Northern Ireland Assembly

Research and Information Service Briefing Paper

Paper No. 51/21 June 2021 NIAR 126 -21

Online Trolling and Abuse

Georgina Ryan - White

1 Introduction

This briefing paper has been prepared in response to a request from the Committee for Justice, which sought research on the following:

- comparing the laws to tackle online trolling/abuse available in other jurisdictions including the UK and the Republic of Ireland;
- outlining examples of international good practice in this area; and
- clarifying what powers are reserved or devolved and what areas the Assembly can either influence or take action on in this area.

2 Background and Context

The rise of the internet and social media in recent decades has offered new opportunities for the way in which we interact with each other and as a society. In 2020, over 70% of UK adults had a social media profile, with the figure increasing to 95% for 16-24-year olds.[1]

Although this rise has brought many benefits, there are also 'associated risks and harms, and it has proved challenging for the law to keep pace with this rapidly changing environment'.[2] The physical boundaries of a home no longer afford safety from a bully and many people can now abuse a single person at once from anywhere in the world. It has contributed to emerging trends such as cyberbullying, online abuse and trolling directed at private persons and public figures.

Trolling involves sending abusive and hurtful comments across all social media platforms. It can often be done anonymously. There is no legal definition of trolling, however, the four main characteristics associated with trolling are:

- deception - acting differently on an online profile to how one would offline;
- aggression - aggressive, malicious behaviour undertaken with the aim of annoying or goading others into retaliating;
- disruption - seemingly pointless behaviour which appears to seek to gain attention rather than advance a conversation; and
- success – achieved by provoking a response to the trolling behaviour. Failure to provoke a response will lead to a troll upping their attempts, until success is achieved.[3]

A number of possible reasons for trolling include: a need for attention, everyday sadism, low self-confidence, lack of empathy, and a desire for amusement. It appears 'that specific kinds of trolling have different motivations, representing heterogeneity within the trolling community'.[4]

Recent research on behalf of the Department for Digital, Culture, Media and Sport suggests an emerging trend appears to be:

> *[…] the shift from trolling by individual internet users as defined above towards an automation of trolling activities, through the use of bots. These are defined generally as either simple algorithmic programs or cyborgs, that provide technological assistance for trolls to multiply their trolling efforts by scaling up*

[1] Ofcom, 2020.

[2] Law Commission (2018) Abusive and Offensive Online Communications Summary of Scoping Report, pg 2: https://s3-eu-west-2.amazonaws.com/lawcom-prod-storage-11jsxou24uy7q/uploads/2018/10/6.5013_LC_Online-Summary-Report_FINAL_WEB.pdf

[3] Centre for Strategy and Evaluation Services, Rapid Evidence Assessment: The Prevalence and Impact of Online Trolling: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/973971/DCMS_REA_Online_trolling__V2.pdf

[4] Ibid

> *responses/posting/re-tweeting etc. Two specific bot types identified in the literature are social bots, which mimic human social media activity, and political bots, which aim to manipulate public opinion by spreading political content or by participating in political discussions online'*.[5]

The level of trolling and online abuse is difficult to ascertain. Victims of abuse may choose to report the abuse to the police and/or to the social media platform. Many online offences or incidents are likely to be underreported. Where reported to the police, it has been noted internationally that 'a number of possible offences may apply to the same conduct, and the same offending may be recorded under different categories'.[6]

The Crown Prosecution Service's Guidelines on prosecuting cases involving communications sent via social media gives an overview of what people suffering online abuse can do:

> *A number of platforms have developed tools to make reporting easier, to secure potential evidence and to prevent unwanted communications, including those that do not amount to a criminal offence. These include:*
>
> - *A report link, so that particular or multiple communications can be reported directly to the platform. Social media sites may then decide to remove content and disable or suspend accounts, although it is not technically possible for a platform to guarantee a user will not return once their account is closed. Note that if a matter is reported to the police, the police should make a data retention request to the platform, so that evidence is secured for any investigation.*
> - *Taking screenshots of the offending material, which can be saved on or off (for example, cloud storage or a USB drive) the device.*
> - *Tools to block or mute the person who has uploaded abusive content, so that they can no longer see posts or have a conversation with the victim.*
> - *Tools to unsubscribe or "un-follow" accounts that produce or share offensive material.*
> - *Login alerts, which prompt the platform provider to send a notification if someone tries to log into an account from a new place.*
> - *Privacy settings, to control who can see posts and information from profiles, such as phone numbers and email address.*

[5] Ibid

[6] Professor Jonathan Clough, Faculty of Law, Monash University. The Criminalisation of Harmful and Offensive Communications in Australia: https://s3-eu-west-2.amazonaws.com/lawcom-prod-storage-11jsxou24uy7q/uploads/2018/11/Australia-J-Clough.pdf

- *Further cyber security advice can be found on the Government's website Cyber Streetwise and on the Government supported website Get Safe Online.*[7]

Certain groups of people seem to disproportionately experience online abuse. Academic commentators have coined the term 'networked misogyny' to describe 'an era that is marked by alarming amounts of vitriol and violence directed toward women in online spaces'. They note that these forms of abuse are not only focus on gender, but are also often racist, with women from ethnic minorities being particular targets.[8]

In 2016, the Guardian newspaper commissioned research into the 70 million comments that had been left on its online news articles in the previous decade. It produced quantitative evidence that:

> *Articles written by women attract more abuse and dismissive trolling than those written by men, regardless of what the article is about. Although the majority of our regular opinion writers are white men, we found that those who experienced the highest levels of abuse and dismissive trolling were not. The 10 regular writers who got the most abuse were eight women (four white and four non-white) and two black men. Two of the women and one of the men were gay. And of the eight women in the "top 10", one was Muslim and one Jewish. And the 10 regular writers who got the least abuse? All men*".[9]

Consequently, there can be an overlap between online abuse and hate crime as a proportion of online abuse is often described as 'online hate':[10]

> *Indeed, a significant subset of online abuse is targeted at people on the basis of their race, religion, gender or disability. However, not all abusive online communications amount to online hate.[…] Equally, hate crime can encompass a wide range of behaviour – including, for example, acts of physical violence against people because of their race or sexual orientation, or criminal damage to businesses or places of worship – as well as hate speech.*[11]

[7] Crown Prosecution Service (2018) Social Media - Guidelines on prosecuting cases involving communications sent via social media: https://www.cps.gov.uk/legal-guidance/social-media-guidelines-prosecuting-cases-involving-communications-sent-social-media

[8] Law Commission (2018) Abusive and Offensive Online Communications: A Scoping Report, pg 58 https://s3-eu-west-2.amazonaws.com/lawcom-prod-storage-11jsxou24uy7q/uploads/2018/10/6_5039_LC_Online_Comms_Report_FINAL_291018_WEB.pdf

[9] Ibid, pg 59

[10] Law Commission (2020) Harmful Online Communications: The Criminal Offences – Summary of the Consultation, pg 10: https://s3-eu-west-2.amazonaws.com/lawcom-prod-storage-11jsxou24uy7q/uploads/2020/09/Harmful-Online-Communications-Consultation-Paper-Summary-1.pdf

[11] Ibid

The UK Government has noted the impact of abuse and cyberbullying on victims:

> *Legal but harmful activity, such as cyberbullying, can also lead to impacts beyond the direct effect on the victim's welfare. Secondary effects of cyberbullying include depression, self-harm and life-long impacts for the victims. An estimated 37% of victims go on to suffer depression as a result and 41% develop social anxiety. In some cases these harms deter people from using online platforms, 26% of people deleted their social media profile after experiencing cyberbullying.*
>
> *The risk of abuse and cyberbullying also impacts how an individual uses online platforms. Half of girls aware of sexist abuse on social media say this has restricted what they do or aspire to in some way. The House of Commons Petitions Committee has highlighted the extreme abuse experienced online by disabled people, which has forced some of them to leave social media. Due to the large user bases of online platforms, and increasing dependence on technology, these harms affect a considerable proportion of the population.*[12]

In April 2018, researchers from the Universities of Oxford, Birmingham and Swansea conducted an extensive literature review, examining the association between cyberbullying involvement as a victim or perpetrator and self-harm and suicidal behaviour in children and young people. It concluded that young people under 25 years, who were victims of cyberbullying, were more than twice as likely to exhibit suicidal behaviour than non victims.[13]

Not all victims will have the same reaction to online abuse and trolling. Victims can often experience different 'shades of harm'. For example, not every victim will react in the same way to reading a threatening message on Twitter or Facebook; some may find it threatening while others will dismiss it.[14]

[12]: Department for Digital, Culture, Media and Sport and the Home Office (2021), The Online Safety Bill, Impact Assessment, pg 18 : https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/985283/Draft_Online_Safety_Bill_-_Impact_Assessment_Web_Accessible.pdf

[13] As cited in the Law Commission (2018) Abusive and Offensive Online Communications: A Scoping Report, pg 53https://s3-eu-west-2.amazonaws.com/lawcom-prod-storage-11jsxou24uy7q/uploads/2018/10/6_5039_LC_Online_Comms_Report_FINAL_291018_WEB.pdf

[14] Ibid pg 51

3 Current Legal Framework in Northern Ireland

The general principle is that what is illegal offline is also illegal online. Depending on the nature and content of the trolling and online abuse, it may constitute criminal activity under existing legislation including:

- the Malicious Communications (NI) Order 1988 which makes it an offence to send indecent, offensive, threatening or false letters or articles with intent to cause distress or anxiety.[15] It attracts a penalty of a fine of up to £2,500.
- the Protection from Harassment (Northern Ireland) Order 1997 which prohibits the act of harassment. The maximum penalty on indictment conviction (heard in a crown court) is up to 2 years' imprisonment and/or a fine. On summary conviction (heard in a magistrates' court), the maximum penalty is 6 months' imprisonment. The Order also provides for the offence of 'putting people in fear of violence'. A person convicted of this offence on indictment conviction is liable to imprisonment for up to seven years, or a fine or both; or on summary conviction, to imprisonment for a term not exceeding six months, or a fine up to £5,000.[16]
- the Communications Act 2003 which makes it an offence to use public electronic communications networks to send a message or any other matter that is grossly offensive or menacing and provides for a penalty of a maximum of six months' imprisonment and/or a fine of £5,000.[17]

The Protection from Stalking Bill, which is currently at Committee Stage, proposes to create a new offence of threatening or abusive behaviour where a person (A) behaves in a threatening or abusive manner and the behaviour would be likely to cause a reasonable person to suffer fear and alarm; and (A) intends by the behaviour to cause fear and alarm or is reckless as to whether the behaviour causes fear or alarm.[18] Behaviour can consist of a single act or omission, or a course of conduct on two or more occasions. It will attract a penalty on summary conviction of up to 12 months' imprisonment or a fine not exceeding the statutory maximum (£5,000) or both. The maximum penalty on conviction on indictment will be 5 years' imprisonment or a fine, or both.

Human Rights Implications

Article 10 of the European Convention on Human Rights[19] provides the following in respect of freedom of expression:

[15] Malicious Communications (NI) Order 1988,Article 3: https://www.legislation.gov.uk/nisi/1988/1849/article/3

[16] Protection from Harassment Order (NI) 1997, Article 3 and Article 6: https://www.legislation.gov.uk/nisi/1997/1180/contents

[17] Communications Act 2003, Section 127: https://www.legislation.gov.uk/ukpga/2003/21/section/127

[18] Protection from Stalking Bill, Clause 2: http://www.niassembly.gov.uk/globalassets/documents/legislation/bills/executive-bills/session-2017-2022/protection-from-stalking/protecton-from-stalking-bill---as-introduced---full-print-version.pdf

[19] European Convention on Human Rights: https://www.echr.coe.int/Documents/Convention_ENG.pdf

> *(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 the disclosure of information received in confidence, or for maintaining the authority and impartiality of the judiciary*.

However, Article 17 provides:

> *Nothing in this Convention may be interpreted as implying for any State, group or person any right to engage in any activity or perform any act aimed at the destruction of any of the rights and freedoms set forth herein or at their limitation to a greater extent than is provided for in the Convention.*

Therefore, a decision to prosecute a communications offence must be compliant with Article 10 unless the prosecution is satisfied 'that Article 17 provides that Article 10 will not be engaged at a freedom of expression aimed at destroying or limiting, for instance, a person's right to a private and family life, or their peaceful enjoyment of property, or their enjoyment of rights in a way discriminatory of them compared to others, will not engage Article 10'.[20]

Legislating in the future - reserved matters in Northern Ireland

Schedule 2 of the Northern Ireland Act 1998 sets out those matters which are 'excepted', meaning the Northern Ireland Assembly cannot legislate in these areas. Schedule 3 sets out matters which are 'reserved', meaning the Assembly cannot legislate in these areas unless the Secretary of State for Northern Ireland lays before Parliament the draft of an Order in Council amending Schedule 3 so that the matter ceases to be reserved. The Secretary of State cannot make such an Order unless the Assembly has passed, with cross-community support, a resolution stating that it wishes the matter to cease to be reserved.[21]

Telecommunications is a reserved policy area.[22] Therefore, any decision on online offences and the regulation of the internet is currently a matter for the UK

[20] Ibid

[21] Northern Ireland Act 1998, Section 4: https://www.legislation.gov.uk/ukpga/1998/47/section/4

[22] Northern Ireland Act 1998, Schedule 3: https://www.legislation.gov.uk/ukpga/1998/47/schedule/3

Government. However, the Northern Ireland Executive does have significant scope to develop and implement policies relating to devolved matters and harms, for example, child abuse safety as a result of its devolved responsibility for education, policing and child protection. The law, therefore, addresses the abuse of children via the internet as well as elsewhere.

As the general position in law is that what is illegal offline is also illegal online, the Executive can keep various aspects of the criminal law under review to ensure that appropriate action is taken to strengthen it where necessary. When discussing the Protection from Stalking Bill, a Department of Justice official indicated that they thought it would be possible, under the bill, to secure a successful conviction based on exclusively online stalking behaviour:

> *I think that the answer should be yes. Essentially, you are looking for a pattern of behaviour, and what you describe would fit the criteria. I have been in contact with a number of victims who have been stalked largely online. In one case, the person lifted stuff from their online site and used it in their place of employment to suggest that the victim was a sex offender. They were working only online, but they were interfering with the person's online identity and putting out false and malicious statements about them online. That, clearly, is stalking behaviour and would certainly fit in to our definition without any problem*.[23]

Hate Crime Legislation in Northern Ireland Independent Review

In June 2019, the Department of Justice announced the appointment of an independent review into hate crime legislation in Northern Ireland to be conducted by Judge Desmond Marrinan. Within the final report published in November 2020, Judge Marrinan commented on, and made some recommendations about, the effectiveness of the Malicious Communications (NI) Order 1988 and the Communications Act 2003. He said:

> *Section 127 of the CA 2003 is specifically concerned with public electronic communications networks and telecommunications and Internet services.*
>
> *These are matters which are reserved to the Westminster Parliament.*
>
> *As indicated above, the Law Commission for England and Wales is currently conducting a major review of abusive and offensive online communication following on from its scoping report of 2018. This review is not focused solely on prejudicial communications but will cover all forms of trolling, harassment and cyber bullying.*
>
> *In this context it should be further noted that Section 1 of the MCA 1998, which covers similar conduct in England and Wales, was amended to become*

[23] NI OR Committee for Justice, 21 January 2021:http://data.niassembly.gov.uk/HansardXml/committee-25076.pdf

triable either way by the Criminal Justice and Courts Act 2015 and is now subject to a maximum penalty of two years imprisonment or fine or both.

It is of concern that Article 3 of the MCO 1998 – the equivalent law applying in Northern Ireland – is only triable summarily with a maximum sentence of a level 4 fine.

I feel constrained by the remit of this review not to make a specific recommendation to bring the sentencing maximum penalty for this offence in line with England and Wales.

However, I see no good reason not to do so.

I suggest that it is a matter which should receive close consideration in the current review of sentencing being conducted by the Department of Justice

It is noted that the offence in Section 127 of the CA 2013 may only be prosecuted summarily and is subject to a maximum penalty of six months imprisonment or a fine or both.

It has been observed that this can lead to significant limitations on its application in practice.

There is a strong argument that Section 127 should be amended to make it triable both summarily and on indictment.

There is now a strong case for bringing the sentencing provisions of the Section 127 offences into line with the provisions applicable to the MCA 1998.

This is another matter which will be addressed by the Law Commission in its current review of abusive and offensive online communications.

Although it would theoretically be possible to make recommendations in relation to reforming the CA 2003 in its application to Northern Ireland – with the agreement of the Secretary of State for Northern Ireland – I am of the view that these particular matters should be left for further consideration by the Law Commission which is already deeply engaged in the subject.

The Law Commission is likely to have reported well before any Hate Crime and Public Order Bill arising from the recommendations made in this review reaches the floor of the Assembly.[24]

[24]Hate crime legislation in Northern Ireland Executive Summary, pg 575-576https://www.justice-ni.gov.uk/sites/default/files/publications/justice/hate-crime-review.pdf

4 Comparable Arrangements in rest of the UK and the Republic of Ireland

4.1 Scotland

Telecommunications is also a reserved matter in Scotland. There are a number of existing offences which can address online abuse and trolling if the behaviour amounts to criminal activity:

- common law offences of breach of the peace and threats;
- threatening and abusive behaviour – section 38 of the Criminal Justice and Licensing (Scotland) Act 2010;
- stalking – section 39 of the Criminal Justice and Licensing (Scotland) Act 2010; and
- improper use of a public electronic communications network - section 127 of the Communications Act 2003.

In May 2018, Lord Bracadale published his report following an independent review of hate crime legislation in Scotland (the Bracadale review).[25] This led to the introduction of a Hate Crime Bill before the Scottish Parliament, which was enacted in April 2021.[26] In May 2017, a public petition PE1652, on abusive and threatening communication, was lodged with the Public Petitions Committee.[27] In December 2018, the petition was considered in light of the final report of the Bracadale review. Although the petitioner welcomed the report, she was concerned that it did not address the issues raised in her petition.

The Scottish Government then considered responses to its consultation on the Bracadale recommendations. It maintained its position that there were:

> *a number of practical difficulties" in relation to delivering what the petitioner was calling for, noting that some matters are reserved to Westminster. The Scottish Government also referred to on-going work on this issue, including the UK Government's white paper on online harms and the Law Commission's review of the law in England and Wales. It stated that it would 'carefully consider any proposals" to change the law in this area, where the relevant powers are devolved.[28]*

In his review, Lord Bracadale noted that:

> *The Law Commission's role is limited to the law of England and Wales. However, it is recognised that various offences in this area also extend to*

[25]Scottish Government (2018) Independent review of hate crime legislation in Scotland: final report https://www.gov.scot/publications/independent-review-hate-crime-legislation-scotland-final-report/

[26] Hate Crime and Public Order (Scotland) Act 2021:https://www.legislation.gov.uk/asp/2021/14/introduction/enacted

[27]SP PE1652: https://archive2021.parliament.scot/GettingInvolved/Petitions/PE01652

[28] Ibid

> *Scotland: the conclusions of that review should therefore also inform UK Government policy development which applies across the UK in relation to reserved matters.*

Although he did not consider that any further legislative changes were necessary at this stage, he went on to say:

> *I would encourage the Scottish Ministers ... to consider whether the outcomes of the Law Commission's work on online offensive communications identify any reforms which would be of benefit to Scots criminal law across reserved and devolved matters.*[29]

The Committee agreed to close the petition on the basis that the Scottish Government had indicated that it remained unconvinced of the practicality of the action being called for, but that it would consider any proposals to reform the law that might fall within the Scottish Parliament's competence in light of the work being undertaken in England and Wales.

4.2 Republic of Ireland

In September 2016, the Law Reform Commission published its *Report on Harmful Communications and Digital Safety*.[30] It contained 32 recommendations for reform and included a draft Harmful Communications and Digital Safety Bill intended to implement these reforms.

The main recommendations related to changes in the criminal law were:

- reform of the existing offence of harassment, to ensure that it includes online activity such as posting fake social media profiles; and that there should be a separate offence of stalking, which is really an aggravated form of harassment; and
- reform of the existing offence of sending threatening and intimidating messages, to ensure that it fully captures the most serious types of online intimidation.

The Report also recommended the establishment of a statutory Digital Safety Commissioner, based on similar models in Australia and New Zealand, to promote digital safety and oversee efficient take-down procedures.

The Harassment, Harmful Communications and Related Offences Act 2020 originated as a Private Member's Bill, sponsored by Brendan Howlin T.D., which was influenced by the Law Reform Commission's Report. Following the publication of the

[29] Ibid at 25

[30] Law Reform Commission (2016) *Harmful Communications and Digital Safety* September: http://www.lawreform.ie/_fileupload/Reports/Full%20Colour%20Cover%20Report%20on%20Harmful%20Communications%20and%20Digital%20Safety.pdf

Bill, the Minister for Justice agreed to work with Deputy Howlin, to amend the provisions therein.[31]

Section 4 of the Act provides for an offence of distributing, publishing or sending a threatening or grossly offensive communication both online or offline which intends to cause harm to the person who is the recipient of the message. Harm is defined to include psychological harm. The maximum penalties for this offence on conviction on indictment are 2 years' imprisonment and/or an unlimited fine.[32]

Section 11 amended section 10 of the Non-Fatal Offences Against the Person Act 1997 with the intention of strengthening the offence of harassment contained therein. The maximum penalty for harassment was increased from 7 years' imprisonment to 10 years' imprisonment.

The General Scheme of the Online Safety and Media Regulation Bill 2020 was approved in November 2020 and was subsequently published in December by the Minister for Tourism, Culture, Arts, Gaeltacht, Sport and Media. It consists of three general themes:

- Parts 2 and 3: The establishment of the Media Commission and dissolution of the Broadcasting Authority of Ireland;
- Part 4: Online Safety; and
- Parts 5 and 6: On-Demand Audiovisual Services and miscellaneous provisions regarding the transposition of the EU Audiovisual Media Services Directive.

The Bill introduces online safety codes which will instruct how designated online service providers should address harmful online content. An Online Safety Commissioner will be established as the regulator to ensure adherence to these codes. The Commissioner will form part of a new multi-person Media Commission, which replaces the Broadcasting Authority of Ireland. Harmful online content is defined as including:

- content by which a person engages in serious cyberbullying,
- content by which a person promotes suicide or self-harm, and,
- content by which a person promotes behaviour associated with eating disorders.

These definitions are being refined during detailed legal drafting of the Bill by the Office of the Attorney General. It is not proposed to define harmful online content as a singular concept. The Government explained its rationale as follows:

> *It is not proposed to define harmful online content as a singular concept as it has not been possible to arrive at a suitable, broad, and principle based*

[31] Harassment, Harmful Communications and Related Offences Bill 2017,Explanatory Memorandum: https://data.oireachtas.ie/ie/oireachtas/bill/2017/63/eng/memo/b63a17d-memo.pdf

[32] Harassment, Harmful Communications and Related Offences Act 2020, Section4: http://www.irishstatutebook.ie/eli/2020/act/32/section/4/enacted/en/html#sec4

> *description of the meaning of this phrase. Instead, it is proposed to enumerate definitions of categories of material that are considered to be harmful online content. In deciding on this policy approach the Department has had regard to a number of other considerations of similar matters, especially that of the Law Reform Commission in their Report on Harmful Communications and Digital Safety and the UK's Online Harms White Paper. Neither of these attempted to define harmful online content or online harm and instead approach this issue by enumerating categories of material or behaviour that they consider to fall within the scope of the notion of harmful online content or online harm. This is indicative of enumeration being a preferred approach to this issue. Further to this, it is worthwhile noting that we have not located a jurisdiction that has attempted to define harmful online content or online harm in their law.*[33]

The category to address cyberbullying has been described as follows:

> *This category has a base in Article 28b(1)(a) and (b) of the revised Directive. Subparagraph (a) concerns material which may "impair the physical, mental or moral development of minors" and subparagraph (b) concerns the "incitement to violence or hatred... based on any grounds referred to in Article 21 of the Charter".*
>
> *The grounds listed in Article 21 of the Charter of Fundamental Rights of the European Union are "sex, race, colour, ethnic or social origin, genetic features, language, religion or belief, political or any other opinion, membership of a national minority, property, birth, disability, age, sexual orientation or nationality". It is difficult to conceive of any reasonable concept of cyberbullying which would not fall within the margin of discretion afforded to Member States in interpreting these two references when applying the revised Directive in their national law. Therefore, the proposed definition of cyberbullying as a category of harmful online content is legally clear in its constituent elements and can be legally attributed to Article 28b(1)(a) and (b) as appropriate.*[34]

Provision is also made in the Bill for the addition of further categories of harmful online content in the future. This process will involve a proposal by the Media Commission, informed by stakeholder consultation and both Government and Oireachtas approval. The purpose of this provision is to futureproof the legislation to avoid the need for ad-hoc legislation to deal with emerging harms in the future.

The General Scheme does not propose to regulate the speech of individuals. It is considered 'an attempt at balancing the harms of online bullying and abuse on the one hand, and the right to freedom of expression on the other'.[35] It also 'does not

---

[33] Government of Ireland (2020) Online Safety and Media Regulation Bill, General Scheme, pg 83: https://www.gov.ie/pdf/?file=https://assets.gov.ie/126000/b174bdcd-e017-47d9-bb48-07b29671330c.pdf#page=null

[34] Ibid at pg 84

[35] Oireachtas Library & Research Service (2020) Online harms – what are the legal issues? pg 3: https://data.oireachtas.ie/ie/oireachtas/libraryResearch/2020/2020-07-09_l-rs-note-online-harms-what-are-the-legal-issues_en.pdf

propose to make the dissemination of any material a criminal offence' as such. A 'regulatory approach is favoured', including the power to administer administrative financial sanctions. This is due 'to the constitutional issues presented by attaching criminal liability to speech'.[36] In the event of a service provider failing to comply with a requirement of an online safety code, the Media Commission will have the power to initiate authorised officer investigations and to issue compliance and warning notices. Failure to comply with a warning notice may lead to the Media Commission seeking to apply a sanction, including financial sanctions of up to €20m or 10% of turnover.[37]

The Joint Committee on Media, Tourism, Arts, Culture, Sport and the Gaeltacht has written to key stakeholders and experts seeking submissions on the Bill as part of its Pre-Legislative Scrutiny of the Heads of the Bill. It is intended that the Bill will be enacted this year.

4.3 England and Wales

Similar to Northern Ireland and Scotland, rather than specific offences, there are a number of existing offences that can address various kinds of online abuse and trolling. These include:

- stalking and "stalking involving fear of violence or serious alarm or distress" - sections 2A and 4A of the Protection from Harassment Act 1997 (as amended)
- harassment - section 2 of the Protection from Harassment Act 1997
- improper use of a public electronic communications network - section 127 of the Communications Act 2003
- sending indecent, grossly offensive, false or threatening communications - section 1 of the Malicious Communications Act 1988.

In 2019, the Solicitor General confirmed that 'the number of prosecutions commenced for offences under the Communications Act 2003 and the Malicious Communications Act 1988 had increased by over 20% in the previous three years'.[38]

Section 103 of the Digital Economy Act 2017 requires the Secretary of State for Digital, Culture, Media and Sport to issue guidance on action which might be appropriate for social media providers to take against bullying, intimidation or insulting behaviour on their sites in advance of the new regulatory framework envisaged in the Online Harms White Paper.[39] This code of practice does not affect

[36] Ibid

[37] Dáil Éireann Debate, Thursday, 17 December 2020: https://www.oireachtas.ie/en/debates/question/2020-12-17/319/?highlight%5B0%5D=online&highlight%5B1%5D=online&highlight%5B2%5D=online

[38] HC Deb 31 January 2019 Vol 653: https://hansard.parliament.uk/commons/2019-01-31/debates/17FA3585-B68F-4A0E-85A5-D215C0211609/InternetTrollingProsecutionRates

[39] Department for Digital, Culture, Media and Sport (2019 Code of Practice for providers of online social media platforms: https://www.gov.uk/government/publications/code-of-practice-for-providers-of-online-social-media-platforms/code-of-practice-for-providers-of-online-social-media-platforms

how illegal content or conduct is dealt with. The Code is directed at providers of social media platforms, but is also relevant to any sites hosting user-generated content and comments, including review websites, gaming platforms and online marketplaces.

The Government expects social media platforms to adhere to the following four principles:

- Social media providers should maintain a clear and accessible reporting process to enable individuals to notify social media providers of harmful conduct.
- Social media providers should maintain efficient processes for dealing with notifications from users about harmful conduct.
- Social media providers should have clear and accessible information about reporting processes in their terms and conditions.
- Social media providers should give clear information to the public about action they take against harmful conduct.

UK Wide Developments – Legislating for the Future

Over the past number of years, the UK Government has begun to examine how the internet can become a safer place for users, through the application of rules and online behaviour. It has done so using a dual approach looking at the regulation of platforms and the effectiveness of current legal provisions:

- The introduction of the Internet Safety Green Paper in 2017 and the Online Harms White Paper in 2019, which focussed on the regulation of platforms, lead to the publication of a draft Online Harms Bill in May 2021;
- Whereas, the Law Commission's work in recent years has examined the criminal law provisions that apply to individuals and not the liability of platforms.

There have been calls 'for a coherent, unified body of law aimed specifically at online activities'.[40] Successive governments have maintained the general legal principle that what is illegal offline is also illegal online, and that existing legislation can be used to tackle online abuse. This was re-affirmed in February 2016 when the Government said it did not 'intend to introduce specific legislation to address online harassment and internet trolling'.[41]

In February 2016, the Conservative government also rejected the idea of making bullying a criminal offence:

[40] HC Library Briefing, 9 June 2017, Online harassment and cyber bullying

[41] HC Parliamentary Question 25115 answered 1 February 2016: http://www.parliament.uk/written-questions-answers-statements/written-question/commons/2016-02-01/25115

> *We do not want to make any form of bullying a criminal offence as to do so would risk criminalising young people. In some circumstances that may be justified, but probably only in a limited number of very serious cases, for which there are already laws in place to protect people. Internet providers, schools and parents all have a role to play in keeping children and young people safe online*.[42]

Most recently, the Government has stated:

> *Online abuse of any kind is unacceptable. To ensure the law is fit for purpose to tackle abuses online, we have asked the Law Commission to review our laws on harmful and abusive online communications and highlight any gaps in the criminal law that cause problems in tackling this abuse. The Law Commission has consulted on provisional reforms and will issue final recommendations by summer 2021, which the government will carefully consider.*[43]

In 2016, the Law Commission consulted on whether reform of the law on online communications should be part of its 13th Programme of Law Reform. The project was subsequently commissioned by Theresa May's Government in February 2018, which asked the Law Commission to 'review the laws around offensive communications and assess whether they provide the right protection to victims online'. In November 2018, the Law Commission published a Scoping Report on Abusive and Offensive Online Communications. The report analysed the relevant criminal law and concluded that there was scope to improve it. In particular, it recommended that:

> *The communications offences in section 1 of the Malicious Communications Act 1988 and section 127 of the Communications Act 2003 should be reformed to ensure that they are clear and understandable and provide certainty to online users and law enforcement agencies.*
>
> *As part of the reform of communications offences, the meaning of "obscene" and "indecent" should be reviewed, and further consideration should be given to the meaning of the terms "publish", "display", "possession" and "public place" under the applicable offences.*
>
> *In addition to a reform of the communications offences, there should be a review to consider whether coordinated harassment by groups of people online could be more effectively addressed by the criminal law.*

[42] HC Parliamentary Question 27104 answered 23 February 2016: http://www.parliament.uk/written-questions-answers-statements/written-question/commons/2016-02-11/27104

[43] HC Parliamentary Question 146942 answered 5th February 2021: https://questions-statements.parliament.uk/written-questions/detail/2021-02-01/146942

> *As part of the reform of communications offences the threshold at which malicious and "false" communications are criminalised should be reviewed.*[44]

In September 2020, the Law Commission published proposals, laid out in a consultation paper that aimed to ensure that the law is clearer and targets serious harm and criminality arising from online abuse. The 'proposals seek to strike the balance between protecting victims from harmful behaviour, whilst also better protecting the right to freedom of expression'. The proposals are 'technologically neutral' so that as technology and behaviours change, the criminal law will be able to adapt'.[45] The Law Commission explained its rationale as follows:

> *One reason for proposing a technologically neutral offence is to mitigate the risk that the law will become redundant or unhelpful in the face of technological change. Given that the CA 2003 covers only communications sent via a "public electronic communications network", it is ill-equipped to deal with technologies like Bluetooth or Apple's AirDrop function. We hope the new offence will avoid this kind of problem – as well as striking the right balance between freedom of expression and the need to protect people from harm.*[46]

The Commission has proposed two complementary offences to replace section 1 of the Malicious Communications Act 1988 and section 127 of the Communications Act 2003:

> *The first new offence relates to a defendant sending or posting a communication that was likely to cause harm to a likely audience. It would apply where a defendant intends to harm, or is aware of a risk of harming when sending or posting a communication, without reasonable excuse for doing so. The offence does not require proof that anyone was actually harmed.*
>
> - *The aim of this proposed reform is to provide an effective mechanism for addressing a range of online behaviours.*
> - *This could cover harmful and abusive emails, social media posts and WhatsApp messages, as well as pile-on harassment.*
> - *The audience could include the recipient of a message, the defendant's social media followers or other people – for example, someone else who sees a harmful tweet on Twitter.*
> - *"Without reasonable excuse" is an element of the offence that must be proven by the prosecution.*

[44] Law Commission (2018) Abusive and Offensive Online Communications: A Scoping Report https://s3-eu-west-2.amazonaws.com/lawcom-prod-storage-11jsxou24uy7q/uploads/2018/10/6_5039_LC_Online_Comms_Report_FINAL_291018_WEB.pdf

[45] Law Commission (2020) News Article: https://www.lawcom.gov.uk/greater-protections-for-victims-of-online-abuse-proposed-by-law-commission/

[46] Law Commission (2020) Harmful Online Communications: The Criminal Offences – Summary of the Consultation, pg 7: https://s3-eu-west-2.amazonaws.com/lawcom-prod-storage-11jsxou24uy7q/uploads/2020/09/Harmful-Online-Communications-Consultation-Paper-Summary-1.pdf

- *"Reasonable excuse" should be defined to include where the communication either was or was meant as a contribution to a matter of public interest. Under the proposals, the jury or magistrate will decide whether the defendant acted without reasonable excuse, but this factor must be considered. This requirement helps to ensure that freedom of expression is adequately protected. For example, it is unlikely that someone criticising the decision of a politician on Twitter, or airing a view on a particularly controversial issue, would be found to lack reasonable excuse.*

The second new offence addresses knowingly false communications. Under the existing offence, it is a crime to send a knowingly false communication for the purpose of causing 'annoyance, inconvenience or needless anxiety'. The Law Commission's proposals would raise this threshold:

- *Our suggested threshold would be met if the defendant sends or post a communication that they know to be false, they intend to cause non-trivial emotional, psychological, or physical harm to a likely audience, and they send it without reasonable excuse.*
- *Our proposals wouldn't cover communications that the defendant believes to be true – no matter how dangerous those communications may be. The issue of 'fake news' lies beyond the terms of reference of this project so is not an issue that we tackle.*

The consultation paper also asked questions but did not put forward proposals on a series of behaviours. Specifically, it asked whether there should be specific offences covering:

- Incitement or encouragement of pile-on harassment;
- Knowing participation in pile-on harassment;
- Glorification of violence or of violent crime; and
- Incitement or encouragement of self-harm.

Regulation of Online Harms

An Online Harms White Paper was published in April 2019, which said that the existing 'patchwork of regulation and voluntary initiatives' had not gone far or fast enough to keep UK users safe.[47] Therefore, it proposed a single regulatory framework to tackle a range of online harms. At its core would be a new statutory duty of care for internet companies, including social media platforms. An independent regulator would oversee and enforce compliance with the duty. The White Paper received mixed reactions. Children's charities were supportive. However, some

[47] HM Government, Online Harms White Paper, April 2019, p30: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/973939/Online_Harms_White_Paper_V2.pdf

commentators raised concerns that harms were inadequately defined. Others were concerned that the proposals could adversely impact on freedom of expression.[48]

Following the White Paper's publication, the Government undertook a 12-week public written consultation, alongside a programme of stakeholder engagement. An initial response to the consultation was published in February 2020. This stated, among other things, that the Government was minded to make Ofcom the regulator for online harms. A full response was published in December 2020. It confirmed that a duty of care would be introduced through an Online Safety Bill and that Ofcom would be the regulator. Again, reaction was mixed.

On 12 May 2021, the Government published the Online Safety Bill. All provisions of the Bill will apply across England, Wales, Scotland and Northern Ireland. In line with the Government's December 2020 response to its Online Harms consultation, the draft Bill would impose duties of care on providers of online content-sharing platforms and search services. Ofcom would enforce compliance and its powers would include being able to fine companies up to £18 million or 10% of annual global turnover, whichever is higher, and have the power to block access to sites.

Part 2 of the draft Bill sets out the duties of care that would apply to providers of user-to-user and search services. All regulated services would have to take action to tackle 'illegal content' and 'content that is harmful to children'. Category 1 regulated services[49] would also have to address "content that is harmful to adults".

The Government has stated:

> *In line with the government's response to the Online Harms White Paper, all companies in scope will have a duty of care towards their users so that what is unacceptable offline will also be unacceptable online.*
>
> *They will need to consider the risks their sites may pose to the youngest and most vulnerable people and act to protect children from inappropriate content and harmful activity.*
>
> *They will need to take robust action to tackle illegal abuse, including swift and effective action against hate crimes, harassment and threats directed at individuals and keep their promises to users about their standards.*
>
> *The largest and most popular social media sites (Category 1 services) will need to act on content that is lawful but still harmful such as abuse that falls below the threshold of a criminal offence, encouragement of self-harm and mis/disinformation. Category 1 platforms will need to state explicitly in their terms and conditions how they will address these legal harms and Ofcom will hold them to account.*

[48] HC Library Briefing 28 May 2021, Regulating online harms: https://researchbriefings.files.parliament.uk/documents/CBP-8743/CBP-8743.pdf

[49] These are high risk and high reach platform providers such as Twitter and Facebook

> *The draft Bill contains reserved powers for Ofcom to pursue criminal action against named senior managers whose companies do not comply with Ofcom's requests for information. These will be introduced if tech companies fail to live up to their new responsibilities. A review will take place at least two years after the new regulatory regime is fully operational*.[50]

The meaning of harmful content is set out in the lengthy clauses of 45 to 47 of the draft Bill. In summary, 'regulated content' would be considered harmful:

- if it is designated in secondary legislation as "primary priority content" that is harmful to children or "priority content" that is harmful to children or adults;
- if a service provider has "reasonable grounds to believe that the nature of the content is such that there is a material risk of the content having, or indirectly having, a significant adverse physical or psychological impact" on a child or adult of "ordinary sensibilities"; and
- if a service provider has "reasonable grounds to believe that there is a material risk" of the dissemination of the content "having a significant adverse physical or psychological impact" on a child or adult of "ordinary sensibilities".[51]

In a December 2020, Julian Knight MP, Chair of the Digital, Culture, Media and Sport Committee, stated that he welcomed the duty of care 'with the threat of substantial fines levied on companies that breach it'. However, he warned that 'even hefty fines can be small change to tech giants and it's concerning that the prospect of criminal liability would be held as a last resort'. He also cautioned 'against too narrow a definition of online harms that is unable to respond to new dangers'.[52]

The framework would not put any new limits on online anonymity. However, under the duty of care, companies would be expected to address anonymous online abuse that is illegal through 'effective systems and processes'. Where companies providing Category 1 services prohibited legal but harmful online abuse, they would have to ensure their terms and conditions were clear about how this applied to anonymous abuse.[53]

The Secretary of State for Digital, Culture, Media and Sport has stated:

> *On anonymity, we have not taken powers to remove anonymity because it is very important for some people—for example, victims fleeing domestic violence and children who have questions about their sexuality that they do*

---

[50] Gov.UK DCMS/Home Office Press Release 12 May 2021: https://www.gov.uk/government/news/landmark-laws-to-keep-children-safe-stop-racial-hate-and-protect-democracy-online-published

[51] Draft Online Safety Bill, Clause 45-47: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/985033/Draft_Online_Safety_Bill_Bookmarked.pdf

[52] DCMS Committee News, 15 December 2020: https://committees.parliament.uk/committee/378/digital-culture-media-and-sport-committee/news/137895/chair-comments-on-online-harms-legislation/

[53] As cited in HC Library Briefing 28 May 2021, Regulating online harms, pg 16: https://researchbriefings.files.parliament.uk/documents/CBP-8743/CBP-8743.pdf

> *not want their families to know they are exploring. There are many reasons to protect that anonymity*.[54]

The Samaritans have claimed that the Bill doesn't go far enough to ensure a 'suicide-safer internet' because only the largest and most popular platforms would be required to address content that is legal but harmful to adults which risks the most harmful suicide and self-harm content moving to less prolific or popular sites.

The Department for Digital, Culture, Media and Sport has indicated that, there are a number of areas within the regime where there is possible interaction with devolved competencies, and so government is working closely with the Territorial Offices (TOs) and Devolved Administrations (DAs) to ensure that such issues are taken into account. This includes issues such as harms in scope and media literacy.[55]

It has also clarified that:

> *While some of the harms relate to offences in Scottish or Northern Irish Law, and therefore involve devolved competences, the legislation is not seeking to change the law in relation to these offences. Instead, our proposals seek to clarify the responsibility of businesses to tackle this activity on their services.*
>
> *The Department for Culture, Media and Sport has said that it 'engaged regularly with the DAs, TOs, and OFCOM's offices in the devolved nations as proposals have been developed, and it will continue to engage throughout the legislative process*.[56]

The Justice Minister, Naomi Long MLA, has confirmed:

> *Telecommunications legislation is a reserved matter but many of the harms covered in the Government White Paper on Online Harms relate to devolved matters. On that basis my officials have been liaising with the Department for Culture, Media and Sport [DCMS] to ensure the interests of Northern Ireland are fully met in the process.*
>
> *Alongside the work on the Online Harms legislation, the Law Commission in England and Wales is conducting a review to ensure the criminal law is fit for purpose to deal with online communications. The Commission will provide final recommendations to DCMS in early 2021, which could inform the government's future position in relation to illegal online abuse. Officials here will continue to keep in touch with the DCMS as this work progresses.*

---

[54] HC Deb 15th December 2020 Vol 689: https://hansard.parliament.uk/commons/2020-12-15/debates/1B8FD703-21A5-4E85-B888-FFCC5705D456/OnlineHarmsConsultation

[55] Ofcom's definition of media literacy is: 'the ability to use, understand and create media and communications in a variety of contexts.

[56] Department for Digital, Culture, Media and Sport and the Home Office (2021), The Online Safety Bill, Impact Assessment, pg 111:https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/985283/Draft_Online_Safety_Bill_-_Impact_Assessment_Web_Accessible.pdf

I took the opportunity to raise this issue when I met with Priti Patel during the summer. The Home Secretary expressed her commitment to working closely with us on this issue […].[57]

[57] NI AQW 10651/17-22: http://aims.niassembly.gov.uk/questions/printquestionsummary.aspx?docid=316917

5 Arrangements in some international jurisdictions

5.1 Australia

The Enhancing Online Safety for Children Act 2015 established the Office of the eSafety Commissioner with a mandate to coordinate and lead online safety across government, industry and the not-for profit community.[58] The legislation was introduced after the death of Charlotte Dawson, a TV presenter and a judge on Australia's Next Top Model, who killed herself in 2014 following a campaign of cyber-bullying against her on Twitter. She had a long history of depression.

When the Office was first established, the eSafety Commissioner's functions and powers primarily related to enhancing online safety for children. In 2017, the Act was amended to expand the Commissioner's remit to promoting and enhancing online safety for all Australians.[59]

The Act established a complaints service for victims who experience serious cyberbullying and gives the Commissioner the power to investigate complaints about serious cyberbullying material.

The Act established a two-tiered scheme for the removal of cyberbullying material from participating social media services. The two Tiers are subject to different levels of regulatory oversight. The Act does not automatically apply to all services which fit the definition of a social media service. A service must be categorised as either a tier 1 or tier 2 service before it becomes subject to the regulatory power of the Commissioner. Therefore, a service will escape the scrutiny of the Commissioner if it falls outside either classification.

To become classified as tier 1[60], a service must apply to the Commissioner, who has to be satisfied that the service complies with basic online safety requirements. The intent is that tier 1 services should have robust systems in place to address content internally. The Commissioner can issue requests to remove content within 48 hours following receipt of a complaint from a child, parent or third party with the consent of the child.

Tier 2 services are large social media services which have been selected by the Minister on recommendation of the Commissioner. The Commissioner has greater powers with respect to tier 2 services, including the ability to impose civil penalties and issue formal warnings. Under section 40 of the Act, the Commissioner may also draft and publish a notice on the Office's website to that effect.

On 11 December 2019, the Department of Communications and the Arts began a consultation on its proposal to create a new Online Safety Act. This followed recommendations made in a 2018 review to reform and expand the existing

[58] Enhancing Online Safety for Children Act 2015: https://www.legislation.gov.au/Details/C2017C00187
[59] Office of the eSafety Commissioner website, Legislation: https://esafety.gov.au/about-the-office/legislation
[60] Any social media service may apply to eSafety to be declared a tier 1 service under section 23 of the Act.

patchwork of online safety laws.[61] On the same day, the Government also issued an Online Safety Charter, outlining expectations for industry to protect Australians from harmful online experiences. The Online Safety Bill 2021 was introduced in February 2021 and is currently awaiting assent.[62] When enacted it will repeal the Enhancing Online Safety for Children Act 2015.

Key aspects of the Online Safety Act include:

- a set of basic online safety expectations focusing on user empowerment, transparency, service integrity and collaboration with government and civil society;
- an extension of the Enhancing Online Safety for Children Act's cyberbullying scheme for children to cover relevant electronic services and designated internet services, as well as social media services;
- a new cyber abuse scheme for adults, which would include a new end user take-down and an associated civil penalty regime to combat menacing, harassing or offensive material intended to cause serious distress or serious harm;
- consistent take-down deadlines for image-based abuse, cyber abuse, cyberbullying and seriously harmful online content, so that online service providers will have to remove that material within 24 hours of a request from the eSafety Commissioner;
- a requirement for the Australian technology industry to take a more active and extensive role in addressing access to harmful online content, and give the eSafety Commissioner greater powers to address illegal and harmful content hosted overseas; and
- a requirement for online service providers to offer the best available technology to prevent children's access to harmful content, complemented by a new accreditation scheme to evaluate available tools and an obligation to proactively advise users about available opt-in tools and services.

The Bill has proved controversial. The Australian Greens Party is seeking to have the Bill repealed, citing it was rushed and requires more thought before it can be enacted. They have been highly critical of the Bill to date as they are concerned that it will make the eSafety Commissioner the ‘sole arbiter of internet content in Australia’.[63]

The Senate Standing Committee for the Scrutiny of Bills also expressed ‘significant scrutiny concerns with respect to the broad discretionary power granted to the

[61] Report of the Statutory Review of the Enhancing Online Safety Act 2015 and the Review of Schedules 5 and 7 to the Broadcasting Services Act 1992 (Online Content Scheme) https://www.communications.gov.au/publications/report-statutory-review-enhancing-online-safety-act-2015-and-review-schedules-5-and-7-broadcasting

[62] Parliament of Australia, Online Safety Bill 2021: https://www.aph.gov.au/Parliamentary_Business/Bills_Legislation/Bills_Search_Results/Result?bId=r6680

[63] ABC News Article 15th June 2021: https://www.abc.net.au/news/2021-06-15/new-laws-esafety-online-abuse-penalties-trolling/100217376

Commissioner by provisions in the bill that leave significant matters to delegated legislation'.[64]

5.2 Canada

There is no specific provision in Canada's Criminal Code for trolling or online abuse. However, when the behaviour reaches the level of criminal conduct, charges under the following sections of the Criminal Code may be considered:

- Criminal harassment;
- Uttering threats;
- Intimidation;
- Mischief incitement of hatred;
- Child pornography;
- Counselling suicide;
- Sharing of an intimate image without consent; and
- Revenge porn.

Nova Scotia

In 2013, Nova Scotia introduced the Cyber Safety Act in response to alleged acts of child pornography and cyberbullying against a teenager, Rehtaeh Parsons, who committed suicide in April 2013. However, in the case of *Crouch v. Snell* (2015) the Nova Scotia Supreme Court struck down the Act on the ground that it unjustifiably interfered with the rights to freedom of expression and liberty under the Canadian Charter.[65] The court described the overreaching definition of 'cyberbullying' in the Act as a 'colossal failure' because of the extent to which it interfered with freedom of expression. The court found that the Act did not provide any defences or required a proof of harm and therefore did not outweigh the right to free expression.

In 2017, the Intimate Images and Cyber-protection Act was introduced.[66] This Act allows the victims of cyberbullying, or their parents, to apply to the Supreme Court of Nova Scotia for a court order, called a cyber-protection order. An application for a cyber-protection order is a court process for private legal disputes and is not a criminal process. The victim must decide if they want to apply for the order themselves.

The Supreme Court can make an order prohibiting a person from making communications that amount to cyber-bullying and /or order prohibit the person from

[64] Standing Committee for the Scrutiny of Bills, Scrutiny Digest 7 of 21: https://www.aph.gov.au/-/media/Committees/Senate/committee/scrutiny/scrutiny_digest/2021/PDF/d07_21.pdf?la=en&hash=2409CBCD02D4D5374BD85F60189B90F477E796C1

[65] Crouch v Snell (2015) NSSC 340: http://www.courts.ns.ca/decisions_of_courts/documents/2015nssc340.pdf

[66] Intimate Images and Cyber-protection Act 2017: https://www.canlii.org/en/ns/laws/stat/sns-2017-c-7/latest/sns-2017-c-7.html

future contact with the applicant or another person. A court can also award damages to a victim of cyberbullying.[67]

The Act defines cyberbullying as:

> *[…] an electronic communication, direct or indirect, that causes or is likely to cause harm to another individual's health or well-being where the person responsible for the communication maliciously intended to cause harm to another individual's health or well-being or was reckless with regard to the risk of harm to another individual's health or well-being, and may include (i) creating a web page, blog or profile in which the creator assumes the identity of another person, (ii) impersonating another person as the author of content or a message, (iii) disclosure of sensitive personal facts or breach of confidence, (iv) threats, intimidation or menacing conduct, (v) communications that are grossly offensive, indecent, or obscene, (vi) communications that are harassment, (vii) making a false allegation, (viii) communications that incite or encourage another person to commit suicide, (ix) communications that denigrate another person because of any prohibited ground of discrimination listed in Section 5 of the Human Rights Act, or (x) communications that incite or encourage another person to do any of the foregoing;*
>
> *(d) "distribute without consent", in respect of an intimate image, means to publish, transmit, sell, advertise or otherwise distribute the image to or make the image available to a person other than the person depicted in the image while (i) knowing that the person in the image did not consent to the distribution, or (ii) being reckless as to whether that person consented to the distribution.[68]*

5.3 New Zealand

The Harmful Digital Communication Act 2015[69] (HDCA) aims to deter, prevent and mitigate the harm caused to victims by cyber bullying, harassment and 'revenge porn'. It was enacted following recommendations from the Law Commission's review of existing laws in 2012, which found that 1 in 10 New Zealanders had experienced a harmful digital communication at some stage in their lives.

The HDCA includes a range of measures to prevent and reduce the impact of cyberbullying and other modern forms of harassment and intimidation:

- It established an approved agency, NetSafe, to deal with complaints, and introduced a civil court process for serious or repeated harmful digital communications. Victims have to go to NetSafe before they can apply to the court, which can make orders to take down material and other remedies.
- It also included a new criminal offence to send messages and post material online that deliberately causes a victim serious emotional distress. The

[67] Ibid section 6

[68] Ibid Section 3

[69] Harmful Digital Communications Act 2015: http://www.legislation.govt.nz/act/public/2015/0063/latest/whole.html

offence is punishable by up to 2 years' imprisonment or a maximum fine of $50,000 for individuals and a fine of up to $200,000 for companies. A criminal offence under the HDCA is subject to the same youth justice process that applies to other offences. Therefore it is not applied to children under the age of 14, but can be applied to young people aged 14-16 under the youth justice system.[70]

The District Court deals with cases of harmful digital communications that Netsafe has not been able to resolve. The Act introduced new court orders which can order a broad range of remedies, including:

- orders to take down material;
- cease-and-desist orders;
- orders to publish a correction, an apology or give the complainant a right of reply;
- orders to release the identity of the source of an anonymous communication; and
- ordering name suppression for any parties.

It is an offence not to comply with these court orders. Anyone found guilty may be sentenced up to six months imprisonment or fined up to $5,000 (companies can be fined of up to $20,000).[71]

The Act ensures that social media providers should not necessarily be held responsible for others' actions. It includes an optional immunity, which limits providers' liability for harmful content posted by others, but only if they follow a set process for handling complaints.[72] Under that process, hosts have to make it easy for victims to make a complaint about content they're hosting. They also have to follow certain steps within certain timeframes.

The Act also strengthened the law against inciting someone to commit suicide. It is now illegal, regardless of whether or not the victim attempts to take their own life (previously, it was only an offence if the victim committed suicide or tried to). The offence is punishable by up to 3 years' imprisonment.

[70] https://www.netsafe.org.nz/what-is-the-hdca/

[71] Ibid, Section 21
[72] Ibid, section 24