

Law Reform Commission Public Seminar
on
Cyber-crime affecting personal safety, privacy and reputation including
cyber-bullying

Law Society, Blackhall Place, Dublin 2
Wednesday 22 April 2015

Welcome address by Finola Flanagan, Commissioner, Law Reform
Commission, Ireland

I would like to extend a warm welcome to all the participants in the seminar this afternoon on behalf of the Law Reform Commission and its President Mr. Justice John Quirke. I am the coordinating Commissioner for the project on Crime affecting personal safety, privacy and reputation including cyber-bullying. This project forms part of our Fourth Programme of Law Reform and this seminar forms part of the Law Reform Commission's investigation of the topic and part of its public consultation. We expect to learn a lot both from the members of the panel who will speak today and from you the participants.

The Law Reform Commission is an independent statutory body established forty years ago this year. Its role is to keep the law under review and to conduct research with a view to reform of the law.

This project was widely requested for the Fourth Programme. It is highly relevant and law commissions and others across the world are struggling to find answers to the difficult issues that it presents - issues of our time.

The law needs to keep up with technology and respond to changes it brings about in society. Harmful behaviours need to be addressed in effective ways and rights need to be protected in this context, always bearing in mind that

freedom of expression does not guarantee that speech will never cause harm or distress. I will not attempt to catalogue the types of harmful behaviour that can be encountered on the internet. Anybody who reads the newspapers, so to speak, is aware of the abusive, menacing and bullying communications that are posted every day and of their sometimes devastating effects.

The Law Reform Commission is examining 1) whether the current law is sufficient or capable of being adapted to meet the challenges presented by harmful cyber-communications, or 2) whether a dedicated new law is required or 3) whether both of these are required.

The Law Reform Commission always conducts comparative research for its projects. Amongst the approaches taken in other jurisdictions we have seen that the New Zealand Law Commission has completed a report proposing a Harmful Digital Communications Bill together with a civil enforcement body. The Bill is progressing through Parliament now.

In India we note that the offence of sending offensive messages through a communications service which are “grossly offensive or menacing in character” has been declared unconstitutional for vagueness. In Australia “upskirting” has been made an offence in some states and in the UK an offence has been created this year to address the phenomenon of “revenge porn”. In Nova Scotia the Task Force on Bullying and Cyberbullying produced a report in February 2012 entitled *Respectful and Responsible Relationships: There’s No App for That*. The EU examines and reports on child internet safety and on child trafficking and has implemented a data protection regime applicable across the European Economic Area.

At home the matter has received attention too. The Internet Content Governance Advisory Group reported to the Minister for Communications, Energy and Natural Resources in 2014 having examined the general policy

setting and governance arrangements needed to address harmful online material. A joint Oireachtas committee reported on the growth of social media and cyber-bullying in July 2013 by way of example. Our [Issues Paper](#) addresses five issues.

- Whether the offence of harassment contained in the Non-Fatal Offences Against the Person Act 1997 Section 10 which provides that harassment can be committed “by any means including by means of use of the telephone” should refer explicitly to “cyber-harassment”. We ask whether the offence should also apply to indirect cyber-harassment where comments are made about someone on the internet and not directly to them. Harassment as currently defined probably does not catch such communications because the communication is required to be “with” the victim and not only about him or her.
- Should there be a new offence of a single serious interference with another’s privacy through cyber-technology where there is no persistence involved? This would not appear to be caught by Section 10 in its current formulation.
- We ask whether hate crime laws are adequate for cyber-technology and social media?
- We examine penalties and their adequacy and appropriateness, and
- the adequacy of civil law remedies.

We will gratefully consider any other suggestions you might make and there is still time to answer the questions in the Issues Paper.

We already have laws that can be applied to cyber-bullying and related issues. In criminal law we have, for example, the offence of harassment, an offence of sending menacing telephone and text messages which could easily be extended to all cyber-communications, a hacking offence and data protection offences. On the civil side we have a constitutional right to privacy, defamation, civil remedies, and data protection laws in relation to which it would appear that the Court of Justice of the European Union takes a very expansionist approach.

The online world is a new world. We live in a digital age which has given us not just a medium of communication but, and especially for younger people, a real place where people live a large portion of their lives through social media. This place is free and open, uncensored, where free speech is central and anonymous if wished. Yet at the same time every online communication can be permanently associated with the maker.

The question for us is how our laws balance free speech with privacy, acknowledging at the same time that law, whether criminal or civil, is not a complete answer. Regulation of industry, governance and above all education are key elements in developing a proper online behaviour that is respectful of others.

END