RCNI Discussion Document on

Cyber-harassment

(Revised following publication of the Law Reform Commission Report on Harmful Communications and Digital Safety, September 2016)

April 2017

Introduction

Rape Crisis Network Ireland's network of member Rape Crisis Centres must now deal with frequent complaints of cyber-harassment in several forms from our clients, particularly older children and young adults. Not all forms of cyber-harassment are addressed adequately in existing legislation, in our view. Cyber-harassment can and does cause serious harm to its victims, and some cyber-harassment amounts to a form of sexual violence against those victims who experience it in a sexual context. Sexual violence in whatever form can and does have devastating impacts on its victims, and for this reason RCNI is interested in exploring legal options by which sexual cyber-harassment might be prevented and/or punished.

Cyber-Harassment Discussion Document: Structure

This document is a revised version of the RCNI Submission to the Law Reform Commission from January 2015 on its Issues Paper on Cyber-Harassment, updated to take account of the recommendations of the Commission in its Report on Harmful Communications and Digital Safety, published September 2016[1]. Each Issue in the original paper is replaced by the Commission's eventual recommendation(s) in its Report, and the RCNI position is set out under each recommendation. RCNI's position is broadly in line with the Commission's recommendations.

RCNI welcomes very much the inclusion of a new Cybercrime Bill in the current Legislative Programme and urges Government to introduce legislation in this area as soon as possible.

At the end of the document, there is a brief section on the new ICT offences which were created by the Criminal Law (Sexual Offences) Act 2017[2].

RECOMMENDATION on ISSUE 1: SHOULD THERE BE A SPECIFIC REFERENCE TO "CYBER-HARASSMENT" IN SECTION 10 OF THE 1997 ACT?

"4.02 The Commission recommends that section 10 of the Non-Fatal Offences Against the Person Act 1997 should be repealed, and replaced by an offence of harassment that is modelled on section 10 and that includes two additional provisions: (a) that the harassment offence should expressly apply to harassment by any means of communication, including through digital and online communications; […]"

RCNI position: We agree with the Law Reform Commission that specific reference to cyber-harassment is unquestionably necessary.

[1] Available online through this weblink: http://www.lawreform.ie/_fileupload/Reports/Full%20Colour%20Cover%20Report%20on%20Harmful%20Communications%20and%20Digital%20Safety.pdf

[2] Available online through this weblink: http://www.irishstatutebook.ie/eli/2017/act/2/enacted/en/html. Section 8 (inter alia) was commenced 27th March 2017, see: http://www.irishstatutebook.ie/eli/2017/si/112/made/en/pdf

Our Rationale: Section 10 of the *Non-Fatal Offences Against the Person Act 1997* is widely applicable and inclusively worded but in relation to tackling the relatively new phenomenon of cyber harassment there is room for improvement. Incidences of cyber-harassment are growing at an alarming rate. This is not an issue faced solely in our jurisdiction but across all international borders. In Ireland we have a very high proportion of the population using social media: one study recorded that 61% of those surveyed were users of at least one of these services[3]. The popularity of social media has arisen since the publishing of the 1997 Act and while it is still quite applicable to many types of cyber-harassment, such as sending sexually threatening messages and images to the victim, there is a need to update and expand its scope.

- The existing requirement of persistence in order to prove harassment is a major issue. Cyber-harassment can interfere seriously with a person's peace and privacy by causing a great deal of distress in one single action. The requirement of persistence is far more relevant to non-ICT forms of harassment and stalking but does not take into account how damaging one single attack can be on an individual especially if the action is taken towards a victim on a public forum.

- The case of *R v Debnath*[4] is not an everyday example but rather a prolonged and extensive attack on an individual, albeit conducted mostly by indirect harassment (communication with others of false and damaging material of a sexual nature relating to the victim) and the mere question of whether all aspects of the attack could be covered by section 10 of the 1997 Act is a clear indication that changes need to be made to modernise harassment legislation to include cyber (and other) harassment by indirect means, that is, by communication with others or publication. The same can be said for the question mark over the applicability of section 10 of the 1997 Act in relation to the infamous Apple iCloud leak of 2014[5].

- The year this Act was brought into law, harassment by text messages, phone calls and some few emails were the extent of electronic harassment. In 2017, there is a constantly evolving and expanding world of cyber communication which requires legislation that directly applies to it.

RECOMMENDATIONS ON ISSUE 1(b) (paraphrased): SHOULD SECTION 10 OF THE NON - FATAL OFFENCES AGAINST THE PERSON ACT 1997 BE AMENDED TO INCLUDE INDIRECT FORMS OF HARASSMENT, INCLUDING PERSISTENT POSTING ONLINE OF HARMFUL PRIVATE AND INTIMATE MATERIAL IN BREACH OF A VICTIM'S PRIVACY?

[3] Ipsos MRBI (2013). Ipsos MRBI. Available at: http://www.ipsosmrbi.com/social-networking-quarterly-survey-februar-2013.html

[4] R v Debnath [2005] EWCA Crim 3472

[5] This was a large-scale hacking operation which led to the disclosure of material relating to a number of women celebrities. See for instance, this report in The Guardian: https://www.theguardian.com/technology/2014/sep/02/gang-hackers-naked-celebrity-photos-routinely-attacked-icloud

"4.02 The Commission recommends that section 10 of the Non-Fatal Offences Against the Person Act 1997 should be repealed, and replaced by an offence of harassment that is modelled on section 10 and that includes two additional provisions: [….] and (b) that it should deal with indirect forms of communication, such as setting up fake online social media profiles".

4.06 The Commission recommends the enactment of an indictable offence of distributing an intimate image without the consent of the person depicted in the image, or threatening to do so, and with the intent to cause alarm, distress of harm or being reckless as to this […]

4.07 The Commission recommends the enactment of a summary, strict liability offence of taking or distributing an intimate image of another person without the other person's consent.[…]

4.08 The Commission recommends that the definition of "consent" applicable to the intimate images offences should be that a person agrees by choice and that the person has the freedom and capacity to make that choice. […]

(The phrase "intimate image" is defined in some detail in the following two recommendations).

RCNI Position: These or similar provisions are necessary to tackle the problem of image-based abuse (IBA), [6]where a single indirect communication has the power to devastate its victim. This range of offences can address this gap in our law on harassment.

Our Rationale: The comments made by the then Minister for Communications, Energy and Natural Resources in 2013 [7] that the 1997 Act deals with "direct communications with someone" but "it does not deal with communication about someone and is being interpreted in a very narrow sense by the courts" highlight a need for an amendment to include a reference to indirect harassment in section 10 of the 1997 Act. The use of indirect harassment, such as the sending of a sexually explicit photograph of the victim to his/her employer, has the same potential to cause serious harm and distress to an individual as an incident of direct harassment, and the possibility of section 10 of the 1997 Act not being applicable in such an instance leaves a large number of options available to a would-be attacker where they may or may not suffer any legal ramifications for their actions under this act. In the English *Protection from Harassment Act 1997* the possibility of applying the Act in instances of indirect harassment is an example which should be followed in our jurisdiction, as it would provide a much wider range of protection for individuals targeted in this way. The *Criminal Justice and Courts Bill*[8] which is currently going through parliament in the United Kingdom will make the publishing of image based abuse a specific offence punishable by up to 2 years in prison. This move to target image based abuse is an example of the active and forward-looking thinking that we need to tackle this problem to ensure that if a case such as

[6] The phenomenon of image-based abuse (IBA) is commonly but not advisedly, described as "revenge porn"
[7] Joint Committee on Transport and Communications Report on Addressing the growth of Social Media and tackling Cyberbullying (Government Publications, 2013) at 34.

[8] New law to tackle revenge porn - Press releases - GOV.UK. 2015. *New law to tackle revenge porn - Press releases - GOV.UK*. [ONLINE] Available at:http://www.gov.uk/government/news/new-law-to-tackle-revenge-porn.

R v De Silva[9] did arise in Ireland that we would have adequate legal means to handle such an incident.

RECOMMENDATIONS on ISSUE 1(c) (paraphrased): SHOULD SECTION 10 OF THE NON - FATAL OFFENCES AGAINST THE PERSON ACT 1997 BE AMENDED TO PROVIDE EXPRESSLY THAT IT SHOULD HAVE EXTRA-TERRITORIAL EFFECT, PROVIDED THAT EITHER THE VICTIM OR THE PERPETRATOR IS BASED WITHIN THE STATE?

"4.15 The Commission recommends that extra-territorial effect should apply to the harmful communications offences in the Report:

- where a harmful communications offence is committed by a person in the State in relation to a means of communication that is located outside the State, in the State or
- where harmful communications offence is committed by a person outside the State in relation to a means of communication that is located in the State or
- where a harmful communications offence is committed by a person outside the State if the person is an Irish citizen, a person ordinarily resident in the State, an undertaking established under the law of the State, a company formed and registered under the Companies Act 2014 o ran existing company within the meaning of the Companies Act 2014 and the offence is an offence under the law of the place where the act was committed.[….]"

RCNI Position: We think that regardless of any potential technical difficulties with such provisions, they should be included in our law.

Our Rationale: Amending section 10 of the 1997 Act in relation to extra-territorial effect is necessary as the openness and global nature of cyber-communications means that an attack may be perpetrated by an individual in one jurisdiction on another individual in any other jurisdiction. The location of an individual at the time of an incidence of harassment should not negate the protections which could be afforded to a victim. There is a possibility for conflict with rights or laws of other jurisdictions but this is not a reason to abandon entirely the inclusion of such protective measures.

RECOMMENDATIONS on ISSUE 2: WHETHER THERE SHOULD BE AN OFFENCE OF SERIOUSLY INTERFERING THROUGH CYBER TECHNOLOGY WITH ANOTHER PERSON'S PRIVACY?

"4.04 The Commission recommends that section 13 of the Post Office (Amendment) Act 1951 be repealed and replaced with an offence of distributing a threatening, false, indecent or obscene message by any means of communication and with the intent to cause alarm, distress of harm or being reckless as to this. [….]

The following recommendations cited above are also relevant here:

"4.06 The Commission recommends the enactment of an indictable offence of distributing an intimate image without the consent of the person depicted in the image, or threatening to do so, and with the intent to cause alarm, distress of harm or being reckless as to this […]

[9] R v DeSilva 2011 ONCJ 133

4.07 The Commission recommends the enactment of a summary, strict liability offence of taking or distributing an intimate image of another person without the other person's consent.[…]"

RCNI Position: We agree with the Law Reform Commission that Section 13 of the Post Office (Amendment) Act 1951 should be updated, and that serious interference with another person's privacy through cyber-technology, even on a one-off basis, should be a criminal offence, because of the damage it can cause.

Our Rationale: Criminalising once-off incidents of cyber-harassment which cause harm to their victims through publication (or other indirect communication **about** the victim) is a necessity. The potential harm that can be caused by a once-off action, such as the circulation of intimate sexual photographs or videos without the consent of the subject, is too significant not to be addressed.

An update of section 13 of the *Post Office (Amendment) Act 1951 (as amended in 2007)* is required to include the transmission of electronic communications as the use of social media and other online communication services is too commonplace for them to remain unmentioned in a specific manner. While the *Criminal Damage Act 1991* served to reflect the advancement in technology that had taken place up until that point, the advancements in technology since 1991 are above and beyond what was envisaged at that time and new legislation that reflects 21st century communications is vitally important.

The protection afforded by the *Data Protection Act 1988* and the *Data Protection (Amendment) Act 2003* provides a level of protection of individuals' privacy regarding the posting of harmful content but the lack of protection where content is posted to private social networking pages needs to be rectified. Private social networking pages which are available for individuals other than the person to whom the content refers, can amount to a breach of their privacy and amount to indirect harassment of that individual.

As stated in the Law Reform Commission Issues paper[10] voyeurism, where it takes the form of a once-off observation or recording of an individual carrying out a private act may not meet the persistence test in section 10 of the 1997 Act. The United Kingdom and the Australian State of Victoria have criminalised such acts[11] and such offences should be created here also as this kind of behavior can have severely detrimental effects on the victim.

The proposed measures in the Issues paper would be capable of tackling the problem of once-off activity and could as outlined within the paper bring more attention to the protections available to the public who usually are more informed of the criminal law than the civil law. The global reach and permanence of content published online necessitates measures which are capable of addressing once-off and ongoing activities.

[10] P. 19
[11] *ibid*

2(b): If such an offence were to be introduced, do you consider that it should have extraterritorial effect?

There is a need for extra-territorial effect in any legislation dealing with cyber-harassment. The online harassment of an individual, whether direct or indirect in form, should be prevented by our laws as far as possible regardless of the geographical location of the perpetrator.

2(c): Do you consider that any further reforms to the criminal law are needed to target harmful cyber behaviour affecting personal safety, privacy and reputation?

Any new legislation in this area should be drafted with the inevitable evolution of cyber-communication in mind. For example: the development of communication services such as Snapchat[12] and Cyberdust[13] which differentiate themselves from their competition by promising the permanent deletion of communications after a predetermined period of time illustrate another stage of cyber communications. These services provide an individual with the opportunity to transmit explicit and/or private material to a number of other people with no permanent record of the transmission and in the case of Cyberdust, if a picture is taken of a transmission it cannot be used to identify the sender.

Such developments must be taken into account as technology advances to ensure that gaps in the protection available to individuals do not form which could be exploited by sexual predators, both those who are strangers and those who are known to their victims, who would attempt to abuse cyber-technology to find ways to abuse or continue to abuse those victims.

It may be that it is now appropriate to consider whether a new offence aimed at internet service providers (ISPs) of failing to take down material upon request of an affected person, such as a victim of cyber-bullying, should be introduced. We note that the Law Reform Commission in its Report on Harmful Communications and Digital Safety did not go so far, but recommended instead that an Office of a Digital Safety Commissioner should have powers to oversee and monitor take-down procedures run by ISPs, and to intervene by way of application to the Circuit Court on behalf of an aggrieved person, if an ISP failed to take down material. Failure to comply with a Court Order is itself a criminal offence (contempt of court)

Criminal measures cannot take the place of a simple and workable take-down regime which binds all internet service providers, and which can react swiftly to ensure that offensive or damaging material is removed with the minimum of delay following a request from a person affected.

ISSUE 3: WHETHER CURRENT LAW ON HATE CRIME APPLIES TO ACTIVITY THAT USES CYBER TECHNOLOGY AND SOCIAL MEDIA

[12] https://www.snapchat.com/
[13] http://www.cyberdust.com/

[Not covered in original document]

ISSUE 4: PENALTIES ON CONVICTION FOR OFFENCES

Q4: Do you consider that the current penalties under the offences which can apply to cyber-harassment and related behaviour are appropriate?

The current penalties available are probably capable of providing adequate and suitable sanctions on most individuals who commit an offence under the relevant acts and allow for appropriate sentencing in the general run of cases, however RCNI considers that higher maximum penalties, particularly in the case of section 10 of the Non-Fatal Offences against the Person Act 1997 (harassment in general), should be available so that the extreme gravity of the consequences for their victims, of campaigns of pre-meditated cyber (and other) harassment, both sexual and non-sexual, could be reflected in appropriate cases.

RCNI also considers that higher maximum penalties for all the relevant offences listed would send out a powerful signal to at least some potential perpetrators that harassment, including cyber-harassment, is a serious crime and will be punished accordingly.

ISSUE 5: WHETHER CURRENT CIVIL LAW REMEDIES ARE ADEQUATE

5(a): Do you consider that in addition to section 10(5) of the 1997 Act there should be a separate statutory procedure, to provide for civil remedies for cyber-harassment and serious interferences with an individual's privacy, without the need to institute a criminal prosecution?

As already stated above, it would be desirable to expand the reach of section 10(3) of the 1997 Act to include indirect communications as although these do not constitute communication with the other party they can still cause distress or otherwise interfere with the other party's day to day life and cause further harm. Section 10(5) of the 1997 Act should be amended to include explicit reference to indirect communications, as it appears that such communications are not already included in the scope of this subsection.

Also as stated above, RCNI favours the establishment of a simple, swift and workable procedure binding all internet service providers (ISPs), to enable any person or organization affected to request and secure the take-down of any offensive or damaging material which relates to them, with the minimum of delay. In theory, this aim could be achieved by a statutory civil procedure, as long as the formalities are few and it is possible to get a hearing at very short notice, however it may be that an administrative procedure would work quicker and therefore in this context, better. For this reason, RCNI favours the establishment instead of an Office of a Digital Safety Commissioner with oversight and monitoring functions vis à vis take down procedures run by ISPs. This is recommended by the Law Reform Commission in its Report on Harmful Communications and Digital Safety, cited above. They envisage such an Office acting as an appeal body for complainants who had been refused take down by an ISP, and with powers to apply to the Circuit Court for a (civil) order to take down offending material.

RCNI's view is that a criminal offence against ISPs of failing to carry out any take-downs requested and/or ordered by a court within a reasonable time might be rarely used in the current climate, but its existence would reinforce the importance of the need to comply with reasonable requests and/or court orders.

5(b): Do you consider that any further reform of civil proceedings, over and above those in the 2014 Report of the Internet Content Governance Advisory Group , are required?

RCNI endorses the recommendations of the 2014 Report of the Internet Content Governance Advisory Group insofar as they concern the reformation of rules on discovery against a person not a party to proceedings whether known or not yet known, as the identity of the holder of data is not always readily identifiable online.

5(c): Do you consider that complaints of cyber-harassment and other harmful cyber activity affecting personal safety, privacy and reputation should, without prejudice to any criminal proceedings, be considered by a specialist body that would offer non-court, fast yet enforceable remedies?

A specialist body, such as an Office of a Digital Safety Commissioner as proposed by the Law Reform Commission in its Report cited above, would be of great benefit for many reasons. It could provide expertise in a field that is rapidly expanding and developing which may not always be available to many judges at present. Having a swift separate body with a remit and powers to oversee and monitor take down procedures run by ISPS, and also powers of enforcement where necessary, could have the additional effect of encouraging more victims of cyber-harassment to come forward without the distress associated with criminal proceedings, or the hassle, expense and delay involved in civil proceedings. In a recent study 10% of Irish male teenagers surveyed reported being bullied online and 12% of Irish female teenagers surveyed reported being bullied online[14]. These figures show that a significant number of young people are receiving unwanted communications online and if this trend continues or increases a specialist body may be quite necessary to relieve the potential pressure the courts could face.

5(d): Do you consider that further reforms are required to make effective any orders in civil proceedings that would have extra-territorial effect, including in their application to websites located outside the State; and if so do you have any comments on the precise form they should take?

Further reforms to civil proceedings which would have extra-territorial effect may not be necessary at present as within Europe there are procedures available to pursue online defamation cases and other civil proceedings. The biggest obstacles may be found in cases where one party resides in the United States of America as court orders may not be enforced where they are deemed to be in conflict with their guarantee of free speech in the First Amendment of the US Constitution. In cases such as these, it may be that the way forward is for the responsible Government agencies in this country to work with the many multi-national

[14] Machold, C., Judge, G., Mavrinac, A., Elliott, J., Murphy, AM., and Roche, E. (2012) Social Networking Patterns/Hazards Among Irish Teenagers Irish Medical Journal Volume 105(9) (October 2012)

search engine and social media companies based here to secure their agreement to help restrict and/or remove access to any online material which is shown to harm and to contravene the privacy and other rights of its victims.

Conclusion

Rape Crisis Network Ireland recommends the adoption of the approach proposed in the Law Reform Commission Report on Harmful Communications & Digital Safety, cited above, namely the introduction of some specialized cyber bullying offences, together with the introduction of a Digital Safety Commissioner with powers to manage a simple take-down procedure . RCNI also submits that the introduction of a specific offence aimed at ISPs who fail without reasonable excuse to take down offensive or harmful material, should be considered seriously.

Revised April 2017

Rape Crisis Network Ireland

Carmichael Centre, North Brunswick Street,

Dublin D07 RHA 8

www.rcni.ie

RCNI/LPD/2

Appendix 1: New "grooming" offences introduced by Criminal Law (Sexual Offences) Act 2017 and now in force: Use of information and communications technology to facilitate sexual exploitation of a child

8. (1) A person who by means of information and communication technology communicates with another person (including a child) for the purpose of facilitating the sexual exploitation of a child by that person or any other person shall be guilty of an offence and liable on conviction on indictment to imprisonment for a term not exceeding 14 years.

(2) A person who by means of information and communication technology sends sexually explicit material to a child shall be guilty of an offence and shall be liable—

(a) on summary conviction, to a class A fine or to imprisonment for a term not exceeding 12 months or both, or

(b) on conviction on indictment, to imprisonment for a term not exceeding 5 years.

(3) No proceedings for an offence under this section against a child under the age of 17 years shall be brought except by, or with the consent of, the Director of Public Prosecutions.

(4) In this section "sexually explicit material" means any indecent or obscene images or words.

(5) In this section "child" means a person under the age of 17 years.