the state of communications offences in the United Kingdom beyond internet safety. The Law Commission of England and Wales notes that *"offensive and abusive online communications"* was one of the most widely supported areas for reform following consultations it held in 2016 and 2017.[7] Following a lengthy consultation on the subject of

[1] Joint Committee on the Draft Online Safety Bill, *Draft Online Safety Bill: Report of Session 2021-22* (HC & HL 2021-22), para 465.
[2] Online Safety Act 2023.
[3] Department for Culture, Media & Sport and the Home Department, *Online Harms White Paper: Full Government Response to the consultation* (White Paper, CP 354, 2020), para 42.
[4] Department for Culture, Media & Sport and the Home Department, *Online Harms White Paper* (White Paper, CP 57, 2019).
[5] John Woodhouse, Online Safety Bill: Progress of the Bill (Commons Library Research Briefing, Number 9579, 2023) ch 4.
[6] Department of Culture, Media & Sport, *Online Safety Bill: Update*, (Written Ministerial Statement, HCWS39, 29 November 2022).
[7] Law Commission, *Abusive and Offensive Online Communications: A Scoping Report* (Law Com No 381, 2018), para 1.

harmful communications, the Law Commission concluded that the criminal law governing harmful communications offline was unfit for purpose. The Law Commission proposed a new harms-based offence[8] which was intended to replace section 127(1) of the Communications Act 2003[9] (the primary piece of criminal legislation used to prosecute online communications) which would apply to both offline and online communications. Initially, the Law Commission's proposal was well-received, and the harms-based offence to repeal section 127(1) of the Communications Act 2003 appeared in the first version of the bill that entered parliament.[10] However, it was eventually dropped at the report stage in the House of Commons with the government concluding that the sudden repeal of section 127(1) would put victims of domestic abuse at risk, as that provision is often relied upon to prosecute abusive communications sent in this context.[11] Thus, section 127(1) of the Communications Act 2003 remains in force.

Despite the fact that the government abandoned the Law Commission's proposal, there is some common ground between the approach that the government has taken through the Online Safety Act 2023 and the approach suggested by the Law Commission. Both the Online Safety Act 2023 and the proposal by the Law Commission target speech based on its capacity to cause harm. Hence, in assessing the likely impact of this harms-based approach upon free speech, this thesis will answer the following questions:

1. What type of speech causes harm?
2. In what ways does the internet exacerbate harm caused by speech?
3. To what extent might the Online Safety Act 2023 impede upon free speech protections in the United Kingdom?

The thesis is divided accordingly:

Chapter One – Speech and Harm; introduces some of the arguments which are often invoked to justify the protection of free speech. Chapter one also introduces John Stuart Mill's "harm principle", which argues that the only legitimate reason to restrict an individual liberty is to prevent harm to others. The harm principle will be used as a standard to assess the legitimacy of the harms-based offences discussed throughout the thesis. Chapter one also includes discussion on the stance of the European Court of Human Rights in restricting free speech

[8] Law Commission, *Modernising Communications Offences: A final report* (Law Com No 399, 2021), para 2.257.
[9] Communications Act 2003, s.127.
[10] Online Safety HC Bill (2022-2023) [220] s.150.
[11] HC Deb, 5 December 2022, vol 724, col 45.

to protect health, morals, and the rights and reputations of others – all of which are key concerns of the harms-based offences.

Chapter Two – Free Speech and Communications Offences; discusses section 127(1) of the Communications Act 2003 and highlights the free speech concerns of the communications offences. This section will also consider the harms-based proposal of the Law Commission which was intended to replace section 127(1) of the Communications Act 2003 and evaluate the extent to which it might have enhanced protection for free speech in the United Kingdom.

Chapter Three – The Online Safety Act 2023; introduces the Online Safety Act 2023 and discusses the extent to which the Act may adversely affect free speech protections in the United Kingdom

Methodology

Chapter one takes a normative approach in formulating a solution to internet regulation which impedes as little as possible on free speech, by introducing Mill's harm principle and considering how this may be interpreted to tackle the harms present online. Mill's harm principle will be referred to throughout the thesis in the discussion of the harms-based offences, as it provides a model which limits the restriction of free speech only to the extent that such restriction prevents harm to others.

The thesis also takes a doctrinal approach in other respects. In chapter one, the thesis will analyse the case-law of the European Court of Human Rights to ascertain the stance of the European Court of Human Rights in restricting free speech to protect health, morals and the rights and reputations of others. Chapter two will analyse a selection of cases concerning prosecutions under section 127(1) of the Communications Act 2003 and highlight the impact that the prosecution of communication offences under this Act has had upon free speech. And finally, Chapter three will analyse the Online Safety Act 2023, and detail the approach that it has taken to tackle harms online.

This introduction may have illustrated the complexity of online safety (as highlighted by the Joint Committee on the Draft Online Safety Bill), however, little has been said yet on the "fundamental" nature of the challenge facing policymakers worldwide in approaching online safety. To quote Lee Bollinger and Geoffrey Stone, whose 2023 book *"Social Media, Freedom of Speech, and the Future of our Democracy"* provides tremendous insight into

many of the issues discussed throughout this thesis, social media platforms *"far surpass any historical antecedents in their scope and power to spread information and ideas."*[12] The internet is unparalleled as a means of communication, and it has permeated the lives of most adults and children. Furthermore, the capacity of the internet to spread information far and wide applies to harmful communications as well as harmless communications. This is, undoubtedly, what the Joint Committee on the Draft Online Safety Bill was referring to when they categorised online safety as a fundamental policy issue. However, it is just as fundamental that policymakers find the right balance between tackling harmful communications and allowing freedom of speech in seeking to resolve this issue. The internet has allowed for the realisation of free speech where such realisation may not have otherwise been possible. The internet played a crucial role in allowing pro-democracy protestors to exercise their free speech in the pro-democracy protests which swept through the Middle East and North Africa in the early 2010s.[13] Communication platforms such as WhatsApp and Telegram which offer end-to-end encryption allow individuals to communicate with one another around the globe in complete privacy – preventing even the host service from intercepting the communications.[14] Online forums and chatrooms have provided a means for individuals to participate in discussions on all matters. And finally, considering the freedom of expression also includes a right to receive information, the wide (seemingly unlimited) range of information available on the internet should be acknowledged as well as the functionality of search engines which makes information on almost any topic available to any user within seconds. Hence, whilst it is correct to say that ensuring the online safety of users is fundamental, the protection of free speech online is also of crucial importance. By concentrating on the protection of free speech online, this thesis aims to highlight the risk to free speech posed by the communications offences and, most notably, by the Online Safety Act 2023.

[12] L. Bollinger and G. Stone, Regulating Harmful Speech on Social Media: The Current Legal Landscape and Policy Proposals (New York, 2022; online edn, Oxford Academic, 18 Aug. 2022), xxiii.
[13] Howard, Philip N., and Muzammil M. Hussain, 'Digital Media and the Arab Spring, 'Democracy's Fourth Wave? Digital Media and the Arab Spring', [2013] Oxford Studies in Digital Politics, 17, 18.
[14] WhatsApp, *'About end-to-end encrypted backup'* (WhatsApp, 2023) < https://faq.whatsapp.com/490592613091019> accessed 22 September 2023

CHAPTER ONE: SPEECH AND HARM

> *"The only purpose for which power can be rightfully exercised over any member of a civilised community, against his will, is to prevent harm to others."*
>
> - John Stuart Mill, *On Liberty.*[15]

In his seminal essay *On Liberty*, John Stuart Mill argued that there was only one legitimate reason to restrict an individual's liberty: to prevent harm to others. This principle is often referred to as the harm principle. In Mill's view, human liberty comprises; liberty of thought and speech, liberty of tastes and pursuits, and freedom of assembly.[16] The same concepts appear in the constitutions of liberal democracies and international human rights treaties, and are often awarded robust legal protection. For example, several of these same concepts appear in the Universal Declaration of Human Rights 1948 which considers freedom of thought,[17] freedom of expression,[18] and freedom of assembly[19] to be inalienable rights applying to all humans.[20] Hence, Mill's harm principle lends itself well to academic discourse on the limits of our most fundamental rights, as it proposes one single legitimate reason for interfering with these rights.

This thesis will apply Mill's harm principle to the regulation of communications in the United Kingdom. There is good reason to apply the harm principle to the regulation of communications – recent attempts in the United Kingdom to reform communications offences has given rise to several proposals for harms-based communications offences. Some of these proposals have been more successful than others. Chapter two will focus on the unsuccessful proposal by the Law Commission of England and Wales to repeal and replace section 127(1) of the Communications Act 2003[21] with a harms-based offence.[22] Chapter three will focus on the evolution of the bill which became the Online Safety Act

[15] John Stuart Mill, On Liberty (first published 1859), 15.
[16] Ibid.
[17] Universal Declaration of Human Rights 1948, Art. 18.
[18] Ibid, Art. 19.
[19] Ibid, Art.20.
[20] Ibid, Preamble.
[21] Communications Act 2003, s.127.
[22] Law Commission, *Harmful Online Communications: The Criminal Offences - A Consultation Paper* (Law Com No 248, 2020) para 5.49.

2023[23] when it received royal assent in October 2023, which also follows a harms-based approach.

Before examining the legal landscape in the United Kingdom, this opening chapter will answer some preliminary questions. The first section will focus on why free speech is important (and therefore, why it is worth defending). The second section will discuss the grounds on which free speech may be legitimately restricted, through Mill's harm principle and under European human rights law, introducing the two key standards which will be used to assess the appropriateness of the measures proposed to tackle online harms which are discussed throughout this thesis. And finally, the third section will detail the unique aspects of the internet, as compared to other modes of communication, and consider how the capacity for a communication to cause harm may be exacerbated where that communication is sent over the internet.

1.1. The importance of free speech.

One could argue that speech ought to be protected for its epistemic, democratic, or artistic value – however, there is little epistemic, democratic, or artistic value to the grossly offensive, indecent, or menacing communications discussed in chapter two. Nor is there any epistemic, democratic, or artistic value to much of the harmful content that is targeted by the Online Safety Act 2023[24] and discussed in chapter three, (for example, communications which promote or encourage suicide).[25] However, that is not to say that this speech is unimportant or should not be protected. All speech benefits from the argument that speech is an essential component of our humanity. This is reflected in *On Liberty*[26] and the text of human rights treaties (such as, the Universal Declaration of Human Rights 1948).[27] Mill takes this argument further and asserts that allowing free speech is essential for self-development and happiness.[28] Similarly, the Universal Declaration of Human Rights 1948 is drafted to protect the rights which are essential to human dignity and worth.[29] Whilst it makes no comment that the rights contained within should allow for self-development, it is premised on the idea that protecting these rights should allow social progress and better

[23] Online Safety Act 2023.
[24] Online Safety Act 2023.
[25] Ibid, s.61(3).
[26] John Stuart Mill, *On Liberty* (first published 1859), 15.
[27] Universal Declaration of Human Rights 1948, Preamble.
[28] John Stuart Mill, *On Liberty* (first published 1859), 67.
[29] Universal Declaration of Human Rights 1948, Preamble.

standards of living.[30] Hence, it is consistent with Mill's idea that protecting these rights should result in human happiness. This link has also been established by the European Court of Human Rights, which has previously described freedom of expression as *"one of the basic conditions for each individual's self-fulfilment."*[31] This section will first explore this argument that speech is an essential part of our humanity, and that the protection of free speech is essential to human happiness. Additionally, this section will briefly introduce some of the other arguments that are often invoked in defence of free speech (particularly, those which are relied upon by John Stuart Mill and in international law).

Our ability to demonstrate our consciousness, ('consciousness' defined by John Locke as *"the perception of what passes in man's own mind"*[32]), is what makes us human. Humans are not the only conscious beings; however, human beings are more capable of demonstrating consciousness and thought than any other being. Other beings, such as the African grey parrot, are capable of demonstrating consciousness. However, human consciousness is still considered to be the golden standard – this is evident from the *Cambridge Declaration on Consciousness* penned in 2012 which defined the level of consciousness demonstrated by the African grey parrot (the most advanced demonstration of consciousness by any type of bird) as *"near human-like."*[33] Alexander Spirkin, a philosopher and psychologist specialising in consciousness, wrote that *"speech is the material expression of thought."*[34] Mill, who conceptualised freedom of speech as an extension of freedom of thought and consciousness,[35] would likely agree. Speech is an essential part of our humanity because it is an expression of the internal processes which determine that we are human (consciousness and thought).

If we accept that speech is part of what makes us human, then that contention may already sufficiently justify the protection of free speech. However, Mill elaborates further on the importance of protecting free speech. Mill argues that allowing humans to live freely (including allowing them to speak freely), consequently allows humans to develop

[30] Ibid.
[31] *Hurbain v. Belgium* App no 57292/16 (ECtHR, 4 July 2023), 176.
[32] John Locke, *An Essay Concerning Humane Understanding*, (first published 1690, Project Gutenberg 2004), Book II, Ch 1, paragraph 19.
[33] Philip Low, 'The Cambridge Declaration on Consciousness' (The Francis Crick Memorial Conference, Cambridge University, 7 July 2012) < https://fcmconference.org/img/CambridgeDeclarationOnConsciousness.pdf> 23 January 2024.
[34] Alexander Spirkin, *Dialectical Materialism* (Progress Publishers 1983), 191.
[35] John Stuart Mill, *On Liberty* (first published 1859), 15.

individuality, which is essential for their well-being.[36] Mill argues that *"the mental and moral, like the muscular powers, are improved only by being used"*[37], and provides the example that an individual's reason may be weakened if they adopt an opinion that they do not agree with, if they do so simply because others hold that opinion. On the contrary, sharing a contrasting opinion and engaging others in discussion allows individuals to exercise and strengthen their mental powers. Whether they leave the discussion with a different perspective or more steadfast in their own belief is irrelevant, as they have exercised their individuality which is beneficial to their well-being.

Unlike *On Liberty*, the Universal Declaration of Human Rights 1948[38] makes no proclamation as to the importance of respecting liberty (or the rights which Mill argues are essential to human liberty) in order to allow individual development. Instead, the Universal Declaration of Human Rights 1948 draws a direct link between the rights and freedoms contained within and wellbeing. Moreover, the liberties which Mill states must be protected for the sake of individuality and wellbeing are all incorporated in the Universal Declaration of Human Rights 1948. Liberty of thought and speech are explicitly protected by Article 18[39] and Article 19[40] respectively. Freedom of assembly is explicitly protected by Article 20.[41] Whereas, the liberty of tastes and pursuits is awarded no explicit protection, but the freedom of *"framing the plan of our life to suit one's own character"*[42] is protected through the existence of other rights contained within the Universal Declaration of Human Rights 1948. (To name a few of the rights and freedoms which protect the liberty of tastes and pursuits within the Universal Declaration of Human Rights 1948, there is: freedom from discrimination;[43] right to life;[44] freedom from arbitrary detention;[45] freedom to leave one's country,[46] and the right to own property.[47]) Within the preamble of the Universal Declaration of Human Rights 1948, it is noted that *"the advent of a world in which human beings shall enjoy freedom of speech and belief and freedom from fear and want has been proclaimed as the highest aspiration of the common people."*[48]

[36] John Stuart Mill, *On Liberty* (first published 1859), 67.
[37] Ibid, 55.
[38] Universal Declaration of Human Rights 1948.
[39] Ibid, Article 18.
[40] Ibid, Article 19.
[41] Ibid, Article 20.
[42] John Stuart Mill, *On Liberty* (first published 1859), 16.
[43] Universal Declaration of Human Rights 1948, Article 7.
[44] Ibid, Article 3.
[45] Ibid, Article 9.
[46] Ibid, Article 13.
[47] Ibid, Article 17.
[48] Ibid, preamble.

Whilst both *On Liberty* and the Universal Declaration of Human Rights 1948 support the idea that the protection of fundamental rights is essential to improve human well-being, there are additional justifications for the protection of free speech found in both texts. Considering that the legislation and policy proposals to tackle online harms discussed throughout this thesis will be judged with reference to Mill's harm principle and the human rights law concerning free speech in the United Kingdom, it is important to provide a fuller picture of the importance of speech to Mill and to the United Nations in drafting the Universal Declaration of Human Rights 1948.[49] In addition to the argument that the recognition of human liberty will improve well-being, Mill argues that speech has an epistemic value and ought to be protected.[50] On the other hand, a large part of the basis for the inclusion of free speech within the Universal Declaration of Human Rights 1948[51] was the protection of democratic principles. Therefore, the remainder of this section will focus briefly on these additional defences of free speech which provide a fuller picture of its importance according to Mill and in international law, respectively.

Mill arrived at the conclusion that the only legitimate reason to restrict an individual's liberty is to prevent harm to others when considering how best to protect against *"the tyranny of the prevailing opinion and feeling."*[52] Mill goes on to argue:

> *"If all mankind minus one were of one opinion, and only one person were of the contrary opinion, mankind would be no more justified in silencing that one person, than he, if he had the power, would be justified in silencing mankind."*[53]

This is a natural progression of Mill's argument that freedom of speech is an extension of freedom of thought, as it further asserts that all individuals should be free to express their thoughts. Mill describes the silencing of opinions as a *"peculiar evil"*, arguing that:

> *"If the opinion is right, [the human race] are deprived of the opportunity of exchanging error for truth: if wrong, they lose, what is almost as great a benefit, the clearer perception and livelier impression of truth, produced by its collision with error."*[54]

[49] Ibid..
[50] John Stuart Mill, *On Liberty* (first published 1859), 19.
[51] Universal Declaration of Human Rights 1948, Article 19.
[52] John Stuart Mill, *On Liberty* (first published 1859), 9.
[53] Ibid, 18.
[54] Ibid, 19.

The concept articulated by Mill in this passage is often referred to as the *"marketplace of ideas."*[55] It rests on the assumption that a *"free trade in ideas"* will allow truth to prevail.[56] It was also articulated by John Milton more than 200 years prior to Mill, when he wrote:

"Though all the winds of doctrine were let loose to play upon the earth, so Truth be in the field, we do injuriously, by licensing and prohibiting, to misdoubt her strength. Let her and Falsehood grapple; who ever knew Truth put to the worse, in a free and open encounter?"[57]

As aforementioned, John Stuart Mill's argument is framed to emphasise the important role that free speech plays in allowing humans to develop individuality. Hence, protecting all opinions against any *"tyranny of prevailing opinion"* is one of Mill's key concerns. The entirety of chapter two of *On Liberty* is dedicated to asserting the strengths of a marketplace of ideas. Additionally, where Mill makes his argument that free speech is essential to well-being in chapter three of *On Liberty*, this is also based on the argument that entering into a free exchange of opinions can strengthen a person's individuality and well-being.

Whilst Mill emphasises the benefits that allowing free speech may have upon individuals, arguments in favour of the democratic value of speech often emphasise the wider societal benefits of free speech. The Universal Declaration of Human Rights 1948, for example, boldly asserts that the recognition of the rights and freedoms contained within will be the foundation for justice and peace in the world. [58] Naturally, this includes freedom of expression.[59] The Universal Declaration of Human Rights 1948 was the result of a concentrated effort following the end of World War II to prevent states from committing the atrocities of the Nazi government in Germany.[60] It was hoped that by enshrining these fundamental rights and freedoms in international law, it would prevent malevolent actors from disregarding them, as had happened throughout the course of the war.[61] The Universal Declaration of Human Rights 1948 was intended to compel states to uphold the rights and freedoms which are central to human dignity, and to provide a mechanism for states to hold one another accountable. Hence, the Universal Declaration of Human Rights 1948 provides

[55] United States v Rumely 345 U.S. 41, 56 (1953).
[56] Abrams v United States 250 U.S. 630 (1919).
[57] John Milton, Areopagitica (first published 1644).
[58] Universal Declaration of Human Rights 1948, preamble.
[59] Ibid, Article 19.
[60] 'Report of the Drafting Committee to the Commission on Human Rights' Drafting Committee on an International Bill of Human Rights (New York 9-25 June 1947) (1 July 1947) UN Doc E/CN. 4/21.
[61] Ibid.

that limits to the fundamental rights and freedoms shall be determined by law for the purpose of securing the due recognition and respect for the rights and freedoms of others and of meeting the just requirements of morality, public order and the general welfare in a *democratic* society (emphasis added).[62]

Mill's argument that speech has an epistemic value, as well as the democratic concerns surrounding the inclusion of free speech in instruments of international human rights law, have an indirect relevance to this thesis. They may not be useful in mounting a defence of many of the communications which are captured by section 127(1) of the Communications Act 2003[63] or the Online Safety Act 2023,[64] however, they provide a fuller picture of why it was considered important by Mill and by the international community to protect free speech. The rules which were formed by both Mill and the international community in pursuit of this aim will be applied to the approach taken by the United Kingdom in respect of the communications offences detailed in chapter two and the online harms discussed in chapter three.

1.2. Limits of free speech.

On Liberty may be considered one of the most ardent defences of free speech ever written – yet, even Mill does not believe that free speech should be absolute. Similarly, national constitutions and international human rights treaties which protect free speech also often demarcate the limits to this freedom. Where constitutions and treaties contain no reference to any limits of free speech (such as, in the US Bill of Rights 1791),[65] such limits may eventually be set by courts with jurisdiction over free speech matters (such as, the Supreme Court of the United States, which has previously found that true threats,[66] fighting words,[67] obscenity,[68] copyright[69] and incitement to lawless action[70] should not be awarded free speech protection). This chapter will consider the limits to free speech under Mill's harm principle and European human rights law, to the extent that they may apply to harmful communications. This provides two important metrics to assess whether any impediment to

[62] Universal Declaration of Human Rights 1948, Article 29(2).
[63] Communications Act 2003, s.127.
[64] Online Safety Act 2023.
[65] US Bill of Rights 1791, First Amendment.
[66] *Watts v. United States* 394 U.S. 207 (1969).
[67] *Chaplinsky v. New Hampshire*, 315 U.S. 572 (1942).
[68] *Miller v. California,* 413 U.S. 24 (1973).
[69] *Harper & Row v. Nation Enterprises*, 471 U.S. 539 (1985).
[70] *Brandenburg v. Ohio* 395 U.S. 444 (1969).

free speech caused by the communications offences discussed in the following chapters can be justified.

John Stuart Mill argues that the prevention of harm to others is the only reasonable justification for the restriction of free speech.[71] However, Mill does not clearly define *"harm"* within *On Liberty*. And so, in order to gauge the applicability of Mill's harm principle to communications offences, it is important to ascertain what type of harm that could be inflicted upon others would warrant the restriction of speech. Within *On Liberty*, Mill offers one example where the exercise of free speech may cause harm, and thus, warrants punishment.

"An opinion that corn-dealers are starvers of the poor, or that private property is robbery, ought to be unmolested when simply circulated through the press, but may justly incur punishment when delivered orally to an excited mob assembled before the house of the corn-dealer, or when handed about among the same mob in the form of a placard."[72]

From this example, we can interpret the harm principle to include acts of direct physical harm to the corn-dealer. This is the clearest reason why it would be acceptable to express the sentiment that *"corn-dealers are starvers of the poor"* through the press, but not to express the same sentiment to an *"excited mob"*, as it is implied that the mob are prepared to carry out an act of retribution against the corn-dealer. There are other acts of retribution, not amounting to direct physical harm, which could constitute harm. For example, Mill's harm principle could also be interpreted to apply to destruction of property. Supporting this is Mill's argument that *"wherever [...] there is a definite damage, or a definite risk of damage, either to an individual or to the public, the case is taken out of the province of liberty and placed in that of morality or law."*[73] However, beyond examples which include a definite damage or a definite risk of damage, Mill provides no justification for restricting an individual's free speech to prevent any other types of harm to others.

When Mill speaks about harm, he uses terms which imply that the harm must be identifiable (*"damage"* has physical connotations) and that there must be a direct link between the speech and the harm caused (a *"definite risk"*). Therefore, applying the harm principle to speech, it is difficult to justify the restriction of any speech which does not also carry a

[71] John Stuart Mill, *On Liberty* (first published 1859), 15.
[72] Ibid, 52.
[73] Ibid, 75.

definite risk of causing identifiable damage. One of the key challenges facing policymakers seeking to regulate communications is defining the requisite effect that a communication must have upon the recipient in order to be considered criminal. For example, in the proposal for a harms-based offence put forward by the Law Commission of England and Wales which is discussed in chapter two, it is proposed that harm should be defined as emotional harm or psychological harm amounting to, at least, serious distress.[74] However, *"serious distress"* is not easily identifiable, and so, it is doubtful that Mill's harm principle could be interpreted to allow for the restriction of speech on the basis that it may cause serious distress to others unless the individual was able to demonstrate or evidence that distress.

Mill's harm principle provides a framework for determining the appropriate limits of our fundamental rights. However, it is also important to consider the limits which exist in practice, as set by the European Convention on Human Rights 1953.[75] Additionally, the European Court of Human Rights (ECtHR), which was established to uphold the rights contained within the convention, has deliberated on the limits within the convention and established certain principles in relation to free speech in Europe. The United Kingdom incorporated many of the rights contained in the European Convention on Human Rights 1953 (including the right to free speech) into domestic law through the Human Rights Act 1998.[76] Article 10 of the European Convention on Human Rights 1953 reads, as follows:

> *"1. Everyone has the right to freedom of expression. This right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers. This Article shall not prevent States from requiring the licensing of broadcasting, television or cinema enterprises.*
>
> *2. The exercise of these freedoms, since it carries with it duties and responsibilities, may be subject to such formalities, conditions, restrictions or penalties as are prescribed by law and are necessary in a democratic society, in the interests of national security, territorial integrity or public safety, for the prevention of disorder or crime, for the protection of health or morals, for the protection of the reputation or rights of others, for preventing*

[74] Law Commission, *Modernising Communications Offences: A final report* (Law Com No 399, 2021), para 2.257.
[75] European Convention on Human Rights 1953, Art.10(2).
[76] Human Rights Act 1998.

the disclosure of information received in confidence, or for maintaining the authority and impartiality of the judiciary."[77]

The possible justifications for restriction to free speech are often referred to as the *"legitimate aims."* Only two of these legitimate aims have been invoked by policymakers to justify the harms-based offences discussed in chapters two and three. Firstly, part of the justification behind the two communications offences discussed in chapter two is the protection of morals (though, not the protection of health). This includes section 127 of the Communications Act 2003, and its predecessor, section 10(2) of the Post Office (Amendment) Act 1935.[78] Whereas, the justification for the harms-based offence which was proposed by the Law Commission of England and Wales to replace section 127 of the 2003 Act[79] (and which is also discussed in chapter two) is based partly on the protection of health (though, not morals) and on the protection of the rights of others. Additionally, the types of content which are considered harmful under the Online Safety Act 2023 (discussed in chapter three), have also been designated as such for the protection of health (e.g., content which promotes of instructs self-harm or suicide),[80] and for the protection of the rights of others (e.g., bullying content).[81] Therefore, the remainder of this section will focus only on the legitimate aims of protecting health, morals, and the rights and reputation of others, and illustrate the approach taken by the ECtHR in a few selected cases.

Before delving further into the legitimate aims, it is important to note that any interference to free speech must also be prescribed by law and necessary in a democratic society, in order to be justified under Article 10.[82] In determining whether the interference is *"necessary"*, the court must establish that there is a *"pressing social need"* for the interference.[83] To establish a pressing social need, the restriction must be relevant and sufficient, and the interference must be proportionate to any one of the legitimate aims.[84] Therefore, like Mill, the European Court of Human Rights (ECtHR) also have a test to ensure that speech may be restricted only where the undesired effect is a direct result of that speech.

[77] European Convention on Human Rights 1953, Art.10.
[78] Post Office (Amendment) Act 1935, s.10(2).
[79] Communications Act 2003, s.127.
[80] Online Safety Act 2023, s.61.
[81] Online Safety Act 2023, s.62(5).
[82] European Convention on Human Rights 1953, Article 10(1).
[83] *Lingens v Austria* (1986) 8 EHRR 407, para 39-40.
[84] Ibid.

"For the protection of health or morals" is rarely invoked as compared to the other legitimate aims provided in Article 10. As of 22nd January 2024, there are 139 results on the ECtHR's online database for free speech cases concerning the protection of morals, and 104 results for free speech cases concerning the protection of health,[85] less results than exist in respect of any other legitimate aim. Whilst the protection of health and the protection of morals are grouped together in the text of Article 10, they can often be separated into two distinct aims.

In itself, *"speech which endangers health"* is a narrow field. It is difficult to imagine many instances of speech which endangers health to such a degree that there is a pressing social need to censor the speech in question. Speech which promotes the use of harmful substances (such as, alcohol or drugs) may fall within this category. *Ringier Axel Springer Slovakia, A.S. v. Slovakia (No 4)*[86] was a case brought before the ECtHR concerning a broadcasting company who claimed that their right to free speech was violated when they were fined for breaching laws relating to the promotion of drug use. The alleged offence occurred when one of their journalists interviewed a popular Slovak singer (identified as 'X' in the judgment) who spoke in favour of the legalisation of marijuana and suggested that he enjoyed using the drug.[87] It was acknowledged that the broadcasting company did not make the comments but disseminated them.[88] The ECtHR found that there had been a violation of the broadcasting company's free speech, arguing that the domestic courts *"did not give "relevant and sufficient" reasons indicating that the programme had intended to promote marijuana or induce drug use."*[89] Hence, there was no pressing social need to take action against the company which had broadcast the X's comments. The ECtHR has also previously considered the restriction of speech which promotes suicide, in the case of *Lings v. Denmark.*[90] In this case, the Supreme Court of Denmark had found a retired physician guilty of assisting suicide for offering advice to an individual who had sought his guidance on ending their life.[91] Interestingly, the Supreme Court of Denmark acknowledged that the publication of a guide by that same physician called *"Medicines suited for suicide"* which contained the same advice was perfectly legal, but that the physician had committed a crime

[85] European Court of Human Rights, 'HUDOC' (*European Court of Human Rights*) < https://hudoc.echr.coe.int/#{%22documentcollectionid2%22:[%22GRANDCHAMBER%22,%22CHAMBER%22]}> accessed 22 January 2024.
[86] *Ringier Axel Springer Slovakia, A.S. v. Slovakia (No.4)* App. no. 26826/16 (ECtHR, 23 September 2021).
[87] Ibid, para 5.
[88] Ibid, para 37.
[89] Ibid, para 39.
[90] *Lings v. Denmark* (application no. 15136/20, 12 April 2022).
[91] Ibid, 37.

by issuing advice to an individual based on this same guide.[92] The ECtHR found no fault with this argument, and agreed that there had been no violation of the physician's free speech in finding him guilty of assisting suicide.[93] Beyond demonstrating the types of speech that may be considered a danger to health, both of these cases also demonstrate that the publication or dissemination of this speech is not necessarily sufficient to warrant an interference with the individual's freedom of speech. In both cases, intent played a crucial role. The lack of intent to promote drug use absolved the broadcasting company of any wrongdoing in *Ringier Axel Springer Slovakia, A.S. v. Slovakia (No 4)*.[94] Whereas, in *Lings v. Denmark*, the performance of a *"specific act of assistance with the intent that an individual commit suicide"*[95] meant that Mr. Lings had committed a criminal act.

Regarding *"speech which may endanger morals"*, it seems archaic to criminalise speech on the basis of its moral character. Speech which is considered immoral may be indecent or offensive, but not necessarily harmful. The ECtHR delivered one of its most infamous defences of free speech in *Handyside v. United Kingdom*,[96] which was a case concerning a publisher who was convicted of breaching the Obscene Publications Act 1959 in England.[97] The Obscene Publications Act 1959 prohibits the publishing of all material which *"deprave[s] and corrupt[s] persons who are likely to have encountered it"* in England and Wales.[98] The obscene material in question in *Handyside v. United Kingdom* was a book called "The Little Red Schoolbook" which features a lengthy section on sex. [99] The ECtHR argued that:

> *"[Freedom of expression] is applicable not only to "information" or "ideas" that are favourably received or regarded as inoffensive or as a matter of indifference, but also to those that offend, shock or disturb the State or any sector of the population. Such are the demands of that pluralism, tolerance and broadmindedness without which there is no "democratic society."*[100]

Despite this seemingly defiant stance in support of offensive, shocking and disturbing speech – the ECtHR ultimately found that the authorities in the United Kingdom had acted within

[92] Ibid.
[93] Ibid, 57.
[94] *Ringier Axel Springer Slovakia, A.S. v. Slovakia (No.4)* App. no. 26826/16 (ECtHR, 23 September 2021), para 39.
[95] *Lings v. Denmark* (application no. 15136/20, 12 April 2022), 37.
[96] *Handyside v UK* (1976) 1 EHRR 737.
[97] Obscene Publications Act 1959.
[98] Ibid, s.1(1).
[99] *Handyside v UK* (1976) 1 EHRR 737, 20.
[100] Ibid, 49.

their margin of appreciation in restricting the publication of The Little Red Schoolbook[101] and that no violation of Article 10 had occurred.[102] It was noted that several other signatory states of the European Convention on Human Rights 1953 had allowed the publication of The Little Red Schoolbook and that each state was entitled to take their own approach to obscene material having regard to *"the different views prevailing there about the demands of the protection of morals in a democratic society."*[103] It is doubtful that the view that obscene material should be censored for the protection of morals would prevail in the United Kingdom today. Societal attitudes have changed dramatically since *Handyside v. the United Kingdom* was decided by the ECtHR in 1976. Jacob Rowbottom notes that there were only two convictions under section 2 of the Obscene Publications Act 1959 in England and Wales in 2015,[104] stating *"the kind of material targeted by the authorities which caused alarm in the 1960s, 70s and 80s [seems] relatively tame by contemporary standards."*[105] Hence, it is doubtful that the authorities in the United Kingdom would interfere with freedom of expression to prevent the publication of material which is akin to The Little Red Schoolbook in 2024, and even less likely that they would do so *"for the protection of morals*". Whilst states remain free to determine what restrictions to free speech are necessary based on an assessment of the prevailing views within that state on the protection of morals, the ECtHR's ruling that free speech should extend to speech which may *"offend, shock or disturb the State or any sector of the population"*[106] leaves no room for interferences to free speech for the protection of morals which fall outside this margin of appreciation.

The legitimate aim of *"protecting the rights and reputation of others"* allows the ECtHR to ensure that the exercise of free speech does not impede upon the other rights contained within the European Convention on Human Rights 1953.[107] It also allows for the existence of defamation laws. However, a difficulty arises when an objectively true statement is made which is prejudicial to the rights of others. The ECtHR often finds itself balancing an individual's freedom of expression as guaranteed by Article 10 with another individual's right to respect for privacy and family life as guaranteed by Article 8.[108] The ECtHR has also

[101] Ibid, 57.
[102] Ibid, 59.
[103] Ibid, 57.
[104] Jacob Rowbottom, The Transformation of Obscenity Law [2018] Information & Communications Technology Law, pg. 1.
[105] Ibid.
[106] *Handyside v UK* (1976) 1 EHRR 737, 49.
[107] European Convention on Human Rights 1953.
[108] Ibid, Article 8.

interpreted the protection offered by Article 8 to include reputational damage which could cause personal, social, psychological or economic suffering to the individual.[109] All things considered, this would appear to pose a threat to free speech protection, particularly as it relates to press freedom, as it would theoretically allow the subjects of press reporting to claim that their Article 8 rights are being infringed by a press report which they find objectionable (even if that report is true). However, to mitigate the impact upon press freedom, the ECtHR duly considers any element of public interest in cases of this kind. *Hurbain v. Belgium*[110] provides an interesting insight in to how the ECtHR balances free speech with the right to respect for privacy and family life where the speech in question is an objectively true statement and the claim under Article 8 relates to an individual's right to protection from reputational damage which could cause psychological suffering.[111] Additionally, it was determined that the statement in question in *Hurbain v. Belgium* did not contribute to a debate on a matter of public interest,[112] which reduces the legal question facing the ECtHR to its core elements. Removing the public interest element, the ECtHR was simply being asked whether or not factual information may be censored simply because it has had an adverse effect on a particular individual. This echoes the key challenge facing policymakers identified above: what effect should a communication have upon an individual to warrant limiting the free speech of the communicator? Unfortunately, the ECtHR missed its opportunity to articulate a clear answer to this question.

Hurbain v. Belgium concerned a news publisher (*Le Soir*) who was ordered to anonymise the name of an individual (referred to in the judgment as 'G') in an old article which appeared in their publicly accessible internet archives. The article concerned a fatal road traffic accident in 1994, where G had been the responsible driver.[113] G had requested that the article was anonymised in accordance with his *"right to be forgotten"* (a right guaranteed by the Charter of Fundamental Rights of the European Union.)[114] In ordering *Le Soir* to anonymise the article, the Liège Court of Appeal found that G had suffered psychological harm from the continued availability of the article.[115] The ECtHR appeared to recognise the difficulty presented by the ambiguous definition of *"psychological suffering"* and noted that any person wishing to restrict another's access to information *"must demonstrate the actual*

[109] *Hurbain v. Belgium* App. no. 57292/16 (ECtHR, 4 July 2023), 189.
[110] Ibid.
[111] Ibid, 189.
[112] Ibid, 225.
[113] Ibid, 1.
[114] Charter of Fundamental Rights of the European Union 2000, Article 17.
[115] *Hurbain v. Belgium* App. no. 57292/16 (ECtHR, 4 July 2023), 234.

existence of significant harm."[116] This approach should ensure that any claim of personal, social, psychological or economic suffering caused by reputational damage is sufficiently serious before allowing an interference to free speech. It would even satisfy John Stuart Mill, as it appears entirely consistent with the harm principle. However, despite their argument that a strong harms-based approach was required to navigate this difficult legal question, the ECtHR ultimately took no such approach. Instead, they seemed satisfied that the Liège Court of Appeal had *"attached importance to the serious harm suffered by G"*,[117] who had concluded that the article was a *source* of harm[118] to G (emphasis added). In a dissenting opinion drafted by Judge Ranzoni (and joined by Judges Kūris, Grozev, Eicke, and Schembri Orland), it was argued that *"G did not provide evidence that he had suffered serious harm, nor did the national courts demonstrate specifically that the continued availability of the article online was a source of such harm to his reputation."*[119] Hence, the dissenting judges share the view that the ECtHR allowed for the interference of free speech, despite the absence of any demonstration that G had suffered actual significant harm. *Hurbain v. Belgium* may be considered an anomaly, where the ECtHR deviated from their own safeguard against frivolous claims brought under Article 8 and allowed an interference to free speech which they ought not to have done. Nevertheless, it demonstrates the threat to free speech posed by the loosely defined concept of *"psychological suffering"*, wherever there exists a law that allows the curbing of free speech to prevent psychological suffering. *Hurbain v. Belgium* was decided on 4th July 2023, and it remains to be seen whether the ECtHR will demand the demonstration of actual existence of significant harm in future cases, or whether this case is the genesis of a new (more relaxed) approach which prioritises the protection of individuals from psychological suffering over free speech.

John Stuart Mill and the European Court of Human Rights share a lot of common ground in their views on the limits of free speech. One could interpret the harm principle to prohibit directly assisting an individual in their attempt to commit suicide, and yet, it would be much more difficult to interpret this principle to prohibit the publishing of a guide on medicines which are fatal to humans. The former presents a direct and identifiable harm, whereas the latter does not. Mill would also likely welcome the outcome in *Ringier Axel Springer*

[116] Ibid, 231.
[117] Ibid, 255.
[118] Ibid, 234.
[119] Ibid, Dissenting Opinion of Judge Ranzoni, joined by Judges Kūris, Grozev, Eicke and Schembri Orland, 17.

Slovakia A.S. v. Slovakia (No 4)[120], as it is doubtful that the harm principle could ever be interpreted to prohibit the promotion of harmful substances. (Responding to an abolitionist who asserted that the consumption of alcohol by other violated his social rights, Mill argued that this stance *"[ascribed] to all mankind a vested interest in each other's moral, intellectual, and even physical perfection"*[121] which is a complete interference with individual liberty.) Similarly, the proclamation in *Handyside v. United Kingdom* that the protection of free speech should extend to speech which offends, shocks or disturbs the state or any sector of its population[122] is entirely consistent with the harm principle – where there is no harm, there should be no interference. And although the ECtHR failed to demonstrate the actual existence of a significant harm in *Hurbain v. Belgium*, the approach which it sought to take directly mirrors the harm principle.

1.3. The "online" variable.

Most providers of online services carry out their own regulation of content on their platform. For example, Facebook uses artificial intelligence technology and human reviewers to *"find, review and take action on content"* that breaches their standards.[123] However, in the view of some policymakers, the self-regulation of platforms has been insufficient in protecting people from harms online. In the United Kingdom, the Online Safety Act 2023[124] (as discussed in chapter three) has been brought into force to allow OFCOM, the UK's communications regulator, to oversee the regulation of online services. This section will illustrate the features of the internet which are distinct from other modes of communication, and hence, have allowed for the amplification of harms online.

The internet is now an omnipresent force in the lives of many individuals. Therefore, where there is harm online, the risk of individuals encountering this harm has increased alongside the number of ways to access the internet. Additionally, internet users may be passively harmed by encountering harmful content online which is not necessarily directed towards them. Social media platforms such as Facebook and X have web feed features which collate posts shared by the user's friends or by pages to which the user has subscribed, (they may

[120] *Ringier Axel Springer Slovakia, A.S. v. Slovakia (No.4)* App. no. 26826/16 (ECtHR, 23 September 2021).
[121] John Stuart Mill, *On Liberty* (first published 1859), 83.
[122] *Handyside v UK* (1976) 1 EHRR 737, 49.
[123] Facebook Help Centre, 'How does Facebook use artificial intelligence to moderate content?' (*Facebook*) < https://www.facebook.com/help/1584908458516247> accessed 22 January 2024.
[124] Online Safety Act 2023.

also be recommended by a content recommendation algorithm – as discussed in the below paragraph). Individuals might also passively encounter harmful content whilst watching television. This was the view of the US Supreme Court in *FCC v. Pacifica Foundation*, when it found that broadcast television had limited free speech protection under the US Constitution, on account of the *"uniquely pervasive presence that medium of expression occupies in the lives of [...] people"* which *"extend[s] into the privacy of the home, and [...] is impossible completely to avoid.*"[125] In *Reno v. ACLU*, the US Supreme Court argued that the internet did not have the same uniquely pervasive character as broadcast television.[126] However, this case was decided in 1997 and it is doubtful that the Supreme Court would reach the same conclusion today. There is an argument that the internet has *"become at least as invasive as traditional broadcast media."*[127] Since 1997, there have been vast changes in technology which has increased the invasive character of the internet. Smartphones and tablet computers allow their user to access the internet wherever they are, due to their computer functions and their portability. OFCOM's adult media literacy tracker has found that, in 2020, 88% of adults (over the age of 16) accessed the internet using a smartphone and 43% accessed the internet using a tablet computer.[128] However, this technology was not readily available in 1997. Apple is currently a market-leading smartphone producer, yet the first generation of iPhone was first launched in 2007.[129] On the other hand, Samsung released the first smartphone from its flagship 'Galaxy' line in 2010.[130] The portability, popularity and capabilities of smartphones and tablet computers have all ensured that the internet is now much more invasive than television.

Additionally, the risk of harm posed by harmful content online is exacerbated by hidden algorithmic functions which are entirely unique to the internet. Social media networks (such as, Facebook,[131] X[132] and TikTok[133]) use content recommendation algorithms which collect data as users use their services and use this data to tailor content to the user. This may sound

[125] *FCC v. Pacifica Foundation*, 438 U.S. 726 (1978), 4.
[126] *Reno v. ACLU*, 521 U.S. 844 (1997), 869.
[127] L. Bollinger and G. Stone, Regulating Harmful Speech on Social Media: The Current Legal Landscape and Policy Proposals (New York, 2022; online edn, Oxford Academic, 18 Aug. 2022) xxxii.
[128] OFCOM, *Online Nation 2022 Report* (1 June 2022) 10.
[129] Steve Jobs, *Keynote Speech: MacWorld* (MacWorld Conference, San Francisco, 9 January 2007) < https://www.youtube.com/watch?v=MnrJzXM7a6o> accessed 22 December 2023.
[130] Samsung US, *Samsung Galaxy S - NYC Launch Event* (Samsung Galaxy S - Launch Event, New York City, 29 June 2010) < https://www.youtube.com/watch?v=Wf3uGTAeQy4> accessed 22 December 2023.
[131] Meta Privacy Centre, Privacy Policy (*Meta,* 15 June 2023) < https://www.facebook.com/privacy/policy/?entry_point=data_policy_redirect&entry=0 > accessed 19 November 2023.
[132] X, X Privacy Policy, (*X*), < https://twitter.com/en/privacy > accessed 28 November 2023.
[133] TikTok, Privacy Policy (*TikTok,* 19 November 2023) < https://www.tiktok.com/legal/page/eea/privacy-policy/en > accessed 16 February 2024.

helpful in principle. However, potentially harmful and false content is more engaging than innocuous or truthful content.[134] As a result, content recommendation algorithms can have a sinister effect. For example, a study by the Wall Street Journal determined that users who showed an interest in videos about depression and anxiety would be served mostly depression-related content by TikTok's algorithms. They found that 93% of videos recommended to such a user after having used the app for only 40 minutes were related to depression.[135] Additionally, the UK Government has heard evidence that algorithms also continue to feed individuals misinformation and disinformation after they have engaged with it once.[136] At the most extreme end of this spectrum, is content which glorifies or encourages behaviour associated with eating disorders, self-harm, or suicide. The parents of Chase Nasca, a sixteen-year-old boy from the United States, reported discovering thousands of videos promoting and encouraging suicide on the TikTok app on their son's iPad after he had taken his own life.[137] According to the Nasca family, there was no indication that their son had actively searched for this content – instead, it appeared on his "For You" page which recommends content through algorithms.[138]

There is an argument that Mill's harm principle cannot be applied to prevent acts of self-harm and suicide. After all, Mill argues that the only purpose which power can be rightfully exercised over an individual is to prevent harm to others - *"his own good, either physical or moral, is not a sufficient warrant."*[139] Hence, it would be difficult to argue that one should be prevented from seeking out information that could assist them in their attempt to cause themselves harm. However, considering that private companies are allowing for the disproportionate dissemination of such information through their platform to vulnerable individuals, it is consistent with Mill's harm principle to argue that their liberty should be restricted to prevent harm to others. It is also consistent with the approach taken in *Lings v. Denmark*[140] (as discussed in the previous section). If one sends a communication to an individual with suicidal tendencies encouraging them to commit suicide or promoting the concept of suicide, there is a definite risk that the individual will be prompted to do so (which presents an identifiable damage).

---

[134] Joint Committee on the Draft Online Safety Bill, *Draft Online Safety Bill: Report of Session 2021-22* (HC & HL 2021-22), para 38.
[135] Ibid, para 40.
[136] Ibid.
[137] The Nasca Family, http://chasenasca.com (The Nasca Family) <http://chasenasca.com> accessed 2 March 2024.
[138] Ibid.
[139] John Stuart Mill, *On Liberty* (first published 1859), 15.
[140] *Lings v. Denmark* (application no. 15136/20, 12 April 2022), 37.

Some have also argued that the capacity of the internet to store information leads to an increased risk of harm to individuals. This was the part of the reasoning of the European Court of Human Rights in *Hurbain v. Belgium* (discussed in the previous section), in finding that the there was no violation of free speech by the domestic authorities who had ordered a newspaper publisher to anonymise an article which appeared in their internet archives.[141] Considering the article concerned a fatal road traffic accident and included the name of the individual responsible, the Liège Court of Appeal had found that the individual responsible had suffered *"serious harm"* as a result of the *"continued online availability of the article with unrestricted access, which was apt to create a "virtual criminal record."*[142] The ECtHR took this into account in reaching the decision that the measures taken by the domestic authorities were *"necessary and proportionate"* and hence, there had been no violation of the publisher's right to free speech.[143] (As discussed in the previous section, the ECtHR satisfied themselves that this article was a *"source of harm"*, however, one could take the view that it was not demonstrated before the court that the applicant had actually suffered serious harm.) Whilst archives are not entirely unique to the online world, it is much more convenient for users to search archives which are made available on the internet. Additionally, the concern of the individual at the centre of *Hurbain v. Belgium*, was that the article could be discovered accidentally by any of his colleagues just through performing a general search of his name through any internet search engine.[144] Notwithstanding the argument in the previous section that there was no direct and identifiable harm to the applicant, the contention that any harm posed by online content could be exacerbated by the continued availability of that content seems valid. If it has already been established that an article in a newspaper caused direct and identifiable harm to one individual, then that individual could continue to sustain harm for as long as that article remains available. The old English adage that *"today's newspaper is tomorrow's fish and chip paper"* is no longer applicable in the digital era.

It has been argued that social media platforms *"far surpass any historical antecedents in their scope and power to spread information and ideas"*, due to the number of users and the promotion of content through algorithms.[145] Taking this argument further, it is not only

[141] *Hurbain v. Belgium* App. no. 57292/16 (ECtHR, 4 July 2023).
[142] Ibid, 234.
[143] Ibid, 254.
[144] Ibid, 20.
[145] L. Bollinger and G. Stone, Regulating Harmful Speech on Social Media: The Current Legal Landscape and Policy Proposals (New York, 2022; online edn, Oxford Academic, 18 Aug. 2022), xxiii.

social media that has surpassed historical antecedents in their power to spread information and ideas, but the internet generally. The enormous user bases and the promotion of content on social media networks allows for the dissemination of potentially harmful content online, whereas the permanent nature of the internet ensures that potentially harmful content remains accessible. However, whilst the internet may have revolutionised the spread of information, this is its only unique contribution to speech which makes potentially harmful content more problematic online as compared to offline. Hence, policymakers seeking to regulate the internet should avoid a content-based approach which could unjustly target content that is legal offline, and instead focus on the systems which exacerbate harms in a way that is unique to the online world. Tackling hidden algorithmic functions, for example, could be done without treating the promoted content in a manner that is different to how it is treated offline – hence, action could be taken without giving rise to any new concerns on the restriction of free speech.

1.4. Conclusion on speech and harm.

The battle to regulate the internet is already well underway. In the United Kingdom, the Online Safety Act 2023 was passed in October 2023.[146] In the European Union, proposals to allow judicial authorities to take measures to detect Child Sexual Abuse Material (CSAM) online have been met with criticism by the European Parliament's Civil Liberties Committee. The committee notes that *"balance between need to fight child sexual abuse online and to avoid generalised monitoring of the internet"* is required.[147] Consequently, proposals to regulate the internet are already having an impact on online services. WhatsApp has responded to proposals to end-to-end encryption in the United Kingdom by stating that they would not comply.[148] Meta's Head of WhatsApp, William Cathcart stated *"we've recently been blocked in Iran […], but we've never seen a liberal democracy do that."*[149] For other internet services, the pressure associated with conforming to new safety standards and

[146] Online Safety Act 2023.
[147] Civil Liberties Committee, 'Child sexual abuse online: effective measures, no mass surveillance' (*European Parliament*, 14 November 2023) < https://www.europarl.europa.eu/news/en/press-room/20231110IPR10118/child-sexual-abuse-online-effective-measures-no-mass-surveillance> accessed 1 December 2023
[148] Alex Hern, 'WhatsApp would not remove end-to-end encryption for UK law, says chief' (*The Guardian*, 9 March 2023) < https://www.theguardian.com/technology/2023/mar/09/whatsapp-end-to-end-encryption-online-safety-bill#:~:text=8%20months%20old-,WhatsApp%20would%20not%20remove%20end%2Dto%2Dend%20encryption,for%20UK%20law%2C%20says%20chief&text=WhatsApp%20would%20refuse%20to%20comply,in%20the%20UK%20in%20doubt.> accessed 1 December 2023.
[149] Ibid.

regulations has already caused them to close their operations. In a public statement, Leif K-Brooks (founder of the chatroom service Omegle) announced that he was closing the website down permanently, citing the stress and expense of meeting safety standards *"that are not humanly possible."*[150] Perhaps coincidentally, this announcement arrived less than ten days after the Online Safety Act was granted royal assent. K-Brooks' statement continued *"if something as simple as meeting random new people is forbidden, what next? [...] A healthy, free society cannot endure when we are collectively afraid of each other to this extent."*[151]

[150] Leif K-Brooks, Farewell Statement (*Omegle*, 4 November 2023) <www.omegle.com> accessed 1 December 2023
[151] Ibid.

CHAPTER TWO: FREE SPEECH AND COMMUNICATIONS OFFENCES

> *"Any offence that criminalises communication will almost certainly be an interference with freedom of expression. […] Nonetheless, the right comes first; it is the interference that requires justification."*
>
> - The Law Commission of England and Wales. [152]

Following a review of the communications offences, the Law Commission of England and Wales recommended that section 127(1) of the Communications Act 2003 and the Malicious Communications Act 1988 should be repealed and replaced with a new harms-based offence.[153] This chapter is primarily concerned with section 127(1) of the Communications Act 2003,[154] which is frequently used in the context of online communications, as it has been interpreted to apply to any communications sent through the internet.[155] Section 127(1) of the Communications Act 2003 reads, as follows:

> *"(1) A person is guilty of an offence if he—*
>
> *(a) sends by means of a public electronic communications network a message or other matter that is grossly offensive or of an indecent, obscene or menacing character; or*
>
> *(b) causes any such message or matter to be so sent."*[156]

It is similar to the section 1 of the Malicious Communications Act 1988,[157] however, there are two key differences. Firstly, criminality may only be found under section 1 of the Malicious Communications Act 1988 where the communication has been to another person.[158] As noted by the Law Commission, this *"[limits] the use of the offence to address communications posted in public fora such as Twitter and other social media platforms and websites."*[159] There is no such requirement in section 127(1) of the Communications Act 2003. Secondly, section 1 of the Malicious Communications Act 1988 expressly states that

---

[152] Law Commission, *Harmful Online Communications: The Criminal Offences - A Consultation Paper* (Law Com No 248, 2020) para 2.1.
[153] Law Commission, *Modernising Communications Offences: A final report* (Law Com No 399, 2021), para 2.38.
[154] Communications Act 2003, s.127(1).
[155] *Chambers v Director of Public Prosecutions* [2012] EWHC 2157 (Admin) [23]-[24].
[156] Communications Offences Act 2003, s.127(1).
[157] Malicious Communications Act 1988, s.1.
[158] Ibid.
[159] Law Commission, *Modernising Communications Offences: A final report* (Law Com No 399, 2021), para 1.4.

a person must intend to cause *"distress or anxiety"* to the recipient (or to any intended recipient) in order to be found guilty of an offence.[160] In contrast, there does not need to be an intended recipient to find a person guilty of an offence under section 127(1) of the Communications Act 2003 and the reaction of any recipient is irrelevant (as discussed in section 2.2). These are just two of the factors which make section 127(1) of the Communications Act 2003 more problematic than the Malicious Communications Act 1988. However, one key feature of both Acts is the criminalisation of speech based on character, which is also problematic considering the subjective nature of the term *"grossly offensive"* (criminalised under both Acts). Whilst section 1 of the Malicious Communications Act 1988 has been partly repealed and replaced by the Online Safety Act 2023 (only so far as it relates to the sending of false communications[161] and threatening communications),[162] section 127(1) of the Communications Act 2003 was untouched by the Online Safety Act 2003 and remains in full effect.

The first section of this chapter will examine the history of section 127(1) which has its roots in section 10(2) of the Post Office (Amendment) Act 1935[163] and offer some reflections on the applicability of this approach to communications in the modern age. Section two will demonstrate the flaws of section 127(1) in practice, by analysing cases where individuals have been held liable for sending grossly offensive, indecent, obscene and menacing communications over public electronic communications networks. And finally, the third section will consider the suitability of the Law Commission's proposed harm-based offence as a replacement for section 127(1).

Section 2.1: The Purpose of Section 127(1).

"The purpose of the legislation which culminates in section 127(1)(a) was to prohibit the use of a service provided and funded by the public for the benefit of the public for the transmission of communications which contravene the basic standards of our society" stated Lord Bingham in *DPP. v. Collins.*[164] As a result, the focus of section 127(1) is primarily to protect the integrity of the network, rather than to protect individuals from particular communications. To understand this approach to the criminalisation of communications, it

[160] Malicious Communications Act 1988, s.1.
[161] Online Safety Act 2023, s.179.
[162] Ibid, s.181.
[163] Post Office (Amendment) Act 1935, s.10(2)a.
[164] *Director of Public Prosecutions v Collins* [2006] UKHL 40 [7]

is important to understand the justification for the Post Office (Amendment) Act 1935, which followed the same approach.

2.1.1. The purpose of S.10(2) of the Post Office (Amendment) Act 1935.

Section 10(2) of the Post Office (Amendment) Bill was first proposed in order to protect telephone switchboard operators in the performance of their duties.[165] However, when this bill arrived at the Committee Stage of the House of Commons it was suggested that the protection of section 10 should be extended to customers of the General Post Office.[166] (The General Post Office controlled nearly all telephone services in the United Kingdom from 1 January 1912. The only exception was a municipal service owned by Hull Corporation, later Hull City Council).[167] Thus, the final product made it an offence for any person to send any message which was grossly offensive, indecent, obscene or menacing through the telephone.[168] The Postmaster General, Sir Kingsley Wood (Conservative Member of Parliament for Woolwich West) who proposed the provision argued that this was necessary *"in view of the considerable extension of the telephone."*[169] Hence, to understand the purpose of section 10(2)a of the Post Office (Amendment) Act, further consideration must be given as to why the general public needed protection in view of the *"considerable extension of the telephone"*, and why criminal legislation was the most appropriate means to meet this aim.

Firstly, the invention of the telephone had revolutionised social interaction. For the first time, individuals could instantly communicate with others over long distances. However, with the invention of the telephone came a new way for individuals to insult, abuse and threaten one another. Additionally, there was a lack of alternative non-legal remedies to deal with this issue. This matter was raised by the Postmaster General at the second reading in the House of Commons: *"complaints come through at all hours of the day, and the only remedy at the moment is to cut the person off the telephone altogether."*[170]

One must also consider that the General Post Office was a government service, and naturally, it was the responsibility of the government to regulate its own services. Several pieces of

[165] HC Deb, 15 March 1935, vol 299, col 769
[166] Ibid.
[167] The National Archives, *'Records created or inherited by the Post Office Telegraph and Telephone Service'* (The National Archives, 1853-1969) < https://discovery.nationalarchives.gov.uk/details/r/C343#:~:text=On%204%20April%201896%2C%20the,to%20the%20State%20in%201912.> accessed 29 June 2023
[168] Post Office (Amendment) Act 1935, s.10(2)a/
[169] HC Deb, 15 March 1935, vol 299, col 771
[170] Ibid, col 770

legislation had already come into force to bestow regulatory powers upon the Postmaster General over the services of the General Post Office. The power to *"acquire, work and maintain electric telegraphs"* had been conferred on the Postmaster General by the passage of the Telegraph Act 1868.[171] Forty years later, the Post Office Act 1908 allowed the General Post Office to regulate the sending or delivery by post of communications which were indecent, obscene, libellous, or grossly offensive.[172] Therefore, when the Postmaster General proposed to amend the Post Office Act to outlaw grossly offensive, indecent, obscene, and menacing communications by telephone, he was simply regulating the telecommunications under his control as he had done previously with the telegraph and the postal service.

2.1.2. The Communications Offences Act 2003 as a successor to the 1935 Act.

The only difference between the text of the two Acts is that the former prohibits communications of the proscribed character by telephone, and the latter prohibits communications of the same proscribed character by public electronic communications network. However, there have been broad political, technological, and societal changes between 1935 and 2003, which this one simple change in the text of the legislation fails to account for.

The difference between the reach of the 1935 Act and the 2003 Act is stark. The 1935 Act regulated a service entirely operated by the government for which there may have been no alternative means of regulation other than with the passage of legislation. The 2003 Act regulates the use of publicly owned infrastructure by users of privately-owned services. These privately-owned services are primarily responsible for the regulation of their own platforms. Similarly, the Postmaster-General was the individual primarily responsible for the regulation of the telephone services in 1935. .

Whilst it was noted in the discussions surrounding the Post Office (Amendment) Bill 1935 that there were no alternative non-legal remedies available to the recipient of a grossly offensive, indecent, obscene or menacing telephone call, there is now an abundance of non-legal remedies available to users of public electronic communications networks. Social media websites, such as X, typically have a range of user empowerment functions which allow users to control the content that they encounter on the platform.[173] The justification

[171] Telegraph Act 1868
[172] Post Office Act 1908, s.16
[173] Twitter Help Center, *'Using Twitter'* (Twitter) < https://help.twitter.com/en/using-twitter> accessed 29 June 2023

provided by the 1935 Act that there were no alternative remedies available to the public does not hold much weight today.

Finally, there is also an argument to be made that the change in social attitudes over the 20th century has negated the need for legislation against communications which are grossly offensive or obscene or indecent. To recall the statement made by Lord Bingham, which is cited at the opening of this section, the purpose of the legislation that culminated in section 127(1) was to prevent public communications networks being used for the transmission of communications which contravene the basic standards of our society. However, whilst the basic standards of our society have changed massively since 1935, this has not been reflected in the legislation as the terminology has remained unchanged. In their review of the communications offences, the Law Commission stated, *"it is striking that the offences in section 127 of the CA 2003 are almost a word-for-word repetition of the 1935 offences."*[174] This is also in spite of the fact that courts which protect freedom of expression in the United Kingdom have repeatedly emphasised that this protection should extend to offensive and obscene speech (such as in *Handyside v. United Kingdom*[175] as discussed in chapter one). In *Redmond-Bate v. DPP*, [176] Sedley LJ reaffirmed the principle that freedom of expression should extend to offensive speech, stating that *"freedom only to speak inoffensively is not worth having."*[177]

2.2. The Effect of Section 127(1).

An examination of the caselaw under section 127(1) supports the conclusion of the Law Commission that the criminal law concerning communications offences is misaligned.[178] As a consequence of this misalignment, criminal liability for the sending of grossly offensive communications can be found where the recipients have not felt grossly offended (*DPP. v. Collins*). There is also a wealth of alternative legislation which criminalises communications on a more appropriate basis, for example, if those communications incite racial hatred or if those communications constitute abuse. However, acts which could have been prosecuted under alternative legislation have instead been prosecuted under section 127(1), on the basis that the communications are grossly offensive (*Chabloz v. Crown Prosecution Service*), or

[174] Law Commission, *Abusive and Offensive Online Communications: A Scoping Report* (Law Com No 381, 2018) para 4.60
[175] *Handyside v UK* (1976) 1 EHRR 737
[176] *Redmond-Bate v Director of Public Prosecutions* [1999] EWHC Admin 733.
[177] *Redmond-Bate v Director of Public Prosecutions* [1999] EWHC Admin 733 [12].
[178] Ibid.

indecent (*Sutherland v HM. Advocate*). And finally, in the case of *Chambers v. DPP*,[179] a joke which made use of violent hyperbole resulted in a criminal conviction on the basis that it constituted a menacing communication, a conviction which was only overturned after a lengthy legal battle.

The cases selected for discussion here are not necessarily representative of prosecutions under section 127(1). They have been selected because they highlight the folly of prosecuting individuals based on the character of their communication, and the impact that this could have upon free speech. To provide a fuller picture of the effect of section 127(1), it is important to note that data from the Crown Prosecution Service suggests that 46% of prosecutions brought under section 127(1) relate to communications sent in the context of domestic abuse.[180] A further 18% of prosecutions from the same sample related to threats made to public sector workers and service providers (including social workers, health care professionals, housing officers and school staff).[181] The Law Commission of England and Wales noted that part of the reason that section 127(1) is relied upon in these instances is because section 127(1) does not require *"a course of conduct"* as per other harassment offences, and so, criminality can be established based on a single instance of a grossly offensive, indecent or menacing communication. The application of section 127(1) to tackling domestic abuse will be discussed further in section 2.3.2, as this was the ultimate reason provided by the government for failing to repeal section 127(1) through the Online Safety Act 2023.[182]

2.2.1. Grossly offensive communications.

There are two main reasons why the inclusion of grossly offensive communications in section 127(1) is problematic. The first issue, which has been identified by the Law Commission of England and Wales in their review of communications offences, is that the term *"grossly offensive"* is subjective.[183] The second reason, as argued in the previous section, is that protection of free speech ought to extend to offensive speech. This section will explore two of the cases which have been brought against individuals who misused the

[179] *Chambers v Director of Public Prosecutions* [2012] EWHC 2157 (Admin).
[180] Law Commission, *Harmful Online Communications: The Criminal Offences - A Consultation Paper* (Law Com No 248, 2020) para 3.108.
[181] Ibid.
[182] HC Deb, 5 December 2022, vol 724, col 45.
[183] Law Commission, *Modernising Communications Offences: A final report* (Law Com No 399, 2021), para 2.1.

public electronic communications networks by using them to send grossly offensive communications. In doing so, this section will illustrate that this is an insufficient basis on which to criminalise speech.

2.2.1.1. DPP. v. Collins

Collins was a resident in North West Leicestershire – the constituency of the former Member of Parliament for the Labour Party, David Taylor.[184] Collins contacted David Taylor's constituency office on several occasions to air his views on immigration and asylum policy.[185] He spoke to some members of staff within Taylor's office, and occasionally, left messages on the answering machine. On a number of these occasions, he used racist language (*"wogs", "pakis", "black bastards"* and *"niggers."*)[186] He was convicted under section 127(1) for using a public electronic communications network to send messages which were grossly offensive. The High Court judges found that the language used was not grossly offensive,[187] whereas the House of Lords found that the language used was grossly offensive and overturned the High Court's decision.[188]

At the High Court, Sedley LJ stated that *"what is offensive has to be judged by the standards of an open and just multiracial society"*[189] and *"whether a telephone message falls into this category has to depend not only on its content but on the circumstances in which the message has been sent and, at least as background, on Parliament's objective in making the sending of certain messages a crime."*[190] Applying this criteria to the communications in question, one could concede that the fact that Collins was a constituent trying to address his Member of Parliament is a relevant fact – this was also accepted by the House of Lords upon appeal.[191] However, the High Court placed great weight on the fact that nobody was grossly offended by the message. *"Had the respondent nevertheless found himself speaking on any of his calls to a member of an ethnic minority, it might well have been impossible, however stoically the hearer might have brushed it aside, to avoid the conclusion that the message was grossly offensive."*[192]

---

[184] *Director of Public Prosecutions v Collins* [2006] UKHL 40, [2]
[185] Ibid.
[186] Ibid.
[187] *Director of Public Prosecutions v Collins* [2005] EWHC 1308 (Admin), [3]
[188] *Director of Public Prosecutions v Collins* [2006] UKHL 40, [13]
[189] *Director of Public Prosecutions v Collins* [2005] EWHC 1308 (Admin), [11]
[190] Ibid.
[191] *Director of Public Prosecutions v Collins* [2006] UKHL 40, [12]
[192] *Director of Public Prosecutions v Collins* [2005] EWHC 1308 (Admin), [12]

At the House of Lords, Lord Bingham stated that criminal liability under section 127(1) cannot depend on the reaction of those who may hear or see the communication, as this is an unforeseeable contingency.[193] Lord Bingham took the view that a communication will be considered grossly offensive if it is couched in terms to cause gross offence to whom it relates,[194] and so it should make no difference whether the communication causes gross offence to the recipient. The outcome at the lower court may have been entirely different if this test had been applied, as Sedley LJ had conceded that the message had the capacity to be grossly offensive (and that it would be considered grossly offensive had someone who is a member of an ethnic minority group had heard it).[195] Considering that the message was couched in terms to cause gross offence to whom it relates and the language had been selected for its *"highly abusive, insulting, pejorative and offensive character"* the House of Lords reversed the decision of the High Court and found Collins guilty of sending a grossly offensive communication through a public electronic communications network.[196]

Collins illustrates a much larger problem with section 127(1). It is argued in section 2.1 that communications should not be criminalised on the basis that they are offensive. Section 127(1) criminalises communications on the basis that they have the capacity to cause gross offence (and that they are sent over a public electronic communications network). Hence, despite the fact that it is noted that none of the recipients were grossly offended, Collins was still charged with sending a grossly offensive communication. The House of Lords were correct in their application of the law, but the law itself is misaligned. Hence, the decision reached by the High Court seems more reasonable – Collins' actions should not be criminalised on the basis they are grossly offensive where they have not caused offence.

2.2.1.2. Chabloz v. Crown Prosecution Service.

Alison Chabloz had been in attendance at a meeting of a right-wing organisation called the London Forum at the Grosvenor Hotel in London.[197] Chabloz performed two antisemitic songs which she had written entitled *"Nemo's Antisemitic Universe"* and *"(((Survivors)))"*.[198] These performances were recorded and uploaded to YouTube by another individual. Chabloz then posted a hyperlink to the two videos on her blog

[193] *Director of Public Prosecutions v Collins* [2006] UKHL 40, [8]
[194] Ibid, [9]
[195] *Director of Public Prosecutions v Collins* [2005] EWHC 1308 (Admin), [12]
[196] *Director of Public Prosecutions v Collins* [2006] UKHL 40, [13]
[197] *Alison Chabloz v Crown Prosecution Service* [2019] EWHC 3094 (Admin), [7]
[198] Ibid.

"tellmemorelies.wordpress.com."[199] She faced two charges for sending a grossly offensive message by means of a public electronic communications network in respect of both of these hyperlinks.[200] Additionally, Chabloz faced a third charge for uploading a video to YouTube of herself performing another antisemitic song which she had written *"I like the story as it is – SATIRE!"*[201]

This case called before the High Court as an application for judicial review. Interestingly, there was no challenge to the conclusion that the songs themselves were grossly offensive.[202] Instead, Chabloz sought to challenge the lawfulness of the decision to prosecute her under section 127(1) of the Communications Offences Act 2003, as she claimed that her actions did not constitute the sending of a communication. In respect of the first two charges, counsel for Chabloz argued that the posting of a hyperlink did not *"cause an offensive message or other matter to be sent"* and that it was a neutral act by Chabloz.[203] In respect of the third charge, counsel for Chabloz argued that Chabloz had sent the video to the YouTube servers in California – and hence, no communication had occurred as one cannot communicate with an inanimate object.[204]

The issue presented by *Chabloz* is pertinent when considering the applicability of section 127(1) to online communications. There is no analogue equivalent of hyperlinks – they are unique to the online world. This new form of communication has presented a way for criminals to evade justice for more serious crimes by providing them with a way to distance themselves from illegal content. For example, in the parliamentary discussions on the Online Safety Bill prior to its enactment, John Nicholson (Scottish National Party Member of Parliament for Ochil and South Perthshire) warned about the practice *of "digital breadcrumbing"* by paedophiles online.[205] Digital breadcrumbing involves posting non-sexualised images of children on large platforms and using these pictures to link paedophiles to other unregulated websites.

In *Chabloz*, Coulson LJ took the view that the court must assess whether the sender is endorsing the material contained in the hyperlink, to establish if they had the intention to cause the message of the proscribed character to be sent.[206] Naturally, Chabloz endorsed the

[199] Ibid, [8].
[200] Ibid, [7].
[201] Ibid, [9].
[202] Ibid, [18].
[203] Ibid, [10]
[204] Ibid, [11]
[205] HC Deb, 19 April 2022, vol 712, col 128.
[206] Ibid, [33].

material contained in the videos, as they were recordings of her performing songs which she had composed. The court found that, by hyperlinking the material, Chabloz was not committing a neutral act but instead was endeavouring to widen the distribution of her own material.[207] Finally, the court determined that Chabloz had *"set in train the sending process"* by posting the hyperlink to her own blog. By putting in place the process under which the video was sent, Coulson LJ argued, it cannot be said that Chabloz did not send the video.[208] The defence offered by *Chabloz* in respect of the third charge that there was no communication, as the video was posted to a server which was an inanimate object and communications could not be made with or to an inanimate object, was quickly struck down by Lord Justice Coulson. There is nothing in section 127(1) which requires the communication to be made with a human being.[209] Such was the case in *Collins*, where the accused had left several grossly offensive messages on an answering machine. Hence, the application for judicial review was refused[210] and Chabloz was sentenced to 20 weeks imprisonment suspended for two years and banned from social media for 12 months.[211]

There is no doubt that the acts committed by Chabloz should be punishable by law, however, it is doubtful that section 127(1) of the Communications Offences Act 2003 was the most suitable means by which to prosecute Chabloz. Alternatively, Chabloz could have been prosecuted under section 19 of the Public Order Act 1986[212] for publishing written material which was abusive or insulting with intent to stir up racial hatred or in circumstances which racial hatred was likely to be stirred up. This provision was previously relied upon for the prosecution of a man who had uploaded antisemitic material to the internet in the case of *R v Sheppard & Whittle*.[213] The material uploaded by Sheppard, a pamphlet called *"Tales of the Holohoax"*, was found by the court to be likely to stir up racial hatred against Jewish people on the basis that it casts doubt on the existence of the Holocaust and suggests that Jewish people have a history of inventing false stories about the Holocaust.[214] The three songs composed by Chabloz share the same theme as Tales of the Holohoax. *"(((Survivors)))"*, for example, is written to cast doubt on the stories of Holocaust victims Irene Zisblatt, Elie Wiesel and Anne Frank by highlighting supposed inconsistencies in their

[207] Ibid, [28]
[208] Ibid, [30]
[209] Ibid, [37]
[210] Ibid, [42]
[211] BBC News, *'Alison Chabloz avoids jail over anti-Semitic songs'* (BBC News, 14 June 2018) <https://www.bbc.com/news/uk-england-derbyshire-44484632> accessed 29 June 2023
[212] Public Order Act 1986, s.19
[213] R v Sheppard & Whittle *[2010] EWCA Crim 65.*
[214] Ibid, [8]

stories.[215] In the chorus, Chabloz refers to the first two as *"fake survivors"* and suggests that they are fabricating their stories for financial gain. Not only does the Public Order Act 1986 allow for the prosecution of such material when published to the internet, but it also better suited to deal with the issue posed by Chabloz' actions. Ideally, Chabloz should not have been prosecuted on the basis that she used a public electronic communications network to send a grossly offensive communication, but rather, she should have been prosecuted on the basis that she distributed material which was likely to stir up racial hatred. *"Distributing material which is likely to stir up racial hatred"* is a more specific description of Chabloz' actions, and it conveys the seriousness of her offence in a way that *"sending grossly offensive communications by means of a public electronic communications network"* does not.

Despite this, it is nonetheless a positive aspect of *Chabloz* that Coulson LJ interpreted section 127(1) to apply to hyperlinked content. The view that the sender's connection with the hyperlinked material (for example, whether or not they endorse the material) is constructive, as it could prevent criminals from evading justice by distancing themselves from illegal content whilst also protecting free speech. For example, reporting on *Chabloz*, the MailOnline quoted the following lyrics from *"(((Survivors)))"*: "*did the Holocaust ever happen? 'Was it just a bunch of lies? Seems that some intend to pull the wool over our eyes."*[216] It has already been established that this communication is grossly offensive, and hence, the MailOnline have sent a grossly offensive communication through a public electronic communications network by sharing their article online. However, it is not reasonable to say that they should be subject to criminal proceedings over the transmission of language which they do not endorse.

2.2.2. Indecent or obscene communications – Sutherland v. HM Advocate.

Prosecutions for sending messages of an indecent or obscene character are the rarest of all prosecutions under section 127(1). This could be due, in part, to the alternative legislation which exists to deal with obscene and indecent communications. For example, section 33 of the Criminal Justice and Courts Act 2015 made it an offence to disclose private sexual photographs and films of others, without their consent with the intention to cause them

[215] Stephen Parker, *((Survivors)) - Alison Chabloz* (19 August 2022) <https://www.youtube.com/watch?v=SKA_5FPUW04> accessed 29 June 2023

[216] Chloe Louise, 'Anti-Semitic blogger, 58, who said gas chambers 'saved lives' and dubbed Auschwitz a 'theme park' appeals latest jail term for mocking Jewish people by changing lyrics of an Oliver Twist song' (Daily Mail, 23 February 2023) <https://www.dailymail.co.uk/news/article-11785867/Alison-Chabloz-said-gas-chambers-saved-lives-appeals-latest-jail-term.html> accessed 29 June 2023

distress.[217] Additionally, in Scotland, section 2 of the Abusive Behaviour and Sexual Harm (Scotland) Act 2016 makes it an offence to disclose or threaten to disclose an intimate photograph or film of another.[218] Even prior to the passage of the 2015 and 2016 acts, victims of revenge porn brought claims under the Data Protection Act 1998[219] (alleging that their right to privacy had been breached)[220] and the Criminal Justice and Licensing (Scotland) Act 2010[221] (claiming that the individual who had shared their photographs had behaved in a threatening or abusive manner by doing so).[222] *Sutherland v. HM Advocate*[223] stands as one of the few prosecutions under section 127(1) of the Communications Act 2003 for the publication of revenge porn. In this case, the victim had consensually shared a picture of her vagina with Sutherland, which Sutherland later posted to his own Facebook profile.[224] Sutherland pled guilty in Kilmarnock Sheriff Court.[225] As part of his sentence, Sutherland was subject to notification requirements under section 60 of Schedule 3 of the Sexual Offences Act 2003.[226]

This case only called at the High Court as an appeal against sentence, as Sutherland sought to have the notification requirements removed. Hence, the matter which the court had to deal with was not whether or not the message sent by Sutherland was of an indecent or obscene character (Sutherland had already pled guilty in this respect).[227] Instead, the court had to assess whether there was a *"significant sexual aspect"* to Sutherland's behaviour which allowed the sheriff to impose notification requirements under section 60 of the Sexual Offences Act.[228] Section 60 of Schedule 3 of the Sexual Offences Act 2003 only allows courts in Scotland to subject individuals to notification requirements under the Sexual Offences Act 2003, if they consider that there was a significant sexual aspect to the offender's behaviour in committing the crime.[229] This exists to protect the public from offenders from whom there is an *"ongoing perceived danger"* (such as, other sexual offenders, for whom there are automatic notification requirements).[230] The court stressed

[217] Criminal Justice and Courts Act 2015, s.33.
[218] Abusive Behaviour and Sexual Harm (Scotland) Act 2016, s.2.
[219] Data Protection Act 1998.
[220] *MM v BC, RS, Facebook Ireland Limited* [2019] NIMaster 5
[221] Criminal Justice and Licensing (Scotland) Act 2010
[222] *Aidan McHugh v Procurator Fiscal, Airdrie* [2015] HCJAC 86
[223] *Adam Sutherland v Her Majesty's Advocate* [2017] HCJAC 22
[224] Ibid, [6] – [7].
[225] Ibid, [1].
[226] Sexual Offences Act 2003, Sch 3 s.60
[227] *Adam Sutherland v Her Majesty's Advocate* [2017] HCJAC 22, [1].
[228] Ibid, [29].
[229] Sexual Offences Act, Sch 3 s.60
[230] Ibid, Sch 3.

that it was unclear how Sutherland would gain sexual gratification from posting the picture to his Facebook profile, as he already had unlimited access to the picture *"for whichever purpose he wished."*[231] Hence, they rejected the view of the appeal sheriffs who had initially refused leave to appeal that there was a voyeuristic element to the offence.[232] Sutherland's appeal against sentence was successful.

Despite the fact that no assessment of the criminality of the communication under section 127(1) was required by the court for the purpose of this appeal, Lord Turnbull offered some fascinating insights as to the operation of section 127(1) in relation to indecent and obscene communications. The most crucial observation made by Lord Turnbull is that, in this case, the communication would have been of the same indecent character when sent by the complainer to Sutherland as it was when Sutherland shared the picture to his Facebook profile. Whilst Lord Turnbull also notes that *"proportion and common sense"* shall restrain the Crown from bringing proceedings against the consensual sharing of intimate images,[233] this nevertheless demonstrates that section 127(1) is not suitable for dealing with cases of revenge porn. From a basic reading of section 127(1), the complainer would be guilty of the same crime as the accused.

2.2.3. Menacing communications – Chambers v. DPP.

As acknowledged by the Law Commission of England and Wales, menacing communications are *"more obviously worthy of criminalisation"* than grossly offensive or indecent communications.[234] There are several pieces of criminal legislation outlawing various forms of threats. Section 16 of the Offences Against the Person Act 1861 makes it an offence to threaten to kill another person, with the intent that other person would fear the threat would be carried out.[235] Section 1 of the Malicious Communications Act 1988 makes it an offence to send a threat to another person which causes distress or anxiety to the recipient.[236] However, unlike the other pieces of criminal legislation, section 127(1) makes no mention of a requisite intent by the sender or a requisite effect that the communication must have upon the recipient to induce criminal liability.

---

[231] *Adam Sutherland v Her Majesty's Advocate* [2017] HCJAC 22, [20]
[232] Ibid, [34]
[233] Ibid, [25]
[234] Law Commission, *Harmful Online Communications: The Criminal Offences - A Consultation Paper* (Law Com No 248, 2020) para 5.207
[235] Offences Against the Person Act 1861, s.16
[236] Malicious Communications Act 1988, s.1

The lack of clarity regarding the intent of the sender and the significance of the reaction of the recipient was at the heart of the case in *Chambers v. DPP*.[237] Paul Chambers was an individual who had booked a flight from Robin Hood airport in Doncaster. In the weeks prior to sending the communication, there had been disruption to travel from Robin Hood airport due to adverse weather conditions.[238] Eventually, Robin Hood airport had decided to close – prompting Chambers to post the following message on Twitter (now called 'X'):

"Crap! Robin Hood Airport is closed. You've got a week and a bit to get your shit together otherwise I am blowing the airport sky high!"[239]

Chambers was charged with sending, by means of a public electronic communications network, a message that had a menacing character.[240] This was the first case to call before the High Court concerning a prosecution under section 127(1) for the transmission of menacing communications.[241]

The Lord Chief Justice took the view that a communication must create a sense of fear or apprehension in those who would read it in order to be considered menacing,[242] but further noted that to assess whether there is criminal liability arising from a menacing messaging, the precise terms and any inferences from the precise terms need to be examined in the context in which it was sent.[243] There were several contextual factors surrounding the communication which absolved Chambers of any criminal wrongdoing. Firstly, the Lord Chief Justice described the tweet as a *"conversation piece"* which was only intended to draw attention to himself and his predicament.[244] Secondly, the tweet was not actually sent to any of the airport staff or directed towards a twitter account belonging to the airport - it was just posted to Chambers' public profile.[245] Additionally, the Lord Chief Justice noted that the language and punctuation signify that the tweet was not intended to be taken as a serious warning.[246] And finally, the Lord Chief Justice stated that *"it is difficult to imagine a serious threat in which warning of it is given to a large number of people in ample time for the threat to be reported and extinguished."*[247]

---

[237] *Chambers v Director of Public Prosecutions* [2012] EWHC 2157 (Admin)
[238] Ibid, [12]
[239] Ibid.
[240] Ibid, [1]
[241] Ibid, [26]
[242] Ibid, [30]
[243] Ibid, [31]
[244] Ibid.
[245] Ibid.
[246] Ibid.
[247] Ibid.

It is significant that the court considered the lack of any panicked reaction from those who read the tweet as a mitigating factor in respect of Chambers' criminality. The Lord Chief Justice explained that this was not inconsistent with the approach taken in *Collins*, where Lord Bingham stated that criminality cannot hinge upon the unforeseeable contingency of the recipient's reaction:

"Lord Bingham was saying no more than that a message proved by an objective assessment, applying the standards of an open and multi-racial society to be of a prescribed kind, does not cease to be so just because it was not received or because the person who received it was not, in the context of the present prosecution, menaced."[248]

The tweet only came to the attention of the police once it was discovered by a member of staff at Robin Hood Airport.[249] The threat was considered non-credible by the airport staff, but in accordance with standard airport procedure, was reported to the airport police who took no action other than to refer the tweet to South Yorkshire police.[250] The court found that the message lacked menace, on account of the fact that nobody was menaced.[251] Whilst the court found no offence had been committed, the Lord Chief Justice commented briefly on the *mens rea* required for such an offence. It was found that the *mens rea* element would only be satisfied if the sender intended the message to be of a menacing character, or if he recognised the risk at the time of sending the message that it may create fear or apprehension in any reasonable member of the public who reads it.[252] As such, it is unlikely that section 127(1) could ever apply to communications are intended to be read as jokes.

Notwithstanding the argument made in section 2.1 that the application of section 127(1) to private services operating through a public electronic communications network amounts to overreach, the court reached a sensible decision in relation to the characterisation of the message. In their response to the consultation by the Law Commission of England and Wales, English PEN cited this case as a guiding principle for any future communications offences:

"Such an offence would need to be drafted to take into account the infamous 'Twitter joke trial' which the Court of Appeal acknowledged should not have been prosecuted. This

[248] Ibid, [32]
[249] Ibid, [13]
[250] Ibid.
[251] Ibid, [33]
[252] Ibid, [38]

could be addressed with a strong mens rea element that rules out jokes and unfocused rants that happen to include threatening language."[253]

2.2.4. Concluding thoughts on the effect of section 127(1).

Many of the prosecutions brought about under section 127(1) could be prosecuted under alternative, more suitable, legislation – such as in the cases of *Chabloz* and *Sutherland*. Other prosecutions brought under section 127(1) seem ludicrous, as they concern communications which did not elicit a menaced or offended response from their recipients – such as in the cases of *Chambers* and *Collins*, respectively.

There is also an argument (as presented in section 2.1) that communications should never be prosecuted solely on the basis that they cause offense. Joseph Kelly, an individual who was recently prosecuted under section 127(1) for sending a grossly offensive communication over Twitter, has announced his intention to appeal his case to the European Court of Human Rights.[254] The communication in question was a tweet relating to Captain Tom Moore, a veteran of the Second World War who raised £30 million for charities supporting the NHS during the COVID-19 pandemic.[255] Upon the death of Captain Moore, Kelly tweeted *"The only good Brit soldier is a deed one, burn auld fella, buuuuurn."*[256] The tweet was posted for 20 minutes before Kelly decided to remove it. The most troubling aspect of the decision to prosecute Kelly, is that Sheriff Cottam noted that *"the deterrence is really to show people that despite the steps you took to try and recall matters, as soon as you press the blue button that's it."*[257] The court acknowledged that the prosecution could promote self-censorship, and then facilitated that chilling effect. Considering the vagueness that surrounds *"gross offensiveness"* and the lack of objective criteria, it is disturbing that the court decided to weaponise this ambiguity as a cautionary tale for anyone who may wish to speak freely and whose speech may be considered offensive. The Strasbourg court has not yet considered the lawfulness of a decision to prosecute an individual under section 127(1) for grossly offensive communications, and so, the outcome of Kelly's appeal could prove to be fundamental in

[253] Law Commission, *Modernising Communications Offences: A final report* (Law Com No 399, 2021) para 3.104

[254] Scottish Legal News, '*Scot convicted over 'grossly offensive' tweet appeals to European Court of Human Rights*' (Scottish Legal News, 27th October 2022) <https://www.scottishlegal.com/articles/scot-convicted-over-grossly-offensive-tweet-appeals-to-european-court-of-human-rights> accessed 29 June 2023.

[255] Ibid.

[256] Ibid.

[257] The National, *'Joseph Kelly spared jail for tweet about Captain Tom Moore'* (The National, 30th March 2022) < https://www.thenational.scot/news/20031940.joseph-kelly-spared-jail-tweet-captain-tom-moore/> accessed 29 June 2023.

securing protection for free speech by reaffirming, once more, that the freedom to speak only inoffensively is not worth having.

2.3. The Repeal of Section 127(1).

Ultimately, the Law Commission of England and Wales found that the communications offences suffered from *"sufficient serious problems to require significant reform."*[258] The Law Commission stated that all problems arising from the communications offences fell into one of five categories: unsatisfactory targeting and labelling; vagueness/uncertainty; overcriminalisation; under-criminalisation; and overlapping offences.[259]

This section will first consider the proposal by the Law Commission of England and Wales to repeal section 127(1) of the Communications Act 2003 and to replace this with a new harm-based offence, which could have combatted the issue of unsatisfactory targeting and labelling. The proposed offence is also less ambiguous than section 127(1) which would have resolved the conflict with the overlapping offences and the overcriminalisation and under-criminalisation which exists as a result. The second part of this section will discuss why the government ultimately rejected this proposal by the Law Commission.

2.3.1. Recommendation of the Law Commission.

The harms-based offence proposed by the Law Commission reads, as follows:

> *"(1) the defendant sent a communication that was likely to cause harm to a likely audience;*
>
> *(2) in sending the communication, the defendant intended to harm a likely audience; and*
>
> *(3) the defendant sent the communication without reasonable excuse.*
>
> *(4) For the purposes of this offence, definitions are as follows:*
>
> > *(a) a communication is an electronic communication, letter, or article;*

[258] Law Commission, *Harmful Online Communications: The Criminal Offences - A Consultation Paper* (Law Com No 248, 2020) para 3.173.
[259] Ibid, para 3.112.

(b) a likely audience is someone who, at the point at which the communication was sent by the defendant, was likely to see, hear, or otherwise encounter it; and

(c) harm is emotional or psychological harm, amounting to at least serious distress.

(5) When deciding whether the communication was likely to cause harm to a likely audience, the court must have regard to the context in which the communication was sent, including the characteristics of a likely audience.

(6) When deciding whether the defendant had a reasonable excuse for sending the communication, the court must have regard to whether the communication was a contribution to a debate in the public interest."[260]

This proposal addresses the unsatisfactory targeting of communications based on their character, as it departs from the character-based approach of section 127(1). This is consistent with the view of John Stuart Mill, that *"the only purpose for which power can be rightfully exercised over any member of a civilised community, against his will, is to prevent harm to others."*[261] It is also more consistent with the approach of the European Convention on Human Rights 1953 which allows interference to freedom of expression where the interference is necessary, proportionate and in pursuit of a legitimate aim.[262] As covered in chapter one, the legitimate aims in Article 10(2) of the European Convention on Human Rights 1953 all relate to the prevention of some kind of harm (perhaps, with the exception of *"for the protection of morals"*). Additionally, the new offence would prevent communications from being targeted on the basis that they have been sent through a public electronic communications network – the proposed offence applies to all electronic communications, letters, and articles. This would address the issue raised by the Law Commission that communications sent through private networks (such as Bluetooth or a local intranet) are inexplicably not covered by the same legislation which covers those sent through public electronic communications networks.[263]

The Law Commission originally proposed the idea of including a non-exhaustive list of factors that courts may consider in their assessment of the likelihood that a communication

[260] Law Commission, *Modernising Communications Offences: A final report* (Law Com No 399, 2021), para 2.257
[261] John Stuart Mill, On Liberty (first published 1859), ch 1.
[262] European Convention on Human Rights 1953, Art. 10
[263] Law Commission, *Harmful Online Communications: The Criminal Offences - A Consultation Paper* (Law Com No 248, 2020) para 3.143.

could cause harm[264] (in the style of New Zealand's Harmful Digital Communications Act 2015).[265] The list of factors included in the Harmful Digital Communications Act of New Zealand includes the extremity of the language used.[266] However, providing an indicative list of factors for a court to assess the likelihood that a communication could cause harm may revert to a character-based approach, which is open to subjectivity. For example, a communication may be considered likely to cause harm if it is grossly offensive. Any indicative list should be careful not to include any subjective factors if the law is to remain as clear as possible.

By realigning the criminal law, the Law Commission hope to redress the overcriminalisation and under-criminalisation which results from section 127(1). It seems unlikely that the proposed offence could have been used to prosecute Paul Chambers, for instance, where he had no intent to cause any harm. It also seems improbable that the proposed offence could be used to prosecute grossly offensive language where there was no intent to cause harm to an individual, nor does it seem likely that the new offence could apply to the consensual sharing of intimate images. Hence, the proposed offence would go a long way to redressing the overcriminalisation of certain acts covered in section 2.2.

2.3.2. Parliament's response.

When the Online Safety Bill was introduced to Parliament, the recommendation for a new harmful communications offence which would replace section 127(1) of the Communications Offences Act 2003 was included in section 150.[267] However, during the report stage within the House of Commons, Paul Scully, Conservative Member of Parliament for Sutton and Cheam and current Minister for Tech and the Digital Economy, announced that the government would not repeal section 127(1) or introduce the harm-based offence proposed by the Law Commission.[268] When explaining the reason that the government had decided not to introduce the proposed harms-based offence, Paul Scully MP stated that *"parliamentarians and stakeholders have expressed concern that the threshold that would trigger prosecution for the offence of causing serious distress could bring robust but legitimate conversation into the illegal space."*[269] Paul Scully MP further argued that

[264] Ibid, 2.88.
[265] Harmful Digital Communications Act 2015 *(New Zealand)*.
[266] Harmful Digital Communications Act 2015 *(New Zealand)*, s.22(2).
[267] Online Safety HC Bill (2022-2023) [220] s.150.
[268] HC Deb, 5 December 2022, vol 724, col 45.
[269] Ibid.

section 127(1) could not be repealed, as it provides essential protection to victims of domestic abuse.[270]

As aforementioned, section 127(1) is frequently used to prosecute behaviour in the context of domestic abuse, which the Law Commission of England and Wales has attributed to the flexibility of section 127(1) and the fact that there is no requirement to establish a course of conduct under section 127(1).[271] However, the Law Commission of England and Wales makes no comment as to why section 127(1) of the Communications Act 2003 is preferable to section 1 of the Malicious Communications Act 1988[272] in this respect. The latter also does not require a course of conduct to establish criminality. As aforementioned, the key difference between both Acts is that section 1 of the Malicious Communications Act 1988 requires the message to be directed to an individual and there must be an intent to cause the intended recipient distress or anxiety.[273] Whilst it is touted as a strength of section 127(1) of the Communications Act 2003 that criminality can be established in the context of domestic abuse despite any requirement for a course of conduct, an intended recipient, or a particular effect upon that intended recipient; it raises the questions as to why all three of these factors are required in criminal offences which exist exclusively to tackle domestic abuse. For example, the Domestic Abuse (Scotland) Act 2018[274] requires a person to engage in a course of conduct towards a specific person[275] which would cause that person to suffer physical or psychological harm[276] before finding that person guilty of a criminal offence. Remarking on the requirement for a course of conduct, Scottish Women's Aid (who had campaigned for more than 10 years for this Act) noted that *"moving away from constructing domestic abuse as an incident to a pattern of behaviour is one of the most important elements of the law in Scotland."*[277] Hence, whilst the Law Commission of England and Wales considered it to be a *"strength"*[278] of section 127(1) of the Communications Act 2003 that communications sent in the context of domestic abuse may be considered criminal despite the absence of these three factors, one could also argue that this is another example of overcriminalisation. Considering that the Law Commission of England and Wales concluded

[270] Ibid.
[271] Law Commission, *Harmful Online Communications: The Criminal Offences - A Consultation Paper* (Law Com No 248, 2020) para 3.108.
[272] Malicious Communications Act 1988, s.1.
[273] Ibid.
[274] Domestic Abuse (Scotland) Act 2016.
[275] Ibid, s.1(1)a.
[276] Ibis, s.1(3).
[277] Scottish Women's Aid, *'Domestic Abuse + the Law'* (Scottish Women's Aid) <https://womensaid.scot/information-support/domestic-abuse-and-the-law/> accessed 22 February 2024.
[278] Law Commission, *Harmful Online Communications: The Criminal Offences - A Consultation Paper* (Law Com No 248, 2020) para 3.106.

that section 127(1) suffers from *"sufficient problems to warrant significant reform"*, the government should cease relying upon this provision to provide *"essential protection"* for victims of domestic abuse and ensure that the alternative (and currently "less flexible") legislation is fit for purpose.

Regarding the proposal to replace section 127(1) with a harms-based offence, Paul Scully MP was correct to note that there were concerns raised by parliamentarians regarding the criminalisation of harmful content. Adam Afriyie, Conservative Member of Parliament for Windsor, stated at the second reading in the House of Commons:

> *"If we say that something that is harmful should not be there, should not be transmitted and should not be amplified, we start to get into difficult territory, because what is harmful for one person may not be harmful for another."* [279]

Additionally, it is also true that other stakeholders raised concerns about the criminalisation of harmful communications. For example, the Free Speech Union argued that robust speech which may cause distress should be protected. In particular, they stressed that this effect could create a *"heckler's veto"*, where speech would be unduly censored because it causes harm to a minority, and that irrefutable proof of serious harm should be required.

The grounds under which it was decided not to repeal section 127(1) are unsatisfactory. Whilst there are concerns that the new offence could criminalise speech which ought not to be criminalised, section 127(1) already does so. Parliament ought to have used the opportunity to either agree the wording of the new harmful communications offence to ensure that it would have a minimal impact upon free speech, or alternatively, they should have used the opportunity to draft targeted offences which would provide recourse for those who still rely upon section 127(1) for protection (notably, victims of domestic abuse). Either one of these moves would have negated any need for section 127(1) which is unfit for purpose. The Law Commission noted that there was substantial support for their proposal to repeal section 127(1) across the 132 consultees who responded. By refusing to repeal section 127(1) and replace it with a new harms-based offence within the Online Safety Act 2023, the government have missed a chance to bring much needed reform to communications offences.

[279] HC Deb, 19 April 2022, vol 712, col 117.

2.4. Conclusion on Free Speech and Communications Offences.

The 132 consultees who responded to the Law Commission's consultation mostly agreed that section 127(1) ought to be repealed. However, there is less consensus on how section 127(1) ought to be replaced. By understanding the origins of section 127(1) and the elements which are no longer applicable, as well as the free speech concerns surrounding both section 127(1) and the proposed harm-based offence from the Law Commission of England and Wales, this chapter can offer some guiding principles for the replacement of section 127(1).

First and foremost, section 127(1) falls short of the basic standard of free speech protection which is expected in a liberal democratic society. Any replacement provision should seek to be consistent with *Handyside* and *Redmond-Bate*. To that end, it is difficult to see any justification for criminalising speech based on its offensiveness. If speech is to be criminalised based on its capacity to cause harm, then due regard must be given to the threshold of harm that must be incurred before criminal liability can arise. The Law Commission were correct to insist upon an explicit intent to cause harm, excluding reckless behaviour from their proposed offence. Such reckless behaviour should not be criminalised – as to do so could have a chilling effect on free speech. A series of targeted offences directed to the most serious types of harmful speech is an attractive alternative to the offence proposed by the Law Commission. The benefit of a targeted approach is that it removes any ambiguity as to which speech should be included. Many would argue that the downside is that it could leave gaps in the law, allowing harmful communications to go unchallenged unless there is a specific law to address them. However, from a free speech perspective, this approach is preferable to a broad-based offence which risks capturing communications which should never have been criminalised in the first place. Perhaps it was not appropriate for the government to attempt to incorporate the recommendations of the Law Commission into the Online Safety Act 2023. The offence proposed by the Law Commission relates not only to online communications, but any potentially harmful communications. Additionally, the purpose of the Online Safety Act 2023 is to create a framework whereby OFCOM can regulate internet services.[280] Hence, the focus of the Online Safety Act 2023 extends far beyond which communications ought to be criminalised. As such, there are several aspects of the Online Safety Act 2023 which are unrelated to the harmful communications offences, but still impact upon free speech. Chapter three will discuss the Online Safety Act 2023 and the impact that it is likely to have upon free speech protection in the United Kingdom.

[280] Online Safety HL Bill (2022-2023) [151]

CHAPTER THREE: THE ONLINE SAFETY ACT 2023

"Anyone who has actually read the bill will recognise that its defining focus is the tackling of serious harm, not the curtailing of free speech."

– Nadine Dorries, Secretary of State for Digital, Culture, Media and Sport (2021-2022).[281]

The Online Safety Act 2023 makes provisions for OFCOM to regulate internet services.[282] This is a major reform of the current system, which relies heavily on providers of online services to regulate their own platforms.[283] The Report of the Joint Committee on the Draft Online Safety Bill concluded that this system of self-regulation had failed to tackle harms which are present online.[284] As the bill progressed through Parliament, much of the debate focused on the need to protect free speech whilst tackling harms online. It was argued in section 1.3 that policymakers attempting to regulate the internet should avoid taking a content-based approach, which could criminalise speech which is legal offline only by virtue of the fact that it is shared online. In contrast, a systems-based approach would tackle the unique methods of content dissemination which are unique to the online world and seem to disproportionately promote harmful content. However, the Online Safety Act 2023 contains a hybrid approach which tackles harmful content as well as harmful systems. As the bill progressed through Parliament, many members of parliament voiced their opposition to provisions which targeted harmful content. Lucy Powell, Labour and Co-operative Member of Parliament for Manchester Central, argued at the second reading of the bill in the House of Commons that *"had the Government chosen to follow the Joint Committee recommendations for a systems-based approach rather than a content-driven one, the Bill would be stronger and concerns about free speech would be reduced."*[285]

Following several substantive changes, the Online Safety Act 2023 is now remarkably different from the bill that was first introduced to Parliament. Notably, provisions which sought to tackle content on the basis that it could cause harm to adults (even where that content was legal offline) have been removed. The Online Safety Act 2023 only seeks to tackle illegal content and content that could cause harm to children (even where that content

[281] HC Deb, 19 April 2022, vol 712, col 99.
[282] Online Safety Act 2023.
[283] Joint Committee on the Draft Online Safety Bill, *Draft Online Safety Bill: Report of Session 2021-22* (HC & HL 2021-22) para 51.
[284] Ibid.
[285] HC Deb, 19 April 2022, vol 712, col 102.

is legal offline).[286] Nevertheless, despite improvements, there are still two prominent threats to free speech within the Online Safety Act 2023. The first threat is found in section 121(2) which gives OFCOM a new power to require providers of online services to develop and/or use technology to search their platforms for Child Sexual Exploitation and Abuse (CSEA) material, which could subvert the protection offered by end-to-end encryption on some platforms. This is discussed in detail in section 3.1.2 of this chapter. The second threat to free speech arises from the general approach to content that is harmful to children, as discussed in section 3.2.2 of this chapter.

Considering the Act contains enhanced measures to tackle harms affecting children online, this chapter will be split into two sections. Section 3.1 will examine harms facing adults online, the approach of the Act in tackling these harms, and the potential free speech implications. Whereas, section 3.2 will consider harms facing children online, and the free speech implications of the provisions within the Act to tackle these harms.

3.1. Online Harms to Adults.

From the inception of the Online Safety Act 2023 as a bill, forming an approach to online harms facing adults proved to be the most difficult aspect of the legislative process. Consequently, the provisions concerning online harms to adults changed dramatically since the bill was first introduced to parliament – more so than any other aspect of the bill. The end result has been the *"triple shield approach"*, which now appears within the Online Safety Act 2023. The triple shield approach was defined by Michelle Donelan MP, whilst acting in her former role as Secretary of State for Digital, Culture, Media and Sport, as below:

> *"Our new triple shield mechanism puts accountability, transparency and choice at the heart of the way we interact with each other online. If it is illegal, it has to go. If it violates a company's terms and conditions, it has to go. Under the third and final layer of the triple shield, platforms must offer users tools to allow them to choose what kind of content they want to see and engage with."*[287]

This section will first briefly explain how the triple shield approach is intended to work and the types of content which will be targeted by each layer of the shield. The second part of this section will demonstrate how certain aspects of the triple shield approach threaten free

[286] Online Safety Act, s.1(2).
[287] Ibid, col 165.

speech online (in particular, section 121(2) of Online Safety Act 2023 concerning illegal content).[288]

3.1.1. The "triple shield" approach.

The first layer of the triple shield targets illegal content. "Illegal content" includes any content which breaches the law where the victim (or intended victim) is an individual.[289] However, there are also enhanced measures within the Act to combat content which amounts to a "priority offence." Priority offences comprise terrorism offences,[290] offences related to child sexual exploitation and abuse,[291] assisting suicide, threats to kill, public order offences, harassment, stalking and fear or provocation of violence, drugs and firearms offences, assisting illegal immigration, human trafficking, sexual exploitation, sexual image offences, proceeds of crime offences, fraud, financial service offences, foreign interference and animal welfare offences.[292] Furthermore, terrorism content and CSEA content (content relating to child sexual exploitation and abuse offences) are subject to further enhanced measures[293] over and above content which amounts to any of the other priority offences (within the Act, the remainder of the priority offences excluding terrorism offences and offences related to child sexual exploitation and abuse are termed "the other priority offences.")[294] The Act imposes a duty on OFCOM to carry out risk assessments to identify and assess the risk of harm presented by illegal content on user-to-user services and search services to all individuals in the United Kingdom.[295] Furthermore, the Act imposes a duty on all user-to-user services[296] and search services[297] to conduct risk assessments on the likelihood of individuals encountering illegal content on their platform. Additionally, OFCOM are granted new powers under the Act to take action against providers of online services in respect of terrorism content or CSEA content.[298] This includes the power to issue a notice to providers of online services ordering them to use technology to identify such content and prevent individuals from encountering it on their platform.[299] Considering this aspect of the Act only

[288] Online Safety Act 2023, s.122.
[289] Ibid, s.59(5).
[290] Ibid, Sch 5.
[291] Ibid, Sch 6.
[292] Ibid, Sch 7.
[293] Ibid, s.121.
[294] Ibid, Sch 7.
[295] Ibid, s.98(1).
[296] Ibid, s.9(5).
[297] Ibid, s.26(5).
[298] Ibid, s.121.
[299] Ibid, s.121(2).

focuses on content which is already illegal, it does not create any new criminal offences. In this respect, it does not impede on free speech any further than the original pieces of criminal legislation which have been incorporated into this Act by reference. (For example, in respect of terrorist content, section 12(1A) of the Terrorism Act 2000 regarding expressing an opinion or belief supportive of a proscribed organisation[300] has been incorporated into this Act as a priority offence under Schedule 5).[301] However, there still exists free speech concerns surrounding OFCOM's new powers to compel providers of online services to take action against terrorism content or CSEA content (particularly, the latter), as discussed in section 3.1.2.

The second layer of the triple shield involves bolstering the terms and services of providers of online services. Under the Act, providers of online services must provide a certain level of information within their terms of services. This includes information relating to how users are protected from illegal content[302] and a user's right to bring a claim for breach of contract if they are suspended or banned from using the service or if their content is removed.[303] Category 1 services must provide additional information on matters such as the outcome of their latest illegal content risk assessment[304] and their user identity verification process.[305] (Category 1 services are the most popular user-to-user services. OFCOM are set to publish the register of categorised services by the end of 2024,[306] and it is understood that the threshold for a Category 1 service will be set by reference to the number of users and the functionalities of the service.)[307] There is also a duty on Category 1 services to refrain from taking action against user-generated content except in accordance with their terms of service.[308] This is intended to protect the free speech of users, and to pacify critics who raised concerns that providers of online services might react to the Online Safety Act 2023 by over-censoring user-generated content on their platforms to avoid having any action taken against them under the Act.

[300] Terrorism Act 2000, s.12(1A).
[301] Online Safety Act 2023, Sch 5.
[302] Ibid, s.10(5).
[303] Ibid, s.72(1).
[304] Ibid, s.10(9).
[305] Ibid, s.64(3).
[306] OFCOM, 'Ofcom's approach to implementing the Online Safety Act' (OFCOM, 26 October 2023) < https://www.ofcom.org.uk/online-safety/information-for-industry/roadmap-to-regulation> accessed 22 January 2024
[307] OFCOM, *'Preparing to regulate Online Safety: Categorising regulated services'* (OFCOM, 11 July 2023) < https://www.ofcom.org.uk/news-centre/2023/preparing-to-regulate-online-safety-categorising-regulated-services> accessed 22 September 2023
[308] Ibid, s.71.

The third layer imposes a duty on Category 1 services to offer their users a certain level of control over the content that they encounter online, known as *"user empowerment duties."*[309] Not only will this duty only apply to Category 1 services – Category 1 services will also only be obligated to offer user empowerment tools in respect of the most harmful types of content. This includes content that encourages suicide, deliberate self-injury, or behaviours associated with eating disorders.[310] It also includes abuse that targets race, religion, sex, sexual orientation, disability, or gender reassignment.[311] The content which is targeted by this section was previously subject to much harsher treatment in earlier iterations of the Act. It was often referred to by members of parliament as *"legal but harmful"* content, as it was subject to many of the same restrictions as illegal content, yet it is content which may be considered legal offline. The legal but harmful provisions were removed from the Act, so far as they applied to adults, largely due to concerns over free speech.[312] Nevertheless, this aspect of the triple shield is intended to tackle what was previously called *"priority content that is harmful to adults"* by the Joint Committee on the Draft Online Safety Bill.[313] This includes content which disproportionately impacts vulnerable users, such as content which encourages behaviours associated with poor mental health (eating disorders, self-harm and suicide),[314] and abusive content targeting individuals on the basis of protected characteristics.[315]

3.1.2. Free speech concerns of the triple shield approach.

Despite the fact that many of the free speech concerns of the Online Safety Act 2023 were resolved when the decision was made to substitute the *"legal but harmful to adults"* approach with the triple shield approach, the triple shield still poses a serious through to free speech. The threat stems from section 121(2) of the Act, which provides OFCOM with the new power to order providers of online services to use technology to identify CSEA content on their platform.

Section 121(2) forms part of the first layer of the triple shield approach which exists to protect adults against illegal content and activity online. Under this section, OFCOM can

[309] Online Safety Act 2023, s.15.
[310] Ibid, s.16(3).
[311] Ibid, s.16(4).
[312] HC Deb, 5 December 2022, vol 724, col 45.
[313] Joint Committee on the Draft Online Safety Bill, *Draft Online Safety Bill: Report of Session 2021-22* (HC & HL 2021-22), para 162.
[314] Ibid.
[315] Ibid, para 52.

give notice to a provider of an online service to use, develop, or source technology to identify and remove terrorism content or CSEA content.[316] In respect of terrorism content, these powers only apply where the content is communicated publicly.[317] However, in respect of CSEA content, OFCOM can order a provider of any online service to use[318] or develop[319] technology to identify and prevent individuals encountering CSEA content where this content is communicated publicly or privately.[320] This threatens the privacy of users of communication platforms – particularly those which offer end-to-end encryption, such as Telegram and WhatsApp. According to WhatsApp, *"end-to-end encryption ensures only you and the person you're communicating with can read or listen to what is sent. Nobody in between, not even WhatsApp, can access the content of your communications."*[321] Hence, any form of moderation – even if it is to identify CSEA content – could undermine the protection offered by end-to-end encryption. Commenting on the new powers granted to OFCOM to subvert end-to-end encryption, Barbora Bukovská, Senior Director for Law and Policy at Article 19, stated *"the simple truth about encryption is this: it either protects everyone, or protects no one."*[322]

The government has made several other attempts to subvert the protection offered by end-to-end encryption in order to tackle crime. The Investigatory Powers Act 2016 empowers the Secretary of State to compel operators to remove electronic protection applied to any communications or data.[323] Under the 2016 Act, there are three conditions which must be satisfied before the Secretary of State can serve a technical capability notice upon an operator requiring them to remove any electronic protection. Firstly, the Secretary of State must consider that it is necessary to serve a notice for the operator to be able to comply.[324] Secondly, the Secretary of State must consider that issuing a notice is proportionate to *"what is sought to be achieved."*[325] Finally, the decision to issue the notice must be approved by a Judicial Commissioner.[326] Judicial commissioners are individuals who hold (or have held) a

[316] Ibid, s.121.
[317] Ibid, s.121(2)a (i).
[318] Ibid, s.121(2)a (iv).
[319] Ibid, s.121(2)b.
[320] Ibid, s.121(2)a (iv).
[321] WhatsApp, *'About end-to-end encrypted backup'* (WhatsApp, 2023) < https://faq.whatsapp.com/490592613091019> accessed 22 September 2023
[322] Article 19, 'UK: Online Safety Bill risks undermining privacy around the world' (Article 19, 5 September 2023) < https://www.article19.org/resources/uk-online-safety-bill-risks-undermining-privacy-around-the-world/> accessed 21 September 2023.
[323] Investigatory Powers Act 2016, s.253(5)c.
[324] Ibid, s.251(1)a.
[325] Ibid, s.251(1)b.
[326] Ibid, s.251(1)c.

high judicial office and are appointed by the Prime Minister to assist the Investigatory Powers Commissioner.[327] Similarly, before OFCOM may issue a notice to a provider of an online service to develop technology to deal with terrorism content or CSEA material, they must also consider that it is necessary and proportionate to do so.[328] However, OFCOM are under no duty to first gain approval from a Judicial Commissioner. Instead, they must obtain a skilled person's report[329] - which is a report to be completed by a person deemed by OFCOM to have the skills necessary about the relevant matters who has been appointed by the provider of the online service (after being nominated or approved by OFCOM).[330] Before issuing a notice requiring the use of technology, OFCOM must also issue a warning to the provider of the online service[331] and take into consideration a list of factors listed in section 124(2).[332] These factors include, but are not limited to: the functionalities of the service; the user base; the level of risk of harm to individuals in the UK; the contents of the skilled person's report; and the extent to which the use of the specified technology would or might result in interference with users' right to freedom of expression within the law.[333]

The European Parliament are currently considering similar legislation. The *"Proposal for a Regulation of the European Parliament of the Council laying down the rules to prevent and combat child sexual abuse"* was published on 11th May 2022.[334] If successful, this will empower national authorities to issue detection orders to identify CSAM online.[335] The proposed EU regulation contains several of its own prerequisites which must be met before a detection order can be issued, Firstly, detection orders should only be issued after a diligent and objective assessment leading to the finding of a significant risk of the specific service concerned being misused for online child sex abuse.[336] Specifically, the risk must go beyond the extent that the service is used for isolated and relatively rare instances of online child sex abuse.[337] Before issuing a detection order, the national authorities must diligently assess the likelihood and seriousness of any potential negative consequences on other parties affected by the order, any consequences on users' fundamental rights[338] (including free speech).

[327] Ibid, s.125.
[328] Online Safety Act 2023, s.121(1).
[329] Ibid, s.122.
[330] Ibid, s.104(6).
[331] Ibid, s.123.
[332] Ibid, s.124(2).
[333] Ibid.
[334] European Commission, 'Proposal for a Regulation of the European Parliament and of the Council laying down rules to prevent and combat child sexual abuse' COM (2022) 209 final.
[335] Ibid, para 20.
[336] Ibid, para 21.
[337] Ibid.
[338] Ibid, para 22.

These prerequisites are similar to those contained in the Online Safety Act 2023 – however, the proposed EU regulation also contains certain provisions to limit any negative impact of a detection order which the Online Safety Act 2023 lacks. This includes a requirement to ensure that detection orders are targeted and specified so that any negative consequences on other parties affected by the order *"do not go beyond what is strictly necessary to effectively address the significant risk identified."*[339] Where possible, detection orders should be limited to any identifiable part or component of the service, such as specific channels available on interpersonal communications services or to specific users.[340] The Online Safety Act 2023 contains no analogous measures to limit the impact of the implementation of an OFCOM notice on the free speech of other users. Under the Online Safety Act 2023, there is nothing to discourage providers of online services from developing or using technology which will override the end-to-end encryption offered to all users, in order to identify CSAM content. Yet, the EU proposal is still proving to be controversial, and has not yet become law. Considering the proposal, the Civil Liberties Committee stressed the need *"to avoid mass surveillance or generalised monitoring of the internet."*[341] On 15th February 2024, the EU Parliament agreed to an extension of temporary measures which allow providers of online services to derogate from EU privacy rules for the voluntary detection of child sexual abuse until 3rd April 2026.[342] It seems evident that the EU are not hopeful that the permanent legislation which is intended to replace these temporary measures will arrive any time soon. Additionally, two days prior to this extension (on 13th February 2024), the European Court of Human Rights found that there had been an interference with the right to privacy of Telegram users,[343] after Russian authorities had requested Telegram to decrypt messages sent through their platform and provide these to the Federal Security Service (the 'FSB') to allow the FSB to investigate individuals suspected of terrorism-related activities.[344] Whilst there was no argument that the Russian authorities had interfered with freedom of expression, the court noted that *"measures for encryption contribute to ensuring the enjoying of other fundamental rights, such as freedom of expression."*[345]

[339] Ibid, para 23.
[340] Ibid.
[341] Civil Liberties Committee, 'Child sexual abuse online: effective measures, no mass surveillance' (*European Parliament*, 14 November 2023) < https://www.europarl.europa.eu/news/en/press-room/20231110IPR10118/child-sexual-abuse-online-effective-measures-no-mass-surveillance> accessed 1 December 2023
[342] European Parliament, *'Child sexual abuse online: agreement on extending current rules until April 2026'* European Parliament News (15 February 2024).
[343] *Podchasov v. Russia* App. no. 33696/19 (ECtHR, 13 February 2024), 80.
[344] Ibid, 7.
[345] Ibid, 76.

The protection offered by end-to-end encryption already faces a larger threat in the United Kingdom outside of the Online Safety Act 2023, through the Investigatory Powers Act 2016 (discussed above). However, the Online Safety Act 2023 weakens the protection further by giving OFCOM the power to force providers of online services to develop technology to search for illegal content, even if this means subverting electronic protection. Additionally, the lack of any measures to mitigate the impact on the rights of other users means that the free speech of users in the United Kingdom is under greater threat than exists in the proposed EU legislation. The Online Safety Act 2023 would benefit from measures akin to those proposed in the EU, in order to protect free speech. In their performance of their duties under section 121(2), OFCOM are under a duty to consider the interference with freedom of expression before they act – however, it remains to be seen whether this will act as a sufficient protection for free speech. Free speech also could have been awarded stronger protection by inserting a requirement for OFCOM to consult a legal professional, such as a Judicial Commissioner, before requiring online service providers to use technology on their platforms to identify terrorism content or CSEA material. The expected input of a Judicial Commissioner under the 2016 Act is not the same as the expected input of a skilled person under the Online Safety Act 2023. Judicial Commissioners are qualified to advise on the legality of a request to subvert electronic encryption, whereas the only essential qualification for a skilled person within the Online Safety Act 2023 is that they appear to OFCOM to have the necessary skills to prepare a report on the *"relevant matters."*[346] Where the relevant matter is the use of technology to identify terrorist content or CSEA material, the purpose of the report is *"to assist OFCOM in deciding whether to give a notice [...], and to advise about the requirements that might be imposed by such a notice if it were to be given."*[347] There is no requirement on OFCOM to solicit an independent opinion from a legal expert on the relevant law and freedom of expression. Currently, OFCOM has permission to act without much oversight. Similarly, it was a lack of any adequate safeguards against abuse of the power to decrypt encrypted communications which lead the ECtHR to conclude that the measures taken by the Russian authorities in *Podchasov v. Russia* were not necessary in a democratic society and amounted to an interference with the right to privacy.[348] The lack of adequate safeguards against arbitrary use of this new power conferred upon OFCOM opens the door to potential interferences with free speech.

[346] Ibid, s.105(6)
[347] Ibid, s.123(2)
[348] *Podchasov v. Russia* App. no. 33696/19 (ECtHR, 13 February 2024), 80.

3.2. Online Harms to Children.

In addition to harm from illegal content online, children are particularly vulnerable to harms posed by content which could impact their mental health during the developmental stages of their life. Much of this content is perfectly legal and may have a lesser impact or no impact at all upon fully developed adults. Age-sensitive content can be divided into two main categories: pornography and content related to mental health.

The report of the Joint Committee heard evidence from experts that exposure to pornography can distort children's view of healthy relationships, sex and consent, and lead to addiction.[349] In the offline world, the Video Recordings Act 1984 makes provisions for pornographic videos to be classified as unsuitable for those under the age of 18.[350] Additionally, certain pornographic videos may only be sold in licensed sex shops.[351] Furthermore, steps have been taken to reduce the unintentional exposure of children to pornographic content offline. Following increased pressure from campaign groups such as Lose the Lads Mags, many newsagents and magazine retailers took steps to prevent children from encountering magazines which featured sexualised images on the front cover. In 2014, the National Federation of Retail Newsagents (NFRN) issued guidelines that adult material should be placed on top shelves out of reach of children.[352] And yet, pornographic material remains widely available online. The Office of the Children's Commissioner reports that over half of 11–13-year-olds have seen pornography online.[353] Evidence collected by the Joint Committee found that the largest providers of pornography online do not require any age verification at all, and that they feature videos which play automatically on their homepages.[354] Additionally, it has been reported that malicious actors have been able to subvert the content moderation on platforms such as TikTok[355] to upload pornographic content, leading to an increased risk of children using these services being unintentionally exposed to pornography.

[349] Joint Committee on the Draft Online Safety Bill, *Draft Online Safety Bill: Report of Session 2021-22* (HC & HL 2021-22) para 18.
[350] Video Recordings Act 1984, s.4.
[351] Ibid, s.12.
[352] John Woodhouse and Philip Ward, Briefing paper: Adult magazines in shops (House of Commons, Number 2039, 2016) pg 4.
[353] Joint Committee on the Draft Online Safety Bill, *Draft Online Safety Bill: Report of Session 2021-22* (HC & HL 2021-22) para 39.
[354] Joint Committee on the Draft Online Safety Bill, *Draft Online Safety Bill: Report of Session 2021-22* (HC & HL 2021-22) para 39.
[355] Joe Tidy, 'TikTok loophole sees users post pornographic and violent videos' BBC News (London, 21 April 2021)

There are several kinds of content which deal with mental health that can cause harm to children. This ranges from content which deals with distressing themes, to content that actively promotes dangerous behaviour (notably, eating disorders, self-harm, and suicide).[356] Evidence gathered by the Joint Committee found that 26% of young people in hospital for self-harm injuries or suicide attempts have accessed related content online.[357]

Tackling online harms to children has always been the primary focus of this Act. Upon introducing the Online Safety Bill to Parliament, Nadine Dorries noted *"the bill has our children's future, their unhindered development and their wellbeing at its heart."*[358] Despite the fact that the approach to target content solely on the basis that it can cause harm was scrapped as far as it related to harms that can affect adults, the Online Safety Act 2023 still targets content solely on the basis that it may cause harm to children.

3.2.1. The "legal but harmful to children" approach.

All regulated services must carry out a "children's access assessment" to determine whether it is possible for children to access any part of their service;[359] whether there is a significant number of children who are users of any part of their service; or, whether any part of their service is likely to attract a significant number of users who are children.[360] Section 36 of the Act makes further provisions for the administration of children's access assessments. For example, under section 36, children's access assessment must not be carried out more than one year apart.[361] Additional children's access assessments must be carried out before a provider of an online service makes any significant change to any aspect of their service's design or operation which may affect the children's access assessment, in response to evidence about reduced effectiveness of age verification or age estimation used on the service, or in response to evidence about a significant increase in the number of children using the service.[362] Finally, a provider of an online service can only conclude that it is not possible for children to access a service, or part of it, if age verification or age estimation is used effectively on the service.[363] Age verification is defined as any measure designed to

[356] Joint Committee on the Draft Online Safety Bill, *Draft Online Safety Bill: Report of Session 2021-22* (HC & HL 2021-22) para 19.
[357] Ibid.
[358] HC Deb, 19 April 2022, vol 712, col 95.
[359] Online Safety Act 2023, s.35(1)
[360] Ibid, s.35(4)
[361] Ibid, s.36(3)
[362] Ibid, s.36(4)
[363] Ibid, s.35(2)

verify the exact age of users, whereas age estimation means any measure to estimate the age or age-range of users.[364] For services that are likely to be accessed by children, there are children's risk assessment duties and children's safety duties.

The children's risk assessment duties for user-to-user services which are likely to be accessed by children are laid out in section 11 of the Act[365] and the children's risk assessment duties for search services which are likely to be accessed by children are contained within section 28.[366] Both are displayed in the table below. As with children's access assessments, a new children's risk assessment must also be carried out before the service provider makes any significant change to any aspect of the service's design or operation, assessing the impacts of the proposed change.[367]

Table 1: Factors to consider when carrying out a children's risk assessment

User-to-user services[368]	**Search services**[369]

• User base, including the number of users who are children in different age groups.
• Level of risk of children encountering:
  ○ each kind of primary priority content that is harmful to children (see table 2).
  ○ each kind of priority content that is harmful to children (see table 2).
  ○ non-designated content that is harmful to children.
  ○ any features, functionalities or behaviours on the service that are harmful to children.
	• Level of risk of children encountering:
	  ○ each kind of primary priority content that is harmful to children (see table 2).
	  ○ each kind of priority content that is harmful to children (see table 2).
	  ○ non-designated content that is harmful to children.
	• Level of risk of harm to children presented by different kinds of content that is harmful to children, giving separate consideration to children in different age groups and

[364] Ibid, s.231
[365] Ibid, s.11
[366] Ibid, s.28
[367] Ibid, s.11(4)
[368] Ibid, s.11
[369] Ibid, s.28(5)

• Level of risk of harm to children presented by different kinds of content that is harmful to children, giving separate consideration to children in different age groups and separate consideration to certain characteristics or members of a certain group. • Level of risk of functionalities of the service facilitating the presence or dissemination of content that is harmful to children, identifying and assessing those functionalities that present higher levels of risk, including functionalities enabling adults to search for and contact other users of the service (including children). • The different ways in which the service is used, and the impact of such use on the level of risk of harm that might be suffered by children. • The nature and severity of the harm that might be suffered by children, giving separate consideration to children in different age groups. • The design and operation of the service (including the business model, governance, use of proactive technology, measures to promote users' media literacy and safe use of the service, and other systems and processes) may reduce or increase the risks identified.	separate consideration to certain characteristics or members of a certain group. • Level of risk of functionalities of the service facilitating the presence or dissemination of content that is harmful to children, identifying and assessing those functionalities that present higher levels of risk, including functionalities enabling adults to search for and contact other users of the service (including children). • The nature and severity of the harm that might be suffered by children, giving separate consideration to children in different age groups. • The design and operation of the service (including the business model, governance, use of proactive technology, measures to promote users' media literacy and safe use of the service, and other systems and processes) may reduce or increase the risks identified.

Providers of search services have less duties than providers of user-to-user services when undertaking a children's risk assessment, due to the difference in functionality between the services. For example, it may be impossible for search services to carry out an assessment of their "user base", considering most search services do not require user registration.

The table below displays the types of content which are designated as *"primary priority content that is harmful to children"* and *"priority content that is harmful to children"* within section 61 and 62 of the Act respectively. Primary priority content is content which is considered to pose the most serious risk of harm to children online.

Table 2: Designation of content within the Online Safety Act 2023.

Designation	**Types of content**
Primary priority content that is harmful to children [370]	- Pornographic content. - Content which encourages, promotes, or provides instructions for suicide or acts of deliberate self-injury. - Content which encourages, promotes or provides instructions for an eating disorder or behaviours associated with an eating disorder.
Priority content that is harmful to children[371]	- Abusive content which targets or incites hatred against the protected characteristics under the Equality Act 2010. - Content which encourages or provides instruction for acts of serious violence against a person. - Bullying content. - Content which depicts real or realistic serious violence against a person, or real or realistic serious injury of a person in graphic detail. - Content which depicts real or realistic serious violence against an animal, or real or realistic serious injury of an animal in graphic detail.

[370] Ibid, s.61
[371] Ibid, s.62

	- Content which depicts serious violence against a fictional creature or the serious injury of a fictional creature in graphic detail. - Content which encourages, promotes, or provides instructions for a challenge or stunt highly likely to result in serious injury to the person who does it or someone else. - Content which encourages a person to ingest, inject, inhale, or in any other way self-administer a physically harmful substance or a substance in such quantity to be physically harmful.

There are different safety duties imposed upon providers of online services in respect of both categories. Primary priority content is deemed to pose the most serious risk of harm to children, and so providers of online services are under a strict duty to prevent children of any age from encountering this content.[372] In contrast, in relation to priority content that is harmful to children, there is only a duty to protect children in age groups which are judged to be at a risk of harm.[373] Additionally, OFCOM is under a duty to carry out assessments on the risk of harm to children presented by content that is harmful to children and to publish a risk profile detailing their findings in respect of each regulated provider of online services.[374]

The Act is intended to protect children from harm through policing content and systems. Providers of online services will be placed under a duty to mitigate the impact of harm to children presented by content on their service,[375] as well as the impact of harm to children presented by features and functionalities enabled or created by the design or operation of the service.[376]

[372] Ibid, s.12(3)a.
[373] Ibid, s.12(3)b.
[374] Ibid, s.99(1).
[375] Ibid, s.12(2)b.
[376] Ibid, s.12(2)c.

3.2.2. Free speech concerns of the "legal but harmful to children" approach.

Children's wellbeing was heavily prioritised in drafting the Online Safety Act 2023, hence, there was little focus on children's freedom of speech as the bill progressed through Parliament. It is widely accepted that there is a greater need to safeguard children from harm in society. Even John Stuart Mill argued the harm principle *should "apply only to human beings in the maturity of the faculties"*[377] adding *"we are not speaking of children [...] those who are still in a state to require being taken care of by others must be protected against their own actions as well as from external injury."*[378] Nevertheless, children's right to freedom of expression should not be discounted entirely.

Alex Davies-Jones, Labour Member of Parliament for Pontypridd, was one of the few members of Parliament to raise concerns over the potential impact of the Online Safety Act 2023 on children's free speech:

"The Government are thus at real risk of excluding children from being able to participate in the digital world freely and safely. The Bill must not lock children out of services they are entitled to use; instead, it must focus on making those services safe by design."[379]

Davies-Jones MP advocated for a solely systems-based approach – which could have gone a long way to making the internet a safer place for children without impeding at all on their free speech. As per the report of the Joint Committee, services which are designed to keep users engaged may use algorithms to collect information about their interests and then serve them progressively more extreme content in order to maximise the user's engagement.[380] Targeting systems such as this would help to prevent the rabbit hole effect which exposes children to harm from the promotion of the most harmful forms of content (for example, suicide or self-harm content, or content which promotes eating disorders). Furthermore, it would provide a way to target these systems without unduly locking children out of services that they are entitled to use.

Additionally, very little consideration was given to how the internet has empowered children's freedom of expression and the effects that the Online Safety Act 2023 may have

[377] John Stuart Mill, On Liberty (first published 1859), 14.
[378] Ibid.
[379] HC Deb, 19 April 2022, vol 712, col 129.
[380] Joint Committee on the Draft Online Safety Bill, *Draft Online Safety Bill: Report of Session 2021-22* (HC & HL 2021-22) para 71.

upon this. Kirsty Blackman, Scottish National Party Member of Parliament for Aberdeen North raised this at the second reading of the bill in the House of Commons:

"A quarter of LGBQ and disabled girls found online forums and spaces an important source of support. So, we need to make sure that children and young people have the ability to access those sources of support."[381]

Freedom of expression under the European Convention on Human Rights 1953 includes the right to access and receive information.[382] Online forums are an important resource for children to access information on sensitive topics which they may feel uncomfortable discussing in real life, for example, on LGBTQ+ issues. *"Abusive content which targets or incites hatred against the protected characteristics under the Equality Act 2010"* has now been designated as priority content which is harmful to children within the Act.[383] There is a risk that informational content on LGBTQ+ issues may be mischaracterised and subject to the same regulation as abusive content which targets or incites hatred on the basis of gender, sex, or sexual orientation. Furthermore, there is no element of user empowerment for children. Hence, if content is mischaracterised, children may not be able to opt to access the content regardless, as service providers will be under an obligation to restrict their access. It should be noted that the outgoing regulatory regime, which relies heavily on providers of online services to regulate their own platforms, already often results in the mislabelling and erroneous restriction of LGBTQ+ content. In a written submission to the Joint Committee on the Draft Online Safety Bill, LGBT foundation stated:

"It is particularly important that "harm to children" be clearly defined, given significant evidence of non-explicit LGBT-related content being discriminatorily mis-classified as 'mature' or 'adult' by large platforms such as Tumblr and YouTube. This resulted in young people being unable to access content about LGBT rights, history, identity, and discrimination, including in one/ case advice videos produced by an LGBT youth charity, while browsing in Restricted Mode on YouTube."[384]

[381] HC Deb, 19 April 2022, vol 712, col 113.
[382] European Convention on Human Rights, Art. 10.
[383] Online Safety Act 2023, s.62(2).
[384] Joint Committee on the Draft Online Safety Bill, *Draft Online Safety Bill: Report of Session 2021-22* (HC & HL 2021-22), written submission (OSB0045).

A General Comment from the United Nations Committee on the Rights of the Child was published on the issue of safeguarding the internet for children without impeding free speech or access to information:

"States should require businesses and other providers of digital content to develop and implement guidelines to enable children to safely access a diversity of content while protecting them from such harmful material in accordance with their evolving capacities, and recognising children's right to information and freedom of expression."[385]

Despite the potential of the Online Safety Act 2023 to encroach upon children's freedom of expression (particularly as it relates to their right to access information), most groups concerned with children's rights seem to agree that the approach is warranted to tackle harms online. Rachel de Souza, the Children's Commissioner for England, stated that she was *"pleased to see [that the] Online Safety Bill has became law"* and announced her intention to *"continue working with Ofcom to ensure children are heard and protected."*[386] A representative of the Children and Young People's Commissioner for Scotland previously argued that the internet is a *"a crucial place, a space where children can realise their full range of civil, political, social, cultural, economic and environmental rights"*[387], however, they stopped short of arguing that any changes were required to the legal but harmful approach of the Act. Instead, they emphasised that children should have direct access to share concerns and complaints with OFCOM.[388] A right to complain, and a means to complain which is accessible and understandable to children, may mitigate any potential impact of this Act upon the free speech of children. Section 169 of the Online Safety Act 2023 allows "an eligible entity" to make complaints to OFCOM about any feature of online services which presents a material risk of adversely affecting the right to freedom of expression of users of online services or members of the public.[389] A consultation on the eligible entity criteria and complaints procedure was launched by the government on 16th November 2023 and closed on 11th January 2024.[390] At the time of writing, the government are yet to publish the responses to this consultation - however, one might hope that there is

[385] UNCRC 'General Comment 25 on children's rights in relation to the digital environment' (2021) UN Doc CRC/C/GC/25.
[386] Tweet by Children's Commissioner for England (X, 26 October 2023) < https://twitter.com/childrenscomm/status/1717525638083395776> accessed 25 February 2024.
[387] Gina Wilson, 'Children's rights in the digital world: the UK's opportunity to create ground breaking legislation' (*CYPCS*, 8 February 2022) <https://www.cypcs.org.uk/news-and-stories/childrens-rights-in-the-digital-world/> accessed 21 February 2024.
[388] Ibid.
[389] Online Safety Act 2023, s.169.
[390] Department for Science, Innovation & Technology, *Super-complaints eligible entity criteria and procedural requirements* (White Paper, 2023).

a mechanism which will allow an eligible entity to raise concerns about the impact of the Act on free speech on behalf of children (if not by children themselves).

3.3. Conclusion on the Online Safety Act 2023.

The Online Safety Act 2023 may succeed in meeting its grand objective to make the United Kingdom *"the safest place in the world to be online."*[391] It has strong provisions to curb the spread of illegal content and safeguard children from harm. However, in pursuit of this aim, the Act will undoubtedly weaken protection for free speech online.

The protection offered by end-to-end encryption has already been eroded by the Investigatory Powers Act 2016. However, the Online Safety Act 2023 exacerbates the damage by issuing OFCOM with a new instrument to bypass end-to-end encryption. This heightens the risk that free speech could suffer from undue interference. As it stands, this provision is likely to place the United Kingdom behind the EU in its commitment to protect free speech. It is not certain that the EU will successfully pass the regulation which will allow the authorities to bypass end-to-end encryption in member states – however, if they are successful, the EU regulation in its current form contains far greater safeguards to protect free speech than exist in the Online Safety Act 2023.

There seems to be little concern that the Online Safety Act 2023 could have an impact on the free speech of children. However, there exists a real threat that children's access to information online could be impacted by the mischaracterisation of content as harmful. It is hoped that, in the implementation of the Act, OFCOM will establish an effective complaints procedure which will allow any impact on children's free speech to be challenged.

All things considered, the Online Safety Act 2023 has weakened the protection of free speech online in the United Kingdom. Firstly, there is the real damage to free speech protection caused by the new power of OFCOM to overturn a user's privacy to search for illegal content. Secondly, there is the potential risk that children's free speech, particularly as far as it extends to their right to access information, could be impeded by the mischaracterisation of content online. The Online Safety Act 2023 may have reduced the risk of one encountering harm online, however it has subsequently increased the risk that one's right to freedom of expression may be impeded by providing new avenues for interference.

[391] HC Deb, 19 April 2022, vol 712, col 95.

CONCLUSION - FREE SPEECH ONLINE

> *"The war against the internet rages on. […] I worry that, unless the tide turns soon, the Internet I fell in love with may cease to exist, and in its place, we will have something closer to a souped-up version of TV - focused largely on passive consumption, with much less opportunity for active participation and genuine human connection."*
>
> - Leif K-Brooks, founder of Omegle.com.[392]

In his written statement announcing the closure of Omegle.com (quoted at the end of chapter one), K-Brooks describes the recent push to regulate the internet (particularly online communication services) as *"the war against the internet."*[393] It is worth discussing K-Brooks' statement further, as he touches on many of the issues discussed throughout this thesis. He explains how the internet facilitated his freedom of expression when he was just a teenager:

"As a young teenager, I couldn't just waltz onto a college campus and tell a student: "Let's debate moral philosophy!" I couldn't walk up to a professor and say: "Tell me something interesting about microeconomics!" But online, I was able to meet those people, and have those conversations."[394]

K-Brooks writes that *"the internet opened the door to a much larger, more diverse, and more vibrant world"*, and that becoming an *"active participant"* in that world helped him to *"grow into a more well-rounded person."*[395] The experience of K-Brooks is reminiscent of the benefits of realising personal liberty and exercising free speech outlined by Mill in *On Liberty*. If *"freedom"* and *"variety of situations"* are the two prerequisites for personal development,[396] then K-Brooks found both online as a teenager. In addition to the fact that there are more opportunities for free discussion on any topic online than exist offline, K-Brooks argues that the anonymity of the internet enabled him to enter these discussions. K-Brooks was the victim of rape in his childhood, and he argues that the internet allowed him

[392] Leif K-Brooks, Farewell Statement (*Omegle*, 4 November 2023) <www.omegle.com> accessed 1 December 2023
[393] Ibid.
[394] Ibid.
[395] Ibid.
[396] John Stuart Mill, On Liberty (first published 1859), 54.

to interact with strangers without *"risking [his] physical body."*[397] He argues that exercising his free speech online, in a way that he was unable to do offline, facilitated his personal development.

K-Brooks' experience is typical of many individuals (of all ages) who exercise their freedom of expression online (including their right to access information). K-Brooks explains how the chatroom service, Omegle, allowed others to *"explore foreign cultures, get advice about their lives from impartial third parties, and to help alleviate feelings of loneliness and isolation."*[398] K-Brooks then warns against the potential effects that internet regulation could have upon other communication services:

> *"Virtually every online communication service has been subject to the same kinds of attack as Omegle; and while some of them are much larger companies with much greater resources, they all have their breaking point somewhere."*[399]

It is doubtful that any policymakers would see the closure of online spaces such as Omegle.com as a welcome result of their efforts. In the case of the Online Safety Act 2023, it is clear that the government intended to minimise the impact on the user experience and interfere only so far as is necessary to protect users from harm. Recalling the words of Nadine Dorries, acting in her role as Secretary of State for Digital, Culture, Media and Sport, the defining focus of the legislation is supposed to be *"the tackling of serious harm, not the curtailing of free speech."*[400] However, despite the intent of the government to exclusively target harmful communications (and indeed, the intent of the Law Commission of England and Wales in their proposal discussed in chapter two), both harms-based offences risk undermining free speech protection in the United Kingdom. This thesis concludes with some final thoughts as to the general impact of harms-based communications offences on free speech online, revisiting the three questions posed in the introduction.

The first question asked in the introduction is *"what type of speech, if any, causes harm?"*. The answer to this question, as well as the extent to which any harms-based approach interferes with free speech, will depend upon how harm is defined. The interpretation of

---

[397] Leif K-Brooks, Farewell Statement (*Omegle*, 4 November 2023) <www.omegle.com> accessed 1 December 2023
[398] Ibid.
[399] Ibid.
[400] HC Deb, 19 April 2022, vol 712, col 99.

Mill's harm principle in chapter one (that any *"harm"* should cause an identifiable damage) allows us to identify some of the types of speech which could cause harm (threats, incitement to lawless action, speech which endangers health, and speech which infringes upon the rights and reputation of others). This is consistent with the approach of the European Court of Human Rights, which only allows for interferences to freedom of expression where it is satisfied that the interference is necessary in a democratic society in pursuit of a legitimate aim, and that the measure taken is proportionate to the harm which it seeks to address. Hence, if the national authorities cannot demonstrate that an interference to free speech is necessary to prevent any of the harms identified in Article 10(2) of the European Convention on Human Rights 1953,[401] that interference will not be allowed. Alternative approaches to tackling harm may capture entirely different forms of speech (such as, offensive or immoral speech). However, it is incredibly unlikely that any such approach would be consistent with Mill's harm principle, which only extends to the prevention of identifiable harms. Furthermore, despite the fact that the European Convention on Human Rights 1953 allows for interferences to free speech for the protection of morals, this provision is seldom relied upon and appears to only apply so far as allowed for by the margin of appreciation. Another alternative approach, which may capture offensive and immoral speech, is to tackle speech based on its capacity to cause emotional harm. This is the approach suggested by the Law Commission of England and Wales in their proposed offence discussed in chapter two, which seeks to criminalise communications sent with the intention of causing emotional or psychological harm amounting to, at least, serious distress.[402] Whilst the proposal of the Law Commission of England and Wales is preferable to the character-based approach of section 127(1) of the Communications Act 2003 (which criminalises speech regardless of whether any harm has been incurred by anybody[403]), emotional harm is also difficult to demonstrate or identify. Hence, this approach may also fall foul of Mill's harm principle and the practice of the European Court of Human Rights, which both insist on the demonstration of harm before allowing an interference to free speech.

The second question asked by this thesis is *"in what ways does the internet exacerbate harm caused by speech?"*. There is little doubt that the speech tackled by the Online Safety Act 2023 can cause harm. However, this speech does not only exist online. Section 1.3 argues that the harmful speech has a greater capacity to cause harm where it is spread online, due

[401] European Convention on Human Rights 1953, Art.10(2).
[402] Law Commission, *Modernising Communications Offences: A final report* (Law Com No 399, 2021), para 2.257.
[403] Communications Act 2003, s.127(1).

to the omnipresent and pervasive character of the internet. Additionally, this section highlights the role of algorithms which disproportionately promotes harmful content online – particularly content which encourages acts of suicide, self-harm, or behaviours associated with eating disorders. This content all now falls under the designation of *"primary priority content which is harmful to children"* within the Online Safety Act 2023.[404] There is still no clear answer as to why this speech is only targeted where it appears online (with the exception of speech which encourages suicide, which may be captured offline by the Suicide Act 1961). [405] There is no equivalent legislation which criminalises the encouragement of self-harm or promotion of behaviour associated with eating disorders offline. If we accept that this speech causes harm offline, then it would make sense to target this with criminal legislation which applies offline. On the other hand, if this speech only becomes dangerous where it appears online, then one would assume that this is due to the methods of dissemination online which can exacerbate the harm caused by this speech – in which case, policymakers should focus on targeting systems rather than content as argued in chapter one. The same argument in respect of the priority content that is harmful to children. Where such speech is already criminalised offline (such as, incitement of racial hatred), then a systems-based approach would avoid any overlap in criminal law by exclusively targeting the method of dissemination which exacerbates this speech when it appears online.

More than three years after it was first proposed, the Online Safety Act 2023 has now been enacted. OFCOM has announced their intention to roll out the new duties for providers of online services in a phased manner, with the first coming into effect towards the end of 2024.[406] The final question which this thesis asks is *"to what extent might the Online Safety Act 2023 impede upon free speech protections in the United Kingdom?".* Chapter three highlights the risk that children's freedom of expression will be hampered by the targeting of harmful content, particularly as far as that freedom extends to their right to access information. This risk may be managed by the implementation of an appropriate complaints procedure – however, the details of the complaints procedure are not yet known. Chapter three also highlights the great threat to free speech posed by the new powers of OFCOM to subvert end-to-end encryption.[407] The lack of sufficient safeguards against abuse of this

[404] Online Safety Act 2023, s.61.
[405] Suicide Act 1961.
[406] OFCOM, 'New rules for online services: what you need to know' (OFCOM, 27 February 2024) < https://www.ofcom.org.uk/online-safety/information-for-industry/guide-for-services#:~:text=The%20Online%20Safety%20Act%20makes,in%20the%20UK%20safe%20online> accessed 12 March 2024.
[407] Online Safety Act 2023, s. 121(2).

provision is a direct threat to free speech protection in the United Kingdom – a threat which the European Union is being careful to avoid in formulating their own approach to tackling illegal content online. Beyond these threats to free speech within the Online Safety Act 2023, the Act also represents a failure to address the free speech concerns surrounding the communications offences which currently exist in the United Kingdom. Namely, the passage of the Online Safety Act 2023 was a missed opportunity to repeal section 127 of the Communications Act 2003[408] (discussed in chapter two).

A quote often attributed to Lyndon B. Johnson (36th President of the United States), is that *"you do not examine legislation in the light of the benefits it will convey if properly administered, but in the light of the wrongs it would do and the harms it would cause if improperly administered."*[409] The extent to which the Act will impede upon free speech relies largely on the administration by OFCOM – firstly, how they administer the complaints procedure will prove crucial in ensuring that children are not unduly denied their right to access information. Secondly, how they administer their new power to subvert end-to-end encryption could unduly interfere with the right to privacy and free speech of internet users. At this stage, we cannot be sure how OFCOM will carry out their new duties, nor can we conclude with certainty how providers of online services will react (in particular, whether companies such as WhatsApp will make good on their threats to stop operating in the United Kingdom). Nevertheless, there is a great risk that the *"improper administration"* of this legislation by OFCOM could damage free speech online in the United Kingdom.

[408] Communications Act 2003.
[409] Statement of George R. Whittington, National Board for Promotion of Rifle Practice, US Congress Hearing on Proposed Amendments to Firearms Acts (January 1965), 493.

LIST OF CASES

European Court of Human Rights

Handyside v UK (1976) 1 EHRR 737.

Hurbain v. Belgium App. no. 57292/16 (ECtHR, 4 July 2023).

Lingens v Austria (1986) 8 EHRR 407.

Lings v. Denmark (application no. 15136/20, 12 April 2022).

Ringier Axel Springer Slovakia, A.S. v. Slovakia (No.4) App. no. 26826/16 (ECtHR, 23 September 2021).

Podchasov v. Russia App. no. 33696/19 (ECtHR, 13 February 2024), 80.

United Kingdom

Adam Sutherland v Her Majesty's Advocate [2017] HCJAC 22.

Aidan McHugh v Procurator Fiscal, Airdrie [2015] HCJAC 86.

Alison Chabloz v Crown Prosecution Service [2019] EWHC 3094 (Admin).

Chambers v Director of Public Prosecutions [2012] EWHC 2157 (Admin).

Director of Public Prosecutions v Collins [2005] EWHC 1308 (Admin).

Director of Public Prosecutions v Collins [2006] UKHL 40.

MM v BC, RS, Facebook Ireland Limited [2019] NIMaster 5.

R v Sheppard & Whittle [2010] EWCA Crim 65.

Redmond-Bate v Director of Public Prosecutions [1999] EWHC Admin 733.

United States of America

Abrams v United States 250 U.S. 630 (1919).

Brandenburg v. Ohio 395 U.S. 444 (1969).

Chaplinsky v. New Hampshire, 315 U.S. 572 (1942).

FCC v. Pacifica Foundation, 438 U.S. 726 (1978), 4.

Harper & Row v. Nation Enterprises, 471 U.S. 539 (1985).

Miller v. California, 413 U.S. 24 (1973).

Reno v. ACLU, 521 U.S. 844 (1997), 869.

United States v Rumely 345 U.S. 41, 56 (1953).

Watts v. United States 394 U.S. 207 (1969).

TABLE OF LEGISLATION

United Kingdom

Abusive Behaviour and Sexual Harm (Scotland) Act 2016.
Communications Act 2003.
Criminal Justice and Courts Act 2015.
Data Protection Act 1998.
Domestic Abuse (Scotland) Act 2016.
Human Rights Act 1998.
Investigatory Powers Act 2016.
Malicious Communications Act 1988.
Offences Against the Person Act 1861.
Online Safety Act 2023.
Post Office Act 1908.
Post Office (Amendment) Act 1935.
Public Order 1986.
Sexual Offences Act 2003.
Suicide Act 1961.
Telegraph Act 1868.
Terrorism Act 2000.
Video Recordings Act 1984.

United Kingdom – Bills

Online Safety HC Bill (2022-2023) [220].
Online Safety HL Bill (2022-2023) [87(Rev)].
Online Safety HL Bill (2022-2023) [151].

International law

Universal Declaration of Human Rights 1948.
European Convention on Human Rights 1953.
Charter of Fundamental Rights of the European Union 2000.

International law – Proposals

European Commission, 'Proposal for a Regulation of the European Parliament and of the Council laying down rules to prevent and combat child sexual abuse' COM (2022) 209 final.

New Zealand

Harmful Digital Communications Act 2015.

United States of America

US Bill of Rights 1791.

BIBLIOGRAPHY

Books

- Bollinger, L. and Stone, G. Regulating Harmful Speech on Social Media: The Current Legal Landscape and Policy Proposals (New York, 2022; online edn, Oxford Academic, 18 Aug. 2022).
- Locke, J. An Essay Concerning Humane Understanding, (first published 1690, Project Gutenberg 2004).
- Mill, J. S. On Liberty (first published 1859).
- Milton, J. Areopagitica (first published 1644).
- Spirkin, A. Dialectical Materialism (Progress Publishers 1983).
- Woolley, S. C. "Bots and Computational Propaganda: Automation for Communication and Control" in Nathaniel Persily and Joshua A Tucker (eds), Social Media and Democracy: The State of the Field, Prospects for Reform (Cambridge University Press 2020).

Command Papers and Law Commission Reports

- Department for Culture, Media & Sport and the Home Department, Online Harms White Paper (White Paper, CP 57, 2019).
- Department for Culture, Media & Sport and the Home Department, Online Harms White Paper: Full Government Response to the consultation (White Paper, CP 354, 2020).
- Department of Culture, Media & Sport, Online Safety Bill: Update, (Written Ministerial Statement, HCWS39, 29 November 2022).
- Department for Science, Innovation & Technology, Super-complaints eligible entity criteria and procedural requirements (White Paper, 2023).
- John Woodhouse and Philip Ward, Briefing paper: Adult magazines in shops (House of Commons, Number 2039, 2016).
- John Woodhouse, Online Safety Bill: Progress of the Bill (Commons Library Research Briefing, Number 9579, 2023).
- Joint Committee on the Draft Online Safety Bill, Draft Online Safety Bill: Report of Session 2021-22 (HC & HL 2021-22).
- Law Commission, Abusive and Offensive Online Communications: A Scoping Report (Law Com No 381, 2018)
- Law Commission, Harmful Online Communications: The Criminal Offences - A Consultation Paper (Law Com No 248, 2020)
- Law Commission, Modernising Communications Offences: A final report (Law Com No 399, 2021).

Journal articles

- Howard, Philip N., and Muzammil M. Hussain, 'Digital Media and the Arab Spring, 'Democracy's Fourth Wave? Digital Media and the Arab Spring', [2013] Oxford Studies in Digital Politics.
- Jacob Rowbottom, The Transformation of Obscenity Law [2018] Information & Communications Technology Law, pg. 1.

Debates

- HC Deb, 5 December 2022, vol 724.
- HC Deb, 15 March 1935, vol 299.
- HC Deb, 19 April 2022, vol 712.
- HL deb 17 July 2023, vol 831.
- Statement of George R. Whittington, National Board for Promotion of Rifle Practice, US Congress Hearing on Proposed Amendments to Firearms Acts (January 1965), 493.

Newspaper articles and press releases

- Alex Hern, 'WhatsApp would not remove end-to-end encryption for UK law, says chief' (The Guardian, 9 March 2023) < https://www.theguardian.com/technology/2023/mar/09/whatsapp-end-to-end-encryption-online-safety-bill#:~:text=8%20months%20old-,WhatsApp%20would%20not%20remove%20end%2Dto%2Dend%20encryption,for%20UK%20law%2C%20says%20chief&text=WhatsApp%20would%20refuse%20to%20comply,in%20the%20UK%20in%20doubt.> accessed 1 December 2023.
- BBC News, 'Alison Chabloz avoids jail over anti-Semitic songs' (BBC News, 14 June 2018) <https://www.bbc.com/news/uk-england-derbyshire-44484632> accessed 29 June 2023.
- Chloe Louise, 'Anti-Semitic blogger, 58, who said gas chambers 'saved lives' and dubbed Auschwitz a 'theme park' appeals latest jail term for mocking Jewish people by changing lyrics of an Oliver Twist song' (Daily Mail, 23 February 2023) <https://www.dailymail.co.uk/news/article-11785867/Alison-Chabloz-said-gas-chambers-saved-lives-appeals-latest-jail-term.html> accessed 29 June 2023.
- Civil Liberties Committee, 'Child sexual abuse online: effective measures, no mass surveillance' (European Parliament, 14 November 2023) < https://www.europarl.europa.eu/news/en/press-room/20231110IPR10118/child-sexual-abuse-online-effective-measures-no-mass-surveillance> accessed 1 December 2023.
- European Parliament, 'Child sexual abuse online: agreement on extending current rules until April 2026' European Parliament News (15 February 2024).
- Joe Tidy, 'TikTok loophole sees users post pornographic and violent videos' BBC News (London, 21 April 2021).
- Scottish Legal News, 'Scot convicted over 'grossly offensive' tweet appeals to European Court of Human Rights' (Scottish Legal News, 27th October 2022) <https://www.scottishlegal.com/articles/scot-convicted-over-grossly-offensive-tweet-appeals-to-european-court-of-human-rights> accessed 29 June 2023.
- The National, 'Joseph Kelly spared jail for tweet about Captain Tom Moore' (The National, 30th March 2022) < https://www.thenational.scot/news/20031940.joseph-kelly-spared-jail-tweet-captain-tom-moore/> accessed 29 June 2023.

Websites and blogs

- Article 19, 'UK: Online Safety Bill risks undermining privacy around the world' (Article 19, 5 September 2023) < https://www.article19.org/resources/uk-online-safety-bill-risks-undermining-privacy-around-the-world/> accessed 21 September 2023.
- European Court of Human Rights, 'HUDOC' (European Court of Human Rights) < https://hudoc.echr.coe.int/#{%22documentcollectionid2%22:[%22GRANDCHAMBER%22,%22CHAMBER%22]}> accessed 22 January 2024.
- Facebook Help Centre, 'How does Facebook use artificial intelligence to moderate content?' (Facebook) < https://www.facebook.com/help/1584908458516247> accessed 22 January 2024.
- Tweet by Children's Commissioner for England (X, 26 October 2023) < https://twitter.com/childrenscomm/status/1717525638083395776> accessed 25 February 2024.
- Gina Wilson, 'Children's rights in the digital world: the UK's opportunity to create ground breaking legislation' (CYPCS, 8 February 2022) <https://www.cypcs.org.uk/news-and-stories/childrens-rights-in-the-digital-world/> accessed 21 February 2024.
- Leif K-Brooks, Farewell Statement (Omegle, 4 November 2023) <www.omegle.com> accessed 1 December 2023.
- Meta Privacy Centre, Privacy Policy (Meta, 15 June 2023) < https://www.facebook.com/privacy/policy/?entry_point=data_policy_redirect&entry=0 > accessed 19 November 2023.
- The Nasca Family, http://chasenasca.com (The Nasca Family) <http://chasenasca.com> accessed 2 March 2024.
- The National Archives, 'Records created or inherited by the Post Office Telegraph and Telephone Service' (The National Archives, 1853-1969) < https://discovery.nationalarchives.gov.uk/details/r/C343#:~:text=On%204%20April%201896%2C%20the,to%20the%20State%20in%201912.> accessed 29 June 2023.
- OFCOM, 'Preparing to regulate Online Safety: Categorising regulated services' (OFCOM, 11 July 2023) < https://www.ofcom.org.uk/news-centre/2023/preparing-to-regulate-online-safety-categorising-regulated-services> accessed 22 September 2023
- OFCOM, 'Ofcom's approach to implementing the Online Safety Act' (OFCOM, 26 October 2023) < https://www.ofcom.org.uk/online-safety/information-for-industry/roadmap-to-regulation> accessed 22 January 2024
- Samsung US, Samsung Galaxy S - NYC Launch Event (Samsung Galaxy S - Launch Event, New York City, 29 June 2010) < https://www.youtube.com/watch?v=Wf3uGTAeQy4> accessed 22 December 2023.
- Scottish Women's Aid, 'Domestic Abuse + the Law' (Scottish Women's Aid) <https://womensaid.scot/information-support/domestic-abuse-and-the-law/> accessed 22 February 2024.
- Stephen Parker, ((Survivors)) - Alison Chabloz (19 August 2022) <https://www.youtube.com/watch?v=SKA_5FPUW04> accessed 29 June 2023.
- Steve Jobs, Keynote Speech: MacWorld (MacWorld Conference, San Francisco, 9 January 2007) < https://www.youtube.com/watch?v=MnrJzXM7a6o> accessed 22 December 2023.

- Twitter Help Center, ‘Using Twitter’ (Twitter) < https://help.twitter.com/en/using-twitter> accessed 29 June 2023.
- WhatsApp, ‘About end-to-end encrypted backup’ (WhatsApp, 2023) < https://faq.whatsapp.com/490592613091019> accessed 22 September 2023
- X, X Privacy Policy, (X), < https://twitter.com/en/privacy > accessed 28 November 2023.
- TikTok, Privacy Policy (TikTok, 19 November 2023) < https://www.tiktok.com/legal/page/eea/privacy-policy/en > accessed 16 February 2024.

Reports

- Drafting Committee on an International Bill of Human Rights, 'Report of the Drafting Committee to the Commission on Human Rights’ (New York 9-25 June 1947) (1 July 1947) UN Doc E/CN. 4/21.
- OFCOM, Online Nation 2022 Report (1 June 2022).
- UNCRC ‘General Comment 25 on children’s rights in relation to the digital environment’ (2021) UN Doc CRC/C/GC/25.
- Philip Low, 'The Cambridge Declaration on Consciousness' (The Francis Crick Memorial Conference, Cambridge University, 7 July 2012) < https://fcmconference.org/img/CambridgeDeclarationOnConsciousness.pdf> 23 January 2024.