Dear reader,

Online harassment has emerged as a key issue for our time and has caused many people, especially women, to self-censor, step back, or remove their online social or professional presence in hopes of avoiding online harassment.

As a response, in January 2016 we launched HeartMob (iheartmob.org), the first platform of its kind, where users can report the harassment they face and ask a community of bystanders to support them. The project won "Best New Product" at Netroots Nation, the largest progressive conference in the United States, this year.

Our continuing work in this space has led us to ask: what best practices and policies exist to address online harassment? In this quickly changing field, we want to know what people have tried and what has been working. We are especially eager for solutions that could fill the gaps we’ve identified on the ground, such as inadequate (or nonexistent) police training and the increasingly large role social media companies have in defining the line between free speech and hate speech.

We know from our work addressing street harassment that further criminalizing online harassment can present challenges. These laws disproportionately target people of colour, and many victims do not file a report either because they fear legal systems, don’t think it will change the outcome, or don’t think they will be believed. Yet still, there are some forms of online harassment so heinous as to warrant criminalization, and there are gaps in existing policy where the law simply has not kept pace with the quickly changing landscape shape of online harassment. Ultimately, it is up to the individual being harassed to determine what the best course of action is for them and their families - and it is up to all of us to advocate for more options.

DLA Piper generously put together this comprehensive report comparing online harassment laws across the UK, Australia, Canada, and the US. We hope that you will find this report useful as you consider and explore where we need to go next to protect the voices of women, people of color, LGBTQ+ individuals, and others who are increasingly marginalized by online harassment.

Sincerely,

Emily May
Co-Founder and Executive Director of Hollaback!
CONTENTS

1. Preface ........................................................................................................... 1
2. Australia .......................................................................................................... 3
3. Canada ........................................................................................................... 14
4. United Kingdom ............................................................................................... 20
5. United States .................................................................................................. 37
1. PREFACE

1.1 This report has been created to inform the charity Hollaback! on how governments across Australia, Canada, UK and USA are attempting to prevent online harassment, and how they are engaging with companies and platforms where it is happening, including:

1.1.1 The relevant legal framework in each jurisdiction;

1.1.2 Laws and policies in force focussing on training the police in dealing with online harassment;

1.1.3 Government level conversation about online harassment and free speech, and the interplay between the two; and

1.1.4 The extent to which each jurisdiction sees online harassment as an area that requires government attention.

1.2 The research in this report focusses on domestic law, and an analysis of international online harassment law falls outside the remit of this note. However it is worth noting that all four jurisdictions (Australia, Canada, the U.K. and the U.S.) have ratified the Council of Europe Convention on Cybercrime ("Convention"). The Convention’s main objective is to pursue a common criminal policy aimed at the protection of society against cyber-crime, mainly by adopting appropriate legislation and fostering international co-operation.

1.3 The Convention addresses a broad range of cyber-related crimes, not all of which come under the auspices of online harassment. Areas of particular focus in the Convention where State parties are obliged to enact domestic legislation to tackle, and which are likely to offer redress to victims of online harassment once such domestic legislation is enacted include:

1.3.1 Offences related to child pornography (particularly in cases of revenge porn with an underage victim);

1.3.2 Offences related to infringement of copyright and related rights (particularly in cases of revenge porn, or setting up a fake social media account using pictures of the victim); and

1.3.3 Offences related to hate crimes.

1.4 This publication is intended as a general overview and discussion of the subjects therein and does not constitute legal advice. No reliance should be placed on this publication without taking further specialist legal advice. DLA Piper UK LLP will accept no responsibility for any actions taken or not taken on the basis of this publication.

1.5 The report has been prepared by lawyers and trainee lawyers from the UK performing desk based research. We have endeavoured to make the report as comprehensive as possible, but it should not be regarded as exhaustive.

1.6 The lawyers and trainee lawyers preparing this report are not experts on online harassment, but have applied their general research skills to create the report.
1.7 All information is accurate at the time of writing, but may not reflect more recent developments.
2. AUSTRALIA

2.1 Summary

The purpose of this research note is to investigate the issue of online harassment in Australia. In particular, this note outlines the relevant legal framework addressing online harassment and discusses how such laws are applied in Australia. Further, the interplay between freedom of expression and protection from harassment will be discussed.

At a State level, on the whole, legislation criminalising stalking amply covers electronic forms of stalking, with the notable exception of New South Wales. However, at a national level, while some progress was made with regards to online harassment (with the Australian Law Reform Commission ("ALRC") briefed to draft a report on issues pertaining to online activities), this progress was put on hold with the ascendancy of Tony Abbott’s coalition government. While the work done by the Commission may be referred to by subsequent governments, it appears unlikely that it will be used by the present government to address online harassment.

2.2 Legal Framework

Commonwealth Statute

Online harassment can give rise to a number of offences under the Criminal Code Act 1995 ("the Act"), which is a Commonwealth Statute.

Cases involving online harassment are currently dealt with under section 474.17 of the Act which establishes a commonwealth offence to use a "carriage service to menace, harass or cause offence". The maximum penalty that may be imposed is three years' imprisonment. "Carriage service" is defined as "a service for carrying communications by means of guided and/or unguided electromagnetic energy".

There are no criminal offences that directly address the act of online harassment, however, there are two other offences contained in the Act which it is submitted may be used in cases of online harassment:

- Under section 474.15 of the Act, it is an offence to send a threat to kill or cause serious harm to another person with the intention of making that person fear that such threats will be carried out. The maximum penalty that may be imposed is ten years' imprisonment;
- Section 478.1 of the Act makes it an offence to log on to another person's online accounts without authorisation. The maximum penalty that may be imposed is two years' imprisonment.

---

2.3 Federal Statute

In addition to the above crimes under the Commonwealth Act, which covers the entirety of Australia, each state has further enacted federal statutes, applicable within the enacting state, which provide additional opportunities for redress in criminal law for victims of online harassment.

2.4 Queensland

National law in Queensland is augmented by the Criminal Code 1899. This contains two main sections which it is submitted may be applicable to cases of online harassment:

- Section 308 establishes an offence, punishable up to seven years' imprisonment, to directly or indirectly cause any person to receive a document threatening to kill them; and
- Section 359B makes it an offence to stalk an individual using electronic communications. The Act prescribes a broad definition of stalking which non-exhaustively includes "leaving offensive material where it will be found by, given to or brought to the attention of, a person", as well as committing an "intimidating, harassing or threatening act". The maximum penalty is five years' imprisonment.

2.5 Victoria

In Victoria, the Crimes Act 1958 complements the Commonwealth Criminal Code Act at a state level, with three key offences capable of satisfaction by online harassment:

- Section 20 makes in an offence to, without lawful excuse, make to another person a threat to kill that person or any other person, intending or being reckless as to whether the other person would fear the threat would be carried out. The maximum penalty is ten years' imprisonment;
- Section 21 replicates section 20's requirements, but relates instead to threats to inflict serious injury. The maximum penalty is five years' imprisonment;
- Section 21A relates to stalking, and is punishable by ten years' maximum imprisonment. The definition of stalking includes contacting the victim, including by text message, email or other electronic communication, or by any other means whatsoever. Subsection (2)(ba) also includes:


4 Subject to an exclusion where an individual: threatens or uses violence against property; possesses a weapon; contravenes an injunction or order imposed by a court or tribunal, in which case the maximum penalty is seven years imprisonment (s 359E).
“publishing on the Internet or by e-mail or other electronic communication to any person a statement or other material - (i) relating to the victim or any other person; or (ii) purporting to relate to, or to originate from, the victim or any other person”.\(^5\)

Other actions defined as stalking include causing an unauthorised computer function in a computer owned or used by the victim or any other person (this includes unauthorised access to or modification of data held in the computer, or unauthorised impairment of electronic communication to or from a computer),\(^6\) and tracing the victim’s or any other person’s use of the Internet, e-mail or other electronic communications.

### 2.6 New South Wales

- In New South Wales, the Crimes Act 1900 is the key piece of state criminal legislation. However, this Act appears relatively scant on sections which may be used in cases of online harassment.
- It is an offence, under section 31 of this Act, punishable up to ten years’ imprisonment, to send or deliver any document that threatens to kill or inflict bodily harm on another person.
- It seems that stalking is only an offence in relation to police or other law enforcement officers in the execution of their duties, persons in a domestic relationship with a law enforcement officer, and students or school staff members while they are at the school.\(^7\)

### 2.7 Western Australia

The Criminal Code 1913 for Western Australia features three main offences which could be used at state level to tackle online harassment:

- Section 338B makes it an offence to unlawfully make threats to kill (punishable by up to seven years’ imprisonment, or more if the offence is racially aggravated) and/or to make any other threats (punishable up to three years’ imprisonment, or more if the offence is racially aggravated);
- Section 338C prohibits a persons from making statements and acts that create a false apprehension to another person as to the existence of a threat or danger; and
- Section 338E establishes an offence of stalking another person with the intent to intimidate that person, or a third person.

### 2.8 Australian Capital Territory

The Crimes Act 1900 relating to the Australian Capital Territory introduces three further measures at a state level in addressing online harassment:

- Sections 30 and 31 of the Act criminalise threats to kill and to inflict grievous bodily harm respectively. The offence is committed if the perpetrator intends, or is reckless as to whether, the other person would fear that the threat would be carried out, and the threat is

---

\(^5\) Crimes Act 1958, S21A(2)(ba)
\(^6\) Crimes Act 1958, Division 3. Subdivision (6)
\(^7\) Crimes Act 1900, Sections 60, 60A, 60B and 60E
made in circumstances in which a reasonable person would fear that the threat would be carried out; and

- Under section 35 of the Act, it is an offence in the Australian Capital Territory to stalk another person in a way that causes apprehension or fear of harm; to cause harm; or to harass. This includes giving or sending offensive material to the stalked person, sending them electronic messages, sending electronic messages about that person to anyone else, or making such electronic messages about them available to anybody else.

2.9 **Northern Territory**

In the Northern Territory, the Criminal Code 1983 contains two key provisions which may provide redress to a victim of online harassment at state level:

- Section 166 of the Code criminalises making, or causing any person to receive, a threat to kill with intent to cause fear, if that threat is of such a nature as to cause fear to any person of reasonable firmness and courage; and

- Section 189 prohibits stalking, including by electronic means such as telephone or electronic messages, that causes physical or mental harm to the person, or arouses fear and apprehension in the person regarding their own safety, or that of another person.

2.10 **South Australia**

In the state of South Australia, the Criminal Law Consolidation Act 1935 details two offences which may be applicable in cases of online harassment:

- Section 19 makes it an offence to send threats to kill or endanger the life of another, intending to arouse fear and apprehension that such threats may be carried out; and

- Section 19AA establishes the offence of unlawful stalking. A person stalks another if on at least two separate occasions they (among other, non-electronic criteria) publish or transmit offensive material by means of the Internet or other electronic communication; or communicate via mail, telephone, facsimile transmission, the Internet or any other form of electronic communication in a manner that could reasonably be expected to arouse fear and apprehension in another person.

2.11 **Defamation Act 2005**

The tort of defamation has "long protected personal reputation from untruthful attacks". Since 2005, the Australian States have adopted uniform defamation laws which, subject to changes expressed in statute, leaves the tort of defamation as defined in the general law untouched. Section 7 of the Act maintains that the distinction between slander and libel remains abolished, meaning that the "publication of defamatory matter of any kind is actionable without proof of special damage".

---


2.12 Common Law

There is no cause of action that directly addresses the issue of online harassment.

The High Court left open the possibility of introducing a common law tort for invasion of privacy in *Australian Broadcasting Corporation v Lenah Game Meats Pty Ltd (2001)*. This case involved an application for an interlocutory injunction to restrain the broadcasting of a film that had been made in a clandestine manner. The respondent invited the court to consider whether a new common law tort of privacy should be implemented to adequately deal with the rapid encroachment into private life. Whilst the court granted an injunction based on the existing tort of confidence, the judgment left open the possibility of a new tort of privacy in the future.

2.13 Policies to train the Police force in dealing with Online Harassment

The Australian Cybercrime Online Reporting Network (“ACORN”) is a national policing initiative of the Commonwealth, State and Territory governments which collaborates with all Australian police agencies. ACORN's agenda is to provide "information on how to recognise and avoid common forms of cybercrime" including cyber-bullying and to provide advice for victims. It achieves this through a national online system that enables members of the public to securely report instances of cyber-crime.

Further, the Australian Federal Police have a partnership with Microsoft Australia, Datacom and the Commonwealth Bank called ThinkUKKnow Australia, a cyber-safety program which aims to educate and raise awareness amongst parents, teachers and carers about how young people are using technology, and how to help them overcome the challenges they may face online, including cyber-bullying. It is delivered in collaboration with state police forces.

In addition to this police-led approach to dealing with online harassment, on 1st July 2015, the first Children's e-Safety Commissioner was appointed as a statutory office within the Australian Communications and Media Authority. The Commissioner provides online safety education for children, a complaints services for those experiencing cyber-bullying, and addresses illegal content.

There do not appear to be any specific laws at commonwealth or federal level that are targeted at the police for when they are dealing with the issue of online harassment.

2.14 Governmental discussion surrounding online harassment and free speech

The coalition government in their campaign election stressed the importance of free speech, and they are unsupportive of heavy handed regulation of the Internet that would impinge on this right. Consequently, the Australian government, like many other jurisdictions, has no desire to impinge upon the fundamental rights of freedom of speech and freedom of expression. However, this stance can become problematic when trying to tackle issues such as online harassment.

Many legal and enforcement methods that combat online harassment encroach on the fundamental right of free speech and therefore have been opposed by the public or have hindered any adoption of stringent regulation. Australian Senator George Brandis stated that "the measure of a society's commitment to political freedom is the extent of its willingness to respect the right of every one of its citizens to express their views, no matter how offensive, unattractive or eccentric they may seem to others." Problematically, online harassment can include the expression by one person of offensive views to another, and therefore limiting this expression results in infringing freedom of speech.

The government has recently been the target of criticism for its e-safety policy, which included the establishment of an e-safety commissioner, notably to advise on child e-safety and tackle cyber-bullying. The commissioner's powers, which include the power to remove material from social media sites, have been said to "clearly threaten free speech", and the new e-safety policy has been described as the government "doing more to restrict free speech than it is to defend it." Consequently, it is unsurprising that the government when looking at online harassment more generally, does not appear to be proposing or discussing forms of stringent regulation of the Internet.

---

2.15 Governmental discussions on the legal framework for harassment

**Serious Invasions of Privacy in the Digital Era**

In 2014, the ALRC published a final report on "Serious Invasions of Privacy in the Digital Era". This was in response to Terms of Reference issued by the Attorney-General on 12 June 2013. This inquiry was undertaken due to a perceived need for a cause of action for serious invasion of privacy, which currently does not exist in Australian law. Such invasions of privacy were considered to "occur with increasing ease and frequency in the digital era, when the mobile phones in our pockets are all potential surveillance devices... and personal information once put online seems impossible to destroy or forget".

The ALRC recommended a new action in tort for serious invasion of privacy, enacted in a Commonwealth Act. They also recommend that the Commonwealth Government enacts surveillance legislation to replace existing state and territory surveillance device laws in a technology neutral manner.

The ALRC go on to recommend that "if a statutory cause of action for serious invasion of privacy is not enacted, state and territory governments should enact uniform legislation creating a tort of harassment".

Since the reference to the ALRC was made, a new government (that of Prime Minister Tony Abbott) has been elected, with the incoming Attorney-General stating that "the government..."
has made it clear on numerous occasions that it does not support a tort of privacy". Nevertheless, the ALRC’s report has been duly finalised, and may be considered by a future government.28

2.16 Legal framework encompassing offline and online harassment

Currently there are both civil and criminal remedies at the state or Commonwealth level available to victims of harassment.29 The fact that some criminal conduct occurs on the Internet makes no difference to the criminality of that conduct.30 Therefore some argue that, in lieu of further regulation of the Internet, the legal framework for offline harassment is sufficient to also address online harassment.31

There are consequently proposals for a Commonwealth Harassment Act, to update and reform the legal framework addressing harassment, an Act which would encompass both offline and online harassment.32 The Australian Law Reform Committee ("ALRC") created the proposal with the aim to clarify and consolidate existing harassment offences stating that "the offences should relate to harassment, irrespective of whether it occurred through online or telecommunications platforms, or through other physical or personal means".33

Therefore, although there are discussions ongoing with a view to reforming the law on harassment, there is no discussion specifically focusing on online harassment and its inherent differences to offline harassment.

2.17 Governmental discussions on invasions of privacy in the digital ERA

**Nexus between privacy and harassment**

An invasion of privacy that is serious may also amount to harassment. Consequently, publishing personal data online or reading private online communications can both be categorised as online harassment and an invasion of privacy. This invasion of privacy is an area of discussion, and the ALRC in particular is keen to address the issue in their proposal for a Commonwealth Harassment Act. The current legal protection offered with regards to invasions of privacy is not deemed sufficient by the ALRC and therefore they have proposed a new tort for serious invasions of privacy. They have also proposed a new tort or civil action for harassment which would aim to encompass legal protections for these invasions of privacy in a digital era, which is discussed below.

**Discussions on the criminalisation of the unauthorised sharing of intimate photos**

The unauthorised sharing of intimate photos is an area which, through the medium of publishing private data without consent, can amount to online harassment. Certain states, notably Victoria and South Australia, have introduced their own laws to criminalise the unauthorised sharing of intimate photos, dealing directly with the issue of revenge pornography. Currently there are no federal laws prohibiting the practice. This however may be set to change as this year the Senate Legal and Constitutional Affairs References Committee has recommended to the federal government to introduce a national law to criminalise the sharing of intimate photos without consent. Labor’s Tim Watts stated that “criminalising the practice would send a strong message that the community did not accept

---


37 See Summary Offences Act 1966 - Sections 41DA and 41DB (inserted in 2014) for state law in Victoria; See Summary Offences Act 1953 (SA), sections 26B and 26 C for relevant state law in South Australia.


the use of the internet to shame or harass.” Although this recommendation is on a particular area, it is evidence of further regulation on negative Internet use being discussed.

2.18 Degree to Which Online Harassment is Seen as an Area That Needs Government Attention

Online harassment is becoming an increasing concern, attracting the concern of governmental bodies, NGOs and social media sites. Facebook and Twitter have become increasingly aware and proactive to the issue, for instance by making it easier for users to report any violations. However, online harassment could be said to not be seen as an issue requiring a high degree of government attention, perhaps because a certain level of responsibility is perceived by the public to fall with the social media sites themselves. This is demonstrated in a public petition for 'Charlotte's Bill' to be introduced in Australia, a Bill to tackle online harassment, and which gave an increasing amount of responsibility to social media sites as well as calling the government into action.

However, issues such as serious invasions of privacy and revenge pornography are viewed by the public as requiring government intervention or legislative change, demonstrated by both the media attention on the issue and Senate Committee proposals. Another issue that has largely been focused on by the public, charities and the government itself is that of cyber-bullying and online harassment of children. This is an area which has received an increasingly high level of government intervention with the creation of the new Office of the Children’s e-Safety Commissioner, as an independent statutory office within the Australian Communications and Media Authority.

---


41 See the following: ACORN; Bully Zero Australia Foundation. See the following actions of social media sites: Facebook has introduced a tool available globally to combat online harassment (See further details at http://www.irishtimes.com/news/education/facebook-introduces-new-tool-to-tackle-harassment-online-1.2609652) see also further action taken by twitter at http://www.ibtimes.com/wam-twitter-tackle-problem-online-harassment-women-


2.19 Conclusion

The sentiment in Australia appears to be that online harassment can be adequately tackled through existing commonwealth and federal criminal laws. However, it is apparent that the level of protection against online harassment afforded by some states’ legislation is far less comprehensive than that afforded by other states.

While there has been historical research into the introduction of a Commonwealth Act addressing issues pertaining to online harassment, there has since been a change in the political climate, which sees privacy prioritised above protection from online harassment. Thus any potential progress in protection from online harassment at a national level has been effectively rejected.
3. CANADA

3.1 Summary

The purpose of this research note is to investigate the issue of online harassment in Canada. In particular, this note outlines the relevant legal framework addressing online harassment and discusses how such laws are applied in Canada. Further, the interplay between freedom of expression and protection from harassment will be discussed.

While the existing laws on harassment are drafted widely and therefore can be applied to online harassment with relative ease, it appears that governmental authorities struggle to accurately draw a line between online harassment and expression of opinions covered by the principle of freedom of speech. The Canadian government is, however, taking positive action to address the issue both in terms of police training and governmental strategy.

3.2 Legal Framework

Under federal Canadian law, online harassment can be addressed either under civil law or under criminal law depending on the facts of the case. This note will examine both approaches.

3.3 Federal Law

Civil Law

According to Media Smarts, the Canadian charity for Digital and Media Literacy, there are three ways in which online harassment can be against the law under civil law.\(^{47}\) These three ways in which online harassment can be tackled under civil law are widely cited in other Canadian online resources, and are often attributed to the Media Smarts website, however, these methods of civil redress are not attributed on the Media Smarts website. Further, an independent search of these causes of action has not yielded any results referring to Canadian statute or additional case law. The causes of action, as they appear on the Media Smarts website, are as follows:

3.3.1 Defamation occurs in cases where the harassment takes the form of the harasser causing harm to someone’s reputation by spreading false information about them.\(^ {48}\) The false information may be in the public sphere temporarily (in which case it is called slander) or permanently (in which case it is called libel);

---


\(^{48}\) Murphy v. LaMarsh (13 DLR 3d 484)
3.3.2 Creating an unsafe environment by making the victim feel like he/she cannot go to school without fear of violence, bullying or exclusion. In this case the school can be sued by the victim if it can be shown that the school did not do everything in its power to provide a safe environment. Those who are victims of online harassment may often feel like it is unsafe for them to go to school, for instance, if that is where their online harassers are likely to be. Further, as will be expanded on below, children and teenagers appear to be considered particularly vulnerable to online harassment; and

3.3.3 Responsibility has been imputed for any reasonably foreseeable consequences arising from a harasser's conduct, for example, telling a suicidal person to kill themselves, resulting in them committing the act.

Actions under any of the three limbs outlined above would be actions in tort and possible remedies include compensation and/or injunctive relief. Victims of harassment may sue in both civil and criminal courts but often actions will only be brought in the criminal court because bringing a civil action is very expensive and, further, it may be difficult to obtain substantial damages if the victim cannot show loss.

3.4 **Criminal Law**

Private prosecutions are capable of being brought in Canada, which means that a criminal proceeding can be initiated by an individual, such as a victim of online harassment.\(^{49}\)

Under section 264 of the Criminal Code\(^ {50}\) harassment is a crime punishable by up to 10 years in prison. Harassment may take the form of:

3.4.1 repeatedly following from place to place the other person or anyone known to them;

3.4.2 repeatedly communicating with, either directly or indirectly, the other person or anyone known to them;

3.4.3 besetting or watching the dwelling-house, or place where the other person, or anyone known to them, resides, works, carries on business or happens to be; or

3.4.4 engaging in threatening conduct directed at the other person or any member of their family.


Section 264 has been drafted widely to cover all possible forms of harassment and it specifically states that the threats may be conveyed, uttered or caused to be received “in any manner”, suggesting that it includes all forms of communication, whether they be online or offline. There is no separate provision in the Criminal Code addressing online behaviour only.

Section 319 of the Criminal Code deals with the public incitement of hatred, and is drafted so as to cover incitement “in any public place”, via communication that includes “by telephone, broadcasting or other audible or visible means”. It would thus appear that this section would cover statements inciting hatred online.

In addition the Criminal Code states that a defendant may be imprisoned for up to two years for publishing defamatory libel and for up to five years for publishing defamatory libel which the defendant knows to be false. This provides a more powerful deterrent than civil action, but equally, the threshold for imposing such a serious punishment on a defendant is higher than in civil action, making it imperative that the claimant be able to prove their case beyond reasonable doubt.

As stated above, an action in criminal law is often a less expensive route for the victim. However, the burden of proof in the criminal courts is higher and, as will be discussed further below, it may be difficult to show that the harasser's conduct amounted to harassment rather than being merely an expression of opinions.

3.5 Provincial and Territorial Law

Some states have created more specific laws to deal with the ever increasing problem of harassment.

Ontario has a section in the Education Act (section 1.2) prohibiting bullying, and it is expressly stated that this includes cyber-bullying.

In Quebec, schools are strongly encouraged to take action to tackle all forms of harassment and they have a legal obligation to create anti-bullying plans in which all staff have to take part.

Alberta went a step further and revised the Education Act in 2012 to not only to include cyber-bullying but also to require students to report cyber-bullying should they witness it. Penalties for non-compliance include suspension and expulsion from school.

The increasingly strong stance taken in some states reflects the general acknowledgement of harassment being a serious issue that has evolved with the increased use of technology to

---

51 Criminal Code (R.S.C., 1985, c. C-46) sections 300-301
52 For more details on how the Education Act was amended please see Bill 14, Anti-Bullying Act, 2012 published by the Legislative Assembly of Ontario at http://www.ontla.on.ca/web/bills/bills_detail.do?locale=en&BillID=2550
53 Education Act (R.S.Q., chapter 1-13.3) section. 75.1
54 Sections 31 (division 1) and 36-37 Education Act 2012 (Alberta, chapter E-0.3)
take on new forms which are not adequately addressed by the current law. The fact that so many legal developments are focused on the education sector suggests that particularly children are considered vulnerable to online harassment and as such should be protected from it by law.

3.6 Discussion Surrounding Online Harassment and Freedom Of Expression

Freedom of expression is a long-enshrined part of Canadian life and is found in Section 2(b) of the Charter of Rights and Freedoms. However, as valuable as this right is it is not absolute and is subject to reasonable limits prescribed by law as can be demonstrably justified in a free and democratic society.

The most notable examples of these reasonable limitations are sections 264 and 319 of the Criminal Code, dealing with criminal harassment and public incitement of hatred respectively. These applies equally to online and offline forms of communication as is made clear in the legislation where communication is defined widely including “communicating by telephone, broadcasting, or other audible or visible means.”

A recent criminal case law example of this interplay being discussed is in the case of R v Elliott, which saw the Ontario Court of Justice according such a weight to freedom of expression as to render the requirements for harassment not made out. This case involved Gregory Elliott sending numerous tweets of a homophobic nature over the course of several months to two women.

The Ontario Court of Justice ruled that there had been no offence. The most important factor in this case was the fact that the women did not fear for their safety. This may be the first case in Canada to analyse the use of Twitter in relation to freedom of expression, and the judge described Twitter as “a public forum open to different opinions.” It was noted that the tweets, although obscene and homophobic, were not threatening and therefore not illegal.

Justice Brent Knazman specifically stated that any limitation on Twitter’s use “that is not necessary to prevent criminality will limit its potential”. This conveys the Judge’s unwillingness to interfere with the constitutional right of freedom of expression when using Twitter. He went into further detail particularly focusing on the public nature of hashtags on Twitter analogising them to a “billboard or an orator with a loudspeaker at a street corner”, as such ideas can be spread broadly or someone specific may hear them when passing by.

Therefore the same laws in respect of freedom of expression apply on Twitter as would apply to an orator in a public square. It is submitted that this case shows the difficulties in interpreting the law which arise with modern forms of communication such as Twitter, and the

55 Section 1, The Canadian Charter of Rights and Freedoms.
56 Section 319(7), Criminal Code
57 2016 ONCJ 35
58 Columbia University; Global Freedom of Expression: R v Gregory Alan Elliot Case Analysis; available at https://globalfreedomofexpression.columbia.edu/cases/r-v-gregory-alan-elliott/
distinction of what is acceptable to post online can be unclear. This case however illustrates a great weighting given to the importance of freedom of expression online.

### 3.7 Policies to Train the Police Force in Dealing With Online Harassment

The Department of Justice has published a Handbook for Police and Crown Prosecutors on Criminal Harassment (the "Handbook"), which is intended to provide the police and Crown Prosecutors with guidelines for the investigation and prosecution of criminal harassment cases. It is described as a "starting point" for police and Crown Prosecutors and as such is not legally binding. The Handbook instead details the Department of Justice’s guidelines for best practice. Section 1.6.1 specifically deals with "cyber-stalking" and "online harassment" and makes clear to police and crown prosecutors which sections of the criminal code apply to online situations. The Handbook explains the vast number of ways technology can be used to facilitate harassment and it also makes clear the strong link between online and offline harassment and the likelihood that online harassment will often continue offline.

The Handbook also looks at cyber-bullying and the disturbing news accounts of cyber-bullied teens in Canada committing suicide. It is even suggested that online bullying may be more traumatic than the more traditional forms of stalking due to the fact that, owing to the growth in use of smartphones and other forms of mobile technology, the impact of social media, and forms of bullying conducted through it, is pervasive. The humiliation may also be greater because of the public nature of the bullying or harassment. This guide gives advice for investigating criminal conduct but is far more focused on traditional forms of harassment than online forms, however much of the advice regarding interview techniques of the complainant and evidence collection are still relevant. Of particular relevance is Section 2.6 of the Handbook which specifically advises police and Crown Prosecutors on collecting technological evidence.

The inclusion of online harassment in the Handbook as a unique form of harassment is progressive in terms of educating law enforcement of the changing landscape of criminal activity that they may be faced with.

### 3.8 Government Approach to Online Harassment

Section 1 of the Canadian Charter of Rights and Freedoms gives the Government power to pass laws that limit free expression so long as the limits are reasonable and can be justified. The laws passed by various states (as discussed above) are a manifestation of this power to legislate within reasonable limits and demonstrates that should the government wish to do so, it would be within their power to enact national legislation similar to that found in some states.


The Government's approach to preventing online harassment primarily revolves around education, including the issuing of the above-mentioned Handbook. Another example of this educative approach in action is The Royal Canadian Mounted Police's website which provides Canadians with age-appropriate crime prevention messages to prevent youth crime and victimisation. The Canadian Government's website also provides information on cyber-bullying and the legal consequences on its page "Get Cyber Safe".

In the summer of 2016 the Status of Women minister Patricia Hajdu began a consultation on what the federal government can do tackle online harassment. This is still in the early stages and as of yet there is no news of its progress but it is a step towards online harassment being included in government strategy. Ms Hajdu's campaign is primarily focused on harassment towards women but the principles can be applied to both genders equally.

3.9 Conclusion

The situation in Canada is that laws created for tackling the traditional crime of harassment are being used against the issue of online harassment. It is clear that although these laws are largely satisfactory, the fact that states such as Alberta have felt the need to draft laws specifically tackling the problem shows that more could be done to ensure the whole of Canada has equal protection in this area.

This note concludes that while this is a problem which is being tackled in Canada, specific legislation targeting online harassment as a crime would help clarify the murky boundary between freedom of expression and harassment caused by the plethora of new forms of online communication.

---

4. UNITED KINGDOM

4.1 Summary

The purpose of this research note is to investigate the issue of online harassment in the UK. In particular, this note outlines the core laws and policies addressing online harassment, and policies and laws passed with a view to training the police in dealing with online harassment. Further, parliamentary discussion surrounding online harassment, free speech and the interplay between the two will be addressed, along with discussion of the degree to which the UK Government views online harassment as an issue requiring its attention.

UK law referred to in this note will generally apply to Scotland and Northern Ireland, unless stated otherwise.

4.2 Introduction

In the United Kingdom the approach to addressing online harassment such as cyber-bullying, trolling, and other forms of online harassment has been described as "piecemeal". There is a gradually growing consensus that the laws addressing online harassment require consolidation to ensure that the legislation governing this area reflects the reality of these types of behaviour and can deal with the increasing growth in these types of offences being committed online.

The NSPCC, a children's charity, outlines that cyber-bullying, a type of online harassment, can include:

4.2.1 sending threatening or abusive text messages;
4.2.2 creating and sharing embarrassing images or videos;
4.2.3 "trolling" - sending menacing or upsetting messages on social networks, chatrooms or online games;
4.2.4 excluding children from online games, activities or friendship groups;
4.2.5 setting up hate sites or groups about a particular child;
4.2.6 encouraging young people to self-harm;
4.2.7 voting for or against someone in an abusive poll;
4.2.8 creating fake accounts, hijacking or stealing online identities to embarrass a young person or cause trouble using their name;

---

63 HC Deb 7 July 2016, vol 612, 1065, 1077 and 1086
64 HC Deb 7 July 2016, vol 612
4.2.9 sending explicit messages, also known as sexting; and
4.2.10 pressuring children into sending sexual images or engaging in sexual conversations.\(^6^5\)

Whilst some of these activities are covered by current offences, not all of them are, particularly as there are no specific offences of either cyber-bullying or trolling under UK law. Even where these activities are caught by current laws, there is currently no guarantee of a successful prosecution particularly as these offences are often not prosecuted due to the Crown Prosecution Service ("CPS") or its equivalent in Scotland, the Crown Office and Procurator Fiscal Service ("COPFS")\(^6^6\) considering the prosecution of these offences not to be in the public interest.\(^6^7\)

Commentators have also discussed the need for more practical measures to be put in place, for example additional police resources and training to enable the legal system to cope with the growing amount of offences committed online as the use of social media and other online communications continues to grow.

4.3 Legal Framework

Criminal Law

Harassment

If an individual is subjected to a course of conduct which causes them distress or alarm this may give rise to a criminal cause of action under the Protection from Harassment Act 1997 ("PHA"). The offence of harassment covers a wide range of conduct including verbal harassment, stalking and physical acts meaning that online activities such as cyber-bullying and trolling may be caught under this offence.

Two types of harassment are prohibited under the PHA:

4.3.1 Section 1(1) - this prevents a person from carrying out a "course of conduct" amounting to harassment (by causing fear or distress) providing that person either knows, or ought to know, that his conduct amounts to harassment. That is, a reasonable person would consider that the course of conduct amounts to

---


\(^6^6\) Although COPFS generally take a harder line approach

\(^6^7\) PLC, 'Social media offences', available at [http://uk.practicallaw.com/3-616-4951](http://uk.practicallaw.com/3-616-4951) accessed 9 September 2016
harassment. A “course of conduct” is at least two instances of harassment, which are sequential, rather than distinct and distant events. 68

4.3.2 **Section 1(1A)** - this prohibits a person pursuing a course of conduct which involves harassing two or more persons with the intention of persuading any person (whether or not they are one of the harassment victims) not to do something which they are either entitled or required to do, or to do something which they are not under an obligation to do.

Harassment is a summary offence and a person found guilty of this can be imprisoned for a term of up to six months or given an unlimited fine. 69 A person guilty of pursuing a course of conduct that puts a person in fear of violence, which is an indictable offence under section 4A, can be imprisoned for a term of up to five years in prison. 70

The PHA also applies to Northern Ireland as section 13 of the PHA makes provision for replicating the PHA in Northern Ireland. 71

Although the PHA does apply to Scotland “no new criminal offence of harassment or causing fear of violence” has been created by the Act as “the existing common law in Scotland already covers”, such conduct. 72 It is considered that harassment may amount to criminal conduct under either the offence of breach of the peace or the offence of threats under Scottish common law. 73 The PHA does however provide additional civil remedies, as discussed below.

Where cases of stalking and harassment are linked to racial or religious hatred, prosecutors can also consider prosecuting under section 32 of the Crime and Disorder Act 1998 where there have been two racially or religiously aggravated harassment offences, provided that the racial or religious aggravation test in section 28 is met. 74

Further to this, section 12 of the Domestic Violence, Crime and Victims Act 2004, in addition to extending the availability of restraining orders to all offences (not just those under the PHA), provides the court with the power to make a restraining order even when a defendant has

---


69 Section 2 Protection From Harassment Act 1997

70 Section 4 Protection From Harassment Act 1997

71 Sections 1-7 and Section 12 Protection From Harassment Act 1997; Protection from Harassment Order (N1) 1997

72 HL Deb vol 577, col 920

73 Sections 8-11 Protection from Harassment Act 1997; Marinello v Edinburgh City Council [2011] IRLR 669, para 27

been acquitted, where the court considers it necessary to do so to protect a victim from ongoing stalking or harassment.75

4.4 Malicious Communications

Section 1 of the Malicious Communications Act 1988 ("MCA") prevents the sending of communications (including online messages or letters) which convey a threat, a grossly offensive or indecent message, or false information, if the sender's intention is to cause the reader or recipient distress or anxiety.77

This offence covers communications that are offensive, obscene, menacing or false. There is no need for the communication in question to reach the subject or intended recipient, merely publishing or sending the communication and intending to cause distress will be sufficient.

This offence is punishable by up to either two years' imprisonment on conviction on indictment, or up to 12 months' imprisonment on summary conviction, in addition to or as well as a fine. There is no limit stated in the statute for this fine.

4.5 Improper Use of a Public Electronic Communications Network

Section 127 of the Communications Act 2003 ("CA 2003") provides for the offence of using public electronic communications equipment to send a message that is false, grossly offensive, or of an indecent, obscene or menacing character. This is punishable by either imprisonment of up to six months, an unlimited fine, or both.

It is also an offence to send a communication through a public network that is intended to cause annoyance, inconvenience or needless anxiety to the recipient.

The sender must intend the unpleasant effect of the message but there is no need for the message to have been received or for the recipient or subject to have been offended by it for the offence to have been committed.

Following confirmation that a Twitter message qualified as a message sent by a "public electronic communications network" it is expected that most communication by social media or other electronic communication will suffice for the purposes of this offence.78


76 Please note that this has also been replicated in Northern Irish law (section 2 Malicious Communications Act 1988) but does not apply to Scotland


4.6 Revenge Pornography

Section 33 of the Criminal Justice and Courts Act 2015 criminalised one particular type of online harassment in England and Wales. Revenge pornography is "the sharing of private, sexual materials, either photos or videos, of another person, without their consent and with the purpose of causing embarrassment or distress" and, if the person is found guilty, can be punished by up to two years in prison.\(^{80}\)

In Scotland, section 2 of the Abusive Behaviour and Sexual Harm (Scotland) Act 2016 will create a new offence of "disclosing, or threatening to disclose, an intimate photograph or film". The defendant must intend to cause the victim fear, alarm or distress or be reckless as to whether the victim will be caused fear, alarm or distress. This legislation is however not yet in force.\(^{81}\)

Section 51 of the Justice Act (Northern Ireland) 2016 criminalises a person disclosing a private sexual photograph or film without the consent of the individual who appears in the photograph or film and with the intention of causing that individual distress.

4.7 Threatening and Abusive Behaviour (Scotland Only)

Section 38 of the Criminal Justice and Licensing (Scotland) Act 2010 provides that a person commits an offence if they behave in a threatening or abusive manner, the behaviour would be likely to cause a reasonable person to suffer fear or alarm, and they intend their behaviour to cause fear or alarm or are reckless as to whether the behaviour would cause fear or alarm.\(^{82}\) It applies to either behaviour consisting of a single act or a course of conduct. A person guilty of an offence will be liable, on conviction on indictment, to imprisonment for a term not exceeding five years, or to a fine, or to both, or, on summary conviction, to imprisonment for a term not exceeding 12 months, or to a fine not exceeding the statutory maximum, or to both.\(^{83}\)

There is a defence if the defendant shows that the behaviour was, in the particular circumstances, reasonable.\(^{84}\)

4.8 Stalking (Scotland Only)

It may also be possible to be prosecuted for online harassment for the offence of stalking under section 39 of the Criminal Justice and Licensing (Scotland) Act 2010. Here, the defendant commits an offence where they stalk another person (i.e. they engage in a course

---

\(^{80}\) House of Commons Library, 'Debate pack: Prevention of online child abuse,' (Number CDP 2016/0146, 14 July 2016), page 3

\(^{81}\) House of Commons Library, 'Debate pack: Prevention of online child abuse,' (Number CDP 2016/0146, 14 July 2016), page 5

\(^{82}\) Section 38(1) Criminal Justice and Licensing (Scotland) Act 2010

\(^{83}\) Sections 38(1) and Sections 38 (3)-(4) Criminal Justice and Licensing (Scotland) Act 2010

\(^{84}\) Section 38 (2) Criminal Justice and Licensing (Scotland) Act 2010
of conduct with the intention to cause the victim to suffer fear or alarm, or they know, or ought to have known, that engaging in the course of conduct would be likely to cause the defendant to cause the victim to suffer fear or alarm) and the victim suffers fear or alarm.\(^{85}\)

Qualifying 'conduct' includes, amongst other activities:

4.8.1 contacting the victim by any means;

4.8.2 publishing any statement or other material relating or purporting to relate to the victim or any other person or purporting to originate from the victim or from any other person;

4.8.3 monitoring the victim's use of the internet, e-mail or any other form of electronic communication; and

4.8.4 acting in any other way that a reasonable person would expect would cause the victim to suffer fear or alarm.

It is likely that various forms of online harassment could fall under this offence.

4.9 Common Law Offences - Breach of the Peace and Threats (Scotland Only)

It is possible that someone committing online harassment would commit the common law offence of breach of the peace if the behaviour was of a nature that would cause concern to other people, for example 'threatening' letters or other forms of communication. To prove a breach of the peace it must be shown that someone was alarmed, annoyed or disturbed by the incident.\(^{86}\) If found guilty of breach of the peace the defendant may face up to 60 days' imprisonment or a fine of up to £2,500.\(^ {87}\) The common law offence of threats may also be used to prosecute online bullying and harassment.\(^ {88}\)

---

\(^{85}\) Section 39 Criminal Justice and Licensing (Scotland) Act 2010

\(^{86}\) 'Scottish Legislation' available at <https://www.police-information.co.uk/legislation/legislationindexsco.html> accessed 9 September 2016


\(^{88}\) Scottish Parliament Written response 10 April 2012; House of Commons Library, 'Debate pack: Prevention of online child abuse,' (Number CDP 2016/0146, 14 July 2016). In respect of the offence of threats, it is difficult to find the common law basis or potential sentencing for this. Even within case law and judicial obiter commentary in the Scots law cases available to us it is merely mentioned that this is a potential offence, rather than any basis for the offence or potential sentencing being provided. This may be as in recent years it has been more likely that this type of behaviour would be prosecuted under section 38 if the Criminal Justice and Licensing (Scotland) Act 2010 and perhaps this information is only available in older cases which aren't readily available to us.
It is however more likely that the defendant would instead be prosecuted under section 38 of the Criminal Justice Licensing (Scotland) Act 2010 which deals with threatening or abusive behaviour (see above).  

There are additional criminal offences that will apply where children are for example pressured into sending explicit pictures or into meeting up online, but as this note focuses primarily on online harassment rather than online abuse as a whole, we have not considered this further.

4.10 Civil Law

Harassment

In England and Wales it is also possible to bring a civil cause of action for harassment.

The offence must qualify as an offence under section 1 of the PHA for the civil remedy under section 3 of the PHA to apply. In the civil proceedings the Claimant can either be a victim of the harassing conduct, or, in the case of section 1(1A), the third party whose behaviour the harassment is intended to impact.

Pursuing the civil offence results in remedies which are not available in the criminal courts. These are injunctions to restrain the individual performing the harassing conduct or damages to compensate for anxiety or financial loss.

There is however also a criminal aspect to civil claims for harassment. A breach of an injunction against harassment entitles the claimant to apply immediately to the civil court that issued the injunction for a warrant for the defendant's arrest. In addition, breaching a civil injunction against harassment without reasonable excuse is automatically a criminal offence under the PHA punishable by imprisonment or a fine. Breaching the civil injunction would also constitute a contempt of court.

The availability of both a civil and criminal cause of action for harassment allows the victim to choose which course to pursue. This is particularly useful where there is doubt whether the burden of proof for the criminal offence of 'beyond all reasonable doubt' will be met, but on the balance of probabilities it is expected that the victim could prove harassment.

---


90 House of Commons Library, 'Debate pack: Prevention of online child abuse,' (Number CDP 2016/0146, 14 July 2016), page 5


Scottish law is governed by sections 8 to 11 of the PHA 1997. The offence of harassment set out in section 8(1) is similar to the provision in section 2. A person must not pursue a course of conduct which amounts to harassment of another and the course of conduct is intended to amount to harassment of that person, or occurs in circumstances where it would appear to a reasonable person that it would amount to harassment. Section 8(2) provides civil liability for harassment. In addition, Section 8A provides for a separate offence of harassment amounting to domestic abuse.

Remedies for these offences provide for either damages, an interdict or interim interdict, or a non-harassment order preventing the defendant from carrying on the conduct in the future.\(95\) Where a person breaches a non-harassment order they will be guilty of a criminal offence and liable on indictment to imprisonment for a term up to five years, or a fine, or both, or, on summary conviction, to imprisonment for up to six months or a fine not exceeding the statutory maximum, or both.\(96\)

As discussed above, the PHA has been replicated in Northern Irish law. With regards to Northern Irish law more generally, we have not found instances where there are completely separate offences dealing with online harassment.

4.11 Defamation

Statements that are made online often make claims or allegations that are potentially damaging as they lower the reputation of the subject in the minds of those reading the content. Examples include criticisms of a person's actions or character or establishing a fake social media profile in someone else's name, which purports to be written by and about that person.\(97\)

To demonstrate that online content is defamatory, a party must show that the content:

- **4.11.1** Was first published within the previous 12 months;\(98\)
- **4.11.2** Lowers the subject in the estimation of 'right-thinking' members of society, or is likely to affect a person adversely in the estimation of reasonable people generally.\(99\)

---

95 Section 8(5) Protection from Harassment Act 1997
96 Section 234A Criminal Procedure (Scotland) Act 1995; Section 9 Protection From Harassment Act 1997
97 PLC,'Social media offences,' available at <http://uk.practicallaw.com/3-616-4951?q=defamation+and+online+harassment#a669485> accessed 3 October 2016
4.11.3 Has caused or is likely to cause serious harm to the subject;¹⁰⁰ and

4.11.4 Is not the truth or honest opinion (with a reasonable basis), nor does it benefit from another of the established defences.¹⁰¹

In Scotland defamation law shares common traits with defamation law in England. What amounts to defamation is the same (a broadcast, statement or publication which lowers a person in the estimation of a right-thinking member of the public), the defences are also broadly the same (albeit the terminology is slightly different) and in general the statutory provisions in the Defamation Act 1952 and Defamation Act 1996 have, for the most part, covered the UK as a whole. The time limitation in Scotland, however, is three years from the date of publication of the statement. For a full overview of the differences in defamation between Scotland and England please see Brodies LLP's article on 'Defamation: Differences between Scotland and England'.¹⁰²

There may also be an action for malicious falsehood under section 3(1) of the Defamation Act 1956, however, as the victim must show quantifiable financial loss this is likely to be difficult to establish in cases of online harassment.¹⁰³

4.12 Policies to Train The Police in Dealing With Online Harassment

Currently no legislation has been passed requiring police to be trained in dealing with online harassment in the UK. Some training on digital crime, digital communications and social media has been provided to police officers with some funding provided by the Home Office, however the training is not mandatory.

There is an acknowledgment by HM Inspectorate for Policing ("HM Inspectorate") that "the police response to digital crime should be capable of being provided by every police officer and member of police staff who deal directly with the public", due to the prevalence of digital

---

¹⁰⁰ Section 1(1) Defamation Act 2013; PLC,'Social media offences,' available at <http://uk.practicallaw.com/3-616-4951?q=defamation+and+online+harassment#a669485> accessed 3 October 2016


¹⁰³ PLC,'Social media offences,' available at <http://uk.practicallaw.com/3-616-4951?q=defamation+and+online+harassment#a669485> accessed 3 October 2016
crime and that this requires police staff to have the relevant training to give them the necessary understanding of the technology. Despite this, an investigation conducted by HM Inspectorate found a "mixed picture" in relation to the "extent to which police officers and staff knew of, and were trained in, digital crimes and modern technology." It identified the need for better understanding and appropriate training to be given to staff to ensure that digital crimes, such as online harassment, are appropriately dealt with by police officers and staff to ensure that victims receive proper treatment.

A number of online courses have been provided to staff by the College of Policing, covering topics including cyber-crime and policing, as well as digital communications and social media. In addition, first responders have been provided with a classroom based course entitled ‘mainstreaming cyber-crime training’. In 2014-15 172,762 online modules were completed and approximately 4,394 officers took the classroom course between its instigation in February 2014 and April 2015. However, there have been complaints made by police staff about difficulties in finding the time to take this course as "protected training days" are often cancelled due to pressure on resources.

Funding for courses from government in respect of this has been limited, meaning that funding of this training is often left to national police bodies who are struggling to deal with cuts without having to implement extra training.

For example, the cyber-crime training course discussed above was subsidised for 14 months to try to ensure that as many officers as possible completed it. Once the Home Office funding

---


110 HC Deb 7 July 2016, vol 612, col 1084
came to an end due to police resources being stretched by cuts to funding by the government the amount of training received on digital crime in general, and online harassment specifically, may not be appropriate.\textsuperscript{111}

There have also been questions about the quality of training in respect of online crime across the UK. Complaints have been made about the equipment provided to staff making it difficult for them to successfully complete the online courses (for example, having no headphones to listen to the course). In addition the course focuses on digital crime generally - although it includes elements relating to social media and digital communications this may not be sufficiently target online harassment. Furthermore, some forces added elements to the standard course rolled out nationally as they did not consider that the course met their requirements. This is likely to have led to inconsistencies in respect of the training received nationally.\textsuperscript{112}

It is estimated that only about "7,500… of 100,000 police officers in England and Wales have been trained" to investigate digital crime, amounting to just 7.5 per cent of officers.\textsuperscript{113}

Gill Furniss MP, in a July 2016 parliamentary debate on online abuse stated that:

"It is obvious that the police are under incredible pressure trying to deal with even the small proportion of online abuse reported to them…[approximately] half of all crimes reported to the police have some digital element, and they expect this to rise to 70% in the next five years. The scale of the problem is such that all police officers need to be in a position to tackle online abuse: to know how to investigate it and secure evidence".\textsuperscript{114}

Gill Furniss MP also noted that any consolidation of legislation relating to online abuse:

"must be backed up by a corresponding overhaul of enforcement… not only a review of the training given to officers but a serious rethink about approaches to police recruitment as…[despite] the strain on police budgets… unless we dramatically expand our police’s ability to clamp down on online crime, we will be stuck trying to apply 20th century methods to 21st century problems".\textsuperscript{115}

\begin{flushleft}
\textsuperscript{113} HC Deb 7 July 2016, vol 612, col 1069; Roberta Blackman-Woods MP
\textsuperscript{114} HC Deb 7 July 2016, vol 612, 1077
\textsuperscript{115} HC Deb 7 July 2016, vol 612, 1077
\end{flushleft}
Ed Vaizey MP also remarked that the:

"police should also think very hard about the people they recruit,… there is every opportunity to recruit people with specialist skills that may not be transferable to the rest of the police service but who could be recruited relatively quickly to do [digital investigative work]."

In this debate there was also some discussion about a further need to investigate enforcement issues in relation to online harassment and abuse such as whether police are trained appropriately, whether they have the resources to conduct necessary investigations and if they are serious about dealing with reports of online abuse.

4.13 Governmental Discussion Surrounding Online Harassment and Free Speech

There has been very little publicised discussion by the Government surrounding online harassment, free speech and the interplay between the two.

However, in a July 2016 parliamentary debate on online abuse MPs outlined that freedom of speech comes with responsibilities to deal with the consequences of the words used.

Maria Miller MP commented that:

"Like every other Member of this House, I believe in freedom of speech, but that freedom of speech has never been an unqualified right. Freedom of speech comes with responsibilities. At present we are not ensuring that people who are expressing themselves online understand that fact".

In addition, Liz McInnes MP commented "with free speech… comes the responsibility to deal with the consequences of one’s words".

Seema Kennedy MP went further, stating that online abuse was not an exercise of free speech, but rather a crime, "online abuse is crime, it is not banter, it is not teasing, and it is not an exercise of free speech".

It is noted however that in revised CPS guidelines for both the MCA and offences under section 127 of the CA 2003, the evidential burden for the CPS to prove is high due to the risk the provisions pose to free speech. Many prosecutions are not pursued, even if the evidence exists, because to do so would not be in the public interest. CPS guidelines emphasise that

---

116 HC Deb 7 July 2016, vol 612, col 1106
117 HC Deb 7 July 2016, vol 612, col 1071
118 HC Deb 7 July 2016, vol 612, col 1063
119 HC Deb 7 July 2016, vol 612, col 1083
120 HC Deb 7 July 2016, vol 612, col 1087
the MCA requires the communication to be "grossly" offensive and that the context of a communication may be key.\textsuperscript{121}

Guidelines published on online media by COPFS, the Scottish prosecuting body, note that free speech necessarily entails that there is a high threshold set before "communications will fall foul of the criminal law and general satirical comments, offensive humour or provocative statements which might be distasteful or painful to some will not reach that high threshold".\textsuperscript{122}

However, COPFS also makes it clear that the perception by some that online speech can provide a "cloak of anonymity can allow such communications to quickly cross the boundary into the inappropriate, indecent and criminal".\textsuperscript{123}

They note that individuals cannot be allowed to believe that it is acceptable to spread hatred or make anonymous threats of violence and harm from their computers and that dialogue such as this may amount to a criminal offence as it "crosses the limits of conventional discourse". COPFS appear to take a harder stance than the CPS, considering that whilst there is a need to consider the public interest in freedom of speech this must be tempered.\textsuperscript{124}

4.14 Degree To Which Online Harassment is Seen as an Area that Needs Government Attention

The Government has historically taken the approach that online harassment is not an area that requires government attention. In February 2016, the Government said that it did "not intend to introduce specific additional legislation to address online harassment and also internet trolling".\textsuperscript{125}

Additionally, in February 2016 when asked about criminalising cyber-bullying, the Government said:

"we do not want to make any form of bullying a criminal offence as to do so would risk criminalising young people. In some circumstances that may be justified, but probably

\textsuperscript{121} PLC, 'Social media offences,' available at <http://uk.practicallaw.com/3-616-4951> accessed 9 September 2016


\textsuperscript{125} PQ 25115, answered 4 February 2016; House of Commons Library, 'Debate pack: Prevention of online child abuse,' (Number CDP 2016/0146, 14 July 2016,' 4
only in a limited number of very serious cases, for which there are already laws in place to protect people”.  

Instead, the Government has placed the onus outside of the legislative environment stating that "internet providers, schools and parents all have a role to play in keeping children and young people safe online…".

Whilst parents and schools can educate children about online safety and social media websites can place safeguards (including age restrictions) on their users and provide mechanisms by which users can report abusive behaviour and by which complaints will be responded to, the "fragmented nature of the current legal framework" has been criticised.

During a July 2016 parliamentary debate a number of MPs including Maria Miller, Chair of the Women and Equalities Select Committee, and Yvette Cooper, made it clear that they believed that a greater level of regulation was required to govern online harassment offences. In addition, several MPs called for consolidation of the current offences during this debate. In response, the Government acknowledged that there had been a "clear call from the House for legislative clarity, both clarity in defining online abuse and clarity about the myriad different Acts and statutes that come to bear in this area".

A number of Bills have been submitted to the Houses of Parliament which could potentially, if passed, change the way in which this area of law is regulated.

4.15 Malicious Communications (Social Media) Bill 2016-17

This Bill has been described as "a bill to make provision about offences, penalties and sentences in relation to communications containing threats transmitted or broadcast using online social media; and for connected purposes".

Given the current use of the MCA to tackle online harassment this new Bill, if passed, may consolidate existing laws in relation to online harassment taking place on social media.

---

126 PQ 27104, answered 23 February 2016; House of Commons Library, 'Debate pack: Prevention of online child abuse,' (Number CDP 2016/0146, 14 July 2016);

127 PQ 27104, answered 23 February 2016; House of Commons Library, 'Debate pack: Prevention of online child abuse,' (Number CDP 2016/0146, 14 July 2016);

128 House of Commons Library, 'Debate pack: Prevention of online child abuse,' (Number CDP 2016/0146, 14 July 2016); HC Deb 7 July 2016 col 1106

129 HC Deb 7 July 2016, vol 612, cols 1064-1065

130 HC Deb 7 July 2016, vol 612, cols 1076 and 1077


132 'Malicious Communications (Social Media) Bill 2016-17,' available at <http://services.parliament.uk/bills/2016-17/maliciouscommunicationssocialmedia.html> accessed 8 September 2016
Anna Turley MP commented in the above parliamentary debate that she would be delighted to work with MPs “to see whether we can use [the Bill]... as a vehicle for... legislative change”. It is however noted that as the text of this Bill has not yet been published it is difficult to know who the Bill will tackle this issue and that any proposals may be watered down during the legislative process.

During the debate Ed Vaizey MP further commented that “the new Government under the new Prime Minister will want to make clarifying and consolidating the legislation a priority”. It is noted that during this debate Ed Vaizey MP was the Minister for Culture, Communications and Creative Industries. Although he no longer has this role, so his comment may not be entirely representative of the current Government's thinking, it is clear from the above comments that the Government do now intend to tackle this.

It is noted that, as the current scope of the Bill appears to be solely restricted to social media, this might not go far enough in addressing issues with the law in relation to current online harassment, e.g. cyber-bullying and trolling that occurs on other sites or through other messaging mediums.

Additionally, this Bill is only at the first reading stage at the time of writing, the first time it will be debated will be during the second reading in the House of Commons on 24 March 2017. There is no guarantee that the Bill will pass and given comments in the parliamentary debate on online abuse in relation to a hesitation by MPs and the Government to stifle business and further investment in the United Kingdom it may be that this Bill is opposed.

4.16 Online Safety Bill 2016-17

This Bill is “to make provision for parents to be educated about online safety”. As discussed above, the Government have previously suggested that education of parents and schools should be the way to deal with online harassment. However, even if this Bill is passed it will not materially alter how online harassment is treated under the law. In addition, it is noted that a Bill of an identical title was in the process of progressing through Parliament last year as agreement on the text was not reached by the end of the parliamentary session.

4.17 Digital Economy Bill 2016-2017

It has also been suggested that this Bill could be a legislative vehicle by which the law in this area could be clarified and consolidated. However, this is not listed as one of the Bill's

---

133 HC Deb 7 July 2016, vol 612, col 1086
134 HC Deb 7 July 2016, vol 612
purposes\textsuperscript{137} and given comments in relation to hesitation by MPs and the Government to stifle business and further investment in the United Kingdom, it may be that adding provisions that would deal with online harassment would be opposed\textsuperscript{138}.

The one area that has been an exception to this is revenge pornography. The Government viewed this form of online harassment as an area that did need addressing and, as a result, created a new offence to regulate this.

Both the CPS and COPFS have published guidelines on prosecuting offences that may be committed by communications by social media in an attempt to clarify the law as it stands\textsuperscript{139}.

In relation to Scotland, the First Minister, Nicola Sturgeon, has been vocal in condemning the current state of online abuse legislation and the Scottish Government "\textit{have provided full funding for Respectme, Scotland's anti-bullying service, which is managed by the Scottish Association for Mental Health}" in an attempt to address the effects of online harassment and abuse\textsuperscript{140}.

SNP MPs have also stated the SNP "\textit{utterly condemns}" online abuse and supports "\textit{any measures that may ensure that those responsible for this abuse are held accountable for their actions}"\textsuperscript{141}.

It is noted that the UK Government have also launched \textit{Stop Online Abuse}, a website to help assist with issues relating to online abuse and harassment and campaign to change the law\textsuperscript{142}.

4.18 Conclusion

The foregoing demonstrates that there are currently laws, both civil and criminal, that can be used to combat online harassment. However, there is a lack of legislation requiring police to be trained in dealing with online harassment in the UK. While there has been some provision of online training to police in dealing with online crime, there have been complaints about

\textsuperscript{137} 'Digital Economy Bill 2016-17,' available at <http://services.parliament.uk/bills/2016-17/digitaleconomy.html> accessed 8 September 2016

\textsuperscript{138} HC Deb 7 July 2016, vol 612, col 1107


\textsuperscript{140} HC Deb 7 July 2016, vol 612, col 1072

\textsuperscript{141} HC Deb 7 July 2016, vol 612, col 1091

access to resources, quality of training and staff finding time to attend training. Further, the training is not targeted at online harassment specifically, and has been implemented inconsistently across forces.

Parliamentary debate on online abuse and freedom of speech has outlined that freedom of speech comes with the responsibility to deal with the consequences. However, this must be balanced against the fact that there has been limited to no publicised discussion by the Government surrounding online harassment and free speech, and that evidential burden for the CPS to prove when prosecuting under the MCA and the CA 2003 is high.

Furthermore, the Government has historically taken the approach that online harassment is not an area that requires government attention. While there have been a number of Bills submitted with the potential to affect the way online harassment is regulated, it remains to be seen whether they make their way into law.
5. UNITED STATES

5.1 Summary

The purpose of this research is to investigate the issue of online harassment in the U.S. In particular, this note outlines the relevant legal framework addressing online harassment and discusses how such laws are applied in the U.S. Further, the interplay between freedom of expression and protection from harassment will be discussed.

While there has been acknowledgment at both state and federal level that online harassment presents a growing issue, any attempts to issue new legislation to tackle it have only been made by individual members of Congress, and have received a lukewarm reception.

5.2 Legal Framework

Given the prevalence of online harassment, there is a desire to see the issue tackled effectively under federal law. With respect to the U.S., the first question which arises in respect of the core laws and policies applicable to online harassment is that of jurisdiction.

5.3 Federal Law

Criminal Law

Generally, behaviour which constitutes online harassment, for example cyber-bullying, online stalking, and so on, is covered by U.S. criminal law. Federal law has provisions against online harassment in 18 U.S. Code § 2261A, which criminalises the use of electronic communication or interactive computer services to cause fear and distress.

Cyber-stalking is also legislated against under federal law: the Violence Against Women Reauthorization Act 2013 incorporates cyber-stalking into the definition of stalking through Section 107. This section prohibits the use of, among other facilities, interactive computer services or electronic communications services with the intent to harass, intimidate or place under surveillance, or to cause reasonable fear of death or serious bodily injury, or substantial emotional distress. The U.S. Code uses similar language to criminalise the offence in the District of Columbia.

143 60% of internet users said they had witnessed someone being called offensive names; Pew Research Centre, "Online Harassment", 22 October 2014, available at http://www.pewinternet.org/2014/10/22/online-harassment/
5.4 Civil Law

In addition to criminal federal law, there are two main civil offences at federal level which may be applicable to cases of online harassment.

The first potential route of civil redress is through defamation law. There have been a small number of cases which have used defamation law to pursue offensive online speech. The question of defamation must always be carefully balanced against the right to free speech under the First Amendment. Content posted by third party users on a platform is generally excluded from the forum host's liability, which can therefore prevent a defamation case, even where the content could be considered defamatory. Civil suits, whether for copyright or defamation, may not always be appropriate due to (i) the nature of the behaviour (where a criminal case would be more appropriate); (ii) practical reasons (where the defendants are unknown or in another state, or the considerable time demands of a civil suit); or (iii) cost (raising a civil case often requires significant upfront costs).

Under U.S. federal law, where online harassment includes the sharing of self-taken photos, there may be a civil remedy available. Copyright forms from the moment the work is created, i.e. when a photo is taken, therefore generally the photographer holds the right to the image. As such, self-taken photos (explicit or not) which are displayed online by someone other than the photographer without consent constitute a copyright violation. This legal avenue may be useful where the online harassment consists of or includes the sharing of self-taken photos, most commonly explicit images, then posted publicly without the permission of the other party. This exertion of ownership over the images allows the victim to pursue remedies under the Digital Millennium Copyright Act, which include forcing the website to remove the images and the potential for civil litigation.

5.5 State Law

Certain states have specific cyber-stalking and harassment laws allowing victims to press criminal charges against their online stalkers/harassers. Some examples of state measures are:

5.5.1 Alabama, Arizona, Connecticut, Hawaii, Illinois, New Hampshire, and New York have included prohibitions against

harassing by means of electronic, computer or e-mail communications in their harassment legislation.

5.5.2 Alaska, Florida, Oklahoma, Wyoming, and California include electronically communicated statements under stalking in their respective anti-stalking laws.

5.5.3 Texas has the Stalking by Electronic Communications Act, 2001.

5.5.4 Missouri state harassment statutes include stalking and harassment by telephone and electronic communications (in addition to cyber-bullying).

The classification of the offence under these laws (and hence the subsequent remedies) varies dramatically from state to state. For example, while some states (such as Arizona or Connecticut) see the offence as a Class C Misdemeanour, attracting maximum penalties of no more than three months in jail, and/or a fine of no more than $500, others (namely Florida) see the offence as a felony of the third degree, attracting a maximum penalty of no more than...

158 Alaska Statute § 11.41.270(a), available at http://www.touchngo.com/lglnctr/akstats/Statutes/Title11/Chapter41/Section270.htm
159 Florida Code Title XLVI Chapter 784 s784.048, available at https://www.criminallawyerjacksonville.com/0784.048.htm
five years in jail, along with the possibility of a restraining order to be awarded for up to 10 years.\(^{165}\)

The sharing of sexual or explicit images, as discussed above, has also been criminalised in various states, such as New Jersey in 2004 with an invasion of privacy statute, followed by California, and a number of other states have Bills under consideration. A total of 34 states (and the District of Columbia) now have laws criminalising the non-consensual dissemination of private images.\(^{166}\)

Similarly, some states have criminal defamation provisions, in addition to the federal civil measures discussed above. However prosecution in these cases is rare, and particularly complicated due to issues with resources, technical training and general awareness.\(^{167}\)

This reflects a desire to take active steps to prevent online harassment beyond the federal level, and a recognition that harassment can include, or entirely consist, of online communication. However due to the nature of independent legal frameworks at state level, there is a lack of a clear overriding policy on criminalisation across states. The examples above highlight the various designations and potential inconsistencies in the categorisation of typical online harassment.

5.6 **Policies to Train The Police Force in Dealing With Online Harassment**

Generally the consensus in the U.S. is that law enforcement is unfamiliar with how to investigate cases of online threats and harassment and is therefore often dismissive of complaints.\(^{168}\)

In response to this need, in March 2016 Congresswoman Katherine Clark put forward a Bill titled the "Cybercrime Enforcement Training Assistance Act of 2016",\(^{169}\) which would direct the Attorney General to make grants to states and units of local government for the prevention, enforcement, and prosecution of cyber-crimes against individuals, among other purposes.

---

\(^{165}\) All maximum penalties given are on the basis that the perpetrator has not committed previous crime.


\(^{167}\) Marwick and Miller, CLIP Fordham Law School, Online Harassment, Defamation, and Hateful Speech: A Primer of the Legal Landscape, June 10, 2014 available at [http://ir.lawnet.fordham.edu/cgi/viewcontent.cgi?article=1002&amp;context=clip](http://ir.lawnet.fordham.edu/cgi/viewcontent.cgi?article=1002&amp;context=clip)


\(^{169}\) H.R. 4740 - Cybercrime Enforcement Training Assistance Act of 2016, available at [https://www.congress.gov/bill/114th-congress/house-bill/4740?q=%7B%22search%22%3A%5B%22cybercrime%22%5D%7D&amp;resultIndex=3](https://www.congress.gov/bill/114th-congress/house-bill/4740?q=%7B%22search%22%3A%5B%22cybercrime%22%5D%7D&amp;resultIndex=3)
However as at September 2016, the Bill had not progressed past the Committee stage and was unlikely to be enacted, given the lack of interest and progress since introduction.\textsuperscript{170}

Further, there was a motion in 2015 for a Bill to amend the Homeland Security Act of 2002 to establish a "National Computer Forensics Institute" to be operated by the U.S. Secret Service. The purpose of this was to enable the Institute to, among other things, educate, train and provide equipment to state, local, tribal and territorial law enforcement officers, prosecutors and judges.\textsuperscript{171} The Bill passed through the initial stages and has remained at the committee stage, with no further discussion having taken place with regard to it.

In terms of existing policy, one example of proactive measures against online harassment is that of the U.S. Government Department of Health & Human Services, working in coordination with the Federal Partners in Bullying Prevention Steering Committee, which hosts a website on stopping bullying, featuring a targeted page on cyber-bullying.\textsuperscript{172} The website aims to improve education on the topic of cyber-bullying, offering suggestions on prevention and reporting.

5.7 Discussion Surrounding Online Harassment and Free Speech

Freedom of speech is a constitutionally protected right enshrined in the First Amendment.\textsuperscript{173} However, U.S. laws and policies must strike a balance between protecting First Amendment rights online whilst ensuring an Internet environment free from threats and harassment.\textsuperscript{174} Such a balance is becoming more pertinent as social media platforms and their usage continue to grow.\textsuperscript{175}

\textsuperscript{170}H.R. 4740 - Cybercrime Enforcement Training Assistance Act of 2016, available at https://www.govtrack.us/congress/bills/114/hr4740
\textsuperscript{172}U.S Department of Health & Human Services, available at https://www.stopbullying.gov/cyberbullying/
\textsuperscript{173}US Constitution First Amendment, available at https://www.law.cornell.edu/constitution/first_amendment
5.8 US Supreme Court

The high-profile U.S. Supreme court case of *Elonis v United States* (Opinion June 1 2015) was the first time the Supreme Court has heard a case considering threats and the limits of free speech on social media.\(^{176}\)

In this case, a man from Pennsylvania made several threats on Facebook against his estranged wife, unspecified elementary schools, and a female FBI agent who visited him to investigate. The Supreme Court reversed Elonis' conviction of threatening to kill and threatening to injure.

The defendant insisted throughout his prosecution that he was simply exercising his First Amendment rights. Nevertheless, the Supreme Court decided to opt out of specifically ruling on the First Amendment issues raised, instead reversing the conviction of the defendant on other grounds. It is therefore suggested that the balance between the law on online threats and First Amendment free speech has yet to be answered under U.S. law.\(^{177}\)

5.9 Congress

On the whole, there has been little discussion in Congress regarding the issue of online harassment (or "cyber-bullying") and its interplay with free speech. The most recent mention of this in the Congressional Record, which outlines the proceedings and debates held in Congress, was in 2013.

On the other hand, there have been a few vocal members of Congress advocating government attention to online harassment in recent years, as highlighted below.\(^{178}\) The shared rationale for such attention has been targeted at the lack of law enforcement caused in part by the absence of specific, uniform legislation and police training.

Senator Bob Casey of Pennsylvania led a speech in the Senate on 21 September 2013 vocally highlighting the need for law enforcement on the issue of "Cyberbullying".\(^{179}\) Joined by Senator Nelson of Florida, the Senators called for federal legislation to address the lack of law enforcement mechanisms for officers to arrest and prosecute online harassers. Senator Nelson cited some disturbing news stories in Florida concerning young girls who had been subjected to online harassment and who consequently took their own lives.

---


\(^{178}\) See paragraphs 3.7-3.10.

\(^{179}\) 113th Congress, 1st Session, Issue: Vol. 159, No.129, available at [https://www.congress.gov/congressional-record/2013/9/19/senate-section/article/s66272?q=%7B%22search%22%3A%5B%22cyber+bullying++harassment%22%5D%7D&resultIndex=3.}
Congresswoman Katherine Clark (Massachusetts) has been a consistent and vocal advocate for government attention towards cyber-bullying. Similar to Casey and Nelson, Clark's primary submission is that law enforcement is not doing enough to prevent cyber-bullying.

Clark persuaded the House of Representatives in May 2015 to support her petition for further U.S. Department of Justice ("DOJ") action on the issue. The House instructed the DOJ to "intensify its efforts to combat this destructive abuse" and to "increase investigations and prosecutions of these crimes".

Targeting improved law enforcement in respect of online harassment, Clark introduced a Bill called the Prioritizing Online Threats Enforcement Act, in February 2015. The proposed Act would give extra resources and an order to the DOJ and FBI to investigate and enforce the existing federal laws regulating online threats. Moreover, as a victim of so-called "swatting" (the process of reporting fake threats at someone’s home in the hope to invite a major SWAT team visit), Clark introduced the Interstate Swatting Hoax Act of 2015 Bill, in an attempt to prohibit such false reporting using the internet or other telecommunications. The Bill was co-sponsored by Congressman Patrick Meehan of Pennsylvania but has yet to be revisited since November 2015.

Nevertheless, as a result of the DOJ’s inaction towards law enforcement, Clark has recently proposed further legislation on 13 September 2016 called the Cybercrime Statistics Act. The legislation intends to reform law enforcement methods to tackle serious online harassment through requiring the DOJ to outline detailed definitions of each category of cyber-crime and add these to the mandatory FBI reporting database. Clark is concerned with both the inactivity of the DOJ to prosecute online harassers under existing legislation, and the...
absence of updated statistics of cyber-bullying offences.\textsuperscript{187} Such reform would impose stricter disclosure rules on the DOJ to reveal the true extent of online cyber-bullying in the U.S.

It is thus submitted that, despite the House of Representatives’ instructions in 2015 for intensified law enforcement, online harassment remains an unaddressed problem with only few members of Congress calling for government action.

5.10 Conclusion

Overall the position in the U.S. is that there is consensus, at state and federal level, that online harassment presents an ongoing issue and that there should be adequate recourse within the law to prevent it. However, there is no real appetite to introduce new legislation on a federal basis, instead reliance is placed on the existing provisions. In practice, active prevention of online harassment is hampered by the lack of knowledge and training amongst law enforcement and a lack of consistency and clarity in with the current legislative regime.

It is suggested that the above illustrates the individual efforts of members of Congress to tackle online harassment, yet little substantive change has been implemented in practice. Bills remain on the table and have yet to be enacted, while additional resources have yet to be given to law enforcement officers. On the other hand, it is clear that members of Congress such as Congresswoman Clark are attempting to use their position to broadcast and inform members of Congress on the seriousness of the issue and the need for a response which is not readily available to victims.
