Cyber Abuse
Introduction and Literature Review

Olivia Gonzalez
BA (NYU), MSc (Oxon), JD (Fordham)

info@highwayonetrust.com
86 Tavistock Place
London
WC1H 9RT

Highway One Trust is an independent grant-making charitable trust founded in 2016.

We fund a wide range of organisations and charities
working to support positive, enduring change.

Research by Olivia Gonzalez BA (NYU), MSc (Oxon), JD (Fordham) Summer 2017
Sources reviewed and updated by Phoebe Thomson BA (Cantab) March 2019

TABLE OF CONTENTS

Foreword **5**
Introduction **7**
1. Cyber Bullying **9**
1.1 Definition 9
1.2 Vulnerable Populations & Impact 9
1.3 Legal Background 12
1.4 International Legal Approaches 12
1.5 Proposed or Possible Solutions 13
1.6 Further Research 15
1.7 Major Organisations 15
2. Nonconsensual Pornography ("Revenge Porn") **19**
2.1 Definition 19
2.2 Vulnerable Populations & Impact 19
2.3 Legal Background 20
2.4 International Legal Approaches 21
2.5 Proposed or Possible Solutions 22
2.6 Further Research 23
2.7 Major Organisations 24
3. Toxic Online Mental Health Communities: Pro-Ana And Pro-Suicide Websites **26**
3.1 Definition 26
3.2 Vulnerable Populations & Impact 26
3.3 Legal Background 27
3.4 International Legal Approaches 28
3.5 Proposed or Possible Solutions 28
3.6 Further Research 30
3.7 Major Organisations 31
4. Fraud and Discrimination in Online Dating Platforms **32**
4.1 Definitions 32
4.2 Vulnerable Populations & Impact 32
4.3 Legal Background 38
4.4 International Legal Approaches 38
4.5 Proposed or Possible Solutions 39
4.6 Further Research 41
4.7 Major Organisations 42
5. Hate Speech Online **44**
5.1 Definitions 44
5.2 Vulnerable Populations & Impact 44
5.3 Legal Background 45
5.4 International Legal Approaches 46
5.5 Proposed or Possible Solutions 48
5.6 Further Research 49
5.7 Major Organisations 49
6. Child Abuse Online **52**
6.1 Definitions 52
6.2 Vulnerable Populations & Impact 52
6.3 Legal Background 54
6.4 International Legal Approaches 54
6.5 Proposed or Possible Solutions 55
6.6 Further Research 56
6.7 Major Organisations 57

7. Terrorist Radicalisation Online 60
7.1 Definitions 60
7.2 Vulnerable Populations & Impact 60
7.3 Legal Background 62
7.4 International Legal Approaches 62
7.5 Proposed or Possible Solutions 63
7.6 Further Research 65
7.7 Major Organisations 65
8. Ethical Design of Technology 68
8.1 Definitions 68
8.2 Vulnerable Populations & Impact 68
8.3 Legal Background 71
8.4 International Legal Approaches (Tracking Cookies only) 71
8.5 Proposed or Possible Solutions 72
8.6 Further Research 73
8.7 Major Organisations 73
9. Conclusion 75

Foreword

Highway One Trust was founded four years ago to support organisations that are following paths towards long term and lasting change. We make grants and provide support and advice to registered UK charities and to international charities, and to other non-profit making bodies whose activities relate to our objects. Our focus is on seven areas: disfiguring medical conditions; women in need; prison and injustice; poverty, economic regeneration and homelessness; internet and mobile networks; singleness; and Christianity.

We commissioned this report in 2017 to inform our giving in the fifth of these areas: internet and mobile networks. It was also to identify gaps in the literature, where we might fund further research. Since then we have supported organisations that focus on anti-bullying, Internet safety for young people, and the development of fair and effective Government policy.

In 2019 we reviewed and refreshed the report, updating the organisations covered, references, and links where necessary.

Effect and challenge of the 2020 Covid Pandemic

There has been much discussion about how our lives will change forever has a result of the 2020 pandemic which we are still living through. It is becoming overwhelming clear that one of the major effects it is having is driving people as never before to dependence on the internet.

Our personal relationships, our shopping, our social interaction, even places of worship, political debates, and processes have moved online, and the "virtual' has become mainstream in all our lives – even those who would have rejected the notion even a few months ago. It is even being used to track infections. The internet has helped us to sustain our way of life, our work and our relationships and protect us from harm as never before.

It is quite possible that the greatest long term effects will not be our reluctance to go to festivals, theatres, embrace each other and use public transport but propel us to a dependence on the internet that is greater than we could ever have imagined even six months ago.

That is what makes the need for informed knowledge and action essential. People who exploit the internet do so for reasons of greed, they desire to control and manipulate other's minds and bodies, they push forward their agendas, or give expression to unhealthy emotions and behaviour. They seek out the vulnerable.

They spread fear, or further conspiracies and misinformation. Even intelligent well intentioned people have spread theories and stories that turn out to be false and damaging. The power and motivation to further such agendas will continue to grow.

The need to understand the issues and identify and support positive and informed initiatives is more relevant than ever.

This Report

The report covers eight areas, focusing on the potential harm to individuals.

(1) Cyber Bullying
(2) Nonconsensual Pornography ("Revenge Porn")
(3) Toxic Online Mental Health Communities: Pro-Ana And Pro-Suicide Websites
(4) Fraud and Discrimination in Online Dating Platforms
(5) Hate Speech Online
(6) Child Abuse Online
(7) Terrorist Radicalisation Online
(8) Ethical Design of Technology

Since 2017, there has been much debate about the lack of regulation on the internet, the ability of foreign powers to apply influence covertly well beyond their borders, and the power of social media and search engine companies to target information and indeed shield information from users. These issues have made it easier to create more divided and polarised societies, and are set out in a September 2019 Oxford Internet Institute report.

Despite this new danger, the Internet's potential for harm to *individuals* remains relatively unabated. As the medium for the fastest and most immersive communication capability in human history it has achieved great advances; but at the same time this capability has amplified many less desirable human characteristics.

We hope that by sharing this report, we can help others who like us are working to make the Internet a better place for everyone.

Highway One Trustees
September 2020

Introduction

Cyber abuse is a term encompassing a wide range of aggressive online activities, including bullying, stalking, and invasions of privacy. While not all forms of online abuse present novel problems, some types of cyber abuse do challenge existing legal and institutional structures and require new approaches.

The objective of this literature review is to evaluate the academic research, legal approaches, and policy solutions to nine topics relating to cyber abuse. In particular, this overview identifies the social, psychological, financial and legal impacts of cyber abuse. Each section highlights populations particularly vulnerable to cyber abuse, focusing on types of abuse such as cyber bullying, sexual exploitation, damage to self-image, and online dating romance scams.

In accordance with the Highway One Trust's mission statement, the aim of this report is to examine "whether and how damage may be caused to individuals and groups." As such, special attention is paid to possible solutions – both social and legal, that may be implemented to address cyber abuse. Since many Internet companies are based overseas, one of the major challenges is enforcing legal remedies: this issue is addressed in each section.

There are many kinds of cyber abuse, and each one affects victims differently. This report will first discuss cyber bullying, a form of Internet aggression primarily affecting children and adolescents. While several studies have found cyber bullying to have negative effects on the victim's mental health, new studies suggest that it may less prevalent than face-to-face bullying. The controversy about cyber bullying's novelty impacts the possible solutions that could be implemented to guard against its deleterious effects on victim welfare.

Hate speech is another category of cyber abuse, primarily affecting minority groups. Regulation of hate speech is a grey area, as laws policing hate speech must strike a balance between preventing abuse and protecting free speech. Because free speech laws vary across countries, policing hate speech results in some regulatory inconsistency. Since the anonymity of the Internet can embolden aggressive behaviour, it is increasingly important to protect minority groups from the harmful effects of online hate speech.

While some cyber abuse occurs between strangers on the Internet, it can also occur in the context of familiar relationships. This will be reviewed in a chapter dealing with online dating platforms. Stalking, harassment of women, and marginalisation of minority users are central problems affecting online dating communities. Romance scams and fraud on dating profiles can wreak emotional and financial harm on victims. While online dating platforms facilitate social interaction, they can also be misused to exploit vulnerable people.

Two chapters in this review will be devoted to sexual abuse online, a phenomenon that affects both adults and children. Nonconsensual pornography, sometimes referred to as "revenge porn", is one such form of sexual abuse. It involves the distribution of sexually graphic images of individuals without their consent. This kind of cyber abuse poses complex questions about the responsibility of social media platforms and Internet Service Providers to respond to and take down this content. The appropriate response to this societal problem involves consideration of existing legal barriers to prosecution and technical barriers to enforcement. This kind of sexual abuse and invasion of privacy most often affects adults. Another chapter of this review will discuss cyber abuses against children, including child pornography and online solicitation. While most jurisdictions legally prohibit child pornography and nonconsensual pornography, tracking down such content and ensuring its removal is often more difficult. Attention will be paid to these existing challenges and their possible solutions.

This review will also dedicate two chapters to discussion of toxic online communities. While social media and online social spaces can create valuable communities, they can also host environments that encourage self-destructive behaviour. One chapter in this review will discuss websites that promote eating disorders and suicide. These websites are particularly damaging for vulnerable individuals, leading to the exacerbation of existing mental health issues. The second chapter on toxic online communities will deal with online radicalisation of terrorists. Radical groups often use social media to recruit isolated, lonely, or mentally ill individuals. This illustrates that online social spaces can be abused to incite violence or target vulnerable people.

Finally, this review will conclude by briefly evaluating the field of ethical design in technology. This involves evaluating the ethical implications of particular technological innovations. The ethical questions posed by technological advances should be considered in order to prevent future cyber abuses. The final section will present this forward-looking inquiry and how future harms can be avoided.

1. Cyber Bullying

1.1 Definition

Cyber bullying is defined as "wilful and deliberately harmful communications carried out by one or multiple people via electronic digital devices including mobile phones, tablets, gaming consoles and computers."[1]

1.2 Vulnerable Populations & Impact

While adults can also fall victim to cyber bullying, research suggests that it primarily affects children and adolescents, with girls being twice as likely to be bullied.[2] According to the National Society for the Prevention of Cruelty to Children, teenagers are more likely to experience cyber bullying than younger children.[3] Young people who have a learning or physical disability, or who identify as LGBTQA+ are particularly vulnerable.[4] Cyber bullying has deleterious effects on mental health, body image, and social cohesion.[5] Young victims have reported suicidal ideation and a fear of attending school as a result of being bullied online.[6] A 2017 study concluded that 41% of surveyed cyber bullying victims developed social anxiety and 37% developed depression.[7] This illustrates the risk of harm to victims of online bullying.

The relative impact of cyber bullying compared to traditional forms of bullying remains controversial. A 2017 survey conducted by Ditch the Label, a UK anti-bullying organisation, concluded that nearly 70% of young people admitted to being abusive towards another person online.[8] This includes activities such as posting negative comments on an individual's photo,

---

1 The Cybersmile Foundation (2017) available at https://www.cybersmile.org/advice-help/category/what-is-cyberbullying

2 Cyberbullying: An analysis of data from the Health Behaviour in School-aged Children (HBSC) survey for England (2017), available at https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/621070/Health_behaviour_in_school_age_children_cyberbullying.pdf

3 '*Always There When I Need You': Childline Annual Review 2014-2015*, available at https://learning.nspcc.org.uk/media/1374/childline-annual-review-always-there-2014-2015.pdf

4 Ditch the Label, The Annual Bullying Survey (2017) available at https://www.ditchthelabel.org/research-papers/the-annual-bullying-survey-2017

5 Phil Mckenna, *The Rise of Cyber Bullying*, 195 New Scientist 2613 (2007) https://www.newscientist.com/article/mg19526136-300-the-rise-of-cyberbullying (Subscription only).

6 *See* Thomas J. Holt, Grace Chee, Ai Hong Ng et al., *Exploring the Consequences of Bullying Victimization in a Sample of Singapore Youth*, 23 International Criminal Justice Review 1 (2013) https://journals.sagepub.com/doi/abs/10.1177/1057567712475305 (Abstract: full report is available to purchase)

7 Ditch the Label, The Annual Bullying Survey (2017) available at https://www.ditchthelabel.org/research-papers/the-annual-bullying-survey-2017

8 *Id.*

wrongfully reporting profiles, sharing another's private information, or impersonating someone.[9] The anonymity of online communications has been shown to play a role in the perpetuation of cyber bullying.[10] Seventeen percent of survey respondents reported being victims of online bullying. This suggests that cyber bullying continues to be a meaningful problem affecting young people.

However, contrary research by the Oxford Internet Institute ("OII") suggests that cyber bullying is actually relatively rare.[11] This study focused primarily on fifteen year olds, finding that only 3% of respondents said bullying happened *both* on and offline. The main conclusion of the OII study was that despite the growth of social media, traditional bullying (such as name calling and exclusion) remains "considerably more common than cyber bullying."[12] Less than 1% of 15 year olds in England reported being bullied online, while more than 27% experience exclusively face-to-face bullying methods. A study conducted by the University of Warwick evaluated almost 3000 pupils and corroborated this finding, stating that cyber bullying rarely occurs in isolation.[13] This suggests, contrary to the Ditch the Label study, that cyber bullying remains a less widespread form of bullying.

Further research is needed to explain this discrepancy. There are a number of factors that could explain this difference. According to the Cybersmile Foundation, children may often be reluctant to admit that they are victims of cyber bullying.[14] Since most studies of cyber bullying involve self-reporting, the reluctance of victims to report their experiences could skew the results. In the 2017 Ditch the Label study, 37% of bullying victims never told anyone about their experiences. This suggests that a tendency towards silence could change the results of these studies. Moreover, education on the phenomenon of cyber bullying remains under-developed. As a result, children and adolescents may not realise they are victims of bullying. Children with low self-esteem or mental health issues may also find it difficult to recognise that they are being treated unjustly.

---

9 *Id.*

10 Christopher Barlett, Kristina Chamberlin, Zachary Witkower, *Predicting Cyberbullying Perpetration in Emerging Adults: A Theoretical Test of the Barlett Gentile Cyberbullying Model*, 43 Aggressive Behavior 2 (2016). https://onlinelibrary.wiley.com/doi/abs/10.1002/ab.21670 (Abstract: full report is available to purchase).

11 Andrew K. Przybylski & Lucy Bowes, *Cyberbullying and adolescent well-being in England: a population-based cross-sectional study*, The Lancet Child & Adolescent Health (2017). https://www.thelancet.com/journals/lanchi/article/PIIS2352-4642(17)30011-1/fulltext

12 *Id.*

13 Dieter Wolke, Kirsty Lee, Alexa Guy, *Cyberbullying: a storm in a teacup?*, 26 European Child & Adolescent Psychiatry 8 (2017). https://link.springer.com/article/10.1007/s00787-017-0954-6

14 The Cybersmile Foundation (2017) available at https://www.cybersmile.org/advice-help/category/what-is-cyberbullying

Another factor that could explain this discrepancy is a difference in social media behaviour. In particular, different social media platforms lend themselves to different kinds of negative speech. Ditch the Label's study highlights Instagram as being the vehicle most used for mean comments. The platform's focus on stylised, edited photographs that emphasise an individual's lifestyle enables users to examine and critique outward appearance. Twitter, by contrast, relies less on photos and more on short, 280-character micro-blogging. Since not all social media platforms lend themselves to the same kinds of cyber bullying, differences across platforms may affect the results of the studies discussed above.

Adults are also susceptible to the harms of cyber bullying. A 2015 Global Survey conducted by the All Rise organisation found that 62% of cyber abuse victims were over 18 years old.[15] Research shows that cyber bullying often occurs among students in their 20s. A 2010 study found that 21.9% of college students reported being cyber bullied.[16] According to a 2014 Pew research study, 40% of adult Internet users have personally experienced some form of online harassment.[17] This includes sexual harassment, stalking, physical threats, purposeful embarrassment, or offensive name-calling.[18]

While the word "bullying" connotes schoolyard fighting between children, cyber bullying takes on many forms. Nonconsensual pornography, or revenge porn, is another form of cyber bullying that primarily affects adults. This phenomenon will be discussed in further detail in chapter two of this review. In 2010, Tyler Clementi, a Rutgers University student took his own life after he found that his roommate had secretly recorded an intimate encounter he had with another man and posted about it online.[19] This shed light on the issue of cyber bullying among university students and its impact on the LGBTQA+ community

Cyber bullying can also involve harassment and trolling. In 2014, a 19 year old Wisconsin student committed suicide after she was harassed online over her choice to appear in pornography.[20] Thus, cyber bullying can manifest itself in a variety of ways, harming adults

---

[15] All Rise, 2015 Global Survey Results, available at https://www.allrisesaynotocyberabuse.com/research?lightbox=dataItem-j2ytdcho

[16] Christine D. MacDonald & Bridget Roberts-Pittman, *Cyberbullying Among College Students: Prevalence and Demographic Differences*, 9 Procedia – Social and Behavioral Sciences (2010). https://www.sciencedirect.com/science/article/pii/S1877042810025413

[17] Maeve Duggan, *Part 1: Experiencing Online Harassment*, Pew Research Center, Oct 22, 2014 available at https://www.pewinternet.org/2014/10/22/part-1-experiencing-online-harassment

[18] *Id.*

[19] *See* Patrick McGeehan, *Conviction Thrown Out for Ex-Rutgers Student in Tyler Clementi* Case, NYTimes, Sep. 9, 2016, available at https://www.nytimes.com/2016/09/10/nyregion/conviction-thrown-out-for-rutgers-student-in-tyler-clementi-case.html (Subscription required)
see also Tyler Clementi's Story, Tyler Clementi Foundation, available at https://tylerclementi.org/tylers-story

[20] Tyler Kingkade, *College Student Alyssa Funke Commits Suicide Following Cyberbullying Over Porn, Huffington Post*, May 22, 2014, available at https://www.huffingtonpost.com/2014/05/22/alyssa-funke-suicide-porn_n_5373138.html

as well as children. The harms of cyber bullying do not exclusively impact college-aged adults or young people. Samuel C. McQuade argues that "contrary to what most people may think, cyber bullying although primarily a youth problem, is not limited to teens and adolescents."[21] He notes that older adults can also become victims. This suggests that insufficient attention is being paid to the proportion of adult victims of cyber abuse.

1.3 Legal Background

While there is no definition of cyber bullying under UK law, there are a number of existing laws that apply to cases of cyber bullying.[22] Communications that fall under the category of cyber bullying can amount to criminal offenses.[23] However, cases of online abuse are difficult to prosecute and must meet a high evidentiary threshold. Prosecutors take into consideration a number of issues, such as (1) whether communications constitute credible threats of violence, (2) whether they specifically target an individual and may constitute harassment or stalking and (3) whether the communications are considered grossly offensive, indecent, obscene or false.[24] While cyber bullying itself is not illegal, a perpetrator may be committing a criminal offense under any one of these other laws.

1.4 International Legal Approaches

(9) Australia: Under Australian law, it is an offense to use the Internet, social media or a telephone to menace, harass or cause offense. The maximum penalty for this offense is three years imprisonment or a fine of more than $30,000. However, each kind of cyber bullying receives its own treatment under Australian law. Online stalking, for instance, carries heavier maximum penalties than many other types of cyber-abuse.[25]

(10) European Union: None of the EU member states has adopted provisions that are explicitly aimed at targeting cyber bullying.[26] European Data Protection

---

[21] Samuel C. McQuade, James P. Colt, Nancy B.B. Meyer, *Cyber Bullying: Protecting Kids & Adults from Online Bullies*, Praeger Publishers (2009).

[22] See e.g., Protection from Harassment Act 1997; Criminal Justice and Public Order act 1994, Malicious Communications Act 1988; Communications Act 2003; Breach of the Peace (Scotland); Defamation Act 2013.

[23] *See also* NSPCC, National Guidance on Cyber bullying available at https://www.nspcc.org.uk/what-is-child-abuse/types-of-abuse/bullying-and-cyberbullying

[24] This final prong will only be considered if prongs (1) or (2) do not apply. *See* Social Media - Guidelines on prosecuting cases involving communications sent via social media (Revised 2018) available at https://www.cps.gov.uk/legal-guidance/social-media-guidelines-prosecuting-cases-involving-communications-sent-social-media

[25] "Cyber Bullying", Australian Cybercrime Online Reporting Network (2017) available at https://www.acorn.gov.au/learn-about-cybercrime/cyber-bullying

[26] "Cyber Bullying Among Young People," Study for the LIBE Committee (2016) available at https://www.europarl.europa.eu/RegData/etudes/STUD/2016/571367/IPOL_STU(2016)571367_EN.pdf

Legislation is now being applied to issues of cyber bullying, online harassment and identity theft. A 2016 study for the European Parliament concluded that "a national framework to prevent and tackle cyber bullying is an essential step towards the concrete protection of children's rights."[27] As a policy matter, the EU study concludes that cyber bullying should be addressed with preventative methods rather than punitive ones. As such, no criminal law exists among EU member states because "criminalising children is not seen as an ideal solution to effectively tackle this phenomenon." The main best practices adopted by EU member states included information campaigns, instituting educational programmes and involving stakeholders like NGOs, youth organisations, and schools.

(11) United States: Each state in the US has its own statutes for cyber bullying. Generally, US law does not always treat cyber bullying criminally, but it provides a range of sanctions depending on the severity of the perpetrator's actions. Generally, state laws include a procedure for reporting the bullying and ensuring that victims receive appropriate mental health support. Under many state laws, school personnel are required to report in a timely manner any incidents of cyber bullying. In California alone, for instance, there are nearly 30 statutes that indirectly cover cyber bullying and its prevention. At present, no federal law in the US directly addresses bullying. However, it sometimes overlaps with discriminatory harassment and is addressed under existing legal frameworks.

1.5 Proposed or Possible Solutions

Solutions to cyber bullying could come from civil society, the technology industry, or from changes in the legal landscape. Thematically, the types of solutions can be grouped around two areas: raising awareness and protecting children.[28] Many jurisdictions have refrained from implementing legal solutions because of a reluctance to criminalise the actions of children. Thus, the proposed solutions are typically preventative rather than punitive.

[27] *Id.*
[28] *Id.*

(1) Civil Society Solutions

Information campaigns educating children and parents about the nature of cyber bullying have been carried out with the aim of helping victims recognise instances of abuse. NGOs such as Cybersmile have responded to the problem of cyber bullying by establishing help hotlines, initiating educational campaigns, and conducting further research. Civil society could prevent cases of cyber bullying by educating the public about its nature and effects. Health classes in schools could include chapters on mental health, educating students on how to identify and respond to cyber bullying. Information campaigns could seek to equip school counsellors and parents with the tools to understand online bullying. These kinds of awareness campaigns can help temper the psychological effects of cyber bullying by ensuring that victims promptly receive the necessary support. Overall, enabling the education sector (which includes schools and NGOs) to conduct successful information campaigns can help address the root cause of cyber bullying.

(2) Technology Solutions

The private sector can also play a role in responding to cyber bullying. Ditch the Label's key recommendations in its 2017 bullying report included a call for technology companies to address concerns from young people and be robust about removing under-age users. Some platforms, such as Facebook and Instagram, include prohibitions against cyber bullying in their community standards. Since cyber bullying is often carried out on public social media platforms, the companies are well placed to stop and de-escalate abuse. While some companies have established such preventative policies, further research is needed into their effectiveness.

(3) Legal Solutions

As previously discussed, very few jurisdictions address cyber bullying within the context of criminal law. However, one proposed legal response involves holding adult bystanders liable if they fail to report severe forms of cyber bullying. In a law review article entitled "The Cyber Samaritans," Heather Benzmiller argues that witnesses of cyber bullying should be held liable under a "Bad Samaritan" law for failing to report the most severe forms of bullying "where the witness reasonably believes the victim will suffer physical harm."[29] This duty to report cyber bullying would undermine adolescents' reluctance to report such abuse by requiring adults to intervene. While such laws may be viable solutions to cyber bullying, many

[29] Heather Benzmiller, *The Cyber-Samaritans: Exploring Criminal Liability for the "Innocent" Bystanders of Cyberbullying*, 107 Northwestern University L. Rev. 3 (2013).

jurisdictions have chosen to apply preventative solutions rather than impose criminal sanctions.

In summary, several solutions have been implemented to address cyber bullying. Social media platforms have changed their standards to ban abusive content. Civil society has responded to cyber bullying by carrying out information campaigns to educate students and parents about the phenomenon. While a law explicitly outlawing cyber bullying has not been passed, its absence is accounted for by existing laws that serve the same function. Overall, a collaborative effort across public and private sector that focuses on education has been the main response to cyber bullying thus far.

1.6 Further Research

As mentioned above, further research is needed in the following areas:

(1) To resolve the discrepancy between the OII study suggesting that cyber bullying is not as prominent as face-to-face bullying, and the Ditch the Label study suggesting the opposite.

(2) To determine whether the social media platform used impacts the frequency of cyber bullying among adolescents and children.[30] While the Ditch the Label report notes differences among platforms, the exact reasons why certain platforms are more prone to cyber bullying remains understudied.

(3) Finally, most research on cyber bullying deals with its effects on children and adolescents. While they are the most vulnerable population, the literature should also address how cyber bullying affects adults and the elderly. This includes examining cyber bullying in the workplace, online sexual harassment, and other manifestations of cyber bullying towards adults. Other sections in this report will address some of these forms of cyber bullying.

1.7 Major Organisations

This section briefly organisations working on cyber bullying issues. This list was compiled by comparing UK and international organisations whose mission statement focuses on combatting and researching online or offline bullying. The organisations here were listed because they have conducted (1) recent or numerous campaigns to reduce cyber bullying (2) produced prolific or comprehensive research reports, or (3) are cited by the media as a

[30] Jane Wakefield, *Instagram Tops Cyber bullying Study*, BBC News (2017) available at https://www.bbc.com/news/technology-40643904 (explaining the role of Instagram in cyber bullying).

participant in the dialogue surrounding cyber bullying. The following organisations are listed in no particular order:

(1) Cybersmile.com: (registered charity in the US and UK): is a charity that conducts research, carries out campaigns against cyber bullying, and produces online educational resources to combat cyber bullying. They are funded by corporate partners such as Twitter, Intel, and Pixelberry Studios. They have won multiple awards for their work on digital abuse and they hold campaigns regularly.

(2) Ditch the Label: (Based in the UK): one of the largest anti-bullying "digital" charities in the world, empowering young people aged 12-25 to overcome bullying. They provide support online for victims and spearhead research related to bullying, earning them several awards for their work supporting young people. Funding partners include the StandUp Foundation, Lynx, The Rumi Foundation, Tudor Trust, The Lottery Fund, and the ClothesWorkers Foundation.

(3) The Northern Ireland Anti-Bullying Forum (NIABF) brings together a range of statutory and voluntary sector organisations from across Northern Ireland, all acting together to end the bullying of children and young people in schools and in communities. NIABF was formed by Save the Children.

(4) Anti-Bullying Campaign, Diana Award (UK Organisation): The Diana's Award Anti-Bullying campaign involves a host of projects aimed at reducing bullying in schools. One of their main projects is the anti-bullying ambassadors programme which has trained over 22,000 young people in the UK in leading anti-bullying campaigns. They also produce training materials and online tools for child safety online. It is run by charity The Diana Award, a registered charity in the name of Princess Diana.

(5) Cyberbullying Research Centre (US Organisation): dedicated to providing research and information on the causes and consequences of cyber bullying. It is directed by two US professors, who launched the site in 2005. They founded the centre as a means to host research on cyber bullying.

(6) All Rise: organisation dedicated to combatting cyber abuse. They are a not-for profit organisation aiming to respond to cyber bullying, trolling, stalking, and other forms of abuse. They also work in partnership with law makers and politicians to ensure cyber abuse is clearly defined and illegal.

(7) Bullies Out (UK Organisation): charity founded in 2006, dedicated to making a "positive difference to the lives of thousands of children and young people affected by bullying." Their research also includes material on cyber bullying. They are funded by several organisations that focus on child welfare or fund philanthropic causes: Children in Need, Comic Relief, The National Lottery Community Fund, and The Moondance Foundation. They've received a number of prestigious awards, including the Cardiff Life Award in 2017.

(8) Anti-Bullying Alliance (UK coalition of organisations): hosts coordinated anti-bullying campaigns. It was established by the National Children's Bureau and the National Society for the Prevention of Cruelty to Children. While they mainly focus on offline bullying, they do also provide some information and training tools on cyberbullying. They're funded by a number of private donations as well as business partners such as Firehorse Productions, Impero Software, and Restorative Thinking Limited.

(9) End to Cyber Bullying (US Organisation): is a non profit aimed and combatting cyber bullying by raising awareness, conducting research, and mobilising affected communities to create safe online environments. They are funded and supported by local public schools, the Girl Scouts of USA organisation, and a number of local New York NGOs.

(10) STOMP Out Bullying (US Organisation): is a US nonprofit that focuses on reducing and preventing bullying, cyberbullying, sexting, and other digital abuse. They also conduct campaigns educating against homophobia, racial hatred and deterring violence in communities. They are primarily funded by large corporate donors such as Disney, ABC Family, Hollister and MTV.

(11) respectme (Scottish organisation): is Scotland's anti-bullying service, launched in 2007. It is fully funded by the Scottish government and managed by the Scottish Association for Mental Health, in partnership with LGBT Youth Scotland. They produce training materials and disseminate information on offline bullying and online safety.

(12) Parents Protect (UK organisation): is a project of The Lucy Faithfull Foundation. It is an information hub for parents dealing with cyber bullying, sexting, and Internet safety. They also host a helpline for victims of online abuse and child sexual abuse online. Parents Protect, and its associated Stop it Now! Campaign against child sexual abuse is funded by the Public Protection and Mental Health Group National Offender Management Service of the Ministry of Justice. The campaigns have also received funding from the Scottish and Welsh governments, as well as charitable trusts. There is no current government funding for England.

(13) Megan Meier Foundation (US Organisation): a global cyberbullying prevention foundation. To this end, they offer counselling services and leadership workshops dealing with cyber bullying. They are organised as a non-profit and are mainly funded by private donations and fundraising. They publish annual financial reports, though they have not updated them since 2014.

(14) National Bullying Helpline (UK organisation): is a privately run dispute resolution organisation, dedicated to serving those who are victims of cyber-bullying, stalking, discrimination, abuse of power, or harassment. They are funded by donations and volunteer-based work. Their website states that they have been recognised and endorsed by the UK Employment Law Solicitors, David Cameron, and the Women's OWN network. The National Bullying Helpline is notable for its unique conflict-resolution model of combatting cyber bullying.

(15) Kidscape (UK Organisation): is a registered charity focused on providing children, families, carers and professionals with advice to prevent bullying. They're funded by local fundraising efforts and corporate partners, including Specsavers.

(16) Safety Net (UK Organisation): works primarily in Brighton and across the South East, providing training on bullying prevention and online safety. They are funded by local fundraising efforts and are currently seeking corporate partnerships and donations.

2. Nonconsensual Pornography ("Revenge Porn")

2.1 Definition

Revenge porn, sometimes referred to as "nonconsensual pornography (NCP), is a growing form of digital sexual violence defined as "the distribution of sexually graphic images of individuals without their consent."[31] While it is frequently referred to as "revenge porn," its motivations are varied and may sometimes intend to harm or embarrass instead. Crucially, not all NCP is successfully distributed and sometimes the mere threat of distributing intimate pictures may suffice to harm the victim.

2.2 Vulnerable Populations & Impact

According to the UK Director of Public Prosecutions, there is a "growing number of offenses occurring through social media" of NCP or revenge pornography. Studies show that young women are disproportionately victimised by NCP. In 2015, of 139 cases reported in the United Kingdom between January and April, 80 percent involved images of women. In the United States, a 2017 study by the Cyber Civil Rights Initiative, 9.2% of surveyed women reported being victims of nonconsensual pornography compared to 6.6% of male respondents. The same survey concluded that women were 1.7 times as likely to have been victims of NCP or have been threatened with NCP compared to men. This illustrates that while some sites do feature images and videos of men, young women are the primary population affected by NCP.

The impact of NCP differs across ages and is reportedly highest among participants between the ages of 34 and 41. The 26-33 age-group had the largest rate of being victimised *or threatened* with NCP.[32]

The distribution of nonconsensual pornography has a number of harmful effects on victims. Those who reported having their intimate images shared without their consent had significantly worse mental health outcomes and higher levels of physiological problems than non-victims, according to the CCRI 2017 Report. Even the mere threat of sharing NCP has been shown to result in mental health burdens. A 2017 study from RMIT University in Australia found that 80% of victims who had experienced threats to distribute an image reported high levels of distress "consistent with a diagnosis of moderate to severe depression

---

[31] Asia A. Eaton, Holy Jacobs, & Yanet Ruvalcaba, *Nationwide Online Study of Nonconsensual Porn Victimization and Perpetration*, Cyber Civil Rights Initiative (2017) available at https://www.cybercivilrights.org/wp-content/uploads/2017/06/CCRI-2017-Research-Report.pdf

[32] *Id.*

or anxiety disorder." The psychological effects of NCP are severe, often culminating in PTSD, suicidal thoughts, anxiety, and depression.[33]

Beyond the psychological harm, victims are also often threatened, stalked, harassed, fired by employers, or forced to change schools.[34] Since employers often rely on Internet representations of individuals while hiring, the presence of intimate photos online may make it difficult for victims to find work at all. NCP also plays a role in intimate partner violence, with abusers "using the threat of disclosure as a means of controlling their partners."[35] One issue particular to NCP is that individuals can be repeatedly victimised. Every time someone types a victim's name into a search engine or discovers the intimate picture, the victim's privacy is newly invaded. The trauma and embarrassment of the experience can make them reluctant to report the abuse. Rebecca Hitchin of the Rape Crisis charity has stated that sexual offence victims are often reluctant to report abuse because of potential backlash from family and peers.[36] Stigma surrounding female sexual behaviour may also play a role in deterring victims from seeking help. Victim-blaming attitudes in response to the harms of NCP also impede appropriate societal solutions. Overall, the harm to victims of NCP, particularly young women, is psychological, physical, and professional.

2.3 Legal Background

As of April 2015, it is an offence in England and Wales to share private sexual photographs or films without the subject's consent. The maximum sentence for this crime is two years imprisonment.[37] According to the 2016 Violence Against Women and Girls (VAWG) report, there have been more than 200 prosecutions under this law since it came into force.[38] However, the number of reported incidents of NCP was nearly six times this figure in 2015.[39] Scotland passed its own revenge porn statute in 2017, making it an offense to "disclose or threaten to disclose, and intimate photograph or film" without the subject's consent.[40]

---

[33] Samantha Bates, *Revenge Porn and Mental Health: A Qualitative Analysis of the Mental Health Effects of Revenge Porn on Female Survivors*, Feminist Criminology (2016) available at https://journals.sagepub.com/doi/abs/10.1177/1557085116654565
(Abstract: full report is available to purchase)

[34] Mary Franks, *Drafting an effective "revenge porn" law: A guide for legislators*, University of Miami School of Law (2015). https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2468823

[35] *Id.*

[36] *Revenge Porn: More than 200 Prosecuted Under New Law*, BBC News, 6 Sep. 2016, https://www.bbc.com/news/uk-37278264

[37] *Revenge Porn: More than 200 Prosecuted Under New Law*, BBC News, 6 Sep. 2016, https://www.bbc.com/news/uk-37278264

[38] Crown Prosecution Service, Violence Against Women and Girls Crime Report (2016) available at https://www.cps.gov.uk/publications/docs/cps_vawg_report_2016.pdf

[39] *Revenge Porn: More than 200 Prosecuted Under New Law*, BBC News, 6 Sep. 2016, https://www.bbc.com/news/uk-37278264

[40] *New Revenge Porn Law Comes Into Force in Scotland*, BBC News 3 July 2017, https://www.bbc.com/news/uk-scotland-40473912

2.4 International Legal Approaches

(1) Australia: In May 2017, a study conducted by Monash University and RMIT University in Australia concluded that 20% of 4,300 respondents surveyed had images of a sexual nature taken without their consent.[41] There are laws in Victoria and South Australia criminalising the distribution of "intimate" or "invasive" images without the subject's consent. It is also a crime to threaten the distribution of these images. However, the aforementioned RMIT study notes that there are gaps in the laws of other Australian states and territories where no such criminal offenses are recognised. At the federal level, there is only a proposal for a civil penalties scheme to assist victims in reporting such abuse.[42] Where these gaps occur, cases of "image-based abuse" are treated under anti-discrimination laws.

(2) European Union: While there is no universal directive on revenge porn, the EU has recognised the issue and deferred to national governments on the appropriate solution. In November 2016, a written declaration was launched before the European Parliament on revenge pornography and cyber bullying. In 2015, a question was submitted for discussion at the European Parliament on what the EU proposes to do about the issue.[43] The official answer situated NCP (referred to as revenge porn) under the right to private life of Article 7 of the EU Charter. Further, the "right to be forgotten" or de-indexed from search results grants individuals in the EU the right to obtain removal of personal data from search engines. The European Parliament recognised that these rights may be implicated but deferred to national public authorities to determine the most efficient protection of victims.

(3) United States: While there is no applicable federal law, nearly 40 US states have laws against nonconsensual porn.[44] However, a 2015 research study from the Cyberbullying Research Center reports that these laws are lacking in uniformity.[45] For instance, some states require the victim to show that the perpetrator intended to cause emotional distress. This often poses evidentiary problems that make the prosecution of perpetrators difficult. The punishments also vary in each state. In California, the punishment for revenge porn can be as low as a $250 fee with 48

---

[41] Nicola Henry, Anastasia Powell, & Asher Flynn, *Not Just 'Revenge Pornography': Australians' Experiences of Image-Based Abuse*, RMIT University (2017).

[42] *Id.*

[43] Parliamentary Questions, European Parliament, E-010481/2015 available at https://www.europarl.europa.eu/sides/getAllAnswers.do?reference=E-2015-010481&language=EN

[44] *See generally* John A. Humbach, *The Constitution and Revenge Porn*, 35 Pace L. Rev. 215 (2014) available at: https://digitalcommons.pace.edu/plr/vol35/iss1/8

[45] *See* Cyberbullying Research Center, *State Sexting Laws*, (2015) available at https://cyberbullying.org/state-sexting-laws

hours of community service. [46] Despite the lack of federal law on revenge porn, the Digital Millennium Copyright Act (DCMA) is often used by victims to sue for copyright infringement when they find images of themselves online.

2.5 Proposed or Possible Solutions

According to the 2017 CCRI study, 96 of 159 surveyed perpetrators of NCP stated that they would have been stopped by the knowledge that conviction would require them to register as a sex offender. Similarly, 88 perpetrators responded that they would have been deterred by the knowledge that they could be imprisoned for sending intimate pictures. This suggests that a possible solution to this kind of cyber abuse is increasing education regarding the criminal penalties of revenge porn and NCP. While the intervention of the criminal law is one proposed solution, scholars like Nicola Henry and Anastasia Powell argue that equal attention should be paid to policies promulgated by civil society and technology companies.[47]

(1) Civil Society Solutions

According to attorney Rebecca Toman, "we need a hard hitting, informative and widespread campaign on the issue not only to educate the perpetrators of revenge porn about the consequences of their actions, but also warn potential victims about the risks involved and how these can be minimised."[48] An important role for NGOs and civil society is to educate the public about the dangers of blaming victims. Meaningful advances in combatting NCP have been impeded due to the stigma surrounding nude photographs and female sexuality. Holding victims responsible for the offenses of their abusers deters them from coming forward and bringing claims. As a result, education campaigns can help better prevent and respond to incidents of NCP.

(2) Technology Solutions

Internet companies such as Facebook, Twitter, and Google have taken a stance against revenge porn on their platforms by, for instance, working with local officials to outline best practices for the content's removal. Additionally, social media platforms have developed tools so that victims can report NCP directly to the company and ask for the images to be removed. Technological advances have also aided the response to NCP. Photo matching technologies have been

---

[46] *Id.*

[47] Nicola Henry & Anastasia Powell, *Sexual Violence in the Digital Age*, 25 Social and Legal Studies 4, 397-418 (2016). https://journals.sagepub.com/doi/abs/10.1177/0964663915624273
The authors have since published a book called *Sexual Violence in a Digital Age*.

[48] Rebecca Toman, *Revenge Porn: Educate to Help the Private Stay Private*, 26 Aug. 2015, https://www.huffingtonpost.co.uk/rebecca-toman-/revenge-porn_b_8038030.html
(Abstract: full report is available to purchase)

implemented to detect and prevent NCP from being disseminated on social media. Facebook has also committed to disabling accounts that perpetrate the distribution of this content. Google has allowed victims to request the content to be removed from search engine results.

(3) Legal Solutions

In the UK, one common critique of existing approaches to NCP is that it remains difficult to prosecute. This is also true in the United States, where a victim must show that the perpetrator "intended to cause distress." There are sometimes evidentiary issues with the successful prosecution of an NCP perpetrator. Changes to the way NCP cases are prosecuted have improved conviction rates in the UK. However, many jurisdictions have only passed regional rather than national legislation.[49] This means that the law on NCP remains inconsistent worldwide. Since the Internet is borderless, these inconsistent legal obligations across countries make it difficult for any one country alone to prosecute perpetrators of NCP.

2.6 Further Research

As mentioned above, further research is needed in the following areas:

(1) The effect of revenge porn on the LGBTQ+ community. Much of the existing research on NCP and revenge porn discusses its effect on women. However, it does not take an intersectional approach to the kinds of women that may be affected, including trans and queer women. Further research is needed to determine how the LGBTQ+ community and its minority members are being affected by NCP.

(2) The evidentiary issues with prosecuting NCP cases. Research explaining the shortcomings of NCP prosecutions could help law enforcement better understand the effectiveness of existing laws. If the laws make it nearly impossible for victims to seek justice, then NCP is not actually meaningfully criminalised.

[49] For a discussion on proposed legislation in the US, *see* Alex Jacobs, *Fighting Back Against Revenge Porn: A Legislative Solution* 12 Nw. J. L. & Soc. Pol'y. 69 (2016).

2.7 Major Organisations

This section lists some of the major organisations cited by the media as key players in the dialogue surrounding revenge pornography. This list was compiled by amassing organisations that produce research related to NCP or revenge porn. Organisations were included here regardless of whether they focus primarily on online spaces or whether they simply organise one-off campaigns related to this kind of content.

The following organisations are listed in no particular order:

(1) Cyber Civil Rights Initiative (Incorporated in the US): End Revenge Porn Campaign. The CCRI is a 501(c)(3) non-profit organisation providing support to victims of nonconsensual pornography. It is also an advocacy organisation, campaigning for technological, social and legal innovation to fight online abuse. Their accomplishments include the inception of a 24-hour Crisis Helpline, the provision of legal services to nonconsensual pornography victims, and having helped 22 US states pass nonconsensual pornography laws. They are organised and funded by Miami Law School. Other partners include Jewish Community Services of South Florida, Twitter, and the Miami-Dade Williams Fund.

(2) Without My Consent (US Organisation): non-profit organisation seeking to combat online abuse. They provide resources to empower individuals to legally defend their privacy, primarily after they were victims of nonconsensual pornography. Their funding and early work was supported by the Technology & Public Policy Clinic at UC Berkeley and Stanford's Center for Internet & Society.

(3) Stay Brave UK, (UK based charity): focused on supporting men, LGBT and non-binary people who have experienced domestic and sexual abuse. They have published some best practices for staying safe while sharing intimate photos with a partner. It is a volunteer-led organisation and its leadership works on campaigns in their spare time. They publish a yearly report on how donations are spent, and their expenditure in 2016 typically related to maintaining the charity's website and core services.

(4) HeartMob (online platform) dedicated to providing real-time support to individuals experiencing online harassment. It is unique in that it focuses on empowering bystanders to act against online abuse. NetRoots named it 2016's "best new product" and its HeartBot feature allows users to report abusive tweets in real time. The organisation is a project of Hollaback!, a nonprofit organisation funded by the Knight Foundation and Digital Trust Foundation. Sassafras Tech Collective, a worker-owned technology co-op, develops the platform and its updates.

(5) SPITE (Sharing and Publishing Images to Embarrass) (UK-based legal advice clinic associated with Queen Mary University) focusing on providing free legal

advice to anyone who has been a victim of revenge porn or subjected to the sharing and publication of images to embarrass by another individual. They have been recognised by the Attorney General's Pro Bono Awards, LawWorks and The Lawyer.

(6) Revenge Porn Helpline UK (UK organisation), is the only support service for victims of this crime. They have recently started a crowdfunding campaign to meet growing demand for their services. They also have a working relationship with the University of London Queen Mary's Legal Advice Centre.

(7) Stop Online Abuse (UK Government website), works to offer practical tips for people who find themselves victims of online abuse, including revenge porn. It is connected with Galop, a UK organisation working to stop online abuse of the LGBT community. The project is funded by the UK Government Equalities Office.

(8) Crash Override (US non-profit), using humane methods to combat online abuse by providing private assistance and policy research. They are a crisis helpline, advocacy group, and resource centre for victims of online abuse. The founders are Zoe Quinn and Alex Lifschitz, two victims of highly-publicised incidents of online abuse. It is primarily supported by Feminist Frequency, a non-profit organisation analysing media's relationship to gender, race, and sexuality.

3. Toxic Online Mental Health Communities: Pro-Ana And Pro-Suicide Websites

3.1 Definition

"Pro-Ana" is a term used to describe websites that promote the behaviours of anorexia nervosa. These websites often feature "thinspiration" photos of emaciated women alongside tips for weight loss. These websites, blogs, and social media accounts often glorify eating disorders and negatively impact the eating behaviour of people with and without these disorders. More generally, websites promoting eating disorders of all sorts are referred to as "Pro-ED."

"Pro Suicide" websites encourage suicide or describe methods of ending one's life. These sites or forums may sometimes facilitate suicide pacts or describe suicidal plans in detail. While toxic online communities encourage different kinds of self-harm, they pose similar societal challenges. Thus, this section will address both Pro-Ana and Pro-Suicide websites, explaining where users are impacted differently.

3.2 Vulnerable Populations & Impact

(1) Pro-Ana and Pro-ED Websites:

Pro-Ana and Pro-ED websites are mainly frequented by women and adolescents. According to a 2010 study published in the American Journal of Public Health, adolescents exposed to such online communities showed higher levels of body dissatisfaction compared to adolescents that have not been exposed.[50] Use of these websites has been positively correlated with the development of eating disorders, and negatively correlated with quality of life among adults. This study concluded that pro-eating disorder websites present graphic material in order to "encourage, support, and motivate site users to continue their efforts with anorexia and bulimia."[51]

The concern surrounding Pro-ED websites stems from the social cognitive theory that vulnerable users will adopt the behaviours conveyed online. In particular, these online communities often feature images of successful models, celebrities, and real people with life-threateningly low body weights. This allows website visitors to perceive extreme dieting as normal rather than symptomatic. Indeed, the ethos of many Pro-ED websites centres around the notion of eating disorders as a "lifestyle

---

[50] *See* Johns Hopkins Bloomberg School of Public Health, *Study Examines Pro-Anorexia and Pro-Bulimia Websites*, June 17, 2010, available at: https://www.jhsph.edu/news/news-releases/2010/borzekowski-e-ana-websites.html

[51] Dina L.G. Borzekowski et al, *e-Ana and e-Mia: A content Analysis of Pro-Eating Disorder Web Sites*, Am. J. Public Health (2010). https://www.ncbi.nlm.nih.gov/pmc/articles/PMC2901299

choice" rather than a disease. Very few Pro-ED websites encourage users to seek help for eating disorders. The aforementioned study revealed that only thirty eight percent of sites included recovery-oriented information or links. This makes young adolescents and users with other forms of mental illness particularly vulnerable to misinformation promulgated by these websites.

(2) Pro-Suicide Websites:

Individuals with existing cases of mental illness or substance abuse are particularly vulnerable to the harmful effects of pro-suicide online spaces. Some preliminary data was also collected in 2008 regarding the gender-based risk. Clarke and van Amerom examined blogs created by depressed people and concluded that depressed men were more likely than depressed women to discuss suicide or self-harm on blogs.[52] However, further research is needed to determine how gender interacts with susceptibility to self-harm websites.

More generally, media portrayal of suicide is known to influence suicidal behaviour, particularly the choice of method used.[53] Suicide itself is a considerable public health problem, leading to more than 1 million deaths worldwide every year. Several studies concluded that social media's influence on suicide should be viewed as a public health issue.[54]

3.3 Legal Background

There are gaps in UK law regarding pro-suicide and pro-ED websites. Under the 1961 Suicide Act, it is illegal to promote suicide, but no website operator has ever been prosecuted under this law.[55] Since many internet companies are based overseas, there are inherent difficulties to policing internet content. Questions of legal jurisdiction over internet speech remain unanswered, and the global nature of the internet poses challenges for the regulation of self-harm sites. As of 2017, Pro-Ana and Pro-Suicide websites are not explicitly illegal in the UK.

---

[52] Clarke J, van Amerom G., *A Comparison of Blogs by Depressed Men and Women*, Issues Ment. Health Nurs. (2008). https://www.tandfonline.com/doi/full/10.1080/01612840701869403 (Abstract: full report is available to purchase)

[53] Lucy Biddle et al, *Suicide and the Internet*, Public Health (2007). https://www.ncbi.nlm.nih.gov/pmc/articles/PMC2292278

[54] *Id.*

[55] Raphael Cohen-Almagor, *Confronting the Internet's Dark Side: Moral and Social Responsibility on the Free Highway*, Cambridge University Press (2015).

3.4 International Legal Approaches

(1) Australia: In 2006, Australia became the first country to criminalise pro-suicide web pages. While the law is difficult to enforce for reasons discussed in this sub-chapter, proponents argued that it sent a strong message that Australians were against the promotion of suicide. Concerns were expressed that the law cast a criminal net too widely and inappropriately interfered with "the autonomy of those who wished to die."[56] Overall, Australia's law served as an expression of societal norms against the promotion of suicidal behaviour. Pro-Ana websites, by contrast, were not regulated in Australia. There are general criminal offenses related to inducing bodily harm which include causing a disorder. However, the publication of pro-Ana or pro-ED material has not been criminalised.[57]

(2) European Union: While there is no EU directive on pro-suicide or pro-Ana websites, some members of the European Union have taken independent action. France has been a leader in passing laws related to body image, in particular. In 2015, France modified in public health code to outlaw material that causes a person to "seek excessive leanness by encouraging prolonged food restrictions which result in exposing the person to life-threatening danger or in directly compromising their health." In France, this crime is punishable by one year in prison. Italy has passed a similar law.

(3) United States: While many state laws in the US criminalise knowingly assisting in a suicide, the legal implications of using the Internet to encourage suicide remain murky. The United States has a legal scheme that strongly protects Internet freedom and free speech. As a result, it is very difficult to pass laws criminalising forms of Internet speech, even when they are as damaging as websites promoting self-harm.

3.5 Proposed or Possible Solutions

There is some controversy over the proposed solutions to the challenges posed by websites that promote self-harm. Some stakeholders argue that these online spaces should be banned or blocked, while others suggest that this would only worsen the problem. For instance, Emily Reynolds argues in a 2016 *Wired* article that banning pro-anorexia websites on Instagram actually worsened the problem. Gemma Cobb similarly argues that censorship by Internet moderators and vilification by the mainstream media has led Pro-Ana online spaces

---

[56] Prinkis J. et al., *Legal Bans on Pro-Suicide Web Sites: An Early Retrospective from Australia,* Suicide Life Threat. Behav. (2009). https://guilfordjournals.com/doi/pdf/10.1521/suli.2009.39.2.190 (Abstract: full report is available to subscribers)

[57] *Should 'pro-ana' websites be criminalized in Australia?* The Conversation, June 22, 2017, https://theconversation.com/should-pro-ana-websites-be-criminalised-in-australia-79197

to deploy "creative devices in order to remain online." In particular, these websites use obscure hashtags such as "#thynspo" to signal "thinspiration" and include disingenuous disclaimers about the nature of the website. Cobb's analysis of these websites concluded that the denial and disguise of Pro-Ana websites has led to a normalisation of the phenomenon.[58] In general, the appropriate approach to websites advocating self-harm remains controversial. Some possible solutions are discussed below:

(1) Civil Society Solutions

The study of websites displaying methods of physical self-harm and suicide has become an important aspect of suicide research. The findings of these studies suggest a need to "organise more specific online support for the victims of violence and online aggression." This is because experiences of victimisation are associated with individuals entering pro-self harm websites.[59] In other words, individuals who have been victimised or otherwise abused are more likely to enter pro-suicide websites. As a result, creating more specific online support spaces is one solution civil society might provide in response to the proliferation of pro-suicide websites. Currently, resources for individuals vulnerable to the suggestions of pro-suicide or pro-ED websites remain limited.

(2) Technology Solutions

One solution, proposed by NGOs like Papyrus, is to require Internet Service Providers to block and filter self-harm sites. Just as certain pornographic and gambling sites are filtered, NGOs focusing on suicide prevention have advocated for similar types of filtering for pro-suicide and self-harm websites. Social media companies have also partnered with NGOs to provide mental health support for individuals suffering from suicidal ideation or eating disorders. These partnerships between technology companies and civil society can be effective solutions to the challenges posed by these online spaces.

---

[58] Gemma Cobb, *This is* not *pro-ana*: *Denial and Disguise in Pro-Anorexia Online Spaces*, 6 Fat Studies 2 (2017). https://www.tandfonline.com/doi/abs/10.1080/21604851.2017.1244801 (Abstract: full report is available to purchase).

[59] Minkkinen J et al., *Victimization and Exposure to Pro-Self-Harm and Pro-Suicide Websites: A Cross-National Study*, Suicide Life Threat Behav. (2017). https://onlinelibrary.wiley.com/doi/abs/10.1111/sltb.12258 (Abstract: full report is available to purchase and to subscribers).

(3) Legal Solutions

A proposed legal solution is a blanket ban on pro-suicide and pro-ED websites. There are several impediments, varying by jurisdiction, that have prevented this legal approach from coming to fruition. A blanket ban is a challenge to enforce, as many suicide related websites are "hosted abroad and remain legal in other countries."[60] While some statutes already exist to prosecute individuals who maliciously encourage suicide online, it remains difficult to categorise "pro-suicide" websites. For example, sites that publish information on suicide methods or host chat forums may not necessarily qualify as pro-suicide for legal purposes. Additionally, some of the discussion on these forums may be protected under free speech laws in certain countries. As a result, a blanket ban on self-harm websites poses complex issues for enforcement.

3.6 Further Research

As mentioned above, further research is needed in the following areas:

(1) How mental health organisations can reach suicidal individuals. While these online spaces create new risks and challenges for suicide prevention, they also present new opportunities for reaching vulnerable people who may need help. Since users concentrate in these online communities, suicide prevention communities can target their efforts more effectively. However, further research is needed on best practices for this kind of targeted outreach.

(2) Gender-based risk and analysis on which populations are most vulnerable to suicide inspiration websites. While some preliminary statistics exist and were discussed in section 3.2 above in this chapter, suicide research is difficult to conduct for a variety of reasons. The variability of social media format, use patterns, and other influences on suicidal behaviour "make it very difficult to test social media as a variable that predicts suicidal behaviour." As a result, qualitative studies may be helpful in further research towards preventing suicide and addressing pro-suicide websites.

(3) How and why suicidal individuals seek solace in online communities. In particular, future studies could help examine why individuals end up in pro-suicide spaces and how positive alternatives can be made more appealing. More precise qualitative studies on how suicidal people use the Internet could be helpful in prevention of future self-harm.

---

[60] Catherine Johnstone, *How and Why do the Suicidal Go Online?* The Guardian, March 25, 2011 https://www.theguardian.com/commentisfree/2011/mar/25/suicidal-online-research-internet-suicide

3.7 Major Organisations

This section briefly describes some of the major organisations cited by the media in reference to Pro-ED and Pro-Suicide websites. This list was compiled by amassing organisations that participate actively in the policy dialogue around this kind of content. Organisations were included here regardless of whether they focus primarily on online spaces or whether they simply organise one-off campaigns related to this kind of content. The following organisations are listed in no particular order:

(1) Beat Eating Disorders, (England & Wales charity) an NGO dedicated to combatting eating disorders. They research and write about the influence social media has on eating disorders, and work with local ISPs to have eating disorder-encouraging websites taken down. They were partially funded by the Amy Winehouse Foundation, and have many other funders and corporate partners such as the BBC's Children in Need Programme, the Big Lottery Research Fund, and the Burdett Trust for Nursing.

(2) PAPYRUS (UK-based organisation) is a charity dedicated to the prevention of young suicide. They have previously held Internet safety campaigns dedicated to removing suicide and self-harm websites. Their funding partners include BBC Children in Need, Schuh, and the Big Lottery Research Fund. In 2016 they won the JUMP Web Design Award.

(3) Samaritans (US-based organisation operating worldwide) is a charity dedicated to suicide prevention. They have been cited as a key voice in the understanding of pro-suicide websites. In particular, they argue against a blanket ban on suicide websites, advocating further study on research into how vulnerable users behave online. Their major donors include large corporations such as the American Red Cross, The New York Community Trust and the Bank of New York.

(4) Butterfly Foundation (Australian organisation) represents individuals affected by eating disorders and negative body image, as well as their family and friends. They are cited by websites discussing pro-Ana websites as an organisation particularly equipped to provide mental health support. Their corporate partners include Dove soap's Self Esteem Project, Sportsgirl, and Future Generation Global Investment Company. They also coordinate with the Australian Department of Health and Aging and the National Eating Disorders Collaboration in Australia.

4. Fraud and Discrimination in Online Dating Platforms

4.1 Definitions

Online dating is the practice of searching for a romantic or sexual partner on the Internet, typically through a facilitating website or application. The landscape of dating applications and websites varies greatly, enabling users to target potential partners by shared religion, geographic location, or sexual orientation.

4.2 Vulnerable Populations & Impact

Dating platforms have meaningfully changed a key aspect of modern social life.[61] However, the platforms are not impervious to many of the same problems that occur in offline dating. While these platforms play an important role in facilitating social interaction, some services can be misused to cause harms like stalking, catfishing, and harassment.

Several core issues face the online dating community. Fraud and privacy issues are implicated since dating platforms manage copious amounts of personal information. Global Personals ("GP"), once one of the largest UK Internet dating companies, notably used stolen photos and fake profiles to induce daters into paying for a GP membership.[62] Additionally, users' profiles were made available to members of different sites on a shared database, often without their informed consent. The UK Information Commissioner's Office investigated this profile-sharing practice. The information commissioner stated in 2012 that, "on the face of it, it's a breach of first data protection principle. It's not fair processing. You've signed up for one thing and you suddenly get approached by people from a different site."[63] This illustrates the larger problem that online dating platforms may not always manage private information properly.

Users may also be at risk of being defrauded by the dating company. In 2015, Ashley Madison, a website facilitating extramarital affairs, used over 70,000 "fembots" (artificial intelligence programmes simulating real women) to encourage male subscribers.[64] These bots spoke many different languages and chatted with users in various countries. The inquiry into Ashley Madison's outreach practices began when journalists grew suspicious about

---

[61] For a general overview of the UK Online dating industry, *see Dating on the Move: Opportunities and Challenges for the Online Dating Industry*, Online Dating Association (2015). https://www.onlinedatingassociation.org.uk/news/online-dating-on-the-move-a-call-for-high.html

[62] Geoff White, *Fools for Love: How an Internet Dating Firm Duped Clients*, Nov. 1, 2012, available at https://www.channel4.com/news/fools-for-love-how-one-internet-dating-firm-dupes-clients

[63] *Id.*

[64] Annalee Newitz, *Ashley Madison Code Shows More Women, and More Bots*, Gizmodo, Aug. 31, 2015, available at https://gizmodo.com/ashley-madison-code-shows-more-women-and-more-bots-1727613924

seemingly exaggerated numbers of female users.[65] In 2016, US Federal Trade Commission ultimately investigated Ashley Madison and it removed the bots. The practices were revealed because of a massive data breach that exposed the personal data of all Ashley Madison subscribers. Thus, online dating websites bear a large amount of responsibility for the amount of private information they host. This is exacerbated when dating platforms possess intimate information, such as an individual's search for extramarital affairs.

Violations of a user's privacy can occur through data breaches or on a more individualised basis, through blackmail threats.[66] Ashley Madison's data breach allowed blackmailers to threaten users with telling their wives or families. In one case, this resulted in the suicide of a New Orleans pastor, whose name was included in the leaked data.[67] While such incidents of blackmail or data breach may not be a daily occurrence on platforms, their consequences can be severe.

Another cyber abuse problem facing online dating sites is that of stalking and harassment. Stalking can consist of any type of behaviour including unwanted communication, physical or sexual assault, or invasions of privacy. According to a report by Dr. Lorraine Sheridan and Network for Surviving Stalking, anyone can be a victim of stalking. Of the 2,292 victims surveyed, the ages ranged from 10 to 73 and included both men and women.[68] Stalking can also sometimes be perpetrated by an ex-partner of the victim. The open channels of communication that online dating platforms provide can sometimes create the conditions for stalking.

This section will first review online harassment and dating fraud schemes such as "catfishing" and romance scams. It will then discuss harms arising from discrimination, whether intentional or unintentional, and how they impact specific groups in society. Despite their value, the design of some online dating platforms can result in discrimination against particular demographics. In particular, racial minorities, women and members of the LGBTQA+ community are most vulnerable to discrimination or abuse on dating platforms.

---

65 *Id.*

66 Mike McPhate, *Ashley Mdaison Faces FTC Inquiry Amid Rebranding*, NYTimes, July 5, 2016, available at https://www.nytimes.com/2016/07/06/business/ashley-madison-ftc-rebranding.html (Subscription or purchase)

67 *Id.*

68 *See* Suzy Lamplugh Trust, *What is stalking?* (2017) https://www.suzylamplugh.org/what-is-stalking

(1) Women and Harassment on Dating Platforms

According to a 2016 opt-in research study by Consumers' Research, 57% of women and 21% of men report experiences of harassment in online dating platforms.[69] While men also experience online sexual harassment, women are generally the primary target. A 2014 Pew Research study on online harassment concluded that young women aged 18-24 experience severe types of harassment at disproportionately high levels. This kind of harassment includes behaviours like stalking as well as receiving unsolicited sexual advances online.[70]

The harassment women experience may also vary depending on the platform. A Consumers' Research survey found that Tinder and OkCupid top the list of platforms where women experience the most harassment.[71] Users reported much lower incidents of harassment on sites like Match.com or eHarmony. This could be explained by the fact that these sites require payment and more in-depth profiles, attracting more serious daters.

(2) Anonymity, "Catfishing," and Romance Scams on Dating Platforms:

The virtual nature of online dating means that users can be victims of fraud or identity theft. Dating platforms vary in their authenticity verifications, meaning that there is a fair amount of anonymity in online dating. A user cannot always know for sure that the person they are speaking to online is who they claim to be. As a result, several forms of relationship abuse and online deception can arise.[72]

"Catfishing," for example, refers to the phenomenon of luring a person into a relationship by means of a fictional online persona. Sometimes the deception involves financial as well as emotional exploitation. The group most vulnerable to catfishing is women over 50. The elderly, divorced, and widowed were more likely

---

69 Daisha Riley, *Women Using Dating Apps Fight Back Against Sexual Harassment*, ABC News, Nov. 30, 2016, available at https://abcnews.go.com/Lifestyle/women-dating-apps-fight-back-sexual-harassment/story?id=43832851

70 Maeve Duggan, *Part 1: Experiencing Online Harassment*, Pew Research Center, Oct 22, 2014, available at https://www.pewinternet.org/2014/10/22/part-1-experiencing-online-harassment

71 Kyle Burgess, *Consumer Survey: The Best Way to "Swipe" a Mate*, Consumers' Research, Mar. 17, 2016, available at https://consumersresearch.org/consumer-survey-the-best-way-to-swipe-a-mate

72 *See generally*, Caspi A, & Gorsky P, *Online deception: prevalence, motivation, and emotion*, Cyberpsychology & behaviour: the impact of the Internet, multimedia and virtual reality on behaviour and society, *9* (1), 54-9 (2006). https://www.liebertpub.com/doi/abs/10.1089/cpb.2006.9.54 (Abstract: full report is available by purchase or subscription).

to "be victims of romance scams, which prey upon loneliness and isolation to 'hook' the vulnerable."[73]

The 2010 documentary *Catfish* presents the most well-known and in-depth exposition of this phenomenon. In this film, Nev Shulman finally meets a woman with whom he has had a long-term online relationship.[74] Upon meeting her, he discovers that she was not in her 20s and single, but in her 40s and married. The illusory relationships of "catfishes" typically extend over a long period of time, which results in significant emotional trauma to the victim of deception.

In some cases, the perpetrator of a catfishing scheme hides behind anonymity in a long-term romantic relationship due to low self-esteem, mental health issues, or insecurity about their sexual orientation or gender identity. However, other perpetrators of catfishing have more nefarious motives, such as gaining access to the victim's bank accounts and credit cards.[75] Some victims are even conned by their perceived romantic partners into sending large amounts of money. According to a 2016 paper analysing dating romance scams, victims of this kind of fraud experience an emotional 'double-hit:' a financial loss and the loss of a relationship.[76]

A third victim of a catfishing scheme is the party that unknowingly lent their identity to a catfisher, who then used it to enter into the romantic relationship. Catfishers often take pictures, names, and personal information from other dating profiles to create fabricated accounts that they use to engage with the romantic partner they are deceiving. [77] Overall, catfishing often implicates a variety of kinds of cyber abuse: identity theft, fraud and cyber bullying.

---

[73] Majid Yar, "Online Crime," Oxford Research Encyclopedia of Criminology (2016), available at https://www.researchgate.net/profile/Majid_Yar/publication/317092621_Online_Crime/links/5925652a0f7e9b997975fa21/Online-Crime.pdf

[74] Aisha Harris, *Who Coined the Term 'Catfish'?*, Slate, Jan. 18, 2013, https://www.slate.com/blogs/browbeat/2013/01/18/catfish_meaning_and_definition_term_for_online_hoaxes_has_a_surprisingly.html

[75] Tim Delaney & Tim Madigan, *Friendship and Happiness: And the Connection Between the Two,* McFarland (2017).

[76] Monica Whitty & Tom Buchanan, *The Online Dating Romance Scam: The Psychological Impact on Victims – Both Financial and Non-Financial*, 16 Criminology and Criminal Justice 2 (2016). https://wrap.warwick.ac.uk/81382

[77] Brent Holmes, *How Rejected Men Use Dating Apps to Torment Women*, VICE, May 25, 2017, available at https://www.vice.com/en_us/article/8x4jbg/when-harassers-use-tinder-and-bumble-to-dox-and-women

(3) Discrimination and Online Dating Platforms

Race and Online Dating

People of colour experience dating sites differently than other demographics. In his book, *Dataclysm*, OKCupid founder Christian Rudder explains that dating site users tend to be biased against black people and Asian men in particular.[78] More generally, Rudder's data shows that racial preferences play a large role in the choices of online daters. When OKCupid members looked at photos and profiles of potential dates and rated their attractiveness from one to five, "people of both genders routinely preferred potential dates of their own race or ethnicity."[79] This kind of racial preference intensified between 2009 and 2014, placing "black women at the bottom of the dating pool."[80] A study conducted by James Henry Johnson analyses the experiences of black women who use Internet dating sites. One conclusion was that black women mostly preferred to date black or African-American men, yet had difficulty finding sites with "viable" black male dating candidates. Free and niche dating platforms were perceived to have black men of "lower class and quality."[81] This highlights a tension in the niche dating industry: dating platforms must at once be non-discriminatory and yet cater to the often discriminatory romantic preferences of users. These studies also suggest that people of colour experience online dating differently, often negatively, compared to other demographics.

Heteronormative Dating Platforms and the LGBTQA+ Community

The default cisgender heteronormativity of many dating platforms leads to the marginalisation of LGBTQA+ users. According to queer journalist Taylor Hatmaker, "there often isn't a category for genderqueer individuals." The lack of appropriate filtering mechanisms in online dating platforms is also problematic within specific subgroups of the LGBTQA+ community. For instance, subcategory terms such as "butch" and "femme" are often used by gay women to navigate the dating world, by denoting aspects of their aesthetic appearance. These and other labels are typically absent in online dating platforms such as Tinder.

---

78 Christian Rudder, *Dataclysm*, Crown/Archetype (2014).

79 Natasha Singer, *OKCupid's Unblishing Analyst of Attraction*, NY Times, Sep. 6, 2014, available at https://www.nytimes.com/2014/09/07/technology/okcupids-unblushing-analyst-of-attraction.html (Subscribers only)

80 James Henry Johnson, *Dating_Misrepresentation.Com: Black Women's Lived Love-Hate Relationship with Online Dating*, Southern Illinois University Carbondale (2017). https://opensiuc.lib.siu.edu/dissertations/1363

81 *Id.*

Moreover, the inherent design of many dating platforms is based on heteronormative and cisgender standards of attraction.[82] Robyn Exton, CEO of a queer women's dating application called "Her," critiques the visually-based format of dating applications that focus on swiping photos.[83] According to Exton, this is designed based on male sexual behaviour, relying on the theory that men respond more readily to visual sexual stimuli. "Her" thus focuses on women connecting with women over mutual interests posted through its Pinterest-like interface. While designing dating profiles based on perceived gender behaviour may be problematic, the presence of platforms like "Her" suggests that there is a market for this type of design. It also suggests that "mainstream" dating platforms neglect the needs of LGBTQA+ groups.

There are several ways in which dating platforms marginalise sexual minorities.[84] One other example, explained in a 2017 article by Stefanie Duguay, involves Tinder's authenticity verification mechanism.[85] In order to use Tinder, an individual's profile must be liked to Facebook, which requires users to provide a "real name." A real name, in this case, is one that corresponds to a legal document such as a driver's license. Transgender people frequently use names different to ones on their legal documents, which often reflect the gender they were assigned at birth. As a result, they are unable to use Facebook or pass Tinder's "authenticity verification" mechanism. This illustrates that the affordances of dating platforms sometimes marginalise minority communities.

---

[82] Kelsey C. Chappetta & Joan M. Barth, *How Gender Role Stereotypes Affect Attraction in an Online Dating Scenario*, 63 Computers in Human Behavior (2016). https://dl.acm.org/doi/10.1016/j.chb.2016.06.006

[83] Natasha Noman, *There May Never Be a Good Dating App for Lesbians – Here's Why*, Mic.com, July 23, 2013, available at https://mic.com/articles/122737/lesbian-dating-apps

[84] For discussions on queer communities and dating platforms, *see*
Lik Sam Chan, *Ambivalence in Networked Intimacy: Observations from Gay Men Using Mobile Dating Apps*, New Media and Society (2017)
Gill Valentine, *Globalizing Intimacy: The Role of Information and Communication Technologies in Maintaining and Creating Relationships*, 34 Women's Studies Quarterly ½ (2006) https://www.jstor.org/stable/pdf/40004765.pdf
Blake Hawkins & Ryan J. Watson, *LGBT Cyberspaces: A Need for a Holistic Investigation*,15 Children's Geographies 1 (2016) https://www.tandfonline.com/doi/full/10.1080/14733285.2016.1216877 (Abstract: full report is available to subscribers)
Matthew H. Rafalow et al., *Racialized Femininity and Masculinity in the Preferences of Online Same-sex Daters*, 4 Social Currents 4 (2017) https://journals.sagepub.com/doi/abs/10.1177/2329496516686621 (Abstract: full report is available to subscribers)

[85] Stefanie Duguay, *Dressing up Tinderella: interrogating authenticity claims on the mobile dating app Tinder*, Information, Communication & Society, 20:3, 351-367 (2017) https://www.tandfonline.com/doi/abs/10.1080/1369118X.2016.1168471 (Abstract: full report is available by purchase or subscription).

4.3 Legal Background

The law applicable to online dating depends on the specifics of each case. Catfishing or using a fake profile to trick victims into sexual contact is not illegal in the UK.[86] However, MP's have responded to public calls for a law against this kind of deceit. The emotional components of catfishing do not alone amount to a criminal offence. However, if a catfisher asks for money from a victim, they commit an offense under the Fraud Act.

If financial exploitation is involved, online dating scams and fraud are dealt with by the National Fraud Intelligence Bureau in the UK. Action Fraud, the UK's cyber-crime reporting centre, receives over 350 reports of online dating scams every month. According to Steve Profitt, deputy head of Action Fraud, each victim loses £10,000 on average.[87] One problem with the enforcement of these fraud laws is that many online dating catfishers and fraudsters live outside of the UK. This makes it difficult for British law enforcement to obtain jurisdiction over them to take action.

4.4 International Legal Approaches

(1) Australia: Like the UK, Australia has a regulatory body charged with handling online scams. The Australian Competition and Consumer Commission ("ACCC") keeps track of the monetary damage caused by scammers. The Australian Cybercrime Online Reporting Network ("ACORN") and Scamwatch handle the processing and reporting of dating fraud cases.[88] However, the policing of online fraud is impeded by its transnational nature, the false identities used on the internet, and the lack of resources to investigate offenders. As a result, Australia focuses on education campaigns for victims and potential victims to counter online fraud victimisation.[89]

---

[86] Adam Lusher, *MPs Urged to Pass Law Against "Catfish" Imposters Tricking Women Into Sex*, Independent, July 17, 2017, available at https://www.independent.co.uk/news/uk/home-news/catfish-catfishing-dating-websites-fake-dating-profiles-sex-online-predators-mtv-legal-illegal-law-a7846011.html

[87] Mario Cacciottolo & Nicola Rees, *Online Dating Fraud Victim Numbers at Record High*, BBC News Jan. 23, 2017, available at https://www.bbc.com/news/uk-38678089

[88] Kate Kill, *The Cruelest of Scams: Victims of Dating and Not Reporting Incidents,* ABC News, Mar. 1, 2017, https://www.abc.net.au/news/2017-03-02/victims-of-dating-scams-not-reporting-incidents-accc-says/8318036

[89] Cassandra Cross, *Policing Online Fraud in Australia: The Emergence of a Victim-Oriented Approach*, *Crime, Justice and Social Democracy: Proceedings of the 3rd International Conference 2015* (2016). https://eprints.qut.edu.au/93198/

(2) European Union: The EU does not have any regulations or directives directly dealing with online dating or online dating fraud. However, such claims would most likely be processed by the European Anti-Fraud Office of the European Commission.[90] An imminent regulation that may affect dating platforms is the General Data Protection Regulation ("GDPR") set to take effect in May 2018. This regulation would require EU app developers to put in place appropriate technical measures to ensure data security.[91] This would also apply to dating websites which typically handle a host of private individual information.

(3) United States: Online dating services are generally not regulated under federal law. The one exception to this is the International Marriage Broker Regulation Act ("IMBRA"), which regulates dating services that focus on connecting US citizens with foreign nationals for the purpose of marriage.[92] Otherwise, regulation of dating sites falls under US state law. Many states have passed Internet Dating Safety Acts independently. For example, the applicable law in New Jersey requires dating platforms to post safety guidelines on their websites and notify users of whether they conduct criminal background checks.[93]

4.5 Proposed or Possible Solutions

(1) Civil Society Solutions

- Solutions to Combat Catfishing and Fraud:

  Education and information campaigns, particularly for people over 40 years old. In a 2017 survey of college students, nearly 78% of male respondents and 90% of female respondents knew what "catfishing" was. Only 3 respondents of the 184 participants answered that they had experience with catfishing. Educating students on the phenomenon of catfishing and other forms of cyber abuse can help promote online safety among young people.[94] However, further education campaigns are needed for older populations who have not received this information in school.

- Solutions to Promote Inclusive Online Dating Spaces:

---

[90] European Commission, European Anti-Fraud Office: https://ec.europa.eu/anti-fraud//home_en

[91] Reform of EU Data Protection Rules, European Commission (2017), available at https://ec.europa.eu/justice/data-protection/reform/index_en.html

[92] 8 U.S.C. §1375 (requiring background checks for US citizens using marriage brokerage services). https://www.law.cornell.edu/uscode/text/8/1375a

[93] *See* Internet Dating Safety Act, L. 2007, c. 272, s.1, available at https://www.njconsumeraffairs.gov/statutes/internet-dating-safety-act.pdf

[94] Brent Holmes, *How Rejected Men Use Dating Apps to Torment Women*, VICE, May 25, 2017, available at https://www.vice.com/en_us/article/8x4jbg/when-harassers-use-tinder-and-bumble-to-dox-and-women

Improving diversity in the dating platform development community. If the programmers of these Internet spaces are overwhelmingly white and male, they are more likely to create dating profiles that cater to their interests and ignore the dating behaviours of women, ethnic minorities, and LGBTQA+ groups.

(2) Technology Solutions

- Solutions to Combat Catfishing and Fraud:
    - Policing of false profiles and scammers by dating services. Dating platforms should monitor profiles for patterns typical of scammers. Once identified, the profiles should be taken down and dating platforms should have a complaint mechanism in place for victims to report potentially dangerous activity.
    - Alerting users to the risks of romantic fraud and catfishing. Publishing best practices for online dating safety and educating users about the risks of catfishing puts users on notice.
- Solutions to Promote Inclusive Online Dating Spaces:
    - Using online dating data for the greater good. In compliance with local privacy laws, online dating platforms can harness the data they have on dating behaviour to create design features that prevent discrimination against particular demographics.[95] As discussed above, OKCupid analysed its data to glean valuable insights into the race-based preferences of online daters. This discovery is the first step to creating solutions that promote more inclusive online dating spaces.

[95] Kath Albury et al., *Data Cultures of Mobile Dating and Hook-Up Apps: Emerging Issues for Critical Social Science Research*, Big Data and Society (2017). https://journals.sagepub.com/doi/pdf/10.1177/2053951717720950

(3) Legal Solutions

Some jurisdictions, including the UK, have called for the creation of a specific offence against catfishing. However, the anonymity of online dating and the international nature of Internet platforms makes these kinds of statutes difficult to enforce. The best legal solution involves the implementation of two complaint processes: one through the dating platform and another through the government. This enables adequate reporting of scammers so that law enforcement can investigate where possible and the dating platforms can warn users of schemes. Moreover, partnerships with the mental health and psychology community could help ensure that victims receive adequate treatment for trauma throughout the complaint process.

4.6 Further Research

As mentioned above, further research is needed in the following areas:

(1) International Cooperation Plans for Taking Action Against Dating Fraud

Most jurisdictions have trouble prosecuting Internet fraud, including online dating fraud, because of the international nature of the Internet. Perpetrators could live in different countries, keeping them outside the legal jurisdiction of the victim's home country. As a result, further research is needed into the creation of international partnerships to combat online dating fraud and romance scams. These kinds of transnational partnerships could enable information-sharing across countries and better equip law enforcement against international fraudsters.

(2) Intersectional Study of Discrimination in Online Dating Platforms:

Academia can combat some of the problems discussed in this section by taking an intersectional approach to the study of discrimination in online dating platforms. As mentioned above, online dating platforms can be inadvertent hosts for discrimination against minority groups. However, none of the discriminated groups discussed above should be considered in isolation. An intersectional approach to analysing discrimination on dating platforms paints a fuller picture. Intersectionality, a term coined by American civil rights advocate Kimberlé Williams Crenshaw, describes the phenomenon of overlapping or intersecting social identities and related systems of discrimination.[96] For example, the experience of a black woman on dating platforms cannot always be divorced from her additional identity as gay. Thus, a gay black woman is subject to two different

[96] Kimberle Crenshaw, *Mapping the Margins: Intersectionality, Identity Politics, and Violence Against Women of Color*, 43 Stanford L. Rev. 1241 (1993). https://www.jstor.org/stable/1229039

forms of discrimination and may be particularly vulnerable to harm or exclusion on dating profiles. This illustrates that an intersectional approach, taking into account multiple identity features, is the best prism with which to analyse discrimination on dating platforms. In addition to those discussed above, many factors such as age, wealth, body type or disability influence a person's success or exclusion on online dating platforms.

4.7 Major Organisations

This section lists some of the major organisations cited by the media as key players in the dialogue surrounding online dating regulation, catfishing, and online dating fraud. This list was compiled by amassing organisations that work on the subject from various angles. Organisations were included here regardless of whether they focus primarily on online spaces or whether they simply organise one-off campaigns related to this kind of content. Some international organisations were also included where relevant to the international approaches discussed above.

The following organisations are listed in no particular order:

(1) Get Safe Online (UK Organisation): source of information about online safety. They also organise national events, partner with law enforcement agencies, and promote awareness of internet safety. They have been cited in the past as key partners in educating the public about romance scams.[97] It is a jointly funded initiative between several UK Government departments and some private sector businesses such as Barclays Bank, PayPal, and Tesco.

(2) Online Dating Association (UK organisation): This is an organisation of Online Dating platforms focused on "taking responsibility for setting and maintaining standards." It offers a complaint mechanism and adjudication process for issues related to online dating profiles.

(3) Action Fraud (UK Government Organisation): This is the national government fraud and cybercrime reporting centre. They offer a live chat and a hot line for reporting cyber crime. While their website seems to focus more on the reporting of cyber attacks, they also deal with Internet fraud.

(4) Society of Citizens Against Romance Scams ("SCARS") (US Organisation): working against the threat of international online fraud and romance scams, providing support to victims of romance scams. They obtain funding by offering individual and corporate memberships, which give subscribers access to guidance on online fraud avoidance, risk mitigation, and feedback from scam victims.

---

[97] Zoe Kleinman, *Online Dating Conmen 'Using Love Letter Templates,'* BBC News, Feb. 12, 2017, https://www.bbc.com/news/technology-38936509

(5) ANYSCAM project: SCARS reporting mechanism for scammers and fraudsters. Not limited to romance scams, catfishing or online dating fraud.

(6) Internet Crime Complaint Center (US Government Organisation): FBI processing mechanism for Internet crime complaints, including dating fraud and scams. It is US government funded and run entirely by the Federal Bureau of Investigation.

(7) Scamwatch (Australian Government Organisation): Provides information to consumers and small businesses about how to recognise, avoid, and report scams. They also deal with cases of fraud on dating platforms. They work in tandem with the Australian Consumer Fraud Task Force (ACFT).

(8) Suzy Lamplugh Trust (UK Organisation): non-profit dedicated to reducing the risk of "violence and aggression through campaigning, education and support." They publish a yearly report of their funding and accomplishments here.

(9) Grassroots Organisations: Law enforcement's inability to find anonymous romance scammers online has encouraged victims to mount their own investigations. The following two websites are examples of these victim-led forums and cautionary information hubs. It is important to note that since they are grass roots, their websites are unprofessional and their organisational structure is dubious. Nevertheless, they are listed below for purposes of completeness.

- Romance Scam through hosting forums and sharing information among victims.
- PigBusters: scammer awareness site dedicated to warning people about online scammers and fake profiles on social media and dating websites.

(10) Individuals and Academics:

- Tom Buchanan (University of Westminster): Psychologist researching violence, online aggression, and online dating romance scam. Co-authored a paper cited above with Monica Witty.
- Bill Dutton (Oxford Internet Institute): sat on the advisory board of a research project related to online dating romance scams. He has previously written a paper on dating culture in the digital age.

5. Hate Speech Online

5.1 Definitions

Hate speech is defined as speech that attacks, threatens or insults a person or group on the basis of national origin, ethnicity, colour, religion, gender identity, sexual orientation or disability.[98]

5.2 Vulnerable Populations & Impact

There are several populations that are particularly vulnerable to hate speech online. As such, they receive added protection under UK law. LGBTQA+ persons, individuals with disabilities, and members of ethnic minorities or religions are often targets for this kind of online abuse. Additionally, those of a different colour, race, nationality or citizenship status may also be targets for online hate speech.[99] Studies have also found that online hate speech also targets people based on class and physical appearance.[100]

In 2015-2016, the Crown Prosecution Service ("CPS"), prosecuted 15,000 hate crime incidents, the highest number ever.[101] However, the number of cases being referred by police to prosecutors also fell by 10%. Several factors could explain this, such as a victim's reluctance to report or the high threshold for prosecuting an online hate crime. Since the investigative process is slow compared to the "fast-moving online world," many hate crimes are never referred for prosecution.[102]

There are a several causes of online hate speech, and some debate about whether it is distinctive from offline hate speech.[103] A 2017 study found that anonymity in social media plays a role in fuelling hate speech.[104] This is consistent with existing social psychology research suggesting that anonymity influences one's behaviour. In particular, people tend to behave "more aggressively in situations where they feel they are anonymous."[105] In an analysis of 512 million Tweets and 27.55 million posts on the social media platform Whisper,

---

98 "Hate Speech," Random House Dictionary (2017).

99 *See e.g.*, Jamie Cleland, *Online Racial Hate Speech*, Cybercrime and Its Victims: Routledge Studies in Crime and Society (2017).

100 Mainack Mondal et al., *A Measurement Study of Hate Speech in Social Media*, Association for Computing Machinery (2017), available at https://homepages.dcc.ufmg.br/~fabricio/download/HT2017-hatespeech.pdf

101 *Hate Crimes: Online Abuse 'As Serious As Face-to-Face,"* BBC News, Aug. 21, 2017, https://www.bbc.com/news/uk-40981235

102 *Id.*

103 *See generally*, Andre Oboler, *Legal Doctrines Applied to Online Hate Speech*, Computers & Law (2014) available at https://www.austlii.edu.au/au/journals/ANZCompuLawJl/2014/4.pdf

104 Mainack Mondal et al., *A Measurement Study of Hate Speech in Social Media*, Association for Computing Machinery (2017) available at https://homepages.dcc.ufmg.br/~fabricio/download/HT2017-hatespeech.pdf

105 *Id.*

a study found that indeed anonymity fuels more hate in online media systems, and the use of anonymity varies with the type of hate speech.[106]

While anonymity may fuel online hate speech, it may not be the main feature that distinguishes it from offline hate speech. A 2017 theoretical analysis by Alexander Brown suggests that anonymity may not actually be a distinctive quality of online versus offline hate speech. Brown argues that "the instantaneous nature of the communication on some parts of the Internet and the spontaneous hate speech that it encourages might be a better, and often overlooked, reason to mark it as different."[107] Thus, further research may be needed to determine whether or how online hate speech is different than its offline counterpart.

Overall, hate speech has repercussions not just for individuals but for entire communities.

According to Jeremy Waldron, the central harm in hate speech is that it undermines the dignity of minority groups.[108] The publication of hate speech "aims to besmirch the basics of their reputation, by associating ascriptive characteristics like ethnicity, or race, or religion with conduct or attributes that should disqualify someone from being treated as a member of society in good standing."[109] In addition to impacting the specific individuals targeted, hate speech can thus have a larger impact for society as a whole.

5.3 Legal Background

While the Internet may often contain offensive material, very little of it is illegal.[110] UK law seeks to strike a balance between freedom of speech and the protection of minority groups. In the UK, CPS treats hate speech under the larger umbrella of hate crimes.[111] CPS defines a hate crime as follows:

> *"Any criminal offence which is perceived by the victim or any other person, to be motivated by hostility or prejudice, based on a person's disability or perceived disability; race or perceived race; or religion or perceived religion; or sexual orientation or perceived sexual orientation or a person who is transgender or perceived to be transgender."*

---

[106] *Id.*

[107] Alexander Brown, *What is so special about online (as compared to offline) hate speech?*, Ethnicities, 1-30 (2017). https://ueaeprints.uea.ac.uk/64133/1/Accepted_manuscript.pdf

[108] Jeremy Waldron, *The Harm in Hate Speech*, Harvard University Press (2012).

[109] *Id.*

[110] "Internet Hate Crime," True Vision (2017) https://report-it.org.uk/reporting_internet_hate_crime

[111] "Hate Crime" Crown Prosecution Service (2017), available at https://www.cps.gov.uk/victims_witnesses/hate_crime/index.html

More recently, CPS has issued guidance on the prosecution of hate crimes which clarifies that online hate crimes are to be treated "as seriously as abuse committed face-to-face."[112] Online hate crime can be carried out by posting content online or broadcasting it on the media. Hate crimes can range from verbal abuse, threats of violence, harassment, stalking or other "anti-social behaviour."[113] The primarily legal ambiguity in these prosecutions is determining where to draw the line between speech that is hostile or merely offensive.

Words linked to violence are a clear example of hate speech. For instance, in 2017 Viscount Rhodri Colwyn Philipps posted online offering £5,000 to anyone who runs over Gina Miller, a businesswoman who campaigned for parliamentary sovereignty. The post also included language referring to Miller's status as a first-generation immigrant.[114] The clear incitement to violence, paired with the racially aggravated nature of the threat make it an example of hate speech. Phillips was convicted of two charges relating to this.

5.4 International Legal Approaches

(1) Australia: Australian hate speech laws give redress to a person who is the victim of discrimination, vilification or injury. The Racial Discrimination Act of 1975 forbids hate speech where an act is "reasonably likely, in all the circumstances, to offend, insult, humiliate or intimidate another person or group of people; and the act is done because of the race, colour, or national or ethnic origin of the other person, or of some or all of the people in this group." More recently, a debate arose in Australia about how this law applies to online hate speech. A recent dispute featured a university student who posted on Facebook: "Just got kicked out of the unsigned indigenous computer room. QUT stopping segregation with segregation?"[115] The hate speech complaint against the student was dismissed by the Federal Court.

Dr. Andre Obler, CEO of the Online Hate Prevention Institute in Australia highlights some laws in Australia that could be used to criminalise hate speech online.[116] However, there is variety in legal protections against hate speech among the different states within Australia.

---

[112] *Hate Crimes: Online Abuse 'As Serious As Face-to-Face,"* BBC News, Aug. 21, 2017, https://www.bbc.com/news/uk-40981235

[113] *Hate Crime: Public Statement on Prosecuting Racist and Religious Hate Crime* (2017) https://www.cps.gov.uk/publications/docs/racist-religious-hate-crime-statement-2017.pdf

[114] *Rhodri Colwyn Phillips Jailed Over Gina Miller Post*, BBC News, July 13, 2017, https://www.bbc.co.uk/news/uk-40599992

[115] Aaron Goonrey, *Hate speech and freedom of speech in Australia,* Mar. 17, 2017 available at https://www.hrmonline.com.au/section/legal/hate-speech-freedom-speech-australia

[116] *See generally*, Andre Oboler, *Legal Doctrines Applied to Online Hate Speech*, Computers & Law (2014) available at https://www.austlii.edu.au/au/journals/ANZCompuLawJl/2014/4.pdf

(2) European Union: The European Court of Human Rights ("ECHR") has robust case law on prohibition against hate speech.[117] Under EU Law, "it may be considered necessary… to sanction or even prevent all forms of expression which spread, incite, promote, or justify hatred based on intolerance."[118] In Delfi AS v. Estonia, the ECHR held that requiring an Internet news portal to take down comments that incite violence does not violate the company's right to free expression.[119] On the other hand, in Pihl v. Sweden, the court held against the victim of a defamatory online comment on a blog, stating that a balance must be struck between an individual's right to private life and the freedom of expression enjoyed by the group running the Internet portal.[120]

In 2016, however, the European Commission and technology companies like Facebook, Twitter, YouTube and Microsoft announced a Code of Conduct on illegal hate speech online.[121] However, Facebook, Twitter, and other tech companies still face pressure from European lawmakers to police hate speech more aggressively online. In Germany, lawmakers are considering legislation that would impose fines of more than $50 million on social media companies that fail to remove hate speech, despite critiques that the measure could curtail free speech.[122]

---

[117] *See* Council Framework Decision 2008/913/JHA (2008) available at https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:328:0055:0058:en:PDF
Twitter recently failed to meet European standards for removing hate speech online.
See Mark Scott, *Twitter Fails EU Standard on Removing Hate Speech Online*, May 31, 2017, available at https://www.nytimes.com/2017/05/31/technology/twitter-facebook-google-europe-hate-speech.html

[118] *See Hate Speech*, European Court of Human Rights Fact Sheet (2017) available at https://www.echr.coe.int/Documents/FS_Hate_speech_ENG.pdf

[119] *Hate Speech*, European Court of Human Rights Fact Sheet (2017) available at https://www.echr.coe.int/Documents/FS_Hate_speech_ENG.pdf

[120] *Id*; *See also*, Robert Spano, *Intermediary Liability for Online User Comments Under the European Convention on Human Rights*, Human Rights L. Rev. (2017) https://academic.oup.com/hrlr/article-abstract/17/4/665/3059638
(Abstract: full report is available to subscribers)

[121] European Commission Press Release, *European Commission and IT Companies Announce Code of Conduct on Illegal Online Hate Speech*, May 31, 2016, https://europa.eu/rapid/press-release_IP-16-1937_en.htm

[122] Amar Toor, *EU Close to Making Facebook, YouTube, and Twitter Block Hate Speech Videos*, May 24, 2017 https://www.theverge.com/2017/5/24/15684168/eu-hate-speech-law-facebook-twitter-youtube-video

(3) United States: The United States Constitution is highly protective of speech, meaning that the government has difficulty regulating speech without running afoul of the First Amendment. As a result, some speech that may be deemed offensive or even harmful cannot be regulated. There are a small number of exceptions to this, including the incitement of violence. As a result, hate speech online has thus far been managed by technology companies and social media platforms. While the government cannot constitutionally curtail most speech, private companies can.[123]

5.5 Proposed or Possible Solutions

(1) Civil Society Solutions

Education campaigns related to hate speech online should focus on acknowledging the harm of hate speech.[124] According to Barker and Jane, many users of social media have "learned to 'see but not see' the graphic misogynist, racist, and homophobic comment sections."[125] This kind of habituated blindness assists internet users in navigating the internet efficiently every day. However, it also results in downplaying the social problems that emerge online. According to Elena Martellozo and Emma A. Jane, academia and civil society must take care to not be "blinded by the obvious."[126]

(2) Technology Solutions

Neural networks and branches of artificial intelligence can assist governments and social media companies in identifying hate speech more quickly.[127] Automating the process of detecting and removing hate speech could save regulators resources and combat the harms of online hate speech more effectively. This kind of technology is still being developed, but social media companies can rely on it to an extent to identify hate speech.

---

[123] For further discussion of US First Amendment jurisprudence and online speech, *see* Section 7.4 (3) of this review, "Terrorist Radicalisation Online".

[124] *See generally*, Sole Alba Zollo & Eugene Loos, *No Hate Speech Movement: Evolving Genres and Discourses in the European Online Campaign to Fight Discrimination and Racism*, 11 Observatorio 2 (2017). https://obs.obercom.pt/index.php/obs/article/view/1022/pdf

[125] C. Barker & E.A. Jane, *Cultural Studies: Theory and Practice*, Sage (2016).

[126] Elena Martellozzo & Emma A. Jane, *Cybercrime and Its Victims*, Routledge Studies in Crime and Society (2017).

[127] Björn Gambäck and Utpal Kumar Sikdar, Using Convolutional Neural Networks to Classify Hate-Speech, Association for Computational Linguistics (2017), available at https://www.aclweb.org/anthology/W17-3013

(3) Legal Solutions

Since Internet companies are the primary platforms for hate speech, some argue that they should be charged with its day-to-day regulation and removal. Alexander Brown, in his 2017 article, suggests that national governments should be working closely with Internet companies to combat online hate speech.[128] However, leaving the day-to-day regulation of online hate speech to Internet companies alone poses some problems for the protection of free speech. In many countries, it is a controversial issue to entrust decisions about free expression to private corporations as opposed to the government. Moreover, if this kind of "outsourcing" scheme ultimately infringes on individual rights, it may be considered illegal in many countries. Nonetheless, social media companies are often better suited to monitoring and implementing standards of conduct on their platforms.

5.6 Further Research

As mentioned above, further research is needed in the following area:

Empirical research into what factors influence hate speech online. Alexander Brown claims that the spontaneity of online communication enables cyber hate, while Mondal's quantitative analysis of Twitter and Whisper data suggests that anonymity plays a large role.[129] Further empirical studies of social media hate speech could provide greater clarity on how online hate speech differs from its offline counterpart.

5.7 Major Organisations

This section lists some of the major organisations cited by the media as key players in the dialogue surrounding hate speech. This list was compiled by searching for general groups against hate speech as well as specialised groups spearheaded by directly impacted communities. Organisations were included here regardless of whether they focus primarily on online spaces or whether they simply organise one-off campaigns related to this kind of content.

---

[128] Alexander Brown, *What is so special about online (as compared to offline) hate speech?*, Ethnicities, 1-30 (2017). https://ueaeprints.uea.ac.uk/64133/1/Accepted_manuscript.pdf

[129] Mainack Mondal et al., *A Measurement Study of Hate Speech in Social Media*, Association for Computing Machinery (2017), available at https://homepages.dcc.ufmg.br/~fabricio/download/HT2017-hatespeech.pdf

The following organisations are listed in no particular order:

(1) Galop (UK-based organisation): focuses on providing support, advice, and research surrounding LGBT+ hate speech. They assist victims of online hate crimes, harassment, and LGBT domestic abuse. They have been providing support to the LGBT+ community for 30 years and they are primarily funded by donations. They partner with other LGBT organisations to provide services.

(2) True Vision (UK Government Organisation): owned by the National Police Chief's Council, True Vision is a website and reporting mechanism dedicated to policing hate crimes online. It provides personal safety tips, information on the prosecution of online hate crimes, and relevant research on hate crimes. It operates within the Department for Communities and Local Government.

(3) Online Civil Courage Initiative (UK Organisation): OCCI is an initiative run by an NGO called ISD. The initiative is funded by Facebook, Google, and Microsoft and it seeks to combat hate speech and extremism online. It is the "first strategic non-governmental effort to mount a proportional response to the propagation of hate, violence and terrorism online, across Europe."

(4) No Hate Speech Movement (EU Organisation, based in France): NHSM is the youth campaign of the Council of Europe for human rights online, to "reduce the levels of acceptance of hate speech and develop online youth participation and citizenship, including in Internet governance processes."

(5) Community Security Trust (UK Charity): a Jewish charity that published a comprehensive guide for those affected by Hate Crime. They also recently partnered with Facebook's Online Civil Courage Initiative to counter online hate speech and extremist content.[130] They are organised as a charity and rely on donations. The website does not provide a list of their donors or board members.

(6) Imams Online (Online Organisation): Network of Imams and Muslim leaders dedicated to educating the public about Islamophobia, facilitating interfaith dialogue supporting the Muslim community, countering extremism and opposing hate speech. They are also among Facebook's OCCI partners.[131]

[130] *Id.*
[131] *Id.*

(7) TellMAMA (UK Organisation): provides a reporting mechanism for victims of anti-Muslim bigotry and hate speech. They are dedicated to challenging anti-Muslim narratives and where there are "blogs, statements, or news articles which promote them." They have also partnered with Facebook's Online Civil Courage Initiative to receive training on identifying extremist content online.

(8) Stand Up! (UK Organisation): is a programme led by Jewish, Muslim, and LGBT groups to empower young people in mainstream schools to learn about and act against discrimination, racism, antisemitism, and anti-Muslim hatred. They are funded by the Department for Communities and Local Government and led by Streetwise (a partnership between Community Security Trust & Maccabi GB) and supported by Tell MAMA, Kick It Out and Galop.

(9) Community Alliance to Combat Hate ("CATCH") (UK Organisation): provides a reporting mechanism for hate crimes, support for victims of hate crimes, and partners with local organisations to monitor hate crimes, including online abuse. Partners include CST, Gallop, Tell MAMA, The Monitoring Group, and Choice in Hackney. The partnership is commissioned by the Mayor's Office for Policing and Crime.

(10) Kick It Out (UK Organisation): campaigning organisation which works with football authorities to combat all forms of discrimination. They often partner with other hate crime organisations to participate in campaigns. Their funders include TheFA For All, the Premier League, EFL, Professional Footballers Association.

(11) The Online Hate Prevention Institute (Australian Organisation): an Australian Harm Prevention Charity. They aim to reduce the risk of suicide, self harm, substance abuse, physical abuse and emotional abuse that can result from online hate. Their focus ranges from cyber-racism, online religious vilification and other group-based forms of online hate, through to the cyber-bullying of individuals. The full charity registration details are on file with the Australian Business register here.

6. Child Abuse Online

6.1 Definitions

There are several forms of cyber abuse against children. Child pornography is a form of exploitation involving a sexually explicit visual depiction of a minor.[132] Online solicitation is defined as using the Internet to groom,[133] command, or otherwise incite a minor to engage in sexual conduct.[134] Since the purpose of this analysis is to signal gaps in the literature, particular attention will be paid to child trafficking as well as grooming and related risks to children online.

6.2 Vulnerable Populations & Impact

A 2016 study by UNICEF concluded that one in three of all Internet users worldwide are children under the age of 18.[135] The number of young children online serves to highlight the importance of teaching and reinforcing safe online behaviour. Moreover, it shows the importance of taking into account the rights of children in Internet governance.

According to the National Society for the Prevention of Cruelty to Children ("NSPCC"), pre and early teens are particularly vulnerable ages for children online. While any child can be affected by sexual abuse, some may be more at risk if they have a history of previous abuse, a disability, or a "disrupted home life."[136] A negative home environment has been shown to correlate with a host of online risks.[137] In particular, "high parental conflict was correlated

---

[132] "Child Pornography," US Department of Justice, July 25, 2017, available at https://www.justice.gov/criminal-ceos/child-pornography
See generally Adam Galpin, "Towards a theoretical framework for understanding the development of media-related needs" Journal of Children and Media (2016) (arguing for a "basic needs approach" to understanding how media-related needs emerge and are expressed through development). https://www.tandfonline.com/doi/full/10.1080/17482798.2016.1194373 (Abstract: full report is available to subscribers)

[133] Grooming is when someone builds an emotional connection with a child to gain their trust for the purposes of sexual abuse, sexual exploitation, or trafficking. *See* "Grooming," National Society for the Prevention of Cruelty to Children, available at https://www.nspcc.org.uk/preventing-abuse/child-abuse-and-neglect/online-abuse

[134] *See* Seto MC & Wood JM et al., *Online Solicitation Offenders are Different from Child Pornography Offenders and lower risk contact sexual offenders.* Law and Human Behavior (2012) https://psycnet.apa.org/record/2011-27115-001 (Abstract: full report is available for purchase)

[135] S. Livingstone et al., *One in Three: Internet Governance and Children's Rights*, Office of Research – Innocenti, UNICEF (2016) available at https://www.unicef-irc.org/publications/pdf/idp_2016_01.pdf

[136] *See Sexual Abuse*, National Society for the Prevention of Cruelty to Children, available at https://www.nspcc.org.uk/what-is-child-abuse/types-of-abuse/child-sexual-abuse/

[137] Andrew Schrock & danah boyd, *Online Threats to Youth: Solicitation, Harassment, and Problematic Content*, Literature Review for the Internet Safety Technical Task Force at Harvard, (2008) available at https://www.danah.org/papers/ISTTF-RABLitReview.pdf
see also Janis Wolak et al., *Online Victimization of Youth: Five Years Later*, National Center for Missing and Exploited Children (2006) available at https://www.unh.edu/ccrc/pdf/CV138.pdf

with higher online sexual victimisation." Children who are victims of online sexual abuse and grooming experience psychological harm and long-lasting damage to their wellbeing.

Since not all incidents of online abuse result in offline meetings, psychologists have queried whether online abuse inflicts different types of harms on children.[138] A 2010 study argues that "there is a need to challenge the perception of internet offending as causing fewer traumas than contact offending, or viewing the risk of harm as minor."[139] Children who are victims of online sexual abuse are indeed presented with trauma due to the fact that the identities of their perpetrators are often unknown. Additionally, children who have their images stolen by online abusers have their privacy newly invaded by an unknown perpetrator every time it is distributed online.

Another form of child abuse carried out online is sex trafficking. This is primarily a problem in the United States, but the UK has also had incidents involving sex trafficking websites.[140] According to Ryan Mahan, Head of Information & Online Campaigns at ECPAT UK, argues that "tech-savvy offenders are increasingly taking to the internet to abuse children in the UK and abroad."[141] In the US, one primary issue centred around a classifieds website called Backpage, which operated as a "hub" for the trafficking of children.[142] Backpage does not deny that its site is used for criminal activity, including the sale of children for sexual services. According to a US Senate Subcommittee Investigation, it argues that it is a "mere host of content created by others and is thus immune from liability under the Communication Decency Act ("CDA")." Judges in the US have sided with the website, citing this law which dictates that platforms are not liable for the postings of users. Child trafficking in the UK hit a

---

[138] *See e.g.* Faye Mishna et al., *Real-World Dangers in an Online Reality: A Qualitative Study Examining Online Relationships and Cyber Abuse*, 33 Social Work Research 2 (2009) https://academic.oup.com/swr/article-abstract/33/2/107/1728408
(Abstract. Full report is to purchase)

[139] Marcella Mary Leonard, *'I did what I was directed to do but he didn't touch me': The Impact of being a victim of internet offending*, 16 Journal of Sexual Aggression 2 (2010) https://www.tandfonline.com/doi/full/10.1080/13552601003690526
(Abstract: full report is available to purchase)

[140] Jamie Grierson, *Tens of Thousands of Modern Slavery Victims in UK, NCA says*, The Guardian, Aug. 10, 2017, available at https://www.theguardian.com/world/2017/aug/10/modern-slavery-uk-nca-human-trafficking-prostitution

[141] *See Enshrine Compensation Rights for Children Exploited Online, Campaigners Say*, available at https://www.ecpat.org.uk/News/enshrine-compensation-rights-for-children-exploited-online-campaigners-say

[142] Staff Report, *Backpage.com's Knowing Facilitation of Online Sex Trafficking*, U.S. Senate, Jan. 10, 2017 available at https://www.hsgac.senate.gov/subcommittees/investigations/hearings/backpagecoms-knowing-facilitation-of-online-sex-trafficking

record high in 2017, which may increase the likelihood that traffickers will resort to similar online classified pages to advertise their victims.[143]

6.3 Legal Background

There are several statutes in the UK dealing with the subject of online child abuse. The Sexual Offences Act 2003 makes sexual grooming an offense, but action can only be taken when authorities have proof that an adult intended to meet a child physically. The Malicious Communications Act 1988 makes it an offence to send a communication with the intention of causing distress or anxiety. This is often applied in cases of online child abuse, but it is often difficult for prosecutors to prove "intent to cause distress or anxiety." The Communications Act 2003 (section 127) makes it an offence to send an electronic message that is indecent or obscene. While an online groomer may not be covered by a law, this does capture some forms of child cyber abuse such as sexting.

6.4 International Legal Approaches

(1) Australia: The Australian Federal Police Child Protection Operations ("CPO") is the main authority investigating international online child sexual exploitation.[144] These matters include matters dealing with Internet Service Providers and Internet content hosts. The types of offences investigated include accessing, sending, or uploading child exploitation and abuse material. The CPO also investigates grooming and procuring of children over the Internet. One difference in Australia is that this offense requires a child to be under the age of 16 in order for a grooming offence to have been committed. According to the Australian Federal Police, the government changed legislation in 2010 to increase penalties applying to these offenses, bringing the sentence to 15 years. These reforms "also enhanced the coverage of offences for using a carriage service, such as the Internet, for sexual activity with a child or for child abuse material."[145]

(2) European Union: The EU's Directive on combatting the sexual abuse and exploitation of children and child pornography is a legal framework covering the investigation and prosecution of perpetrators. It also provides victims with assistant and prevention schemes. The aim of the Directive is to approximate the definition of 20 offences and suggest minimum levels for criminal penalties.

---

[143] May Bulman, *Child trafficking in UK hits record high, figures show*, Independent, April 3, 2017, available at https://www.independent.co.uk/news/uk/home-news/child-trafficking-referrals-in-uk-hit-record-high-figures-show-a7665201.html

[144] *Online Child Sex Exploitation*, Australian Federal Police, available at https://www.afp.gov.au/what-we-do/services/child-protection/online-child-sex-exploitation

[145] *Id.*

Separately, another EU legal framework that may apply to online child sex abuse is the General Data Protection Regulation ("GDPR"). It is one of the most important changes to data privacy regulation in 20 years.[146] The UK Children's Charities Coalition recently published an open letter detailing the ways the GDPR could impact children's rights.[147]

(3) United States: As discussed earlier in this subsection, US is currently in the midst of debate surrounding websites such as Backpage that are used to promote human trafficking online.[148] Thus far, there has been no legal takedown of the website, due to First Amendment free speech protections in the United States.[149] On the one hand, some senators have advocated its removal with the intention of reducing the trafficking. Other advocates argue that closing the website makes it difficult for NGOs to reach potential victims and identify dangerous activity. Some critics are also concerned that shuttering this page would have negative repercussions for the economic and physical safety of adult sex workers who use the website for business.[150]

6.5 Proposed or Possible Solutions

(1) Civil Society Solutions

Increased education about digital safety, particularly for children with limited access to media. According to Jon Brown, disparate access to computers, media, and digital literacy results in "inequalities in terms of access, information and skills."[151] Thus, children with less education about safety measures online are more vulnerable to abuse. One solution to this is to embed education on "online empowerment and online risk" within all regular services that work with children, such as social workers, teachers, health practitioners, and mental health service providers. However, at least one study has concluded that participation in psychoeducational internet interventions is associated with an increase in internet safety knowledge, but not significantly associated with a change in online

---

[146] *See* GDPR Portal: Site Overview, available at https://gdpr.eu
See also: https://ec.europa.eu/commission/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules_en

[147] *See Open Letter to Elizabeth Denham: The GDPR and Children*, May 15, 2017. https://www.chis.org.uk/file_download/81

[148] *See* Sam Levin, *Backpage's halt of adult classifieds will endanger sex workers, advocates warn*, The Guardian (, Jan 10, 2017) https://www.theguardian.com/society/2017/jan/10/backpage-adult-classifieds-sex-workers-danger-trafficking

[149] *Id.*

[150] *Id.*

[151] Jon Brown, *Online Risk to Children: Impact, Protection and Prevention*, John Wiley & Sons (2017). https://onlinelibrary.wiley.com/doi/book/10.1002/9781118977545
(Overview: full book is available to purchase)

behaviour.[152] Though it is important to note that this study included educational materials for all forms of cyber abuse against children, and different results may be observed for educational materials about online sexual exploitation.[153]

(2) Technology Solutions

According to a 2011 study, private technology firms "should recognise that their services and networks are being exploited by traffickers and take steps to innovate and develop anti-trafficking initiatives."[154] Since online classifieds sites and social medias are often hubs for online sex trafficking of children, technology companies can establish ethical policies regarding the commercial exploitation of children. In countries where free speech laws prevent the takedown of problematic sex trafficking websites, their private sector hosts may have greater power.

(3) Legal Solutions

Enabling child victims and their families to claim compensation for sexual abuse online. This kind of initiative was put forth by a children's organisation, ECPAT UK, in a digital manifesto published by the Children's Charities Coalition on Internet Safety.[155]

6.6 Further Research

As mentioned above, further research is needed in the following areas:

(1) The differences between online and offline sexual offenses against children. Some studies have concluded that there is a connection between exploitative material online, grooming, and "contact" offending offline. A 2017 study by Tony Krone and Russell G. Smith calls for further research on "the nature of online child sexual exploitation and its connection to other forms of sexual and violent offenses."[156]

---

[152] *See* Faye Mishna et al., *Interventions to Prevent and Reduce Cyber Abuse of Youth: A Systematic Review*, 21 Research on Social Work Practice 1 (2011) https://journals.sagepub.com/doi/10.1177/1049731509351988 (Abstract: full report is available to subscribers)

[153] *See also*, Victoria Spencer-Hughes, *Screening for Child Sexual Exploitation in Online Sexual Health Services: An Exploratory Study of Expert Views*, 19 J. Med. Internet Res. 2 (2017) https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5331185

[154] Mark Latonero, *Human Trafficking Online: The Role of Social Networking Sites and Online Classifieds*, University of Southern California, Center on Communication Leadership & Policy Research Series (2011) available at https://technologyandtrafficking.usc.edu/files/2011/09/HumanTrafficking_FINAL.pdf

[155] Children's Charities Coalition on Internet Safety Digital Manifesto, Fourth Edition (2015) https://www.ecpat.org.uk/childrens-charities-coalition-on-internet-safety-digital-manifesto

[156] Tony Krone & Russell G. Smith, *Trajectories in Online Child Sexual Exploitation in Australia*, Trends and Issues in Crime and Criminal Justice 524 (2017) https://aic.gov.au/publications/tandi/tandi524

(2) How mobile technologies have changed (either improved or worsened) existing online risks for children.[157]

(3) The extent to which online sexual solicitation occurs between youths. According to a 2008 literature review by Andrew Schrock and Danah Boyd, 43% of minor solicitations online were perpetrated by other minors. This suggests that minor-to-minor sexual risks online may deserve more research and attention.

6.7 Major Organisations

This section lists some of the major organisations cited by the media as key players in the dialogue surrounding child abuse online. This list was compiled by amassing organisations that are influential in advocating against child sex trafficking online, or in conducting research against child victimisation. Organisations were included here regardless of whether they focus primarily on online spaces or whether they simply organise one-off campaigns related to this kind of content.

The following organisations are listed in no particular order:

(1) National Society for the Prevention of Cruelty to Children (UK-based charity, registered in Scotland): leading children's charity fighting to end child abuse in the UK. They run a hotline called Childline, which held over 295,000 Childline counselling sessions with children and young people in the last year. Links to their annual reports can be found on their website.

(2) Every Child Protected Against Trafficking ("ECPAT UK") (UK-based organisation): a children's organisation working to protect children from child trafficking, online abuse, and transnational exploitation. They host campaigns, create training courses, and provide statistics on online abuse. Since 1994, ECPAT's campaigns have facilitated the introduction of new legislation and the ratification of relevant international conventions. They are funded through commissioned partnerships with statutory funders, trusts, foundations and donations. The full list of their funders is available on their website.

[157] Andrew Schrock & danah boyd, *Online Threats to Youth: Solicitation, Harassment, and Problematic Content*, Literature Review for the Internet Safety Technical Task Force at Harvard, (2008) available at https://www.danah.org/papers/ISTTF-RABLitReview.pdf

(3) WeProtect Global Alliance (UK Organisation): this alliance is focused on ending child sexual exploitation online. This includes online grooming as well as the production and distribution of child pornography. It combines two larger initiatives: The Global Alliance, led by the U.S. Department of Justice and the EU Commission and WePROTECT, which was convened by the UK. This new, merged initiative has unprecedented reach, with 70 countries already members of WePROTECT or the Global Alliance, along with major international organisations, 20 large players in the global technology industry, and 17 leading civil society organisations. They are led by a multi-stakeholder board consisting of representatives from key countries. Their missions include developing strategy and governance structures to achieve these ends, as well as "galvanising global action" by meeting with governments, technology companies, and civil society to end violence against children online.

(4) ThinkUKnow (UK Organisation, associated with CEOP, a command of the National Crime Agency): the Thinkuknow education programme that aims to empower and protect children and young people from sexual abuse and exploitation. They provide training, courses, educational materials, and resources for keeping children safe online.

(5) Marie Collins Foundation (UK Organisation): developing an organisation that has the skills and experience to equip agencies and professionals with the knowledge and understanding they need to respond to children who have been abused via the Internet and mobile technologies. Their partners include UNICEF, the UK Department for Education, and private corporations like TalkTalk and Lloyd's Bank.

(6) Childnet International (a UK-based Organisation operating Internationally): Childnet's mission is to work in partnership with others around the world to help make the Internet a great and safe place for children. They have a number of large corporate funders, including Facebook and Microsoft. They've also received support from the Government Equalities Office.

(7) European NGO Alliance for Child Safety Online (Europe-wide Organisation) a pool of online child protection NGOs from different European Countries. Their overriding goal is to create a safer online environment for children by cooperating with other NGOs across the EU. They are completely funded under the Safer Internet plus programme of the European Parliament and of the Council.

(8) I-Safe Ventures (US Organisation): is a hybrid non-profit and for-profit LLC focused on helping commercial organisations comply with statutory regulations guarding child privacy. While they are not a charitable organisation, they are often

contracted to help schools and organisations provide educational materials and instructional programming on online risk.

(9) Crimes Against Children Research Center (US Organisation): focused on combatting crimes against children by providing research and statistics to public policy makers and law enforcement personnel. They also produce and promote research on online risks to children. They're funded by government and private grants from organisations such as the National Science Foundation, UBS, the US Department of Justice, and the National Children's Alliance.

(10) National Center for Missing & Exploited Children (US Organisation): runs a Cyber Tipline that uses technology to help prevent and diminish sexual exploitation of children. It provides public electronic service providers with the ability to report online instances of online child sexual abuse. According to the website, it is funded at least in part by the Office of Juvenile Justice and Delinquency Prevention, within the US Department of Justice. The website's disclaimer clarifies that none of the organisation's components are operated, controlled, or endorsed by the US Department of Justice.

(11) SharedHope International (US Organisation): an advocacy organisation dedicated to combatting child sex trafficking. They are currently working on a campaign against US legal loopholes that enable human traffickers to conduct business online. They are also members of the Evangelical Council for Financial Accountability, which publishes their financial health statistics here yearly.

(12) Internet Watch Foundation (UK Organisation): an organisation dedicated to the global elimination of child abuse imagery. They host a hotline for members of the public to report abuse anonymously. They also provide UK Internet Service Providers with details of websites containing this kind of content, enabling them to block them. They are a not-for-profit funded by the European Commission and by corporate sponsors.

7. Terrorist Radicalisation Online

7.1 Definitions

Radicalisation is the "process of increasing extremity of beliefs, feelings, and behaviours in directions that justify intergroup violence and demand sacrifice in defence of the ingroup."[158]

7.2 Vulnerable Populations & Impact

Extremist groups and terrorist organisations use the Internet and social media platforms to engage in recruitment and radicalisation.[159] Maintaining an online presence allows radical movements to extend beyond their physical borders and influence behaviour more broadly.[160] Moreover, the use of social media enables radical ideologies to spread more quickly and to gain followers who they might not otherwise have reached. Terrorist content online and the spread of terrorism and violent extremism have been recognised by social media platforms like Twitter as a "global problem and critical challenge for us all."[161]

Research into the causes of online radicalisation mainly discuss the psychological traits and life circumstances that enable radicalisation.[162] Research suggests that people who are emotionally vulnerable are more likely to transition to morally justifying violence as a tool to obtain political goals.[163] Emotional vulnerability can emerge because of anger, alienation, or disenfranchisement. Several theories of radicalisation note that a personal crisis or "sense of longing" causes an isolation that enables "cognitive opening," where individuals are receptive

---

[158] *See* Thomas J. Holt et al, *Internet-Based Radicalization as Enculturation to Violent Deviant Subcultures*, 38 Deviant Behavior McCauley 8 (2017) https://www.tandfonline.com/doi/full/10.1080/01639625.2016.1197704 (Abstract: full report is available to purchase)
See also Clark McCauley & Sophia Moskalenko. *Mechanisms of Political Radicalization: Pathways Toward Terrorism*, 20 Terrorism and Political Violence 3 (2008) https://www.tandfonline.com/doi/abs/10.1080/09546550802073367

[159] *See* Thomas J. Holt et al, *Internet-Based Radicalization as Enculturation to Violent Deviant Subcultures*, 38 Deviant Behavior McCauley 8 (2017) https://www.tandfonline.com/doi/full/10.1080/01639625.2016.1197704 (Abstract: full report is available to purchase)

[160] *Id.*

[161] @Policy, *Global Internet Forum to Counter Terrorism*, Twitter Blog, June 26, 2017, available at https://blog.twitter.com/official/en_us/topics/company/2017/Global-Internet-Forum-to-Counter-Terrorism.html

[162] *See* P. Gill & E. Corner, *Is There a Nexus Between Terrorist Involvement and Mental Health in the Age of the Islamic State?*, 10 The CTC Sentinel 1 (2017). https://ctc.usma.edu/is-there-a-nexus-between-terrorist-involvement-and-mental-health-in-the-age-of-the-islamic-state

[163] *See* Thomas J. Holt et al, *Internet-Based Radicalization as Enculturation to Violent Deviant Subcultures*, 38 Deviant Behavior McCauley 8 (2017). https://www.tandfonline.com/doi/full/10.1080/01639625.2016.1197704 (Abstract: full report is available to purchase)

to new world views.[164] This opening is then exploited by individuals initiating the radicalisation process. Individuals who feel emotionally isolated, ostracised by society, or who already subscribe to violent ideologies may seek solace and community on the Internet.

Social media in particular has been critical for the development of terrorist groups like ISIS. A 2015 study by Jytte Klausen highlights the key role social media platforms play in publicising the ISIS message and attracting foreign fighters.[165] Twitter was used as a tool for indoctrination that helped the group build an international community for violent extremism. According to a 2016 network analysis, Twitter alone had approximately 3,000 ISIS-supporting accounts active at any given time.[166] Since 2015, Twitter has shut down 360,000 accounts for violating the company's policies related to the promotion of terrorism. However, supporters continue to create new accounts every day.[167] In addition to facilitating the spread of the organisation's ideology, social media also enables radicalised individuals to plan logistics for international travel or domestic terrorism.

While existing research does not present a unified theory of why criminal activities persist online, the majority of studies do highlight "subcultural norms." Scholars have identified factors that predict participation in terrorist movements such as ISIS and Al-Qaeda inspired groups. A 2004 study used network analysis to study a group of 250 jihadists in Europe, finding that individuals are more likely to become radicalised in "clusters" because peer dynamics play an important role in the radicalisation process.[168] This group dynamic coupled with a sense of belonging motivates vulnerable individuals to join terrorist groups motivated by ideology.[169]

---

[164] Shaul Kimhi and Steven Even, *Tangled Roots: Social and Psychological Factors in the Genesis of Terrorism*, 308-22 (2006)
Tore Bjorgo & John Horgan, *Leaving Terrorism Behind: Individual and Collective Disengagement*, New York: Routledge (2009).

[165] Jytte Klausen, *Tweeting the Jihad: Social Media Networks of Western Foreign Fighters in Syria and Iraq*, 38 Studies in Conflict and Terrorism 1 (2015).
https://www.tandfonline.com/doi/pdf/10.1080/1057610X.2014.974948

[166] J.M. Berger & Heather Perez, *The Islamic State's Diminishing Returns on Twitter: How Suspensions are Limiting the Social Networks of English-Speaking ISIS Supporters*, GW Program on Extremism (2016) available at
https://extremism.gwu.edu/sites/extremism.gwu.edu/files/downloads/JMB%20Diminishing%20Returns.pdf

[167] Audrey Alexander, *How to Fight ISIS Online*, Foreign Affairs, April 7, 2017,
https://www.foreignaffairs.com/articles/middle-east/2017-04-07/how-fight-isis-online

[168] Marc Sageman, *Understanding Terrorist Networks*, University of Pennsylvania Press (2004);
https://dl1.cuni.cz/pluginfile.php/502417/mod_resource/content/1/marc%20sageman-understanding%20terror%20networks-university%20of%20pennsylvania%20press%20%282011%29.pdf
Edwin Bakker, *Jihadi Terrorists in Europe, Their Characteristics and the Circumstances in Which They Joined the Jihad: An Exploratory Study*, The Hague: Clingendael Institute (2006).
https://www.clingendael.org/sites/default/files/pdfs/20061200_cscp_csp_bakker.pdf

[169] Jessica Stern, *Terror in the Name of God: Why Religious Militants Kill*, Harper Collins (2003).

7.3 Legal Background

Incitement to ethnic or racial hatred, the basis of much extremist speech, is a criminal offence under UK law.[170] The Terrorism Act of 2006 also defines sites and content that incites or glorifies terrorist acts. The UK Counter Terrorism Internet Referral Unit maintains a list of sites and content that, in their opinion, falls under this definition. As discussed in Chapter V of this review, the UK's hate speech laws do criminalise extremist speech that amounts to an incitement of violence. However, not all extremist speech may meet this legal definition.

The UK does not create any kind of liability for intermediaries like social media platforms. Often the onus is put on Internet companies to determine whether online content should be taken down. However, there is no existing liability in the UK against companies who fail to remove unacceptable content. If the political pressure from the UK and EU is not enough to motivate the necessary response from technology companies, the UK may consider the creation of new "legal liability for tech companies if they fail to remove content. This could, for example include penalties such as fines for companies that fail to take action."[171] However, NGOs such as the Global Network Initiative have argued that governments should not impose direct or indirect liability on intermediaries "on the basis of content sent or created by third parties."[172] Thus, regulation of extremist speech online remains controversial.[173]

7.4 International Legal Approaches

(1) Australia: The Australian government has in place a reporting mechanism for extremist online content.[174] They specify that this content must be violent, or encourage radicalisation towards violence. The Countering Violent Extremism Unit of the Australian Government is implementing a range of projects to respond to the issues of online terrorist radicalisation. These measures include "reducing the impact of terrorist's use of social media by helping people develop the digital

---

[170] *See e.g.*, Racial and Religious Hatred Act (2006). https://www.legislation.gov.uk/ukpga/2006/1/contents

[171] *UK and France Announce Joint Campaign to Tackle Online Radicalization*, Prime Minister's Office, 10 Downing Street, June 13, 2017, available at https://www.gov.uk/government/news/uk-and-france-announce-joint-campaign-to-tackle-online-radicalisation

[172] Global Network Initiative, *Extremist Content and the ICT Sector: A Global Network Initiative Policy Brief* (2016) available at https://globalnetworkinitiative.org/wp-content/uploads/2016/12/Extremist-Content-and-ICT-Sector.pdf

[173] *See* Michael Holden, *Who is an extremist? UK faces legal challenge over strategy to stop radicals*, Reuters, Aug. 17, 2016, available at https://www.reuters.com/article/us-britain-security-extremism/who-is-an-extremist-uk-faces-legal-challenge-over-strategy-to-stop-radicals-idUSKCN10S12H

[174] *See* Australian Government, *Report Online Extremist Material*, available at https://www.reportextremism.livingsafetogether.gov.au

skills needed to critically assess terrorist's claims and promote alternative messages online."[175]

(2) European Union: The EU has an established standard requiring private companies to remove hate speech online, including extremist speech. The EU treats terrorist propaganda online as hate speech under their existing legal framework. The European Commission has implemented a "code of conduct" in partnership with Facebook, Microsoft, Twitter, and YouTube, "to counter terrorist propaganda" and respond to illegal hate speech. The Code of Conduct requires the removal of material after it has been flagged to the company. The EU Commission has also created a Civil Society Empowerment programme which provides 10 million euros to support civil society in "increasing the volume and effectiveness" of alternative narratives online, which counter extremist speech.[176]

(3) United States: The First Amendment of the United States protects most speech from government regulation. Under Brandenburg v. Ohio, laws that criminalise the dissemination of material advocating terrorism would likely be deemed unconstitutional under US law.[177] In order to be legally restricted terrorist propaganda would need to amount to an "incitement" that is "likely to produce imminent lawless action." Anything short of this would not be constitutional under US law. This makes it difficult for the US Congress to pass any laws regulating terrorist content online. As a result, radical content online has thus far been managed by the technology companies and social media platforms. Despite the inability to regulate, US law enforcement agencies such as the FBI monitor the social media presence of radicalised people and use this to investigate potential terrorist threats offline.

7.5 Proposed or Possible Solutions

Solutions to the problem of online radicalisation are politically sensitive and subject to controversy.[178] Some British policy makers and law enforcement officials call for stricter

---

[175] *Id*; *see also* M. Nasser-Eddine et al., *Countering Violent Extremism Literature Review*, Australian Government Technical Report, available at https://apps.dtic.mil/dtic/tr/fulltext/u2/a543686.pdf

[176] European Commission Press Release, *EU Internet Forum: A Major Step Forward in Curbing Terrorist Content on the Internet*, Dec. 8, 2016, available at https://europa.eu/rapid/press-release_IP-16-4328_en.htm

[177] *See Brandenburg v. Ohio*, 395 U.S. 444, 448 (1969) https://supreme.justia.com/cases/federal/us/395/444
See also Kathleen Ann Ruane, *The Advocacy of Terrorism on the Internet: Freedom of Speech Issues and the Material Support Statutes*, Congressional Research Service (2016) available at https://fas.org/sgp/crs/terror/R44626.pdf

[178] Mark Scott, *After Terror Attacks, Britain Moves to Police the Web*, June 19, 2017, available at https://www.nytimes.com/2017/06/19/technology/britain-encryption-privacy-hate-speech.html (Subscribers only)

regulation of extremist messaging and its distribution online. This means further regulation of social media platforms such as Google, Facebook, and Twitter. The technology companies as well as privacy and civil liberties groups often counter that the government's proposals go too far.

(1) Civil Society Solutions

i. Review and continued development of resources for individuals vulnerable to radicalisation.[179] The availability of counselling and psychological services for individuals who show signs of potential radicalisation may help deter them from committing violent acts.

ii. Interfaith efforts to deter individuals from being radicalised.

(2) Technology Solutions

i. Continue to improve reporting procedures on social media platforms to allow individuals to flag probable hate speech. In the past, Twitter struggled with the reporting procedures in balancing the right to free expression with the need to police extremist content.[180] Reviewing existing reporting procedures and conducting further tests to make sure they are effective is one way to reduce the amount of radicalising content on social media platforms.

ii. Increasing research on artificial intelligence technology to automatically flag and remove terrorist propaganda. While Facebook is using and developing this kind of technology, further work is needed to perfect the algorithms that distinguish between acceptable online content and extremist speech.[181] Investment in the development of this technology could automate and improve policing of this kind of content on social media platforms.

iii. Counterspeech: Technology companies engage in 'counterspeech' initiatives to stymie extremist narratives online. These initiatives include YouTube's Creators for Change, Jigsaw's Redirect Method, Facebook's P2P and OCCI, Microsoft's partnership with the Institute for Strategic

---

[179] The UK has an existing intervention and de-radicalisation programme. For discussion of de-radicalisation and the debate surrounding appropriate strategies *see* Rashad Ali, *De-Radicalization and Integration: The United Kingdom's Channel Programme*, (2015) https://extremism.gwu.edu/sites/extremism.gwu.edu/files/downloads/Rashad%20Ali.pdf

[180] Mark Scott, *After Terror Attacks, Britain Moves to Police the Web*, June 19, 2017, available at https://www.nytimes.com/2017/06/19/technology/britain-encryption-privacy-hate-speech.html (Subscribers only).

[181] Mark Scott, *After Terror Attacks, Britain Moves to Police the Web*, June 19, 2017, available at https://www.nytimes.com/2017/06/19/technology/britain-encryption-privacy-hate-speech.html (Subscribers only).

Dialogue for Counter-Narratives on Bing, and Twitter's Global NGO training programme.[182]

7.6 Further Research

As mentioned above, further research is needed in the following areas:

(1) Causes of seeking extremist content online. Further research is needed to disentangle the factors that influence a person to seek out extremist movements online.

(2) The influence of offline factors in online radicalisation. Study is needed to determine whether similar offline experiences motivate individuals to seek these online communities.

(3) What motivates individuals to act on radical messages received online. Since the majority of persons exposed to radical messages never engage in violence, further research is needed to explain how individuals ultimately decide to act upon the radical messages received.

(4) The different kinds of online radicalisation. While much research focuses on international terrorism and recruitment, social media is also used by white supremacist groups, far left and far right movements. Further research could be conducted to determine the differences between these types of radicalisation movements, and which poses the most immediate threat.[183]

7.7 Major Organisations

This section lists some of the major organisations cited by the media as key players in the dialogue surrounding online terrorist radicalisation. This list was compiled by amassing organisations that work with directly impacted communities, governments, and NGOs to combat terrorist radicalisation online. Organisations were included here regardless of whether they focus primarily on online spaces or whether they simply organise one-off campaigns related to this kind of content.

---

[182] *See* Microsoft Corporate Blog, *Microsoft partners with Institute for Strategic Dialogue and NGOs to discourage online radicalization to violence*, Apr. 18, 2017, available at https://blogs.microsoft.com/on-the-issues/2017/04/18/microsoft-partners-institute-strategic-dialogue-ngos-discourage-online-radicalization-violence

[183] *See* Thomas J. Holt et al, *Internet-Based Radicalization as Enculturation to Violent Deviant Subcultures*, 38 Deviant Behavior McCauley 8 (2017) https://www.tandfonline.com/doi/full/10.1080/01639625.2016.1197704 (Abstract: full report is available to purchase)
See also See also Clark McCauley & Sophia Moskalenko. *Mechanisms of Political Radicalization: Pathways Toward Terrorism*, 20 Terrorism and Political Violence 3 (2008) https://www.tandfonline.com/doi/abs/10.1080/09546550802073367

The following organisations are listed in no particular order:

(1) Online Civil Courage Initiative (UK Organisation): OCCI is an initiative run by an NGO called ISD. The initiative is funded by Facebook, and it seeks to combat hate speech and extremism online.

(2) Hate Speech International (International NGO): Focuses on elevating the public understanding of extremism, reporting on hate speech and hate crimes. While they do not focus exclusively on Internet radicalisation or Internet hate speech, they have produced some reports on ISIS's use of social media for radicalisation. [184] Their two-year pilot project is supported by the Norwegian Freedom of Expression Foundation and the Norwegian Ministry of Foreign Affairs.

(3) Jo Cox Foundation (UK Charity): a memorial charity that dedicates itself to various causes. It recently partnered with Facebook's Online Civil Courage Initiative to counter hate speech and counter extremist content online.[185]

(4) Community Security Trust (UK Charity): a Jewish charity that published a comprehensive guide for those affected by Hate Crime. They also recently partnered with Facebook's Online Civil Courage Initiative to counter online hate speech and extremist content.[186]

(5) Imams Online (Online Organisation): Network of Imams and Muslim leaders dedicated to educating the public about Islamophobia, facilitating interfaith dialogue supporting the Muslim community, countering online extremism and opposing hate speech. They are also among Facebook's OCCI partners.[187]

(6) TellMAMA (UK Organisation): provides a reporting mechanism for victims of anti-Muslim bigotry and hate speech. They are dedicated to challenging anti-Muslim narratives and where there are "blogs, statements, or news articles which promote them." They have also partnered with Facebook's Online Civil Courage Initiative to receive training on identifying extremist content online.

---

[184] *See The Islamic State Propaganda Machine*, Hate Speech International Report (2016) available at https://www.hate-speech.org/the-is-propaganda-machine

[185] *See* Dale Walker, *The Online Civil Courage Initiative Will Help Organizations Fight Extremist Content*, June 23, 2017, https://www.itpro.co.uk/public-sector/27149/facebook-launches-uk-initiative-to-tackle-online-hate-speech

[186] *Id.*

[187] *Id.*

(7) George Washington University Program on Extremism (US Academic Institute): is an organisation of policy analysts and academics dedicated to providing empirical analysis of the threat posed by the Islamic State. Its members frequently produce papers on the social media strategies of terrorist organisations, particularly ISIS.

(8) Counter Extremism Project (International Organisation with Offices in London, NY, and Brussels): is a "not-for-profit, non-partisan, international policy organisation formed to combat the growing threat from extremist ideologies." Among its projects is a social media campaign to "identify and reveal the extremist threat and directly counter extremist ideology and recruitment online."

(9) Global Internet Forum to Counter Terrorism (US organisation): is the recently formed coalition of Internet companies like Facebook, Microsoft, Twitter, and YouTube aimed at dealing with violent extremist content online. Their leadership includes a former US Homeland Security Advisor and several former government officials on the Advisory Board.

8. Ethical Design of Technology

8.1 Definitions

Technoethical design refers to the process of designing technologies in an ethical manner, involving stakeholders in participatory design efforts and considering the possible harms of particular technologies on society.[188]

8.2 Vulnerable Populations & Impact

The goal of ethical design is to prevent future cyber abuses and harms to individuals and groups. For instance, ethical design questions are raised by technologies like addictive smartphone interfaces, tracking cookies, artificial intelligence, and algorithms that predict criminal recidivism.

The interdisciplinary field of technoethics has a long academic history reaching back to the early 1940s.[189] Today, computer ethics can be approached from a variety of different angles such as the ethics of conduct and practice among computer professionals, the consequences of computerisation and automation, and the ways in which technology changes the practice of ethics more generally.[190]

Unlike the previous chapters in this review on cyber abuse, technoethics deals with the prevention of future cyber abuses.[191] A critical ethical analysis of emerging technologies can help the ICT sector pre-empt harms to individuals before they arise.[192] This section will give a broad overview of some technologies that raise these kinds of imminent ethical design issues, breaking them into the following subcategories:

---

[188] Rocci Luppicini, *Technoethics and the evolving knowledge society*, Hershey: Idea Group Publishing (2010).

[189] MIT Professor Robert Weiner is credited with founding the field of computer ethics during World War II while inventing a smart cannon that could track the location of an airplane. See Terrell Ward Bynum, *A Very Short History of Computer Ethics* (2007) available at https://www.cs.utexas.edu/~ear/cs349/Bynum_Short_History.html

[190] *See* David J. Pullinger, *Moral Judgments in Designing Better Systems*, 1 Interacting with Computers 1 (1989). https://academic.oup.com/iwc/article-abstract/1/1/93/686051 *See also* David J. Pullinger, *Information Technology: The Ethical Task*, Gospel and Culture Newsletter (1994).

[191] *See generally*, W. Richard Bowen, *Ethics and the Engineer: Developing the Basis of a Theological Approach*, Studies in Christian Ethics (2010) https://journals.sagepub.com/doi/pdf/10.1177/0953946810368021

[192] For discussion of the responsibility of technologists to design ethically, *see e.g.*, Mario Bunge, *Towards a Technoethics*, 61 The Monist 1 (1977).

(1) Time Well Spent & The Attention Economy

Cell phones, social media platforms, and online shopping platforms are increasingly designed to maximise the amount of time a person spends using them. In his 2016 book, The Attention Merchants, Tim Wu argues that there are deeply rooted business reasons for this "attention economy."[193] Since the success of technology often depends on the number of users and the extent of their attention, products are sometimes designed with addictive properties. Tristan Harris, a former design ethicist at Google, argues that platforms like Google, Facebook, and Apple "aren't neutral" and that the technological design is often built to "exploit" human "lower-level vulnerabilities."[194] A study analysing 200,000 iPhone app users concluded that the apps that make users least happy are the ones they spend the most time using. Apps like The Weather App, Podcasts, Kindle, Evernote and Spotify, averaged under 30 minutes of use daily and reportedly made users most happy. By contrast, apps averaging 45 minutes or more of daily use such as Facebook, WeChat, Candy Crush, or Grindr had higher percentages of unhappy users. Similarly, a 2017 study in Denmark concluded that Danes who stop using Facebook for a week are "happier, less angry, and less lonely than those who continue checking the social network as usual."[195] These studies pose the question of why users spend so much time on applications that make them unhappy. Further research is needed to determine the addictive qualities of particular technologies and how ethical considerations can factor into the production process.[196] More broadly, the wellbeing of users in the attention economy should be an ethical consideration in the design of technology.

(2) Online Anonymity and Privacy: Tracking Cookies

Ethical issues in design often centre around anonymity and privacy online. Tracking cookies can be used by a third party with whom the user has no relationship to identify a particular user or a computer. These kinds of cookies track the online behaviour of a user on a website. For instance, they can help third party vendors provide targeted advertising or are applied to collect data on a user's shopping preferences. According to a 2010 New York Times Article, cookies "are

---

[193] Tim Wu, *The Attention Merchants*, Knopf (2016).

[194] Andrew Keen, *The 'attention economy' created by Silicon Valley is bankrupting us*, TechCrunch, Jul. 30, 2017, available at https://techcrunch.com/2017/07/30/the-attention-economy-created-by-silicon-valley-is-bankrupting-us

[195] Lucie Rychla, *Danish Research: Facebook Makes Users Sad, Depressed and Lonely*, CPH Post Online, Jan. 2, 2017, available at https://cphpost.dk/?p=76900

[196] Nithin Coca, *Why Your Favorite Apps Are Designed To Addict You*, The Daily Dot, Jan. 31, 2016, available at https://kernelmag.dailydot.com/issue-sections/features-issue-sections/15708/addicting-apps-mobile-technology-health

used by virtually all commercial Web sites for various purposes, including advertising, keeping users signed in and customising content."[197] This type of software may be ethically problematic because it passes a user's information on to a third party, often without the user's permission. Even when the user's consent is explicitly requested on a website, they may not always understand the nature of tracking cookies.

(3) Artificial Intelligence Design

The ethics of artificial intelligence ("AI") is typically divided into two branches: robo-ethics and machine ethics. Robo-ethics deals with the ethics of robotic technology and other artificially intelligent beings.[198] Machine ethics, by contrast, deals with the ethical implications of automated algorithms and agents. Predictive algorithms using artificial intelligence technology, for example, have been the subject of debate in the field of technoethics. A 2016 investigation by ProPublica found that a software used in the United States to predict criminal recidivism discriminated against black people.[199] This kind of software is often used in sentencing hearings, meaning that discriminated parties may be subject to higher criminal sentences because of these results.

This is only one example of the AI's fertile ground for ethical research.[200] The World Economic Forum identified nine other ethical issues in artificial intelligence.[201] One issue is unemployment and how jobs would be changed by automation. If some jobs are changed or eliminated by AI, the economy would have to respond to the change. Other issues noted include tech addiction and dependency, cyber security, protecting against unintended consequences of automation, and maintaining control over AI systems. This illustrates the breadth

---

[197] Miguel Helft & Tanzina Vega, *Retargeting Ads Follow Surfers to Other Sites*, NYTimes, Aug 29, 2010, available at https://www.nytimes.com/2010/08/30/technology/30adstalk.html

[198] *See e.g.*, Nick Bostrom, *Superintelligence: Paths, Dangers, Strategies*, Oxford University Press (2014).
For information on controversy regarding robo-ethics research, *see* Mark Henderson, *Human Rights for Robots? We're Getting Carried Away*, The Times, Apr. 24, 2007, available at https://www.thetimes.co.uk/article/human-rights-for-robots-were-getting-carried-away-xfbdkpgwn0v (subscription)
C.f. Robots Could Demand Legal Rights, BBC News, Dec. 21, 2006, available at https://news.bbc.co.uk/2/hi/technology/6200005.stm

[199] Julia Angwin et al., *Machine Bias*, ProPublica, May 23, 2016, available at https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing

[200] *See* Cennydd Bowles, *The Ethics of Digital Design*, July 13, 2015, available at https://www.designcouncil.org.uk/news-opinion/ethics-digital-design

[201] Julia Bossman, *Top Nine Ethical Issues in Aritifical Intelligence*, World Economic Forum, Oct. 21, 2016, available at https://www.weforum.org/agenda/2016/10/top-10-ethical-issues-in-artificial-intelligence

and diversity of ethical issues in AI and the need for ethical inquiry in the innovation process.

8.3 Legal Background

Two of the three subcategories of technoethics above remain within the ethical field and have not yet received legal attention. The exception is tracking cookies, which was subject to some controversial legislation.

Under the UK laws based on the EU's Cookie Directive, websites must inform users if they are using cookies. There must be a clear explanation of what cookies are and what they do, requesting the user's consent. While consent can be "implied" rather than explicit, it "must be knowingly given."[202] According to the Information Commissioner's Office, there is an exception for cookies that are "essential to provide an online service at someone's request (e.g. to remember what's in their online basket, or to ensure security in online banking.)"[203] This law was widely critiqued on the grounds of not addressing privacy concerns and serving as mere "redundant box-ticking."[204]

8.4 International Legal Approaches (Tracking Cookies only)

(1) Australia: Under the Australian Privacy Act, the information collected by online advertisers using tracking cookies may not be sufficient to identify a user.[205] As a result, companies using tracking cookies or other kinds of online behavioural advertising ("OBA") may not need to comply with rules in the Privacy Act about how personal information should be handled. In Australia, general information about the sites a user visits and their interests would not rise to the Privacy Act's definition of "personal information."

(2) European Union: In 2009, the EU attempted to reign in tracking cookies and re-targeting with a Cookie Directive that would later motivate the UK's own domestic law. It defined four types of cookie: 1) strictly necessary 2) performance 3) functional, and 4) targeting. The main problem with the directive is that it required explicit consent for all of these, in practice negating its effectiveness.

---

[202] *Cookies and Similar Technologies*, Information Commissioner's Office, available at https://ico.org.uk/for-organisations/guide-to-pecr/cookies-and-similar-technologies

[203] *Id.*

[204] Nicole Kobie, *Why the Cookies Law Wasn't Fully Baked- And How to Avoid Being Tracked Online*, The Guardian, March 19, 2015, available at https://www.theguardian.com/technology/2015/mar/19/cookies-how-to-avoid-being-tracked-online

[205] *See* Privacy Fact Sheet, Australian Government, Office of the Australian Information Commissioner, available at https://www.oaic.gov.au/privacy/your-privacy-rights/advertising-and-marketing/targeted-advertising/

(3) United States: Use of cookies by US websites and online service providers is routine and not illegal, so long as the cookie data is not combined with personal identifying information. However, when cookies are used to store personal identifying information, some legal challenges may be possible under other statutes such as the federal Wiretap Act or Stored Communications Act.[206]

8.5 Proposed or Possible Solutions

(1) Civil Society Solutions

Research and implement applied methodologies for the ethical assessment of new technologies. A 2011 paper proposing a meta-methodology for the ethical assessment of new technologies notes that there are very few such structured methodologies in place.[207] The ICT sector, in partnership with government, can apply such methodologies such that they are institutionalised in the innovation process. The goal of this is to help organisations and individuals conduct ethical assessments of emerging technologies.

(2) Technology Solutions

Tracking Cookies: Websites and browsers may design their products to minimise the invasiveness of tracking cookies. For instance, Safari's default is to not allow third-party cookies. Other browsers and extensions such as Ghostery have been created which enable users to easily detect and control trackers. Additionally, the Do Not Track header is the proposed HTTP header field, requesting that web applications disable certain tracking features, though its effectiveness will depend on advertisers' willingness to comply.

(3) Legal Solutions

Tracking Cookies: The main problems with existing EU law on tracking cookies may be solved with the EU's GDPR, due May 2018, though time will tell whether this is effective in practice

---

[206] *See e.g.*, *In re Pharmatrak, Inc*., No. 02-2138, 2003 WL 21038761 (1st Cir. May 9, 2003); https://caselaw.findlaw.com/us-1st-circuit/1136968.html
see also Judnick v. Doubleclick, No. 000421 (Cal. Super. Ct. filed, Jan. 27, 2000) https://www.jstor.org/stable/40688010

[207] Ian Harris, Richard C. Jennings, David J. Pullinger, Simon Rogerson, Penny Duquenoy, *Ethical Assessment of New Technologies: A Meta-Methodology*, Journal of Information, Communication & Ethics in Society (2011) https://www.longfinance.net/media/documents/ethical-assessment.pdf

8.6 Further Research

As mentioned above, further research is needed in the following areas:

(1) The addictive properties of technology products and their effects on consumer wellbeing.

(2) Existing ethical design methodologies in the technology sector and their effectiveness.

(3) Ethical solutions to discrimination problems in predictive algorithms.

(4) Economic research related to the impact of AI automation on the labour force, and the ethical implications for innovators of labour-disruptive technologies.

8.7 Major Organisations

This section lists some of the major organisations cited by the media as key players in the dialogue surrounding technoethics. Organisations were included here regardless of whether they focus primarily on online spaces or whether they simply organise one-off campaigns related to this kind of content.

The following organisations are listed in no particular order:

(1) British Computer Society (Ethics Group and Strategy Panel): The BCS is the professional organisation for IT and Computing specialists in the UK. It collaborates with government, industry and relevant bodies to establish good practices and common standards for the role of technology in society. ICT Ethics Specialist Group of the BCS focuses on the ethical implication of ICT provision, use and development.

(2) Time Well Spent (Online Organisation): dedicated to promoting ethical design of technology that serves user interests. They call for ethically designed products that serve user interests, rather than promote corporate monetary gains. It was founded by a current Oxford Internet Institute doctoral candidate, James Williams.

(3) Design Council (UK Organisation): a charity recognised as a leading authority on the use of strategic design. They produce some research on ethical design of technology but they also focus on many other fields. They "use design as a strategic tool to tackle major societal challenges, drive economic growth and innovation, and improve the quality of the built environment." They are also the UK government's advisor on design. They are funded by corporate partnerships and the UK government.

(4) Ind.ie (UK Organisation): a small, politicised company dedicated to producing ethical technology, privacy and human rights. They also raise awareness about ethical issues in design. It is a small team of two people seeking to hire more developers. They do not accept venture capital funding and thus are seeking resources for sustainability.

(5) Digital Ethics Lab (Oxford Internet Institute): an academic cohort dedicated to addressing ethical challenges posed by digital innovation. They attempt to "identify the benefits and enhance the positive opportunities of digital innovation as a force for good."

(6) CLIP Library and Information Association (UK Organisation): seeks to teach and promote the spread of "information and library skills."

(7) Engineers Without Borders (UK Organisation): conducts development projects surrounding engineering education. Deals with ethical issues related to ICT use in human development.

(8) Ethical IT (UK Organisation): provides services across the social change sector to help clients use technology for social aims, focusing primarily on environmental and social issues.

(9) MIT Media Lab (US University Lab): is an interdisciplinary academic research lab dedicated to technology. They recently partnered with the Berkman Klein Center at Harvard to begin a 27 million dollar initiative on the ethics and governance of artificial intelligence.[208]

(10) Berkman Klein Center (US University Institute): an academic think tank dedicated to the research of cyberspace. As mentioned above, they recently partnered with the MIT media lab for a research initiative on the ethics of artificial intelligence.

(11) Alan Turing Institute Data Ethics Group: a group within the larger data science institute dedicated to setting the Institute's research agenda in data ethics. They are very well funded by a number of partnerships including HSBC and academic institutions such as the University of Cambridge.

[208] MIT News, *MIT Media Lab to participate in $27 million initiative on AI ethics and governance*, January 10, 2017, https://news.mit.edu/2017/mit-media-lab-to-participate-in-ai-ethics-and-governance-initiative-0110

9. Conclusion

As illustrated above, cyber abuse can manifest itself in a number of ways. Chapter 1 discussed cyber bullying, highlighting an apparent contradiction in the literature. While some scholars view it as the primary threat, other data shows that it remains less common than face-to-face bullying. While young people are the primary victims, further sociological research is needed to determine the effects of cyber bullying on adults and the elderly. Differences in social media behaviour across ages could reveal distinctions between the kind of cyber bullying affecting adults and children. Organisations like Cybersmile run well-funded education campaigns against cyber-bullying of children by their peers. However, further research is needed to determine whether existing online harassment laws sufficiently protect cyber bullying against adults and the elderly.

Chapter 2 discussed the issue of nonconsensual pornography, the distribution of intimate photos without the subject's consent. There are several ways to prevent the harm of nonconsensual pornography. Most of them require the involvement of the Internet platforms that act as hosts for this kind of content. The literature on the legal responsibility of such third-party intermediaries remains underdeveloped. Several enforcement issues and problems in the legislation also make nonconsensual pornography cases difficult to prosecute. In the US, some legal organisations exist to provide aid for victims of nonconsensual pornography. In the UK however, the University of London Queen Mary's legal clinic is one of few dealing exclusively with this issue. Technologically, social media platforms such as Facebook have developed sophisticated devices to identify and remove pornographic content. However, it is difficult to develop technology that can identify nonconsensual pornography in particular. This issue would need a more complex policy solution that involves participation of victims and Internet platforms. Further research is needed to determine the appropriate solution. There is a dearth of organisations developed to preventing the promulgation of nonconsensual pornography and serving those victimised.

Chapter 3 covered issues related to websites that promote eating disorders and suicide. Again, the responsibilities of social media platforms that host this kind of content remain unclear. For instance, further research is needed to explain how and whether the content should be removed from these online spaces. While platforms like Facebook and Twitter often remove content that violates community guidelines, there is little research on how effective these guidelines are at reducing harmful content.

The enforcement issues present with nonconsensual pornography also exist here. The anonymity of online spaces makes it difficult to ensure that inciters of self-destructive behaviour are held accountable. As discussed in Chapter 3, the more obvious policy solutions

such as removing the content can have unexpectedly harmful policy consequences.[209] The liability of third parties such as Internet platforms is a complex legal and social issue. More academic research should address the pros and cons of third-party liability in this context. Many organisations exist that provide aid to those with eating disorders and suicidal ideation. However, there are very few organisations dedicated to combatting the self-harm narratives of websites that promote eating disorders and suicide.

Chapter 4 dealt with fraud and discrimination in online dating platforms. This chapter addressed two distinct sets of problems. The first involves the types of fraud and harassment present in online dating platforms. This includes romance scams, catfishing, blackmail, fraud by the online dating website, stalking and harassment. These types of cyber abuses can be experienced by anyone, regardless of gender or age. Since police can be underinformed about these kinds of issues, victims of such forms of cyber abuses may not be receiving the attention they need.

The second, separate set of problems addressed by this chapter deals with the exclusivity of some online dating platforms. This means that some groups experience forms of discrimination in these kinds of online dating spaces. Members of ethnic minority groups or the LGBTQ+ communities experience increased levels of discrimination in online dating websites. This suggests that existing online dating platforms may not always cater to the needs of these specific communities. Sociological studies suggest that the culture of some online spaces may result in negative experiences for members of minority groups.

Chapter 5 evaluated issues related to online hate speech. One myth about online hate speech is that its harm to victims is minimal, given that they do not suffer from physical violence. This chapter briefly explains the harmful nature of hate speech and the importance of creating positive cultures in online spaces. Technology corporations like Facebook and Microsoft have partnered with civil society organisations to combat hate speech in social media. This initiative, the Online Civil Courage Initiative ("OCCI"), grants financial and marketing support as well as training to UK NGOs working to counter hate speech and online extremism. One major challenge to policing hate speech online is that it is difficult to ascertain perpetrators, given online anonymity. Additionally, free speech laws vary greatly across jurisdictions and Internet corporations operate in many countries. This legal variety makes a regulatory scheme across countries difficult to implement. This is one area that may benefit from additional research and policy guidance.

Chapter 6 addressed the various forms of cyber abuse against children. This includes child pornography, online solicitation and sex trafficking. Given the importance of this topic, there is a wealth of economic resources already devoted to combatting cyber abuse against children. This chapter cited a number of NGO and government organisations dedicated to the

[209] *See supra* note 58.

issue. Academically, the field could benefit from further research on how or whether mobile technology has changed these risks for children. The increased ease with which a child can access a camera and social media platforms on mobile devices may have changed the landscape of risks. Studies examining the effectiveness of online safety campaigns, particularly those related to mobile devices, would be a valuable contribution to this field.

Chapter 7 explores online terrorism radicalisation, paying particular attention to the question of whether online spaces have changed the radicalisation process. Terrorist groups like the Islamic State of Iraq and Syria ("ISIS") became increasingly adept at locating and recruiting new members using social media. Twitter, in particular, was the main platform for ISIS recruitment. The issues related to the responsibility of social media platform mentioned in chapters 3, 5, and 6 are also present here. There is some debate on whether third parties like Twitter should be held responsible for criminal or nefarious activities that take place on their platforms. The OCCI initiative mentioned in Chapter 5 also operates to counter extremist messaging on platforms. There are several organisations from many religious, ethnic, and national backgrounds working on this project. However, some psychological and sociological research could be helpful on the effectiveness of counter-narrative campaigns in reducing online radicalisation. Additionally, companies can continue to develop technology that helps identify and remove this kind of content automatically from platforms like Twitter. Legal and technical barriers to this should continue to be explored.

Finally, Chapter 8 discusses issues related to the ethical design of technology. This is a broad field with a long history. However, some of its modern manifestations may be important in preventing future kinds of cyber abuse or harmful Internet behaviour. This chapter gave an overview of the work of organisations such as Time Well Spent, which have begun monitoring the addictive properties of technology. The goal of this branch of technoethics is to promote ethically designed technology that does not monopolise the time of the user or promote addictive behaviours. This has been mainly applied to mobile apps and social media platforms like Facebook. Finding further applications for this ethical lens and the other ethical models discussed in this chapter could provide fertile ground for future research. Additionally, this chapter covered the ethical issues related to tracking cookies and privacy.

In summary, there are many equally-pressing issues related to cyber abuse. However, they are not all equally researched or resourced. Issues such as nonconsensual pornography may receive media attention, but there are very few NGOs in the UK dealing with this issue relative to its importance. There are few information campaigns defining nonconsensual pornography, reaching out to victims, and apprehending perpetrators. The visibility granted by social media platforms like Instagram makes victims vulnerable to repeated invasions of privacy. There should be more organisations dedicated to legal and psychological services for victims. Further sociological research could help ascertain the number of potential victims in the UK and whether existing reporting mechanisms are sufficiently effective.

Academically, one of the highest areas of priority should be further investigation of the responsibility of third parties such as Facebook, Twitter, and other Internet platforms. Since Internet companies are multi-national, establishing clear governance is complicated. Given inconsistent legal obligations, there is a lack of clarity on the responsibilities (legal and ethical) of these corporations in light of issues like online hate speech, cyber-bullying, and websites promoting self-destructive behaviours. Further research could also investigate whether users of technology platforms are informed about their rights in cases of cyber abuse. Empowering users and stimulating research into effective governance schemes for technology corporations could improve the status quo. This is a common thread in cyber abuse more broadly that could benefit from additional academic attention.