Irish Council for Civil Liberties

To	Joint Committee on Justice and Equality
Date	6 October 2019
Authors	Elizabeth Farries, Doireann Ansbro, and Grace Tierney

The Irish Council for Civil Liberties (ICCL) thanks the Joint Committee for the opportunity to provide input towards this important topic of online harassment, harmful communications and related offences.

1 Harassment and harmful communications are amplified online[1]

Online harassment and harmful communications are significant social problems, which mirror various structural exclusions occurring offline. Despite early optimistic predictions that online spaces would be safe, we are seeing the opposite - harassing and harmful behaviour is amplified online.[2] The types of various online abuses have been well documented:[3] Stereotyping, objectification, doxing, intimidation, threats and abuse can all spread like wildfire with an easy series of posts and shares.

a. This is a gendered problem

While anyone can be a victim of online harassment or harmful communications, research shows that most victims of certain types of online harassment are women and most perpetrators are men.[4] Indeed, a recent figure shows that **23% of women across the EU have reported experiencing online abuse in their lifetime.**[5] Intersectional factors influence the likelihood of experiencing online harassment. The LGBT+ community is at

[1] This section draws from Farries E and Sturm T (2018) Feminist legal geographies of intimate-image sexual abuse: Using copyright logic to combat the unauthorized distribution of celebrity intimate images in cyberspaces. EPA. Economy and Space 51(5): 1145 – 1165.

[2] See comprehensive work by Mary Anne Franks on this subject, including Franks MA (2011) Unwilling avatars: Idealism and discrimination in cyberspace. Columbia Journal of Gender and Law 20(2): 224–261; Franks MA (2012) Sexual harassment 2.0. Maryland Law Review 71(3): 655–704; Franks MA (2015) Drafting an effective 'revenge porn' law: A guide for legislators. https://papers.ssrn.com/sol3/papers.cfm?abstract_id¼2468823

[3] Citron DK provides an excellent overview at (2014) Hate Crimes in Cyberspace. Cambridge: Harvard University Press.

[4] See Farries E and Sturm T discussion at 1148 Feminist legal geographies of intimate-image sexual abuse: Using copyright logic to combat the unauthorized distribution of celebrity intimate images in cyberspaces. EPA. Economy and Space 51(5): 1145 – 1165. See also https://www.amnesty.org/en/latest/news/2017/11/amnesty-reveals-alarming-impact-of-online-abuse-against-women

[5] James HH (2019) 7 Appalling Facts You Should Know About Online Abuse of Girls and Women. Global Citizen. https://www.globalcitizen.org/en/content/misogynist-online-abuse-digital-harassment-sexism/

increased risk.[6] One's race,[7] religion,[8] ethnicity,[9] mental health,[10] and ability,[11] are also risk factors.

b. Image-based sexual abuse

The Committee is considering responses to extreme forms of gendered online harassment including 'revenge porn', 'upskirting', 'downblousing'. ICCL takes issue with 'revenge porn' as a term. This isn't pornography, it's abuse. It is therefore better to describe these categories of offences as 'image-based sexual abuse'[12] to describe non-consensual creation and/or distribution of private sexual images.[13] This term better captures the sexualized violence, behaviours and harms involved without being reduced to specific motivations like so-called 'revenge'. However, the motivation behind gendered online harassment, in general, is to violate a person's personal autonomy, dignity, and privacy in a sexualised way.[14]

Image-based sexual abuse is widespread. Perpetrators include former/current intimate partners, acquaintances, and/or anonymous trolls. Diverse experiences can range from chilling effects to online participation with peers, withdrawal from public spaces, job loss and loss of economic opportunity, widespread online and offline harassment, and significant

[6] McGlynn and Rackley (2017: 39) for example observe that men who do not conform to conventional masculine norms or stereotypes are at greater risk. McGlynn C and Rackley A (2017) Image-Based Sexual Abuse. Oxford Journal of Legal Studies 37(3): 534–561. Similarly, people who identify as lesbian, gay, or bisexual (LGB) are also at a higher risk: 17% of LGB American internet users have either had an image shared without their consent or have had someone threaten to share an image of them compared to 3% of heterosexual users. Lenart A, Ybarra M and Price-Feemey M (2016) Nonconsensual Image Sharing: One in 25 Americans has been a Victim of 'Revenge Porn'. New York: Centre for Innovative Public Health Research and Data & Society Research Institute. https://datasociety.net/pubs/oh/Nonconsensual_Image_Sharing_2016.pdf

[7] The European Network against Racism reported 256 incidents of reported racism (it should be noted that not all incidents will be reported) in the latter half of 2017, with almost half of these (113) concerning online abuse. (https://www.socialjustice.ie/content/policy-issues/say-no-racism)

[8] The Pew Research Center reports for example that 5% of the American population reports being the victim of online harassment specifically because of their religion. Duggan, M (2017) *Online Harassment 2017*. Pew Research Center: 3. https://www.pewinternet.org/2017/07/11/experiencing-online-harassment/ Additionally, TellMAMA, a Uk-based secure and reliable service that allows people from across England to report any form of Anti-Muslim abuse states the of the reported anti-Muslim incidents reported to them in 2018, 30% occurred online.https://tellmamauk.org/wpcontent/uploads/2019/09/Tell%20MAMA%20Annual%20Report%202018%20_%20Normalising%20Hate.pdf

[9] The Pew Research Center reports that 8% of the American population reports being the victim of online harassment because of their ethnicity. Duggan, M (2017) *Online Harassment 2017*. Pew Research Center: 3. https://www.pewinternet.org/2017/07/11/experiencing-online-harassment/

[10] Merrill, R. M., & Hanson, C. L. (2016). Risk and protective factors associated with being bullied on school property compared with cyberbullied. *BMC public health*, *16*, 145. Being bullied on school property or cyberbullied was significantly positively associated with mental health problems. Of all of the factors examined in their study, Merrill and Hanson state that the association with cyberbullying was highest with mental health problems.

[11] UK-based charity Leonard Cheshire released findings on 11 May 2019 that recorded incidents of online harassment of the disabled are up by almost a third (33%) in the last year. https://www.leonardcheshire.org/about-us/press-and-media/press-releases/online-disability-hate-crimes-soar-33

[12] McGlynn C and Rackley (2017) More than 'revenge porn': Image-based sexual abuse and the reform of Irish Law. Irish Probation Journal 14: 38–51.

[13] McGlynn C and Rackley (2017) More than 'revenge porn': Image-based sexual abuse and the reform of Irish Law. Irish Probation Journal 14: 38–51.

[14] West Coast LEAF (2014) Using and Strengthening Canadian Legal Responses to Gendered Hate and Harassment Online. Vancouver: West Coast LEAF. Available at: www.clicklaw.bc.ca/resource/2867.

mental health impacts including suffering leading to suicide.[15] The harms are cumulative and often extend beyond the individual: the loss of dignity, privacy and sexual autonomy can, working together, instill 'cultural harms that can impact society as a whole'.[16] Other rights affected are the rights to physical and mental health; freedom of expression, assembly and association; the right to participate in civic and political spaces; the right to be treated with dignity and respect and the right to earn a livelihood.

2 Gendered online harassment - the context in Ireland[17]

a. Dara Quigley

Weakness in the Irish legal regime for addressing gendered harassment online can be framed by the tragic case of Dara Quigley. Dara Quigley was an Irish activist and journalist. In 2017, members of An Garda Síochána detained Ms Quigley under Ireland's Mental Health Act for walking naked in a Dublin street. CCTV cameras installed at the location captured Ms Quigley's images. This recording was held by An Garda Síochána, but within days was shared on a WhatsApp group and posted on Facebook.[18] The images were viewed around 125,000 times before removal.[19] Several days following her wide spread experience of image-based sexual abuse, Dara Quigley committed suicide. In a statement, Ms Quigley's family said that the release of the video was 'egregious and deeply hurtful'.[20]

Accountability for this use of Ms Quigley's data and the effect it had on her mental health and right to life remains elusive. No individual or organisation has been held responsible. Questions remain about institutional procedures around storing of data, access to data and the ability to share; as well as company procedures to remove the data.

This is in part because of an inadequate legal framework around the use and abuse of sexualised imagery without consent, a lack of transparency around individual company standards on moderation content and removal, and a culture of online harassment that mirrors real world ills.

b. CCTV use in Ireland and data collection and processing risks

The widespread and increasing installation of CCTV cameras for law enforcement by the state in Irish public spaces is controversial and includes a gendered dimension. Under Irish Law, the Garda Commissioner may authorise the installation and operation of CCTV to secure 'public order and safety in public places by facilitating the deterrence, prevention,

---

[15] Farries, E & Sturm, T (2018) 'Feminist legal geographies of intimate-image sexual abuse: Using copyright logic to combat the unauthorized distribution of celebrity intimate images in cyberspaces.' Environment and Planning A: Economy and Space. DOI: 10.1177/0308518X18786964

[16] C McGlynn and E Rackley, 'More than "revenge porn": Image-based sexual abuse and the reform of Irish Law' (2017) Irish Probation Journal 14, 38-51.

[17] This section draws from Farries, E (2018) 'Gendered Perspectives on Privacy'. Invited submission UN Special Rapporteur on Privacy Annual report to Human Rights Council 2019. A/HRC/40/63 advanced unedited version.

[18] Rónán Duffy, *'Deplorable and revolting' treatment of deceased activist Dara Quigley is raised in the Dáil*, TheJournal.ie (May 2017) http://www.thejournal.ie/dara-quigley-dail-3384651-May2017/

[19] Conor Feehan, *Garda who filmed tragic journalist Dara Quigley to avoid prosecution*, Independent.ie (August 2018) https://www.independent.ie/irish-news/garda-who-filmed-tragic-journalist-dara-quigley-to-avoid-prosecution-37184945.html

[20] Rónán Duffy, *'Deplorable and revolting' treatment of deceased activist Dara Quigley is raised in the Dáil*, TheJournal.ie (May 2017) http://www.thejournal.ie/dara-quigley-dail-3384651-May2017/

detection and prosecution of offences'.[21] However, using CCTV to maintain public order and safety is based on flawed logic: crime levels in Ireland are not sufficiently high to warrant blanket surveillance, there is significant research suggesting CCTV doesn't effectively deter crime more than other methods with less impact on privacy,[22] and footage of crimes does not necessarily lead to higher detection rates.[23] Given this, it's not clear that the legality, necessity and proportionality required to justify CCTV's threat to privacy[24] and data protection rights, together with closely associated rights,[25] are met. Legislation must specify in detail the precise circumstances in which such interferences may be permitted[26] and current Irish law does not provide this level of precision. Given the questions around the effectiveness of CCTV in deterring crime, ICCL questions whether its widespread use is necessary. Further, if there are other methods of deterring crime that would prove as effective but pose less of a threat to rights (such as streetlights), the requirement of proportionality cannot be met.

ICCL is concerned that the more data that is captured by use of both public and private CCTV exposes individuals, and, as demonstrated by Dara Quigley's experience, in particular marginalised individuals, to the risk that the data captured will be shared online. To mitigate this risk, clear legal protections must be in place around the retention, management and oversight of, as well as access to, and sharing of CCTV footage, in particular where intimate images are captured. As Dara Quigley's experience highlights, images are at risk of abusive redistribution and degrading treatment without the subject's consent. The speed and reach of online platforms when sharing such data requires additional safeguards both at the image sharing stage and at the image capture and retention stage.

Additionally, with the advent of facial recognition technology, women become more vulnerable to this form of exposure since their images can now be more directly connected to their identity. In other jurisdictions, women, particularly women of colour, have found themselves at an increased risk of being misidentified by facial recognition technology leading them to being targeted incorrectly by policing authorities.[27] ICCL is firmly against the introduction of facial recognition technology into the Irish policing context.

---

[21] Section 38 of Garda Síochána Act 2005.

[22] See for example this study, which finds CCTV poses no more of a deterrent than street lights: T Lawson, R Rogerson and M Barnacle, 'A comparison between the cost effectiveness of CCTV and improved street lighting as a means of crime reduction' (2018) 68 Computers, Environment and Urban Systems 17-25.

[23] See an excellent discussion by Dr TJ McIntyre, *Duleek use of CCTV to fight crime based on flawed logic*, IrishTimes.com (November 2017) https://www.irishtimes.com/opinion/duleek-use-of-cctv-to-fight-crime-based-on-flawed-logic-1.3297639

[24] These rights are enshrined in numerous regional and international human rights instruments and case law findings including article 40.3 of Ireland's Constitution, *Kennedy and Arnold v Attorney General* [2005] IESC, Article 8 of the European Convention of Human Rights, Article 12 of the Universal Declaration of Human Right and Article 17 of the International Covenant on Civil and Political Rights.

[25] Including freedom of opinion and expression, and to seek, receive and impart information; freedom of peaceful assembly and association; and right to family life. These rights all linked closely with the right to privacy and, increasingly, are exercised through digital media. See Report of the United Nations High Commissioner for Human Rights, *The right to privacy in a digital age* (2018), A/HRC/39/29.

[26] See Report of the United Nations High Commissioner for Human Rights, *The right to privacy in a digital age* (2018), A/HRC/39/29 paras 5 – 11.

[27] See https://www.libertyhumanrights.org.uk/resist-facial-recognition. For a broader discussion on the human rights problems engaged by policing surveillance technology, please see: https://www.inclo.net/pdf/spying-on-dissent-Report_EN.pdf

c. ICCL qualitative findings[28]

ICCL recently engaged with a number of Irish NGOs, academics, and state agencies in order to research the experiences and effects of gendered online harassment and surveillance in Ireland.[29] Respondent bodies detailed anonymised information obtained from clients and stakeholders who told of their experiences of online harassment, including online surveillance by controlling partners in the form of monitoring, observing, tracking and intimidation, as well as public shaming and myriad forms of invasions of privacy.

According to these bodies, most victims of online harassment are women. Age and relationship status appear to be factors: Common victims of online surveillance are women from 16 years of age upwards and perpetrators are most commonly found to be partners, prospective partners, or ex-partners attempting to exert coercive control. Examples include the use of spyware phone applications marketed as parenting tools to help monitor children's activities being used by their partners to spy on women. Women have their movements monitored and are subject to questioning by partners about their activities because of online tracking by their partners. Online surveillance is used to gain control, power, and/ or influence over women.

Controlling or harassing behaviour manifests online beyond observation and resultant manipulation. Harmful text, videos, and photos can be posted online that are designed to humiliate, harass and deter expression and participation. This is true of partners, ex partners, and strangers. Respondents detailed victims feeling targeted online and a continuing pressure of 'feeling watched' even when they were offline, another demonstration of the effect of online abuse offline. Due to such pressure, victims often lose confidence and avoid public places, both online and offline, because they are made to feel ashamed and fear for their safety. Victims of online harassment suffer a double blow to their rights - not only are they subjected to harmful behaviour but they are deprived of a forum for sharing their experiences because of the chilling effect on their participation in public spaces.

3 Regulatory and legal responses

a. Emerging laws

In recent years, state regulators have begun to respond to gendered harassment and harmful communications online. There is an emerging trend in domestic and international law,[30] together with domestic proposals for the criminalisation of image-based sexual abuse, which may provide another avenue for redress.

---

[28] This section draws from Atim, E (2019) 'Gendered Surveillance Online and Associated Harassment of Marginalised Groups (A Case Study in Ireland)'. ICCL would like to thank Esther Atim for her diligent research and Open Society Foundations for their generous support of Ms Atim's research fellowship with ICCL.

[29] ICCL met with Child Rights Alliance, the National Women's Council of Ireland, Rape Crisis Centre, academics, and affected individuals.

[30] See Farries E and Sturm T discussion at 1148 Feminist legal geographies of intimate-image sexual abuse: Using copyright logic to combat the unauthorized distribution of celebrity intimate images in cyberspaces. EPA. Economy and Space 51(5): 1145 - 1165 which states that these laws are often targeted at 'cyberbullying' however and do not address the gendered social harms emerging from cybermisogyny. See also for example the 2018 declaration from the New South Wales Government that laws will be strengthened to protect people from cyberbullying and online trolling and keep up with changes to technology. B Kontominas, *Online trolls and cyberbullies in NSW face up to five years in jail under law change*, ABC.net.au (October 2018) http://www.abc.net.au/news/2018-10-07/online-trolls-and-cyberbullies-in-nsw-face-tougher-new-laws/10348246?pfmredir=sm

- In **England and Wales**, Section 33 of the Criminal Justice and Courts Act 2015 introduced the offence of 'disclosing sexual photographs and films with intent to cause distress'.[31]
- In **Scotland**, the Abusive Behaviour and Sexual Harm (Scotland) Act 2016 introduced the offence of 'disclosing or threatening to disclose an intimate photograph or film'.[32]
- In **Australia**, in addition to regional legislative sanctions, the government has implemented an eSafety Commissioner. This is a statutory body which tackles online abuse, has a reporting system for those experiencing cyberbullying, and removes illegal content online. The establishment of a similar statutory body in Ireland was a key recommendation from the Law Reform Commission.[33]

There are, as yet, no specific laws addressing this phenomenon in Ireland.[34] At present, cases of image-based sexual abuse, and other acts of online abuse and harassment are taken under section 10 of the Non-Fatal Offences Against the Person Act 1997 (NFOAPA). This Act covers general harassment but the language of section 10 is not always directly transferable to cases of online harassment. In addition, the requirement that harassment consist of 'persistently following, watching, pestering, besetting or communicating' means the prosecution have to prove a *pattern* of harassment. This opens a lacuna in the law whereby individual acts of harassment can't be prosecuted effectively. A particular obstacle in the law that needs to be addressed is that fact that currently the crime of harassment requires a pattern. In particular, there is a clear gap within the NFOAPA. Further, ICCL has previously highlighted the way the interception of communications, data retention, and surveillance by the police raise significant issues in which privacy rights under human rights instruments are engaged. The absence of effective laws criminalising online harassment means the perpetrators often go unpunished and victims are left without protection or justice.

The Irish government has committed through a National Action Plan to implement the UN Guiding Principles on Business and Human Rights. This plan requires the government to take action to ensure that companies, including large corporations, engage in due diligence assessments of the impact of their activities on human rights and take action to remedy rights violations. Principle 10 of the implementing standards within the National Action Plan requires the government to encourage businesses to engage with human rights reporting

[31] Section 33 applies to the disclosure of 'private sexual photographs or films,' with private being defined as not 'of a kind ordinarily seen in public.' It is also worth noting that this legislation equally extends to online and offline disclosure, using no technology-specific wording. Criminal Justice and Courts Act 2015, s34(2); s35(2). The introduction of legislation of this nature led to a significant increase in the reporting of distribution activity in the jurisdiction. Between the period of February 2015 (when the Act received Royal Assent) and January 2016, 1,200 cases were reported. This is in comparison to 149 cases during the previous two and a half years. While the legislation had a positive effect on the rate of reporting crimes of this nature, this Act is restricted nature in scope and limited in redress.

[32] The Scottish Act carries a higher punishment in comparison to that of England and Wales. It also covers threats to disclose intimate materials. This is a notable and important extension offence as the threat of such behavior has the potential to be equally harmful as their release, and be used to control or blackmail the individual depicted in the materials.

[33] Report on Harmful Communications and Digital Safety, Law Reform Commission 2016, 143.

[34] We acknowledge the call for legislation from the Law Reform Commission Report at https://publications.lawreform.ie/Portal/External/en-GB/RecordView/Index/37669 and also The Harassment, Harmful Communications and Related Offences Bill, tabled in 2017, currently before the Dáil Éireann https://www.oireachtas.ie/en/bills/bill/2017/63/

standards, including the UN Principles Reporting Framework. This would contribute to greater transparency around the activities of companies and their impact on human rights, including actions on content moderation and responses to complaints of online harassment.

b. Rights concerns attached to regulatory attempts[35]

Our fundamental rights are implicated by state and corporate regulation of harmful content on online platforms, in particular our rights to freedom of opinion and expression, and to seek, receive and impart information; freedom of peaceful assembly and association; and right to family life. These rights all linked closely with our right to privacy [36] and, increasingly, are exercised through digital media.[37] Our rights are not changed or reduced online[38] and apply to all forms of online communication.[39] Legislation in Ireland is required to conform with Ireland's human rights obligations under the Irish Constitution, the European Convention on Human Rights, and the international human rights treaties that Ireland has ratified. Where EU law is engaged, it must also comply with the EU Charter on Fundamental Freedoms.

Introducing online harassment offences may go some way towards filling the identified lacuna of effective responses to online harassment and harmful communications. However, this is just one part of a larger necessary response. Further, the various pieces of legislations must be drafted carefully to ensure that they don't constitute a disproportionate interference with our rights.

Mechanisms used and suggested to limit content online have included a combination of monitoring, reporting, pausing, reducing, removing, filtering, blocking, or censoring online content. Given the potential for rights limitations that content moderation entails, the State must act carefully to ensure such limitations conform to the requirements of the Irish constitution and applicable human rights law. As such, any limitations must conform to the principles of legality, necessity, and proportionality and the strict requirements of the three part test: the restriction must be prescribed by law, pursue a legitimate aim, and be necessary in pursuit of that aim.

In light of these principles, ICCL calls on the Government to ensure that the following points are taken into account when drafting new legislation in this area:[40]

---

[35] This section draws heavily from Farries, E (2019) 'Regulation of online content'. Submission to The Department of Communications, Climate Action and Environment. 5pp. https://www.iccl.ie/news/iccl-submission-to-the-public-consultation-on-regulation-of-online-content/

[36] Our right to privacy is protected by Article of 12 of the Universal Declaration of Human Rights (UDHR), Article 17 of the International Covenant on Civil and Political Rights (ICCPR), Article 8 of the European Convention on Human Rights (ECHR), and Article 7 of the Charter of Fundamental Rights of the EU (EU Charter). In correlation, our personal data is also protected under Article 8 of the EU Charter. In the Irish Constitution, a right to privacy has also been identified as one of the unenumerated rights stemming from the wording of Article 40.3; see *Cullen v. Toibín* [1984] ILRM 577.

[37] See Report of the United Nations High Commissioner for Human Rights, *The right to privacy in a digital age* (2018), A/HRC/39/29.

[38] The United Nations Human Rights Council has stated that the same rights people have offline must also be protected online. This is particularly true for freedom of expression, which is applicable regardless of frontiers and through any media of one's choice, in accordance with articles 19 of the UDHR and the ICCPR. See UN Doc A/HRC/32/L.20.t,https://documents-dds-ny.un.org/doc/UNDOC/LTD/G16/131/89/PDF/G1613189.pdf?OpenElement

[39] The right to freedom of expression for example applies to all forms of electronic and Internet-based modes of expression. See UN Human Rights Committee, General Comment No.34 on Article 19: Freedoms of opinion and expression, CCPR/C/GC/34, (2011). https://www2.ohchr.org/english/bodies/hrc/docs/gc34.pdf.

- **Blanket monitoring is not rights compliant.** Generalised monitoring of online content in order to detect gendered harassment or harmful communication would raise rights concerns.
- **Standardised definitions and removal procedures have proved fallible**. 'Online harassment' and 'harmful communications' would need to be defined with sufficient precision to enable an individual user to understand the prohibited conduct and therefore adapt their behaviour accordingly. At ICCL we are not certain online harassment or harmful communication can be defined with such precision.
- **Transparency problems prevent us from making the best evidenced based decisions.** The 'lack of transparency in relation to decision-making by intermediaries often obscure discriminatory practices or political pressure affecting the companies' decisions'.[41] We need more transparency and information, particularly from companies, in order to best decide how to moderate content most effectively.
- **Effective content moderation is rights compliant moderation.** States should only seek to restrict content pursuant to judicial processes.[42]

4. Recommendations

a. Laws

In order to ensure that any new law respects and protects rights to the greatest extent possible, the Government should:

- **Draft specific laws targeting specific actions in line with international norms,** for example:
  - amend the NFOAPA to criminalise image-based sexual abuse
  - create a civil wrong addressing image-based sexual abuse
- Ensure **accessible civil remedies** for victims of online harassment, including restitution and compensation.
- **Reform legal aid** rules to allow for victims, who otherwise could not afford to, to institute proceedings for rights violations.
- **Don't draft overly broad or poorly defined laws.** ICCL is not certain 'online harassment' or 'harmful communication' can be defined with such precision sufficient precision to enable an individual user to understand the prohibited conduct and therefore adapt their behaviour accordingly.
- No **blanket monitoring by companies or State actors**. This applies to both States and Companies in order to ensure privacy rights are respected. Actions such as content moderation or legal enforcement proceedings should be taken in response to complaints.

[40] See also Farries, E (2019) 'Regulation of online content'. ICCL Submission to The Department of Communications, Climate Action and Environment. 5Pp https://www.iccl.ie/news/iccl-submission-to-the-public-consultation-on-regulation-of-online-content/

[41] Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, A/HRC/17/27, (2011) paragraph 42. https://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf

[42] See more at Freedex, 'The Special Rapporteur's 2018 report to the United Nations Human Rights Council is now online' (*A Human Rights Approach to Platform Content Regulatio*n, 6 April 2019), https://freedex.org/a-human-rights-approach-to-platform-content-regulation/ . ''States should only seek to restrict content, other than criminal behaviour, pursuant to an order by an independent and impartial judicial authority, and in accordance with due process and standards of legality, necessity and legitimacy''

- **Legislate for Corporate and State Transparency.** ICCL supports the recommendations of the Special Rapporteur on Freedom of Expression[43] and also the Santa Fe principles[44] for explicit transparency. Transparency is essential for both corporate and State responses to harmful content. Transparency includes at minimum full disclosure of the rules used to moderate content and how those rules are applied together with functional appeals processes and accountability for wrongful takedown.
- In line with the UN Guiding Principles on Business and Human Rights[45] and Ireland's National Action Plan on Business and Human Rights[46], ensure that social media companies are engaging in proper due diligence when it comes to the human rights impact of their activities and services. In particular, under principle 10 of the implementing standards, encourage businesses to engage with human rights reporting standards, including the UN Principles Reporting Framework.[47]

b. Garda reform

Legislation alone will not achieve protection. It is important to tackle law enforcement culture too.

- **Reframe Irish policing to ground it in principles of human rights that include online and gendered considerations**. The influence and impact of human rights principles and standards remain superficial or absent in many key areas of Garda policy and operations; respect for gendered rights - online and off - when dealing with CCTV footage is but one of them, as explored above.[48] The gendered aspects of rights need to be understood across An Garda Síochána.
- **Assess awareness of gender rights and concerns regarding online harassment across law enforcement units**. Develop and integrate modules that identify the gendered implications of online harassment and harmful communications into training. Deliver training that has measurable short and long term indicators of awareness and success built into the programmes.
- **Develop and integrate risk assessments for gendered harassment online**, including image-based sexual abuse. Appoint liaison-officers who are trained to investigate and respond to these instances of assault through reference to leading international models.

---

[43] UN Doc A/HRC/38/35 (18 June−6 July 2018).

[44] The Santa Clara Principles On Transparency and Accountability in Content Moderation', available at: https://santaclaraprinciples.org. The principles state that, at minimum, companies should (1) publish the numbers of posts removed and accounts permanently or temporarily suspended due to violations of their content guidelines; (2) provide notice to each user whose content is taken down or account is suspended about the reason for the removal or suspension; and (3) provide a meaningful opportunity for timely appeal of any content removal or account suspension. It is the position of ICCL that states should be held to an equally high transparency standard.

[45] UN OHCHR (2011). Guiding Principles on Business and Human Rights. Implementing the United Nations "Protect, Respect and Remedy" Framework https://www.ohchr.org/Documents/Publications/GuidingPrinciplesBusinessHR_EN.pdf

[46] Government of Ireland (2017) National Plan on Business and Human Rights 2017-2020 https://www.dfa.ie/media/dfa/alldfawebsitemedia/National-Plan-on-Business-and-Human-Rights-2017-2020.pdf

[47] The UN Guiding Principles Reporting Framework (nd) https://www.ungpreporting.org/

[48] 'While the Garda Code of Ethics already names Human Rights as one of its three guiding principles, there has not been the comprehensive implementation of human rights throughout the organisation which would deliver real change.' Alyson Kilpatrick, 'A human-rights based approach to policing in Ireland' (2018). https://www.iccl.ie/wp-content/uploads/2018/09/Human-Rights-Based-Policing-in-Ireland.pdf

- **Sanction egregious image-based sexual abuse by law enforcement officials** by both internal disciplinary and external disciplinary means, or through criminal procedures if the behaviour reaches a criminal threshold. Create protocols for victim redress, including consistent and regular communication with victims' and deceased victims' families throughout an investigation and until the matter is satisfactorily concluded.

c. Surveillance technology

- **Don't contribute to online harassment with policing surveillance technology**. Surveillance technology, including CCTV and facial recognition, contribute to rather than solve a culture of gendered online harassment.[49] Given the risks and lack of effective regulation and procedures, such technology causes more harm to than good. Vast networks of surveillance significantly undermine rights and freedoms.[50]
- **For areas with existing public online surveillance, deploy Data Protection Impact Assessments** to consider their ongoing need and create a policy for each system outlining precisely who the data controller is, how to make an access request and the retention periods.[51] We add that risk assessments for surveillance tech should also necessarily carry a gendered component.
- Ensure better regulation of Spyware technology available to consumers. Those being tracked should have to consent to such spyware on their phones, (including children). The impact of such applications on the right to privacy should be assessed and robust privacy protections should be in place before use can be authorised. Nobody should be tracked or monitored by Spyware without their full knowledge and informed consent.

d. Research, education, and awareness

- To properly respond to this issue, the government should undertake a comprehensive research project, supported by civil society organisations, to effectively assess the impact and consequences of different forms of online harassment on victims. The conclusions and recommendations of this research should inform legislative and other responses.
- An education campaign directed at the population as a whole should be undertaken in order to discuss and promote appropriate social norms online. Currently, unacceptable behaviour offline is considered acceptable online. This needs to be addressed.

[49] Also, there are data protection principles at play. We have to date not seen disclosed examples of Privacy Impact or Risk Assessment carried out for the CCTV installations in Ireland. For the various systems installed, I am not able to determine who precisely the data controller is, under what policies and procedures individual garda are given access to potentially sensitive CCTV footage, or what ethical or rights based training - including components training for gendered privacy rights - Gardaí receive to prevent the abuse or degrading treatment of captured images.

[50] Read more at https://www.inclo.net/pdf/spying-on-dissent-Report_EN.pdf

[51] Ireland's Data Protection Commissioner provides further comprehensive advice: https://www.dataprotection.ie/sites/default/files/uploads/2019-05/CCTV%20guidance%20data%20controller.pdf