Law Commission *Harmful Online Communications Offences Consultation*

Cyberflashing and Image-Based Sexual Abuse

Submission by Professor Clare McGlynn and Dr Kelly Johnson, Durham University

Executive Summary

A. **Sexual intrusion:** Cyberflashing should be understood as a form of *sexual intrusion* similar to other forms of sexual violence and abuse and should therefore be treated as a sexual offence.
B. **Victims predominantly women:** Cyberflashing is a common experience, with women, and young women in particular, facing the highest rates of victimisation and disclosing the most negative impacts.
C. **Black and minoritised women particularly affected:** Online abuse has been rising since the pandemic, with black and minoritised women particularly affected.
D. **Men's motives are varied and interconnected** – including threatening, causing distress, sexual gratification, power and control, bravado among men - and the law should not be limited to only motive to cause distress.
E. **Infringes sexual autonomy:** Cyberflashing is always an infringement of an individual's sexual autonomy and is always wrong, regardless of the perpetrator's motive or whether the victim-survivor experiences any particular harm.
F. **Harms wide-ranging and extensive:** The harms of cyberflashing can be serious and can include sexual violation, humiliation, and inducing fear and threat, as well as impacting on women's everyday lives, and on society as a whole.
G. **Sexual offence based on non-consent:** A new criminal offence should be based on non-consent as the core wrong of cyberflashing, without the need to prove particular motives of offenders.
H. **Law cover all penis images:** An offence must not be limited to only images of the perpetrator's penis otherwise it will be unenforceable and fail to recognise the nature of victim's experiences.
I. **Motives should include humiliation:** If the law is to require particular motives, this should include humiliation, as well as causing alarm or distress.
J. **Law should include recklessness:** The law should also cover a perpetrator who is aware of a risk of causing harm, even where that is not his direct intention (recklessness).
K. **Revised communications offence:** support for recommendations based on 'likely harm' to be caused, not proof of actual harm; focus on likely audience, not reasonable person; including awareness of risk of harm.
L. **Educative role of criminal law:** While the criminal law is only ever a first step, and education and prevention initiatives are vital, a new criminal law can send a message to victims that their experiences and harms are understood and recognised, and to society as a whole that this conduct is wrong and should not be normalised or minimised.
M. **Resourcing of support services including specialist for black and minoritised communities:** A new criminal law must be introduced together with sustained and sufficient resourcing of organisations that support victims, particularly those working with black and minoritised women who can experience higher levels of online abuse.

Evidence-Base for this Submission

This submission draws primarily on the following research:

- Clare McGlynn and Kelly Johnson (2021) *Cyberflashing: recognising harms, reforming laws* (Bristol University Press).
- Clare McGlynn and Kelly Johnson (2020) 'Criminalising Cyberflashing: options for law reform' *Journal of Criminal Law*.

Unless otherwise stated, the victim-survivor quotes used in this submission are discussed in detail in the above publications and are drawn from Sophie Gallagher's articles in the *Huffington Post* on cyberflashing, particularly Gallagher (2019).

1. Defining Cyberflashing

1.1 We define cyberflashing as follows: 'The digital distribution of penis images or videos to another without the recipient's consent, including flaccid and erect penises, as well as altered and live-streaming images.'

1.2 We note that this is a narrower definition than that used in the Consultation paper which refers to 'sexual images' (para 3.155; para 4.80). We prefer a narrower definition which focuses on penis images, as 'sexual images' could encompass a far wider range of pornographic materials. Further, as we discuss below, the 'problem' to be tackled is the distribution of penis images without consent, rather than sexually explicit material more generally.

2. Focus on women victim-survivors

2.1 Our research, and this submission, focuses predominantly on the experiences of women being sent unsolicited penis images by men. It is important to emphasise that while women in general are particularly affected by online abuse and cyberflashing, there are differences between and among women which mean that some are targeted more than others, particularly younger and/or black and minoritised women. Further, experiences among men who have sex with men differ and require specific analysis.

3. Understanding cyberflashing as a 'sexual intrusion'

We conceptualise cyberflashing as a 'sexual intrusion' as this term focuses on the deliberate action and wrong of the act, regardless of the perpetrator's motive or the victim's reaction. Terms such as sexual harassment, for example, assume a particular response from victims (they felt harassed). We emphasise the *sexual* nature of the intrusion as cyberflashing often takes place in conjunction with other forms of sexualised harassment, threats or abuse, the infringement is of a victim's sexual autonomy and victim's commonly characterise their experience as one of sexual assault

4. Different contexts of cyberflashing

We emphasise that there are many different contexts within which cyberflashing is perpetrated (as noted by the Commission, para 4.80). We highlight three particular contexts:

4.1 *Cyberflashing in public spaces and on public transport*

Victim-survivor testimonies reveal that women frequently experience cyberflashing in physical public spaces; in supermarkets, libraries, restaurants, museums, university campuses, airports, as well as on various forms of public transport. In many of these circumstances, unknown men send penis images

to women's mobile phones through the use of technology such as Airdrop and Bluetooth. This form of cyberflashing closely parallels physical 'flashing'.

4.2 *Cyberflashing in online dating and hook-up apps*

Cyberflashing is experienced as routine by many using dating apps, including from strangers, acquaintances and potential daters. It is commonly experienced out of nowhere; other times following rejecting the man's advances.

4.3 *Cyberflashing on social media and other digital technologies*

Cyberflashing is regularly experienced by women engaging in social media and other online technologies, in personal and professional capacities, by strangers, colleagues, acquaintances, family friends. It is also now taking place in online video conferencing with terms such as 'zoomflashing' and 'zoombombing' now into language reflecting a rise is various forms of online abuse, including online exposure and distribution of sexually explicit texts online.

5. Prevalence: women and young women particular targets

5.1 While it is important not to generalise, available studies consistently find that cyberflashing is a common experience, with women, and young women in particular, disproportionately facing the highest rates of victimisation and disclosing the most negative impacts.

5.2 YouGov survey in 2018 found that 41% of women had been sent an unsolicited penis picture; for younger women, this rose to almost half of women aged 18-24 (47%) (YouGov 2018). One study found 76% of girls aged 12-18 had been sent unsolicited nude images of boys or men (Ringrose, 2020).

5.3 These findings are paralleled in a number of US surveys, with women and girls most highly victimised.

5.4 Data from UK police FOI reports show that the majority of those reporting cyberflashing are women under thirty, and that while still the 'tip of the iceberg', reports over the last few years are increasing (Gallagher, 2020).

5.5 *Online abuse particularly affecting black and minoritised women:* It is likely incidence of cyberflashing has recently increased, with surveys showing a rise in online abuse generally, particularly among black and minoritised women, since the pandemic began (Glitch UK and EVAW 2020). The differing experiences of harassment, including street harassment (EVAW and Imkaan 2016) and cyberflashing, as experienced by black and minoritised women, must therefore be clearly acknowledged and taken into account in all law and policy reforms.

6. Men's motivations for cyberflashing

6.1 Cyberflashing as 'transactionally' motived

One of the most common explanations for cyberflashing depicts men's behaviour as 'transactionally' motivated, with the hope of receiving sexual images in return, or instigating sexual activity. Research suggests young men draw on common gendered constructions of heterosexuality to explain sending images, particularly sexual double standards that encourage 'active' or aggressive expressions of men's sexuality. This encourages them to take the 'risk', engage in a 'numbers game' of distributing as many penis images as possible, in the hope of a positive response. As one said: 'If the conversation was slowing down, I would sometimes send a dick pic. Because either they stop texting me or I get laid'.

6.2 Sexual gratification and exhibitionism

Other explanations highlight similarities with physical 'flashing', identifying 'compulsive' and/or 'abnormal' sexual arousal from exposure as a form of exhibitionism. In one study, 25% of perpetrators reported cyberflashing 'turned them on' (Oswald et al 2020). The nature of this sexual arousal is particularly disturbing in that exhibitionists' gratification common comes as an 'expression of anger' and their excitement is especially 'heightened by the victim's fright' (Green 2018). In one study, 8% of perpetrator's agreed that: 'I get off on the knowledge that someone was forced to see my penis without their consent' (Oswald et al 2020). In this way, we see that sexual gratification is interconnected with non-consent and force.

6.3 Threatening, harassing and causing distress

Thus, we also need to understand cyberflashing as a behaviour sometimes intended to harm or negatively affect women. YouGov (2018) found that 31% of men who sent unsolicited penis images thought women would find them distressing, and 24% threatening. Oswald et al (2020) found that significant numbers of cyberflashers hope to provoke negative reactions, with some hoping for shock (17%), fear (15%), and disgust (11%). Others admitted that sending penis images gave them a feeling of control over the recipient (10%), and that they liked to make people angry by sending penis images in response to a disagreement (8%). A slightly smaller percentage were motivated by misogyny (6%), agreeing with the statements: 'I don't like feminism and sending dick pics is a way to punish women for trying to take power away from men' and 'I feel a sense of dislike towards women and sending dick pics is satisfying' (Oswald et al, 2020).

6.4 Multiple overlapping motivations: masculinity and entitlement

There are, therefore, multiple motivations for sending unsolicited penis images which overlap, demonstrating that there will rarely be a single, clear motivation for committing this abuse. Further, underpinning these range of motivations are problematic constructions of masculinity, a sense of masculine entitlement, 'homosocial bonding' and desire for exercising power and control.

This complexity mirrors what we know about sexual offending more generally where the motivations are clearly complex and interconnected, and include sexual gratification, revenge and punishment, entitlement, power and control, recreation and adventure. It also echoes research on image-based sexual abuse where findings suggest many differing, multifarious motives including coercion and control, misogyny and entitlement, a 'prank' and causing distress (McGlynn et al, 2019; Henry et al, 2020). In particular, the research on image-based sexual abuse identifies the key role of hegemonic masculinity, homosocial bonding and heteronormative misogyny in encouraging and facilitating these forms of abuse, with men seeking to present themselves as 'real men' by sharing images without consent (Henry et al 2020; Hall and Hearn, 2017).

7. The Harms of Cyberflashing

7.1 We welcome the Commission's recognition that cyberflashing 'causes significant harms, akin to other sexual offences, particularly offline or "real time" forms of indecent exposure' (para 6.112). We outline below the differing the different ways in which harms are experienced and emphasise their interconnection. We also highlight that the harms are deeply gendered, most obviously that women are predominantly targeted, but also that the sexualised form and manner of the abuse, the motivations of perpetrators and the connections with other forms of sexual violence and harassment. Further, women's differing experiences must be recognised, particularly those from black and minoritised communities who experience higher levels of online abuse and harassment (Thiara and

Roy 2020), as well as differing experiences depending on age, sexuality, class, disability and other social, political and cultural positions.

7.2 Infringement of sexual autonomy

At its core, cyberflashing is non-consensual sexual conduct which breaches an individual's right to sexual autonomy, as expressed by one victim-survivor:

> It just came into my inbox and . . . I had no control over that happening … I felt kind of shocked and like disgusted by it … it was quite violating of my personal space and privacy. So, I didn't feel like I had an awful lot of autonomy in terms of dealing with the invasion (Whitney, quoted in Amundsen, 2020).

Accordingly, as with other forms of image-based sexual abuse (McGlynn et al, 2020), it is important to recognise that all instances of sending unsolicited penis images constitute wrongful conduct because it infringes a person's rights to sexual autonomy, integrity and privacy. This is the case regardless of the nature and extent of any further consequential harm, if any, or whether or not the action is actually welcomed by the recipient: it remains a breach of fundamental rights.

7.3 Sexual violation

Some victim-survivors have described their experiences of cyberflashing in terms of violation, describing how they felt: 'utterly violated'; 'really violated'; 'incredibly violated'; 'at its core, it's very invasive'; 'I just felt totally violated'. Marcotte et al (2020) found that almost one third of women reported feeling 'violated' after being sent unsolicited penis images.

This violation is heightened by the sexual dimension of cyberflashing, with women stating: it's an unequivocally 'sexual' practice; the sender is a 'sexual predator'; 'I felt super violated. It's a way of assaulting somebody without touching, of getting into my personal space without getting close'; 'It seems predatory to me because it's subjecting people to unwanted and inappropriate images'.

Central to understanding this experience and harm is that this is a sexual intrusion which violates a person's personal space and which is perpetrated *with a penis*. This emphasises the interconnection of cyberflashing to broader patterns of men's sexual violence against women, with some victim-survivors explicitly comparing cyberflashing to the threat of rape.

This is not to say that the penis is inherently threatening in image or form, but in a non-consensual context, the penis image can function as a figure of power, imbued with gendered heterosexual dynamics of male sexual aggression, and a fundamental lack of sexual safety commonly experienced by women (Paasonen et al 2019).

7.4 Humiliation

Victim-survivors also report experiencing being embarrassed, disturbed, shocked, utterly horrified and ashamed, with one describing the 'heatwave of embarrassment' she felt:

> 'The truth is, no matter how strong I thought I was, he turned me, with a picture, into a weak person, feeling humiliated and with no ability to stand up for myself … the incident still repeats in my mind' (Boulos, 2019).

Combined, these experiences underpin a sense of humiliation, understood as infringing the dignity of the person (Gillespie 2019). The person is dishonoured and humiliated through a failure to show respect and through treatment of others as less than deserving of respect, and as means rather than ends.

7.5 Inducing fear and threat: what might happen next?

Women have frequently connected their experiences to physical sexual exposure: 'it's the same thing as flashing in public'. For many, the harm stems from the 'well-founded fear' of what might happen next, particularly in contexts where unsolicited penis images are sent in public from strangers. Women may not be harmed per se by being sent a penis image, but what it represents and what it might mean in practice; the implicit or explicit threat of further sexual assault.

Women recount, for example, feeling immediately 'frightened', 'terrified', 'vulnerable' and 'exposed' by acts of cyberflashing. They fear escalation of the actions, with women reporting feeling scared as to what might happen next. One victim-survivor stated: 'with cyberflashing, because you don't know who's sent it, and you're in a public space, that threat is never really eliminated'. Another said: 'I was singled out, I was being targeted, and it felt very personal'.

7.6 Cumulative harms and women's everyday experiences of harassment

The harms of cyberflashing must be understood as cumulative and connected to women's other experiences of harassment and abuse, impacting on women's everyday lives; as one survivor notes: 'it felt like [the cyberflashing] was another harassment women have to absorb'. Cyberflashing is not, therefore, experienced as a 'one-off' incident, but as part of the 'continuum of fear and threat' (Kelly 1988, 97-98).

It's important not to minimise the gruelling nature of this cumulation of women's 'routine' experiences of cyberflashing, as one woman stated: 'I know men think women should just deal with these types of micro-aggressions because it's not 'that bad' but it's so constant. Can't I just use Facebook or other social media without worrying this might happen?'.

The result is that some women disengage from public and online life, curtailing social media use, turning off Bluetooth, removing themselves from apps, using men's names as ID's on their phones. Together with other experiences of violence, harassment and abuse, this constrains women's 'space for action', their social expectations, opportunities and experiences (Kelly, 2003).

7.7 Social and cultural harms

Normalising non-consent: The prevalence of cyberflashing, and its detrimental harms and effects, has ramifications across all of society. Cyberflashing may help to sustain a culture – a set of attitudes that are not universal, but which extend beyond those immediately involved as perpetrators or victim-survivors of this abuse – in which sexual consent is marginalised. And, by extension, this means that other acts of sexual violence are perhaps less likely to be recognised as such.

Silencing effect and adverse impact on civic engagement: The cumulative effect of each instance of cyberflashing, together with other forms of online abuse and harassment, contributes to a culture in which victim-survivors feel they have little option but to 'sign off' (or fail to sign on). This is the 'silencing effect' of online abuse and harassment (Amnesty 2017; Glitch 2020) which inhibits women's exercise of rights to freedom of speech and participation in society (Amnesty, 2017). In doing so, this deprives all of society of a richer, more varied public and online discourse (Citron 2014) as recognised by the Commission (para 4.100-4.103).

8. Recommendation: Adopt Specific Sexual Offence of Cyberflashing Based on Non-Consent

We agree with the Law Commission that the current criminal law does not adequately cover all forms of cyberflashing. Accordingly, we recommend the adoption of a specific sexual offence targeting cyberflashing that is based on the core wrong of non-consent.

9. Why a specific sexual offence is appropriate

9.1 Expressive role of criminal law:

Prevention: a new law would make clear that cyberflashing is now considered wrong and potentially harmful. Together with campaigns and other awareness-raising measures, this may begin to shift norms around these practices and aid prevention initiatives.

Victims' sense of recognition: a new criminal law would also send a message to victims that their experiences are now understood and recognised as harmful and justifiably subject to criminal sanction.

9.2 Increased awareness by victims and criminal justice personnel:

A new law may also make it clearer to victims, the public at large and criminal justice personnel that cyberflashing is now clearly against the criminal law and that it can be reported to the police.

9.3 Prosecutions more straightforward with specific offence:

Prosecuting cyberflashing and some other forms of online abuse under more general laws (either existing laws or proposed new offences) can pose challenges because various thresholds have to be satisfied – such as specific levels of harm, likelihood of causing harm, what constitutes harassing or threatening conduct – and due to attitudes that minimise and trivialise such practices, often these thresholds are assumed not to be met.

A specific offence targeting the identified practice can ameliorate these problems as it is written into the legislation that the particular practice, such as cyberflashing, is already determined to be harmful and deserving of criminal sanction. This should make prosecutions easier, as it removes requirements to shoe-horn cyberflashing into other laws

9.4 Following international examples:

Singapore and a number of US states have recently adopted specific laws criminalising cyberflashing and each are characterised as sexual offences. Scots law covers cyberflashing as a sexual offence. Therefore, this approach follows international best practice.

10. Key elements of the bespoke sexual offence

10.1 Sexual offence

Cyberflashing is a sexual intrusion which infringes victim-survivors' rights to sexual autonomy and privacy. It is also experienced by some as a form of sexual assault. It is vital therefore that any new criminal law is framed as a sexual offence, ensuring appropriate recognition of the nature and harms of cyberflashing, and granting anonymity rights, special protections in court and suitable sentencing options. The specific cyberflashing laws that have been adopted in some US states and in Singapore have been are enacted as sexual offences.

10.2 Focus on core wrong of non-consent, not motives of perpetrator

Cyberflashing is problematic because it is *non-consensual* conduct of a sexual nature. Distributing penis images is not per se wrongful, but doing so without the consent of the recipient is. The non-consensual act breaches the individual's rights to sexual autonomy, *regardless of the motive of the perpetrator*. A focus on non-consent as the core wrong is the approach of US states which have adopted specific cyberflashing offences.

While there are real challenges with proving consent in sexual offence cases, a major impetus for a cyberflashing law is to raise awareness, challenge the normalisation of the practice, aid prevention and education initiatives and to let victims know that their experiences are understood and recognised. These aims are met by focussing on the core wrong of non-consent and therefore justify this focus, in preference to a law requiring proof of specific motives.

Motive requirements (such as in the laws on image-based sexual abuse) invariably mean that only some forms of abuse are covered and create a hierarchy of abuses which does not reflect victim's experiences. For example, a law requiring proof of intention to harm (or awareness of risk) will likely exclude some forms of cyberflashing, as well as making prosecutions more difficult because of the threshold being introduced.

10.3 Include all penis images, not only those of the perpetrator

It is vital that the law covers all penis images and is not limited to only those of the perpetrator (as proposed by the Law Commission). Such a limitation does not recognise the nature of the harm experienced which is not dependent on the sure knowledge that the penis in the unsolicited image is that of the perpetrator.

Further, requiring proof that the image is that of the perpetrator's own penis would institute a prosecutorial hurdle that is to all extents and purposes insurmountable. If all a perpetrator must do to halt a prosecution is to declare that the penis in the image is not his, there will be few prosecutions indeed. Seeking proof that a penis belongs to a particular person would be an obviously intrusive process and is likely therefore to only be rarely undertaken. It is also technically challenging to actually prove. Therefore, such a requirement will prove such a significant disincentive to further investigation as to render the offence almost redundant.

10.4 Include altered and fake images

The law must cover images which have been altered or photoshopped, including videos using AI technology such as 'deepfakes'. It must not be made easy for a perpetrator to avoid prosecution by simply altering or enhancing an image. This reinforces the point above that a victim's experiences are not dependent on whether the image is of the perpetrator, or whether or not the image has been altered.

11. Law Commission Two-Part Solution to Gaps in Cyberflashing Laws

The Commission proposes a two-part solution to the lack of legal remedies for cyberflashing, namely:

- a new sexual offence which will apply where the perpetrator sends an image of his own genitals to another with the purpose of causing alarm or distress to the victim (or potentially awareness of risk of causing harm); and
- a new communications offence applying where sending a penis image is likely to cause at least serious emotional distress and the perpetrator intends (or is aware) of causing such harm.

We welcome the Commission's recognition of the potentially serious harms of cyberflashing and its intention to recommend new criminal offences to provide redress for victim-survivors.

We make a number of recommendations below which we think will strengthen these proposals to better ensure that all forms of cyberflashing are covered, that the legal regime is more straightforward and therefore that victim-survivors and criminal justice personnel will be able to better understand the law and feel able to report, investigate and prosecute cases of cyberflashing.

In particular, we emphasise the importance of ensuring that a new sexual offence encompasses all forms of cyberflashing as there is a political risk that only that element of reform proposals is adopted, without any accompanying change to the communications offence.

12. Law Commission's Proposed New Sexual Offence

The Law Commission's proposal is to amend section 66 of the Sexual Offences Act 2003 on physical sexual exposure so that it covers online distribution of genital images, in particular circumstances where: (a) the distribution is of an image of the perpetrator's own genitals to another; and (b) the perpetrator intends by their exposure to cause alarm or distress to the victim (para 6.129).

13. Limitations of Law Commission's proposed offence

13.1 Reject limitation of offence to images of the perpetrator's own genitals

The Commission proposes to limit the offence to images of the perpetrator's own genitals (6.133) as to do otherwise 'would broaden the scope of the offence significantly' (para 6.139) and notes that there is the fall-back option of the new communications offence which would potentially apply to all genital images (para 6.141). We disagree with limiting the offence to only images of the perpetrator's own genitals for the following reasons (Qu 24):

13.2 Harms are not dependent on image being of perpetrator's own penis:

the violation and intrusion, and possible fear and threat, experienced by the victim-survivor are not dependent on the knowledge that the penis in the unsolicited image is that of the perpetrator. To require proof that the image belongs to the perpetrator risks misunderstanding the nature of the experience and its attendant harms; it does not fully recognise the experience of victim-survivors.

13.3 Significant evidentiary problems if require proof that image is of perpetrator's own penis:

Further, requiring proof that the image is that of the perpetrator's own penis would institute a prosecutorial hurdle that is to all extents and purposes insurmountable (as discussed above).

13.4 Possible misunderstanding of motives of offenders

It may be that proposals limiting a sexual offence to images of a perpetrator's own penis assumes offenders are driven by motives similar to those of some physical 'flashers', namely the sexual dysfunction of exhibitionism, with often predatory consequences and a potential pre-cursor to other forms of sexual offending. Viewed from this perspective, the problem to be addressed in legislation is that of the individual exposing his own penis, with the fear of escalating sexual offending.

However, such an understanding neither captures the full range and extent of motivations of physical 'flashing', and even less so the wide-ranging purposes of cyberflashing, including inducing fear, alarm, humiliation and shame. It is vital that the multiplicity of motivations for cyberflashing are recognised and that the scope of any sexual offence is not unduly limited.

13.5 Creates hierarchy of cyberflashing offences which not justified on the evidence

The proposal to offer a two-part legal solution to cyberflashing creates a hierarchy between different forms of cyberflashing which is not justified on the evidence. There is no evidence that cyberflashing is

experienced as 'worse' or more harmful if it involves an image of the perpetrator's own penis. In creating a hierarchy, there is a risk the not all cases of cyberflashing will be taken seriously.

13.6 Reject argument that offence would be too 'broad' if including all penis images

The Commission's justification for limiting its proposal to images of the perpetrator's own penis is that it would make the offence too 'broad' and include a wide range of behaviours which are 'of a different order of threat', such as sending to an acquaintance a publicly available nude image (including genitals) that the recipient knows is not of the perpetrator (para 6.139).

If the Commission's offence were to cover all penis images, this scenario would only be covered if it could be proven that the perpetrator's intention was to cause distress or alarm to their friend (or awareness of risk). If the perpetrator genuinely thinks there is no likelihood of the friend being bothered by receipt of the image, then the offence will not be made out. Further, if the friend is not harmed, in practice, there will be no report to the police and the chances of prosecution are extremely small.

Further, it is certainly possible that in sending the image to his friend, this perpetrator does intend to cause harm, or is aware of the risk of harm, which suggests a wrongful purpose with potentially harmful consequences and which should therefore be covered by the offence. The assumption appears to be that the recipient will experience no adverse impacts, as they know the image is not that of their friend. But it is not necessarily the case that this person will suffer no harm. It is possible that receipt of this image may trigger various harms depending on their own experiences and context.

There are good grounds, therefore, to suggest that the Law Commission's scenario should not dictate the scope of the law. Not only might the recipient in this scenario experience adverse impacts and/or the perpetrator may intend some level of harm, but it is more important that the offence covers the fully range of egregious cyberflashing contexts and a prosecution is practically possible.

13.7 Similarities with non-consensual sharing of sexual images offence

An analogy with the offence of non-consensual sharing of intimate images may be helpful in encouraging a focus on the core wrong and harms of cyberflashing. For example, there may be cases where an intimate image is shared without consent, but for a potentially benign motive, such as for amusement, and the victim experiences no harm, perhaps as they do not mind the image being shared without their agreement and indeed they may even welcome it (Henry et al 2020, 6). But, technically, these actions would constitute a criminal offence in many jurisdictions because the distribution is made without consent, regardless of the particular motives or lack of evident harm (though not necessarily English law which also requires proof of intention to cause distress).

Such jurisdictions have chosen not to limit the offence to either proof of a limited set of motives, or to proof of actual harm to the victim, because to do so would fail to capture the core wrong of these actions (non-consent) and hinder prosecutions by introducing challenging thresholds (though there are defences in some jurisdictions based on reasonable grounds for acting, see Crofts and Kirchengast 2019).

Criminalising all non-consensual distributions is appropriate because in each case there is a wrongful act: the privacy and sexual autonomy of the person in the image has been breached. As the Australian Legal and Constitutional Affairs References Committee stated when reviewing these offences, consent should 'be the central tenet of any non-consensual sharing of intimate images offences' (2016, 51). The emphasis, therefore, is on the significance of the wrong of non-consensual conduct in sexual contexts and that where there are no consequential harms, in practice, prosecutions are extremely

unlikely as there will be no report to the police and no incentive or public interest in pursuing any such case.

14. Recommendations for specific offence covering cyberflashing

14.1 Recommend offence covers all genital images

We recommend, therefore, that the proposed new sexual offence covers all genital images, not only those of the perpetrator (Qu 25). This would ensure both that the offence recognises and understands the potentially significant harms experienced by some victim-survivors, as well as making the offence one that is practicably enforceable.

While mindful of the need to balance differing interests and concerns, we err on the side of ensuring that paradigmatic cases such as the victim-survivor on public transport receiving an unsolicited penis image is protected and prosecutions made possible, rather than a law which is more concerned with someone sending a nude image to an acquaintance.

14.2 Recommend Extending motives beyond direct intention to cause alarm or distress

The current offence of (physical) sexual exposure is restricted in scope as it requires proof of a direct intention to cause alarm or distress. A revised offence should not be so limited for two main reasons:

There are many reasons why cyberflashing is perpetrated and to restrict the offence to alarm and distress fails to recognise the nature and extent of the practice and the harms engendered.

Proof of specific motives will be a particular challenge in cyberflashing cases as commonly only an image is distributed, without any accompanying material or text from which to discern a motive. Therefore, a focus on motives will make proof of the offence particularly difficult.

14.3 Extend to cover awareness of risk of harm

Therefore, if the offence is to be based on motives, we recommend extending the mental element to include an awareness of the risk of causing alarm or distress (Qu 26). This would at least enable inclusion of cases where the perpetrator's principal intention is not to cause alarm or distress, but they are nonetheless aware of this risk.

14.4 Extend motivations to include humiliation

We also recommend that any motivations required to be proven be extended to include humiliation, as discussed above, which is used in similar legislation, including in Scotland and Singapore and in the English 'upskirting' legislation (Qu 26).

15. Challenging Commission's rejection of Non-consent as focus for law

15.1 The Law Commission rejects recommendations that a cyberflashing law centre on non-consent, raising concerns that such a law may be too far-reaching. For example, they suggest that where someone in a 'loving relationship' sends an image of their genitalia to their partner without consent, and where certainly there was no express consent, this should not meet a 'threshold for criminality' (Law Commission 2020, para 1.148). While it may be that in such a scenario there are no consequential harms experienced by the partner, it remains the case that this was non-consensual sexual conduct. The *wrong* therefore of cyberflashing has been committed, even if there are no demonstrable harms. Holding on to the core wrong in sexual offending is important if we are to refrain from only legislating where there is evidence of consequential harms, or only where an individual victim can prove they have experienced harm.

15.2 Further, it seems that the Law Commission's hypothetical rests on assumptions about types of relationships, and assumptions around lack of harm, that may not be borne out in practice. Even in 'loving relationships' consent should be sought for sexual activity and while it might be assumed here that sending a penis image is a low risk of harm, this may not always be the case. It is not difficult to imagine situations where being sent a penis image, without warning, may not be experienced as 'loving', but concerning and potentially threatening. In addition, if we were to shape the law around this example and assume there will never be any harm, we risk denying protection, recognition and redress to those who do not experience receipt of the penis image in the ways imagined. Finally, in the sort of case identified by the Law Commission, with benign motives and an unharmed victim, in practice, prosecutions are extremely unlikely as there will be no report to the police and no incentive or public interest in pursuing any such case.

15.3 Overcriminalisation and under-criminalisation of women's harms

There is a concern, particularly in the UK and US about the over-use of the criminal law and which raises some legitimate concerns. However, this debate is largely gender-free, neglecting to consider that while the law may over-criminalise some actions, it *under-criminalises* and *under-policies* many harms experienced by women (Franks 2017, 1305). Further, even where there are existing laws covering specific activities, they often fail to be interpreted to include women's experiences. For example, many forms of harassment are criminalised, commonly those associated with the public sphere, but less so the more personal and targeted experiences of harassment such as cyberflashing. Therefore, while the criminal law already addresses *some* forms of harassment, the question becomes whether the current myopic coverage, excluding most experiences of cyberflashing, should continue; or whether criminalisation might represent the law (finally) 'catching-up' with some women's experiences.

16. Cyberflashing and proposed new communications offence

The Law Commission justifies the limited scope of its proposed sexual offence on the basis that it is also recommending a new communications offence which will cover some forms of cyberflashing.

We welcome, in principle, the proposal to introduce a new harm-based communication offence (Qu 1). The main elements of the proposed offence, as applied to cyberflashing, are: (a) the defendant sends an image likely to cause harm amounting to at least serious emotional distress; (b) In sending the image, the defendant intended to harm, or was aware of the risk of harm; and (c) The image was sent without reasonable excuse.

16.1 Recommend clarifying 'communication' to include 'deepfakes' and altered images:

We agree that the interpretation of what constitutes a 'communication' should be as broad as possible, including audio (which is becoming increasingly common and easy to use in abusive situations) in order to future-proof the law and ensure that all forms of abuse are covered.

In particular, it is vital that 'communication' is defined as including material altered using artificial intelligence such as 'deepfake' technology and other photoshopping and image-altering tech in order to cover these new and emerging ways in which abuse can be perpetrated (Qu 2).

16.2 Confirm requirement 'likely' to cause harm, not proof of actual harm

We welcome the Commission's proposal that the offence be based on the likelihood of harm to a victim and not proof of actual harm (Qu 4).

It is imperative that this condition is maintained. To require victim-survivors to provide evidence that they have been harmed by abusive communications would indeed compound the abuse, with potentially re-traumatising effects (para 5.84). As psychologists Professor Nicola Gavey and Jade Farley point out in challenging the New Zealand legal requirement to prove a victim's distress: 'Requiring a woman to share with the court personal details that prove the seriousness of the emotional harm she has suffered, could be considered counter-therapeutic at best, and at worst, an act of legal cruelty.' (Gavey and Farley 2020).

In addition, not every victim-survivor experiences emotional distress at the time of, or shortly after, being cyberflashed, as one victim-survivor explained: 'it is only now I realise that it's not ok' (Gallagher 2019, quoted by the Commission at para 4.82). To require proof that the particular victim experienced harm, therefore, would not cover all cases such as where harm manifests at a later date.

Further, a prosecution should not be precluded on the basis that this particular victim did not suffer specific harms (or is unable or unwilling to testify), while many others would have done so.

16.3 Confirm importance of context in determining 'likely audience', not reasonable person

We wholly concur that when determining whether the communication was likely to cause harm, any court must have regard to the context in which the communication was sent or posted, including the characteristics of a likely audience (para 5.117, Qu 6). To require that the communication would be likely to cause harm to a 'reasonable person' would seriously restrict the scope and effect of the law (para 5.135, Qu 7).

It is imperative that the wider context in which a communication is sent and potentially received is considered, so that the nature of the abuse can be properly understood. For example, there is a significant difference between an unsolicited penis image being sent to middle-aged, able-bodied, married white man on a busy train in the middle of the day, than the same image being sent to a young black woman on her own, late at night, in a deserted train carriage.

It is important, in these examples, to understand the wider context of the communication, but specifically the particular characteristics of the potential victim, recognising the heightened experience of abuse by certain groups, particularly black and minoritised women (Glitch and EVAW 2020).

Relying on a 'reasonable person' test would significantly reduce the applicability and effectiveness of the law and most likely do so in discriminatory ways. While courts and adjudicators may strive to apply a reasonable person test in ways that do not produce unequal effects, this is not the experience of many, particularly women. Reasonable person tests tend to assume the norms of dominant classes and groups, neglecting to understand the experiences and perspectives of others. In the context of online abuse, this is likely to mean that the particular experiences of black and minority ethnic people, LGBTQI individuals, women, disabled persons and others who may be vulnerable are not likely to be considered. Even if this is not the aim of the law, it is the likely outcome and therefore an approach that avoids this is imperative.

An instructive example in a similar field comes from a Scottish case involving a 'pick-up artist' who targeted young women, seeking to engage them in conversation in public streets, blocking their movements, sometimes touching them, giving 'compliments' and seeking their personal details (*Ahmed v Her Majesty's Advocate* [2020] HCJAC 37; discussed in McGlynn and Johnson 2021).

Ahmed was charged with the offence of 'threatening or abusive behaviour' requiring proof that the behaviour 'would likely cause a reasonable person to suffer fear or alarm', similar to the English public order offences. His convictions were quashed by the Appeal Court on the basis that 'there was nothing in the appellant's behaviour … which was overtly threatening or which could reasonably be

construed as threatening' (para 51). The behaviour was interpreted by the (male) judges as a 'polite conversational request or compliment' which cannot be construed as threatening 'merely because it is uninvited or unwelcome' (para 51).

This judgment displays a concerning lack of understanding of the nature of public harassment experienced by many women. That behaviour may not appear *overtly* threatening does not mean it is not experienced as such; and more concerning still is the assumption that the behaviour could not 'reasonably' be interpreted as threatening. There is clearly a gulf between what is understood by the senior judiciary as 'reasonable' and the common everyday experiences of young women of public or street harassment, and which may include cyberflashing.

16.4 Concern criminal justice personnel will not consider cyberflashing 'likely to cause harm'

Even if the test remains likely to cause harm *to a likely audience*, we remain concerned that decision-makers in cyberflashing cases –police, prosecutors, magistrates, judges – will not deem cyberflashing to be *likely* to cause the required level of harm because they assume it to be a largely harmless practice, or at least one inducing only 'minor' distress or harm.

16.5 Encouraging a greater understanding of likelihood of cyberflashing inducing harm

If it is to be widely recognised that cyberflashing is indeed likely to cause harm to a particular audience, greater awareness of the adverse impacts of these practices will be required. The Law Commission's report in itself will go some way towards achieving this aim by its discussion of the potential harms of cyberflashing.

However, the fact that the Commission recommends separate offences depending on whose penis is in the particular image risks giving rise to assumptions that only some kinds of cyberflashing are harmful, experienced as a sexual offence, and in need of serious sanctioning.

16.6 Concern over threshold for what constitutes 'harm'

The Commission recommends that harm is defined as 'emotional or psychological harm, amounting to at least serious emotional distress' (para 5.49). Serious emotional distress lies between 'minor emotional distress and a medical condition' (para 5.110). Further, 'serious' is not simply 'anything more than minor', but in fact must be a 'big, sizable harm' (para 5.110).

We understand that in the context of a broad communications offence, there needs to be a threshold of harm so that trivial cases are not included. However, the risk is that in the cyberflashing context, this threshold excludes many cases as they may not be seen as *likely* to induce the required level of harm.

The major way to avoid this risk, and maintain the integrity of the communications offence, is to broaden the sexual offence so that it will encompass all forms of cyberflashing.

Failing such an option, reducing the risk of few prosecutions requires as broad an understanding of serious emotional distress as possible. This means including a broad range of emotions and affects, including those which may, in turn, lead to emotional and psychological harms (Qu 5, para 5.115). The examples given by the Commission as to what might constitute this level of harm are welcome such as reduced workplace productivity, reduced social interactions including limiting social media use, sleeplessness and reduced appetite (para 5.111). A list of factors would be welcome, so long as they were clearly defined as indicative and non-exhaustive (Qu 5).

16.7 Concern scenarios supposedly covered by proposed offence will not be

The Commission outlines a cyberflashing scenario where a man sends a penis image to a woman on public transport without her consent with the purported motive of making a sexual advance (p 165). It is suggested that the perpetrator's actions 'would likely be caught' by the new communications offence as the prosecution 'should' be able to prove that his behaviour was likely to cause harm amounting to serious emotional distress (para 6.119). While we welcome the Commission's understanding of the potentially harmful nature of this type of encounter, we are less convinced that either the perpetrator will have (or can be shown to have) an awareness of the risk of harm, or that police and prosecutors will identify this cyberflashing incident as potentially inducing such harm, due to the overall minimisation of this behaviour. As stated above, the way to ensure that such a case is captured by the law is for a sexual offence to be based on non-consensual conduct.

16.8 Recommend mental element includes awareness of the risk of harm

We support the Commission's proposal that the mental element includes not only an intention to cause harm, but an awareness of the risk of harm (Qu 8, para 5.148). This will help to ensure that a wider range of perpetrators are held responsible for their abusive acts. It will also make prosecutions more likely as demonstrating proof of a direct intention to cause harm is particularly challenging in the online environment where there is often little additional material or context other than the abusive communication. We have seen that a threshold of direct intention to cause distress can limit prosecutions in cases of non-consensual sharing of intimate images, as it acts as a disincentive to police investigations and subsequent prosecutions both in terms of the additional burdens and difficulty of securing the evidence (McGlynn et al 2019; North Yorkshire Police Fire and Crime Commissioner 2018).

We specifically agree that acts such as cyberflashing are undertaken for a variety of motives which often overlap. This may mean that causing harm was not a perpetrator's direct intention, even though they are aware of a risk of harm

The mental element should not be restricted to the defendant having an awareness of the *likelihood* of harm as this would significantly limit the scope of the provision (Qu 9, para 5.153). We do not think that two separate offences are required (Qu 10, para 5.160).

16.9 No 'reasonable excuse' to make abusive communication

In view of the broad reach of the recommended offence, applying to all manner of communications in a wide variety of circumstances, we agree with the proposal that it would need to be proven that the communication was sent without a reasonable excuse (Qu 11, para 5.179). We further welcome the acknowledgement that the unsolicited sending of penis images, as in the example given of a perpetrator sending an image to a stranger on public transport, is unlikely to provide the basis for a 'reasonable excuse'.

The Consultation Paper notes that an alternative would be to require particular motives to be proven. We agree that motive requirements are problematic. They risk enabling a defendant to avoid prosecution by claiming an alternative motive, particularly as motives are difficult to evidence.

17. Is cyberflashing adequately covered by the new communications offence?

The Commission states that so long as the defendant intended or was aware of a risk of harm, cyberflashing 'will likely' be caught by the new communications offence (para 6.117). We have set out in this submission that we are concerned that this will not necessarily be the case. It is for these reasons that we recommend a specific sexual offence covering all forms of cyberflashing.

18. Cyberflashing and Image-Based Sexual Abuse

The proposed new communications offence may also cover some cases of image-based sexual abuse, where nude or sexual images are distributed without consent, supplementing existing legislation in section 33 of the Criminal Justice and Courts Act 2015.

In particular, the new communications offence may provide a remedy where there is a lack of evidence to prove the perpetrator's direct intention to cause distress. This threshold has proven a significant disincentive to police investigations and prosecutions and is considered to be partly responsible for the high attrition rate in these cases (McGlynn et al 2019). Accordingly, it may be that where there is evidence that the defendant was *aware of the risk of harming* the victim, a prosecution may be taken forward.

However, there remain limitations in this provision which may cause problems in cases of non-consensual distribution of nude or sexual images:

Proof of at least serious emotional distress: the defendant has to be shown to have intended or been aware of the risk of harm amounting to at least serious emotional distress. Due to the common minimisation and trivialisation of image-based sexual abuse, it may be that this threshold itself poses a challenge to investigators and prosecutors.

Intention or awareness of harm to a *likely audience*: the defendant must intend or be aware of the risk of harm to a 'likely audience' which is 'someone who, at the point at which the communication was sent or posted by the defendant, was likely to see, hear, or otherwise encounter it' (para 5.49). Our concern is that this will not cover cases where perpetrators share images in closed or private groups with like-minded individuals, without any intention of the victims finding out that their images are being so shared (McGlynn et al 2019; Henry et al 2020). These are cases excluded under the current legislation (as there is no direct intention to cause distress) and also seem unlikely to be covered by this new communication offence.

Therefore, while the inclusion of recklessness in the intention requirements of this offence offers some possibility of prosecuting cases of non-consensual sharing of nude or sexual images, the new offence does not fill all the gaps in the current criminal law.

19. Problem of Limited Framing of Law Reform

While we welcome the Law Commission's recognition of the seriousness of cyberflashing and recommendations for reform, and we note the Law Commission's on-going review of image-based sexual abuse laws and hate crime provisions, that there are three different inquiries risks the connections between these differing forms of abuse not being recognised.

What this means is that while many women experience abuses such as cyberflashing, image-based sexual abuse and forms of hate crime as overlapping and shading into other forms of abuse, for example domestic abuse, and as part of a continuum of sexual violence, in this law reform process, their experiences are separated, categorised and treated as if discrete incidents. Cyberflashing, for example, is a species of image-based sexual abuse, a form of sexual intrusion, akin to physical sexual exposure, as well as forms of street harassment and could be conceptualised in some cases as a hate crime.

In particular, while this report examines cyberflashing, it does so in the context of the communications offences and that is the remit and context within which recommendations must be made. There is no room, therefore, in this process to be able to recommend a broader sexual offence which might, for example, cover many more forms of sexual intrusion abuse (as we discuss in McGlynn and Johnson

2021). The risk is that we enact more very specific provisions which, while applying to the current, known examples of abuse, may soon be overtaken by new ways of perpetrating abuse which are currently not yet imagined. It also means that we do not fully recognise the nature of victims' experiences.

We recognise this is not directly the fault of the Law Commission, but we make this more general point about the law reform process in general, and the lack of understanding of the holistic nature of women's experiences of violence and abuse.

20. Beyond the criminal law: education, prevention and support for victims

The focus of this submission and the Commission report is on reforming the criminal law. Nonetheless, it is vital to recognise that adopting a new criminal law is only the first step towards challenging cyberflashing and must be accompanied by effective awareness-raising campaigns and education initiatives. In addition, sustainable and sufficient resourcing must be granted to organisations supporting victims such as the Revenge Porn Helpline.

Professor Clare McGlynn and Dr Kelly Johnson

18 December 2020

References:

Amnesty International. (2017) 'Amnesty reveals alarming impact of online abuse against women', https://www.amnesty.org/en/latest/news/2017/11/amnesty-reveals-alarming-impact-of-online-abuse-against-women/

Amundsen, Rikke. (2020) '"A male dominance kind of vibe': Approaching unsolicited dick pics as sexism', *New Media & Society*, 20(3): 1085-1102.

Boulos, Janay. (2019) 'Cyber Flashing: "I froze when penis picture dropped on to my phone', *BBC News*, 26 April, https://www.bbc.co.uk/news/uk-48054893

Citron, Danielle Keats. (2014) *Hate Crimes in Cyber Space*, Cambridge, MA: Harvard University Press.

Crofts, Thomas and Kirchengast, Tyrone (2019) 'A Ladder Approach to Criminalising Revenge Pornography' *Journal of Criminal Law* 83(1): 87-103.

End Violence Against Women and Imkaan (2016), 'I'd just like to be free: you women speak out about sexual harassment' Powerful new film - Black women speak out about racist sexual harassment (endviolenceagainstwomen.org.uk)

Franks, Mary Ann. (2017) 'Redefining 'revenge porn' reform: A view from the front lines', *Florida Law Review*, 69(5): 1251-1337.

Gallagher, Sophie. (2019) 'Cyber Flashing: 70 Women on what it's like to be sent unsolicited dick pics', *Huffington Post,* 21 May, https://www.huffingtonpost.co.uk/entry/cyberflashing-70-women-on-what-its-like-to-be-sent-unsolicited-dick-pics_uk_5cd59005e4b0705e47db0195

Gallagher, Sophie. (2020) '"The tip of the iceberg": Cyber-flashing on trains "largely unreported" despite huge rise in incidents', *The Independent,* 18 February, https://www.independent.co.uk/life-style/women/cyber-flashing-incidents-number-2020-a9341676.html

Gavey, N, and Farley, J (in press), 'Reframing Sexual Violence as "Sexual Harm", in New Zealand Policy: A Critique', in Torres and Yllo (eds) *Conceptualizing Sexual Violence in Marriage: Research and Policy* (Routledge).

Gillespie, Alisdair (2019), 'Tackling Voyeurism: Is The Voyeurism (Offences) Act 2019 A Wasted Opportunity?' *Modern Law Review* 82: 1107-1131.

Glitch UK, (2020) 'Impact of online abuse', https://fixtheglitch.org/impactofonlineabuse/
Glitch UK and End Violence Against Women Coalition (2020) *The Ripple Effect: COVID-19 and the Epidemic of Online Abuse* https://www.endviolenceagainstwomen.org.uk/wp-content/uploads/Glitch-and-EVAW-The-Ripple-Effect-Online-abuse-during-COVID-19-Sept-2020.pdf
Green, Stuart. (2018) 'To See and Be Seen: Reconstructing the Law of Voyeurism and Exhibitionism', *American Criminal Law Review*, 55: 203-258.
Hall, Matthew., Hearn, Jeff. (2017) *Revenge Pornography*, London: Routledge.
Henry, N, McGlynn, C, Flynn, A, Johnson, K, et al (2020) *Image-Based Sexual Abuse: A Study on the Causes and Consequences of Non-Consensual Nude or Sexual Imagery* (Routledge).
Kelly, Liz. (1988) *Surviving Sexual Violence*, Cambridge: Polity.
Kelly, Liz. (2003) 'The Wrong Debate: Reflections on why Force is Not the Key Issue with Respect to Trafficking in Women for Sexual Exploitation', *Feminist Review*, 73(1): 139-144.
Marcotte, A et al (2020) 'Women's and Men's Reactions to Receiving Unsolicited Genital Images from Men', *The Journal of Sex Research*.
McGlynn C, Rackley, E, Johnson, K, et al (2019) *Shattering Lives and Myths: a report on image-based sexual abuse* available: http://dro.dur.ac.uk/28683/3/28683.pdf?DDD34+DDD19+
McGlynn, C and Johnson, K (2020) 'Criminalising Cyberflashing: options for law reform' *Journal of Criminal Law*
McGlynn, C, Johnson, K, Rackley, E, (2020) et al '"It's Torture for the Soul": the harms of image-based sexual abuse' *Social and Legal Studies*
McGlynn, C and Johnson, K (2021) *Cyberflashing: recognising harms, reforming laws* (Bristol University Press).
Oswald, F et al (2020) 'I'll Show You Mine so You'll Show Me Yours: Motivations and Personality Variables in Photographic Exhibitionism', *The Journal of Sex Research*, 57(5): 597-609.
Paasonen, S et al (2019) 'The Dick Pic: Harassment, Curation, and Desire', *Social Media + Society*, 2: 1-10.
Ringrose, Jessica. (2020) 'Is there hidden sexual abuse going on in your school?', *TES*, 29 October, https://www.tes.com/news/there-hidden-sexual-abuse-going-your-school
Thiara, Ravi., Roy, Sumanta. (2020*) Reclaiming Voice*, London: Imkaan.
Vera-Gray, F (2017) *Men's Intrusions, Women's Embodiment – A Critical Analysis of Street Harassment* (Routledge).
YouGov (2018) 'Four in ten female millennials have been sent and unsolicited penis photo' (2018), 16 February, https://yougov.co.uk/topics/politics/articles-reports/2018/02/16/four-ten-female-millennials-been-sent-dick-pic