LAW SOCIETY SUBMISSION

ISSUES PAPER ON CYBER-CRIME AFFECTING PERSONAL SAFETY, PRIVACY AND REPUTATION INCLUDING CYBER-BULLYING (LRC IP 6-2014)

LAW REFORM COMMISSION

FEBRUARY 2015

ABOUT THE LAW SOCIETY OF IRELAND

The Law Society of Ireland is the educational, representative and regulatory body of the solicitors' profession in Ireland.

The Law Society exercises statutory functions under the Solicitors Acts 1954 to 2011 in relation to the education, admission, enrolment, discipline and regulation of the solicitors' profession. It is the professional body for its solicitor members, to whom it also provides services and support.

The headquarters of the organisation are in Blackhall Place, Dublin 7.

Contents

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

1(a): Do you consider that section 10 of the Non-Fatal Offences Against the Person Act 1997 should be amended to include a specific reference to harassment by cyber means?

1.1. Section 10 of the Non-Fatal Offences Against the Person Act 1997 is widely applicable and inclusively worded to cover many forms of harmful internet behavior, including cyber-harassment, and the Commission rightly note that section 10(1) provides that harassment may be carried out "by any means including by use of telephone".

1.2. However, while the 1997 Act appears to be applicable to many types of serious cyber-harassment, there is potentially a lacuna in protecting victims from actions which are capable of causing distress in one single action such as the sending of sexually threatening message, 'revenge porn' and uploading images of the victim.

1.3. As pointed out in the Issues Paper the meaning of 'persistence', a central concept in the operation of section 10(1), was most recently examined by Mc Carthy J in DPP (O'Dowd) v Lynch.[1] Mc Carthy J noted that the term "persistently" has been interpreted in a manner that is not dependent on a specific number of incidents or a time frame within which those incidents must have occurred.

1.4. Mc Carthy J also indicated that a single protracted incident, for example one person following another on a car journey for a prolonged period of time, could satisfy the quality of persistence necessary to prove harassment.

1.5. He queried:

> *'The only remaining question….is whether or not one unambiguously continuous act has the quality of persistence'.*[2]

1.6. It is submitted that 'persistence' is specific and flexible enough to allow for the successful prosecution of most types of improper conduct while also allowing individuals to engage in permissible, but perhaps unpleasant, conduct. The idea of persistence is an essential characteristic of Section 10 and to overly distort this would render the concept of harassment over-nebulous and broad.

1.7. While a damaging single attack can exacerbate the harm caused to an individual, particularly given the very public nature of cyber-bullying, it is submitted that prosecuting more serious single attack instances which amount to threats to injury or life may be covered by the scope of sections 2 and 5 of the Non-Fatal Offences Against the Person Act

[1] [2010] 3 IR 434 (HC)
[2] Ibid at paragraph 18

1997. These laws are designed to both safeguard individuals from serious cyber-abuse and threats to life while adequately upholding the right to free speech.

1.8. Section 6 of the Criminal Justice (Public Order) Act 1994 is also useful to this end as it makes it an offence to "use or engage in any threatening, abusive or insulting words or behaviour with intent to provoke a breach of the peace or being reckless as to whether a breach of the peace may be occasioned". Read purposively and in conjunction with authorities such as R vs Stacey[3], which was taken in the United Kingdom under broadly similar legislation, this is another safeguard which could protect an accused against cyber-harassment.

1.9. As noted in the Issues Paper, the Criminal Damage Act 1991 can be applied to cyber communication where an individual's social media account or email is targeted by unauthorised access or hacking to send harmful messages or post harmful material.[4] The 1991 Act extends to the deletion and modification of data under section 2(1). Further civil (and criminal) protection is afforded to individuals under the Data Protection Act 1988 and the Data Protection (Amendment) Act 2003 and Article 8 of the European Convention of Human Rights Act 2003 where personal data is posted online without the consent of the subject. This is discussed further below.

1.10. Despite the abovementioned protections and statutory provisions, certain forms of inappropriate online behavior would potentially go unpunished and the Issues Paper notes:

> 'Limiting harassment to persistent behaviour means that posting content online by a single upload which seriously interferes with a person's privacy will not amount to harassment because the communication will not have been made persistently'.

1.11. In this respect the recommendation contained in the 2014 Report of the Internet Content Advisory Group should be followed. It notes that section 13 of the Post Office (Amendment) Act 1951 provides that it is an offence to send by phone or text any message that is grossly offensive, indecent, obscene or menacing and recommends that it should be updated to include social media and other online communications. This amendment would be a useful way to cover 'hard cases' or one off cases which may fall outside the paradigm of traditional harassment or assault and is something which would mark a positive development in protecting individuals against menacing and abusive forms of online abuse.[5]

1.12. In order to maintain the integrity of the right to free speech and to avoid the 'chilling effect' of disproportionately eroding such a right, it would be unduly harsh to criminalise indecency. Thus it is submitted that, if Section 13 was expanded to cover cyber-communications the protection against 'grossly offensive obscene or menacing' statements would be sufficient to protect permissible, but perhaps unpleasant, conduct while criminalising more unacceptable forms of speech. It is suggested therefore that the idea of criminalising 'indecent' communications, as per section 13, would be important if it was to be broadened to cyber-communications.

---

[3] *R v Stacey* Crown Court 30 March 2012, judgment available at http://www.judiciary.gov.uk/Resources/JCO/Documents/Judgments/appeal-judgment-r-v-stacey.pdf.

[4] "Man avoids jail for 'criminal damage to Facebook page'" *Irish Times* 30 June 2014 available at http://www.irishtimes.com/news/crime-and-law/courts/man-avoids-jail-for-criminal-damage-to-facebook-page-1.1850417

[5] Law Reform Commission *Report on Aspects of Domestic Violence* (2013)

1(b): Do you consider that section 10 of the Non-Fatal Offences Against the Person Act 1997 should 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?

1.1. The Law Reform Commission's 2013 Report on Aspects of Domestic Violence noted that consultees had recommended that indirect harassment should be an offence:

> "The specific language used in section 10 would appear to exclude the indirect type of behaviour involved in Debnath [case]. Similarly, harmful messages posted on a private social networking page such as on Facebook may also not be covered by section 10 if they do not involve direct communication with the subject.[6]"

1.2. They are further correct in noting that:

> "Comprehensively criminalising indirect harassment could be done by amending section 10 to include harassing communications with "any person" rather than just the target of the harassing behaviour.[7]"

1.3. Section 10 currently requires that the accused engage in "following, watching, pestering, besetting or communicating with" the victim. The requirement to communicate with the victim appears, prima facie, to limit the application of section 10 to indirect activity.

1.4. There is no reason in principle why indirect harassment shouldn't be legislated for both under Section 10(3) but also under Section 13 of the Post Office (Amendment) Act 1951.

1(c): Do you consider that section 10 of the Non-Fatal Offences Against the Person Act 1997 should 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?

1.5. It is submitted that extra-territorial effect should be legislated for and, as noted in the Issues Paper, that same is permissible under Article 28.4 of the Irish Constitution. However, there is a question over the exact scope of this type of legislation. Any legislation should allow the State to exercise extra-territorial jurisdiction on the basis of the 'passive personality principle'[8], the 'active personality principle'[9] and the 'protective principle'.[10] This would cover offences which originate outside the jurisdiction but affect victims either based in the State or those who have significant ties to this jurisdiction.

---

[6] ibid
[7] ibid
[8] This permits a State to prosecute a person without a connection to a jurisdiction for a crime committed outside its territory against one of its nationals.
[9] This permits a State to prosecute its nationals for crimes committed anywhere in the world if, at the time of the offence, they were such nationals.
[10] This permits a State to assert jurisdiction over a limited range of crimes committed by individuals outside its territory, where the crime prejudices the State's vital interests

1.6. Attempting to assert universal jurisdiction[11] over the area of cyber-harassment, while seeming pro-active, is arguably very difficult to enforce in practice and is perhaps an unrealistic extension of jurisdiction.

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

2(a): Do you consider that there should be an offence introduced that would criminalise once-off serious interferences with another person's privacy where carried out through cyber technology?

2.1. Part of this question has already been addressed in our response to Question 1(a) where it was concluded that sufficient statutory provisions exist for criminalising and deterring once-off serious interferences. As mentioned above, and strictly in relation to privacy, a high level of civil protection is afforded to individuals by the Data Protection Act 1988 and the Data Protection (Amendment) Act 2003 (the Acts).

2.2. The Acts provide a variety of protections for individuals in relation to the posting of harmful content with regard to the collection, dissemination, use and disclosure of personal or sensitive information or "data" by individuals and organisations. The Acts provide remedies where personal data is posted online without the consent of the subject including the right to erasure of the material and a statutory right under Section 7 of the Data Protection Act 1988 to seek damages in respect of any breach of data protection law.[12]

2.3. As the unlawful activity contrary to the Acts does not have to be done "persistently" once-off incidents are capable of being an offence. It is noted that personal data, sensitive personal data and concepts are demonstrably wide and cover a broad subject matter. For example sensitive personal data is defined in the Act as any information relating to:

a) the racial or ethnic origin, the political opinions or the religious or philosophical beliefs of the data subject,
b) whether the data subject is a member of a trade-union,
c) the physical or mental health or condition or sexual life of the data subject,
d) the commission or alleged commission of any offence by the data subject,
e) any proceedings for an offence committed or alleged to have been committed by the data subject, the disposal of such proceedings or the sentence of any court in such proceedings."[13]

[11] Universal jurisdiction is used in various senses, and often refers to cases where a state asserts jurisdiction over certain crimes committed by people without a connection to a jurisdiction against other individuals without a connection to a jurisdiction occurring outside the state's territory and having no other connection to or impact on the prosecuting state.
[12] See *Collins v FBD [2013] IEHC 137*
[13] Data Protection Acts 1988-2003

2.4. In addition the statutory definition of “processing" is also very wide and would appear to cover a host of behaviour including:

“performing any operation or set of operations on the information or data, whether or not by automatic means, including -

a) obtaining, recording or keeping the information, or data
b) collecting, organising, storing, altering or adapting the information or data,
c) retrieving, consulting or using the information or data,
d) disclosing the information or data by transmitting, disseminating or otherwise making it available, or
e) aligning, combining, blocking, erasing or destroying the information or data”.[14]

2.5. A mechanism exists for initiating summary or indictment proceedings for an offence under the Data Protection Act by virtue of Section 31 of the 1988 Act, although it is recognised that this is a cumbersome procedure and is possibly impractical in prosecuting certain types of case.

2.6. Other civil law remedies remain available for interferences with privacy by virtue of Article 8 of the European Convention of Human Rights Act 2003 and there is a well established body of authorities in relation to same.

2.7. Despite this degree of protection, it is accepted that the right to privacy is not an absolute one either under the Irish Constitution or under the European Convention on Human Rights. There may be cases in which the current law does not act as a sufficient deterrent.[15] Further, the lack of specific privacy legislation in Ireland means that we must be careful to safeguard and vindicate a victim’s and an accused’s rights where possible and it is thus important to seek a protective approach to these rights where possible through statute.

2.8. If a new law was in fact to be enacted, it must be done in a proportionate way. For the correct balance to be struck between the right to privacy and freedom of expression, any potential new law should ensure individuals would not face prosecution for disseminating content online that, while embarrassing or hurtful, was not seriously damaging to the victim’s reputation or privacy. In addition, as noted in the Issues Paper, an essential element of the offence might be that there was no sufficient public interest in disseminating the material and that the posting of material either intended to cause serious harm or was reckless as to whether such harm was caused.

[14] ibid
[15] McGee vs Attorney General [1973] IESC also see Niemietz v Germany [1992] ECHR 80

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

Q3: Do you consider that the Prohibition of Incitement to Hatred Act 1989 and the Criminal Justice (Public Order) Act 1994 adequately address hate speech activity disseminated through cyber technology and social media?

3.1. As noted in the Issues Paper, online hate speech is criminalised by the Prohibition of Incitement to Hatred Act 1989 which prohibits incitement to hatred against a group of persons on account of their "race, colour, nationality, religion, ethnic or national origins, membership of the travelling community or sexual orientation."

3.2. Incitement is a very broad concept which includes publication, broadcast and preparation of materials. It is not limited to offline behaviour as it extends to words used, behaviour or material displayed in "any place other than inside a private residence."[16]

3.3. It is also important to bear in mind that there is a prohibition of certain types of hate speech under Article 10 of the European Convention of Human Rights.

3.4. The European Courts have shown a willingness to ban certain forms of 'hate speech' outright, such as Holocaust denial[17], while categorising other forms of potentially offensive speech as acceptable 'political speech'.[18] The jurisprudence of the European Court of Human Rights has been comprehensively strengthened by Framework Decision 2008/913/JHA on combating certain forms and expressions of racism and xenophobia by means of criminal law which would appear to protect victims against racially motivated online attacks.[19] This would allay a number of concerns that protection from hate speech does not go far enough.

3.5. Section 6 of the Criminal Justice (Public Order) Act 1994 makes it an offence to "use or engage in any threatening, abusive or insulting words or behaviour with intent to provoke a breach of the peace or being reckless as to whether a breach of the peace may be occasioned". This confers a wide jurisdiction to prosecute hate speech or speech which incites hatred to a sufficiently serious degree. On this basis it is unclear how useful any new legislation would be.

[16] Prohibition of Incitement to Hatred Act 1989
[17] See for example the decisions of the ECHR in *Giniewski v France, Witzsch v Germany Lehideux and Isorni v France*
[18] Vajnai v Hungary [2008] ECHR 33629/06 (8 July 2008).
[19] Council Framework Decision 2008/913/JHA of 28 November 2008 on combating certain forms and expressions of racism and xenophobia by means of criminal law.

4. 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?

4.1. It is considered that the current penalties are capable of providing adequate and suitable sanctions on most individuals who commit an offence under the relevant Acts and allow for appropriate sentencing in most cases.

5. ISSUE 5: WHETHER CURRENT CIVIL LAW REMEDIES ARE ADEQUATE

5. 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?

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?

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?

5.1. As already discussed above, adequate civil remedies exist under a number of statutory schemes, particularly under the Data Protection Acts 1988-2003. Adding yet another scheme would over-complicate the existing framework.

5.2. The 2014 Report of the Internet Content Governance Advisory Group, insofar as they consider reforming discovery rules against a person not a party to proceedings whether known or not yet known, is a welcome development given that the identity of the holder of data is not always readily identifiable online. However, this reform is outside the terms of this consultation.

5.3. While it may be expedient to have a specialist body dedicated to investigating such issues, the interests of due process and procedural fairness are better secured by keeping such work within the jurisdiction of the courts. As the cyber world and the world of social media

rapidly expand, the issues and questions involved in prosecuting an individual for cyber-harassment are not at all unknown to the judiciary. While a specialist body might appear to be of great benefit, the Society believes that a court of law is the appropriate venue for dealing with questions of fact.

For further information please contact:

Cormac O Culain
Public Affairs Executive
Law Society of Ireland
Blackhall Place
Dublin 7
DX 79

Tel: 353 1 6724800
Email: c.oculain@lawsociety.ie