The Journal of Criminal Law

The Journal of Criminal Law
1–18

DOI: 10.1177/0022018320972306
journals.sagepub.com/home/clj

Criminalising Cyberflashing: Options for Law Reform

Clare McGlynn
Durham University, UK

Kelly Johnson
Durham University, UK

Abstract

In this article, we examine the phenomenon of cyberflashing, outlining its prevalence, harms, and victim-survivors' experiences. We then consider the extent to which English criminal law currently applies to this form of sexual abuse. We argue that although cyberflashing can be prosecuted in England and Wales, this is only in very limited circumstances; the existing law is confusing, piecemeal, has significant omissions, and consequently prosecutions are extremely unlikely. As such, the current criminal law in England and Wales is failing victim-survivors of cyberflashing. Due to its prevalence, its harmful impacts and similarities with other criminalised forms of sexual violence, comprehensive law reform, which appropriately addresses cyberflashing as a sexual offence, is now critical. Accordingly, we examine legislation in other jurisdictions where criminal laws targeting cyberflashing have been adopted, and provide recommendations for law reform: specifically, we recommend the development of a new criminal offence that purposely targets cyberflashing in all its forms.

Keywords

Cyberflashing, unsolicited dick pics, image-based sexual abuse, online abuse, sexual harassment

Introduction

The criminal law in England and Wales is currently failing victim-survivors of cyberflashing—a practice that most commonly involves a man sending a penis image to another without their prior agreement or consent. Sometimes colloquially referred to as 'unsolicited dick pics', cyberflashing has received considerable public attention of late; and this has only been compounded by the rise of online sexual harassment that has coincided with the increased use of digital technologies during the Covid-19 pandemic.[1] Due to its

1. UN Women, *Online and ICT Facilitated Violence against Women and Girls during COVID-19* (2020) UN Women Headquarters <https://www.unwomen.org /-/media/headquarters/attachments/sections/library/publications/2020/ brief-online-and-ict-facilitated-violence-against-women-and-girls-during-covid-19-en.pdf?la=en&vs=2519> accessed 18 August 2020.

Corresponding author:
Clare McGlynn, Durham Law School, Durham University, Durham, DH1 3LE, UK.
E-mail: clare.mcglynn@durham.ac.uk

prevalence, its harmful impacts, and similarities with other criminalised forms of sexual violence, the fact that cyberflashing is not clearly against the law in England and Wales is a source of great surprise and complaint for victim-survivors.[2] As with other forms of image-based sexual abuse,[3] the criminal law has ultimately failed to keep pace with the emergent ways in which sexual harassment and abuse are being perpetrated against women, through new and evolving technological mediums.

In this article, we examine the phenomenon of cyberflashing—outlining what is currently known about its prevalence, impacts and victim-survivors' experiences—and consider the extent to English criminal law currently applies to cyberflashing. As we will argue, while cyberflashing can be prosecuted in England and Wales, this is limited to very specific circumstances. Therefore, as it currently stands, the law is confusing, piecemeal, has significant omissions, the evidential hurdles are many and, consequently, prosecutions are extremely unlikely. As such, we argue that comprehensive law reform in this area is now critical, to ensure the criminal law adequately covers all cyberflashing practices, reflects the wrong and harm of cyberflashing, and provides women sufficient protection and recourse in the criminal justice realm. The article will then proceed with a detailed consideration of legislation in other jurisdictions where criminal laws specifically targeting cyberflashing have been adopted. The different contours of the various forms of cyberflashing legislation will be examined and evaluated which will in turn inform our recommendations for law reform: specifically, the development of a new criminal offence that purposely targets cyberflashing.

Cyberflashing: Prevalence, Harms and Victim-Survivor Experiences

The term 'cyberflashing' encompasses a spectrum of practices, all of which involve the sending of an unsolicited genital image to another, and most commonly involves men sending pictures of their penises to other individuals without their prior agreement or consent. Although often referred to as 'unsolicited dick pics', we recommend use of the term 'cyberflashing' because it is a commonplace and easily-recognisable phrase, which also reduces trivialisation by elucidating the interconnection between these technological practices (hence the 'cyber' prefix) and other forms of indecent exposure (also known as 'flashing').[4] Victim-survivor testimonies demonstrate that women frequently experience cyberflashing in public spaces, with recent examples taking place in supermarkets, libraries, restaurants, museums, train stations and airports, as well as on various forms of public transport.[5] In many of these

2. See the discussion in S Gallagher, 'What Is Cyber Flashing—And Why Isn't It Illegal In England and Wales?' *The Huffington Post* (10 July 2019) <https://www.huffingtonpost.co.uk/entry/flashing-is-illegal-offline-so-why-do-we-still-tolerate-it-online_uk_5cee8d67e4b0ae67105a3ed8> accessed 20 August 2020.
3. See further C McGlynn and others, *Shattering Lives and Myths: A Report on Image-Based Sexual Abuse* (2019) Durham University; University of Kent <http://dro.dur.ac.uk/28683/3/28683.pdf?DDD34+DDD19+> accessed 19 August 2020.
4. See also L Thompson, 'DickPics Are No Joke: Cyber-Flashing, Misogyny and Online Dating' *The Conversation* (3 February 2016) <https://theconversation.com/dickpics-are-no-joke-cyber-flashing-misogyny-and-online-dating-53843> accessed 14 August 2020; R Thompson, 'It's Time to Stop Saying "Unsolicited Dick Pics": And Here's Why' *Mashable* (19 July 2019) <https://mashable.com/article/cyberflashing-unsolicited-dick-pics-terminology/?europe=true> accessed 14 August 2020. The term 'cyberflashing' has its own limitations; see our further discussion which parallels critiques of 'flashing' as an unsuitable and trivialising term for indecent exposure in C McGlynn and K Johnson, *Criminalising Cyberflashing: Recognising Harms, Reforming Laws* (forthcoming) Bristol University Press.
5. See, eg, the victim-survivors interviewed in S Gallagher, 'Cyber Flashing: 70 Women on What It's Like to be Sent Unsolicited Dick Pics' *The Huffington Post* (21 May 2019) <https://www.huffingtonpost.co.uk/entry/cyberflashing-70-women-on-what-its-like-to-be-sent-unsolicited-dick-pics_uk_5cd59005e4b0705e47db0195> accessed 21 August 2020. We use the term 'victim-survivor', rather than 'victim' or 'survivor', to unsettle and navigate the linguistic and social binaries that have emerged in popular discourses of sexual violence. As Kelly and others note, these two terms can have oppositional connotations and as a result are often used dichotomously. Therefore, we use 'victim-survivor' to emphasise the wrong and harm experienced, while simultaneously recognising agency, strength and resistance: see further L Kelly, S Burton and L Regan, 'Beyond Victim or Survivor: Sexual Violence, Identity and Feminist Theory and Practice, in L Adkins and V Merchant (eds), *Sexualizing the Social: Power and the Organization of Sexuality* (St Martin's Press, New York 1996) 77–101.

circumstances, unknown men, necessarily located nearby, send penis images to women's mobile phones through the use of 'Airdrop' or other WiFi and Bluetooth-based forms technology.[6] Cyberflashing is also documented as being a common experience on dating websites and applications and, for many women and girls, it's an everyday experience when engaging with social media and other technologies in professional and personal capacities.[7] Most recently, with the mass-shift to online working during the Covid-19 pandemic 'zoomflashing' and 'zoombombing' have come to the fore, which has included cyberflashers infiltrating Zoom calls or similar online meetings, and exposing themselves or flashing unwanted penis or other pornographic images onscreen to attending meeting participants.[8]

How Common Is Cyberflashing?

Despite its widespread occurrence across various fora, there is a shortage of data that can identify the extent of cyberflashing perpetration and victimisation, although much needed research in this area is now starting to emerge.[9] Existing studies, although limited in terms of the range of cyberflashing practices and demographic populations addressed,[10] are consistently finding that cyberflashing is commonly experienced by many individuals in society—with women, and young women in particular, disproportionately facing the highest rates of victimisation and disclosing the most negative impacts.[11] Marcotte and others, for example, surveyed single women and found that, among the respondents who had ever received a penis image (50%), almost all (91%) had also received an unsolicited image of a penis.[12] Similarly, another survey found that two out of five British women had been sent a penis picture without their consent; for younger-women victimisation was even more common, with almost half of women (47%) aged between 18 and 24 years old disclosing they had received unsolicited penis images.[13] These research findings are also paralleled in a US survey on online harassment, where 31% of

6. Similar to its Android equivalents, AirDrop requires that 'sending' and 'receiving' devices are within 9 metres of each other. See Apple 'Use AirDrop on Your Mac' (2020) <https://support.apple.com/en-gb/HT203106> accessed 21 August 2020.
7. See Gallagher (n 5).
8. See *Crime Online* 'Florida Man Exposes Himself to Middle Schoolers during Online Math Class' (4 May 2020) <https://www.crimeonline.com/2020/04/05/florida-man-exposes-himself-to-middle-schoolers-during-online-math-class/> accessed 21 August 2020.
9. See, eg, AS Marcotte and others, 'Women's and Men's Reactions to Receiving Unsolicited Genital Images from Men' (2020) J Sex Res 1; MBH Mandau, '"Directly in Your Face": A Qualitative Study on the Sending and Receiving of Unsolicited "Dick Pics" Among Young Adults' (2020) 24(1) Sex Cult 72; R Amundsen '"A Male Dominance Kind of Vibe": Approaching Unsolicited Dick Pics as Sexism' (2020) New Media Soc 1; A Oswald and others, 'I'll Show You Mine so You'll Show Me Yours: Motivations and Personality Variables in Photographic Exhibitionism' (2020) 57 J Sex Res 597.
10. To our knowledge no studies have yet addressed the full spectrum of cyberflashing practices; while research has been conducted on online experiences, or digital romantic and 'sexting' contexts, these studies do not clearly capture 'Air Dropped' images, all forms of social media, unsolicited images sent in professional contexts, and more recently-visible practices such as zoombombing. In addition, research cohorts have varyingly been delimited by age, gender identity, sexuality, and geographic location. See also RM Hayes and M Dragiewicz, 'Unsolicited Dick Pics: Erotica, Exhibitionism or Entitlement?' (2018) 71 Women's Stud Intl Forum 114.
11. Of course, cyberflashing is not experienced uniformly, and there are gaps in knowledge about cyberflashing, including men's experiences. Marcotte and others (n 9) surveyed gay and bisexual (but not heterosexual) men, who disclosed a high incidence of being sent unsolicited penis images, but only a small minority of men disclosed negative impacts. The authors argue women's experiences are best understood within the broader context of men's sexual violence against women (see further below), which might be of less direct relevance to the experiences of male sexual minorities. Clearly further research in this area is needed, but for the purposes of this article we are focusing largely on the experiences of women who have been cyberflashed by men. See also Hayes and Dragiewicz (n 10); Pew Research Centre, Online Harassment 2017 (2017) <https://assets.pewresearch.org/wp-content/uploads/sites/14/2017/07/10151519/PI_2017.07.11_Online-Harassment_FINAL.pdf> accessed 21 August 2020; SJ Matthews and others, 'Not Cool, Dude: Perceptions of Solicited vs. Unsolicited Sext Messages from Men and Women' (2018) 88 Comput Hum Behav 1–4.
12. Ibid.
13. YouGov, 'Four in Ten Female Millennials Have Been Sent an Unsolicited Penis Photo' (2018) <https://yougov.co.uk/topics/politics/articles-reports/2018/02/16/four-ten-female-millennials-been-sent-dick-pic> accessed 20 August 2020.

respondents disclosed being sent an explicit image without their agreement.[14] Victimisation was again distributed unequally across participants; young women faced the highest incidence of victimisation, with 53% of women aged 18–29 disclosing they had been sent unsolicited images. Collectively, the existing data on cyberflashing demonstrates that this abuse is now alarmingly commonplace, and affects a significant number of individuals in society. This is particularly the case for younger women, with all three studies demonstrating consistency in finding approximately half of young women have received unsolicited penis images.

The Harms of Cyberflashing: Victim-Survivor Experiences

Perhaps as a result of its prevalence, cyberflashing is often trivialised and normalised. Indeed, cyberflashing is often discursively framed as a routine and unavoidable part of women's lives. However, cyberflashing is of course not inevitable, and its seriousness—the wrong it entails, the significant harms and impacts it can cause—must not be minimised.

Public accounts from victim-survivors make it clear that, across different contexts, some women commonly experience cyberflashing as a serious form of sexual intrusion or harassment. Accordingly, some victim-survivors have articulated their experiences of cyberflashing in terms of violation, describing how they felt 'totally' and 'utterly' violated by having unsolicited penis images 'forced' upon them; as one victim-survivor summarised the practice of cyberflashing: 'at its core, it's very invasive'.[15] This is also supported by emerging academic research: Marcotte and others, for example, found almost a third of women reported feeling 'violated' after being sent unsolicited penis images.[16] In addition, several women have emphasised the sexual dimension of the cyberflashing violation, by characterising the penis images as unequivocally 'sexual'[17]; the sender as a 'sexual predator'[18]; and their experience of cyberflashing as a form of sexual assault. As one victim-survivor stated: 'I felt super violated. It's a way of assaulting somebody without touching, of getting into my personal space without getting close'.[19]

Many more women have compared their experiences of cyberflashing to other forms of sexual violence, particularly sexual exposure, often referred to as physical 'flashing'. For example, a victim-survivor who has experienced both physical 'flashing' and cyberflashing identified similarities between these two abuses, commenting: 'both are a complete invasion of your private space, whether physically or digitally, and both forms completely blindside you and take you by surprise'.[20] Collectively, these experiences demonstrate the wrong per se of cyberflashing: it constitutes a coercive sexual intrusion[21] which violates victim-survivors' sexual autonomy, privacy, and 'right to everyday life'.[22]

14. See Pew Research Centre (n 11).
15. Gallagher (n 5).
16. Marcotte et al (n 9).
17. *The Times*, 'Cyber Flasher Sends Lewd Image to Woman's Phone' (14 August 2015) <https://www.thetimes.co.uk/article/cyber-flasher-sends-lewd-image-to-womans-phone-t0b00lw2dp9> accessed 24 August 2020.
18. *The Sydney Morning Herald*, 'Ursula Didn't Know What Cyber Flashing was Until the Day at the Museum' (20 June 2019) <https://www.smh.com.au/national/ursula-didn-t-know-what-cyber-flashing-was-until-the-day-at-the-museum-20190512-p51mm6.html> accessed 24 August 2020.
19. S Beattie, 'Canada's Laws Can't Handle "Cyberflashing," A New Type of Sexual Harassment' *The Huffington Post* (13 December 2018) <https://www.huffingtonpost.ca/2018/12/13/cyberflashing-canada-airdrop-dick-pics-subway-sexual-harassment_a_23617459/ > accessed 25 August 2020.
20. Quoted in S Gallagher, 'Cyber Flashing and Flashing Can Be Equally Harmful, Says Woman Who Experienced Both' *The Huffington* Post (4 December 2018) <https://www.huffingtonpost.co.uk/entry/cyberflashing-real-life-vs-flashing-online_uk_5bfe81ede4b030172fa8d278> accessed 24 August 2020.
21. As discussed further in McGlynn and Johnson (n 4). Our conceptualisation builds on key feminist works theorising sexual harassment as men's intrusions, see, eg, F Vera-Gray, *Men's Intrusion, Women's Embodiment: A Critical Analysis of Street Harassment* (Routledge, Abingdon 2017). See also Mandau (n 9).
22. On the right to everyday life, see Y Beebeejaun, 'Gender, Urban Space, and the Right to Everyday Life (2017) 39(3) J Urban Aff 323.

Victim-survivor testimonies also demonstrate the serious *consequential* harms of cyberflashing—the harms that victim-survivors experience as a result of the coercive intrusion and violation of cyberflashing—which often go unrecognised. Perhaps this lack of recognition is due to the flawed assumption that because the penis images are sent digitally, cyberflashing is less 'real', 'serious' or 'harmful' than physical flashing, or other forms of sexual harassment and abuse. On the contrary, victim-survivor testimonies suggest that the harms of cyberflashing, in many respects, parallel that of physical flashing, and can be significant, far-reaching, and long-lasting.[23] As a result, victim-survivors have questioned the logic of differentiating between cyberflashing and its physical counterpart: as one victim-survivor stated, 'I don't see how . . . the guard of glass on a screen differentiates the impact of a man in a Mac walking down the street suddenly opening it [and] exposing himself'.[24]

Fundamentally, it is imperative we recognise that cyberflashing takes place in 'real-life', and therefore can also engender 'real-life' threats, consequences and harms. One key consequential harm of cyberflashing is fear: many women have recounted feeling immediately 'frightened', 'scared', 'terrified', 'vulnerable' and 'exposed' by the cyberflashing, which negatively impacted their sense of safety and trust in both online and offline public spaces. For example, one woman who was Air Dropped penis images by someone while on public transport said she felt 'vulnerable for the rest of my trip . . . it was scary not knowing who it was [that sent the penis images] but that they might be looking at me or potentially follow me off the train'.[25] In this context, the unknown identity and proximity of the perpetrator makes it impossible for victim-survivors to accurately assess the potential risk of escalation and take protective action accordingly.[26] As one victim-survivor stated: 'with cyber flashing, because you don't know who's sent it, and you're in a public space, that threat is never really eliminated'.[27] Other victim-survivors have reflected that the hidden nature of cyberflashing—its visibility often limited to the screen of the victim-survivors' personal technological devices—makes cyberflashing feel all the more threatening and targeted: 'I felt very alone and vulnerable. Because it's not like flashing where everyone can see if it happens to you in public, and might intervene or try to help. It was more internalised—no one knew what was on my phone. I was singled out, I was being targeted, and it felt very personal'.[28]

In addition to making women feel threatened and fearful for their safety, it is important that the broader, cumulative harms of cyberflashing are also recognised. It is clear from the testimonies of victim-survivors that, for many, cyberflashing is experienced as part of a wider pattern of everyday sexism, sexual harassment and sexual violence with which women have to contend. It is part of a continuum of sexual violence which identifies the commonality and interconnection between different practices and experiences of men's violence against women.[29] Therefore, many victim-survivors do not experience cyberflashing as a 'one-off' incident in their lives, but rather see it as another aspect of the everyday objectification, inequality and sexual double standards that women routinely experience and navigate. As one victim-survivor noted: 'it felt like [the cyberflashing] was another harassment women just have to absorb'.[30] Ringrose and Lawrence also found that women and girls have commonly

23. See S McNeil, 'Flashing: Its Effect on Women' in J Hanmer and M Maynard (eds), *Women, Violence and Social Control* (Humanities Press International, Atlantic Highlands 1987) 93. See also *The Huffington Post* (n 5).
24. S Gallagher, '9 Women Tell Us Why the UK Needs a Cyberflashing Law: 'We Need to Feel Safe in Public' *The Huffington Post* (20 November 2018) <https://www.huffingtonpost.co.uk/entry/why-the-uk-needs-a-cyberflashing-law_uk_5bed94c1e4b0dbb7ea6852fc> accessed 24 August 2020.
25. Gallagher (n 5).
26. See also Vera-Gray (n 21).
27. Gallagher (n 20).
28. S Gallagher 'He Was Staring at Me across the Concourse, his Hands Were Shaking: Why Cyber Flashing Isn't Just a Digital Problem' *The Huffington Post* (02 May 2019) <https://www.huffingtonpost.co.uk/entry/he-was-staring-at-me-across-the-concourse-his-hands-were-shaking-why-cyberflashing-isnt-just-a-digital-problem_uk_5ca1ca0de4b0bc0dacab0dd0> accessed 24 August 2020.
29. L Kelly, *Surviving Sexual Violence* (London, Polity Press 1988). See also Hayes and Dragiewicz (n 10)
30. Gallagher (n 24).

described experiencing unsolicited penis images as another attempt by men to exert sexual dominance and control over women.[31]

The gruelling cumulation of women's 'routine' experiences of cyberflashing,[32] or the threat of cyberflashing, must not be minimised. 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?'[33] Accordingly, many women take additional precautionary measures, such as curtailing their use of technology and activity online, in an attempt to evade this abuse.[34] This demonstrates how the pervasiveness of cyberflashing undermines women's ability to freely live their lives and exercise their citizenship in public spaces, both online and offline, without men's routine sexual intrusion and harassment. Cyberflashing then, must also be seen as generative of significant, broader social harms—for individual women and for society as a whole. Namely, it extends the sense of fear, threat and harm that women experience in public spaces; it impinges upon women's civil liberties and civic participation; and, therefore, it normalises and furthers gender inequality.

Cyberflashing Motivations

Such evidence of women's widespread negative experiences of, and reactions to, unsolicited penis pictures has led researchers and victim-survivors alike to question the motivations of those that perpetrate cyberflashing. Again, this area remains under-researched. However, dominant framings of cyberflashing commonly depict men's behaviour as being 'transactionally' motivated—i.e underpinned by the hope of instigating sexual activity or receiving genital images in return. In addition, it can be seen as a 'misguided' attempt at courtship: a problematic but ultimately normative extension of assertive heterosexual male behaviour.[35] While we must develop a nuanced understand of cyberflashing motivations which engages with contemporary gendered sexual norms,[36] we must also be cautious that in doing so we do not normalise this abuse or diminish perpetrators' culpability. These same motivations were at one time employed to explain, normalise and minimise the behaviour of physical flashers,[37] however unreasonable such claims might sound today. In contrast, research has indicated that men are aware that receiving unsolicited penis images can be a threatening, harassing and distressing experience for women.[38] Moreover, a range of overlapping motivations for sending unsolicited penis images have been identified in the literature, which demonstrates there will rarely be a single, clear motivation for committing this abuse. Cited motivation examples include: sexual gratification, a 'laugh', status building or homosocial bonding, boredom, reduced inhibitions, as an exercise of male power and sexual entitlement, and to harass, intimidate, control and distress.[39]

31. J Ringrose and E Lawrence, 'Remixing Misandry, Manspreading, and Dick Pics: Networked Feminist Humour on Tumblr' (2018) 18 Fem Media Stud 686; also L Thompson, '"I Can Be Your Tinder Nightmare": Harassment and Misogyny in the Online Sexual Marketplace' (2018) 28 Fem Psychol 69.
32. See also Amundsen (n 9).
33. Gallagher (n 5).
34. Ibid.
35. Oswald and others (n 9); see also A Walling and T Pym, '"C'mon, No One Wants a Dick Pic": Exploring the Cultural Framings of the "Dick Pic" in Contemporary Online Publics' (2019) 28 J Gend Stud 70.
36. See M Naezer and L van Oosterhout, 'Only Sluts Love Sexting: Youth, Sexual Norms and Non-consensual Sharing of Digital Sexual Images' (2020) J Gend Stud 1.
37. McNeil (n 23).
38. Eg YouGov (n 13).
39. Ibid; and Mandau (n 9); Oswald and others (n 9); Walling and Pym (n 35); Hayes and Dragiewicz (n 10).

The Limits of English Law

From examining victim-survivor experiences, it is clear that cyberflashing can be a significant and harmful form of sexual intrusion that women commonly experience. This makes it all the more important that jurisdictions have legislation that can comprehensively address this pernicious form of abuse. However, the law in England and Wales has failed to keep pace with technological advancements. As a result, the Law Commission is currently investigating reform in this area.[40] With law reform now on the agenda, it is both important and timely that we examine the suitability of the current legislation in England and Wales as it might apply to cyberflashing, and identify lessons to be learned from cyberflashing legislation in other jurisdictions. It is crucial that any law reform proceeds from an appropriate conceptual foundation, as well as being appropriate, clear, forward-thinking and comprehensive.[41]

Cyberflashing as a Sexual Offence?

As cyberflashing constitutes a sexual violation, and clearly parallels other forms of criminalised sexual violence, we first examine the applicability of existing sexual offences. As there is a criminal law against 'flashing' in the streets, it might be assumed this would also extend to cyberflashing. Indeed, due to the similarities between the two forms of abuse, there is no real reason why this should not be the case. However, while there is an offence of 'sexual exposure' in s 66 of the Sexual Offences Act 2003, it appears unlikely that this applies to cyberflashing. That section provides that a person commits an offence if he 'intentionally exposes his genitals' and 'he intends that someone will see them and be caused alarm or distress'. The key question, in this context, is whether exposure of the (offender's) penis online comes within this provision.

On its face, there is nothing in s 66 which precludes this: reference is simply made to 'exposure' of the genitals. It is certainly possible to prosecute a case where the online exposure is in real time, using technology such as Zoom, Facetime or Skype, as happened in *R v Alderton* [2014].[42] The Law Commission recent review of this area of law commented that the s 66 offence relates to 'an act in real-time rather than the distribution and possession of images and recordings' and therefore it is likely to only apply to 'live streamed' online exposure, though it noted that this assumption has not been tested in law.[43] There is no reason in principle why this offence could not apply, providing a remedy where the perpetrator exposes his penis with the intention that it is seen and that the victim is caused alarm or distress. Nonetheless, it seems unlikely that this will be tested or prosecutions brought under this provision.

Despite these limitations with the exposure offence, there are some offences applying specifically to children under 16 which may provide some additional protections. The offences of 'causing a child to watch a sexual act' (s 12) and 'sexual communication' with a child (s 15A) were introduced to target sexual grooming, particularly the preparatory steps prior to any physical sexual offences. However, the observation in s 12 must be of 'sexual activity' and it is not obvious whether this will extend to a penis image and/or whether a distinction may be made between an erect or flaccid penis, with only the former constituting 'activity'. The scope of s 15A is broader,

40. The Law Commission is undertaking a review of the communications offences which is to encompass cyberflashing. See further: <https://www.lawcom.gov.uk/project/reform-of-the-communications-offences/> accessed 25 August 2020.
41. For a brief outline, see K Johnson and C McGlynn, 'Why We Need to Criminalise Cyberflashing Now' (2020) *Social & Legal Studies Blog* <https://socialandlegalstudies.wordpress.com/2020/07/06/criminalise-cyberflashing-now/> accessed 24 August 2020.
42. *R v Alderton* [2014] EWCA Crim 2204.
43. Law Commission, *Abusive and Offensive Online Communications: A Scoping Report* (Law Commission, London 2018) 135; see, eg, *Crime Online* (n 8).

with 'sexual communication' more likely to cover all penis images. It is at least clear that the offences do apply to live online activities.[44]

The differing aims and purposes of these provisions is evident, therefore, in the differing motive requirements, with sexual exposure requiring proof of a motive to cause distress, but proof of sexual gratification being necessary for the exposure offence. Further, even the two provisions protecting children have slightly different definitions for the material to be covered. Nonetheless, the children's provisions provide a possible avenue for redress, even if only for some forms of cyberflashing and in some specific circumstances.

Cyberflashing as Indecent and a Public Outrage?

If current sexual offences are unlikely to cover cyberflashing, another option is the archaic offence of 'outraging public decency'. This is an offence which has usefully been applied to a wide range of public nuisances, including sexual activity in public and 'upskirting' and could conceivably, therefore, be applied to cyberflashing.[45] However, this is not as straightforward as it might seem or be hoped, as there are some specific requirements for this offence to be satisfied. Assuming that cyberflashing constitutes a 'lewd, obscene or disgusting' act,[46] it must still be proven that it is the 'public' that is outraged, not a particular victim and this requires more than one person to be present and could have seen the act.[47] This could happen where, for example, an image is sent to a technological device viewed by more than one person; such contexts of cyberflashing have been documented.[48] However, in focusing on outraging the 'public', the nature of this offence means that if a victim of cyberflashing were to show the image to more than one person, it is possible that she herself might be said to have committed the offence of 'outraging public decency'.[49]

While it might be technically possible to bring cyberflashing within the confines of the outraging public decency offence, it seems likely that the difficulties of establishing that the act outraged the 'public' mean that this offence is not going to prove a useful vehicle for challenging cyberflashing. Similarly, offences under the Indecent Displays (Control) Act 1981 which was introduced to limit the public display of sexually explicit material in shops, are unlikely to apply. While the indecency threshold would likely be satisfied, the material has to be 'visible from any public place' which is unlikely to cover most instances of cyberflashing.

Beyond the hurdles of demonstrating that cyberflashing took place in, and then offended, the 'public', these offences are in any event not suitable for addressing cyberflashing practices because they do not recognise the sexual nature or harms of cyberflashing. As our discussion above has demonstrated, cyberflashing is not merely a 'nuisance' or offensive to the public: it is a coercive sexual violation which can cause significant harm to individuals, as well as society as a whole.

Cyberflashing as Harassment?

The next option to consider is whether cyberflashing might constitute a form of criminal harassment—a remedy which might be suitable, given that we know so many victim-survivors experience cyberflashing as harassing and as a form of sexual harassment (as above).

---

44. As well as acts when offender and child are physically together, Crown Prosecution Service guidelines state that the offence also extends to presence via webcam: <https://www.cps.gov.uk/legal-guidance/rape-and-sexual-offences-chapter-2-sexual-offences-act-2003-principal-offences-and> (accessed 21 August 2020).
45. Law Commission (n 43) 132–36.
46. As the offence requires: *R v May* (1989) 91 Cr App R 157, 159.
47. *R v May* (n 46) 157.
48. See Gallagher (n 5).
49. See further in Law Commission, 'Simplification of Criminal Law: Public Nuisance and Outraging Public Decency' (Law Com No 358 Law Commission, London 2015) para 2.47.

Where there is repeated, persistent harassment, the criminal law does provide a remedy in the form of the Protection from Harassment Act 1997. Enacted specifically in response to women's experiences of stalking and harassment, the Act makes it an offence to harass someone as part of a 'course of conduct', or to put them in fear of violence being used against them by such a course of conduct. Harassment is interpreted as 'causing alarm or distress' and can include repeated attempts to impose unwanted communications on an individual, in a manner that could be expected to cause distress or fear in any reasonable person—such as, for example, repeated sending of unsolicited penis images.[50] It must also be accepted that the conduct is sufficiently harmful such that the conduct must cross 'the boundary between conduct which is unattractive, even unreasonable, and conduct which is oppressive and unacceptable'.[51] As well as proving these conduct elements of the offence, it must also be shown that the offender knew or ought to have known that the conduct amounts to harassment.[52] A conviction, therefore, will only follow if a 'reasonable person' would consider two or more instances of cyberflashing as constituting a criminal level of 'harassment'. While we argue that this ought to be the case, it is not necessarily clear in view of some of the public minimisation and trivialisation of this conduct, as discussed above. Such a context, therefore, risks inhibiting police and prosecutors from pursuing such cases.

While this legislation focuses on harassment targeting specific individuals, harassment is also an important element of a range of public order offences. The Public Order Act 1986 provides two potential avenues for redress, namely s 4A covering 'intentional harassment, alarm or distress', or s 5 'harassment, alarm or distress'. For s 4A to apply to cyberflashing, it would have to be proven: (a) that the defendant intended to cause the victim harassment, alarm or distress; (b) that he used threatening, abusive or insulting words or behaviour or displays any writing, sign or other visible representation which is threatening, abusive or insulting'; and (c) that the behaviour actually caused the victim harassment, alarm or distress.

There are a number of thresholds here which mean any prosecution for cyberflashing is unlikely. The act itself has to be found to constitute threatening, abusive or insulting behaviour. While this should not be difficult, it may be, for reasons already discussed, that police and prosecutors do not assume that the conduct meets such a threshold as they lack an understanding of the nature and harms of the conduct. The requirement to demonstrate a particular motive adds another dimension to an investigation. We know from cases of non-consensual distribution of intimate images that this threshold can provide a challenge for police and prosecutors.[53] This is likely to be even more the case in relation to cyberflashing where there is often only a single distribution of an image, with no other additional text or other actions. Further, even where the behaviour is experienced as threatening and abusive, this may not have been the sender's intention (as stated or in actuality). Finally, this offence also requires proof of a particular result, naming that the victim was actually caused harm, proven from evidence. While this may be possible in many cases, it is a further invasion of a victim's privacy and an unnecessary burden to provide the necessary evidence. The victim-survivor who is understandably incensed by this conduct and the breach of their rights and sexual autonomy, but not suffered demonstrable harm, will have no recourse under this legislation.

The alternative might be prosecution under s 5 which focuses on the behaviour of the perpetrator, but this requires that the defendant 'displays any writing, sign or other visible representation which is threatening or abusive', or 'uses threatening or abusive words or behaviour', and that the conduct take

50. See Gallagher (n 5).
51. *Majrowski v Guy's and Thomas' NHS Trust* [2007] [30].
52. In addition, a single instance of cyberflashing could form part of a larger pattern of harassment including a range of other harassing behaviours such as to justify a prosecution. In such cases, while an act of cyberflashing is part of a prosecution, this is only as part of a broader course of conduct rather than on the harms of cyberflashing per se or on the basis of only one instance of this behaviour.
53. McGlynn and others (n 3).

place 'within the hearing or sight of a person likely to be caused harassment, alarm or distress thereby'. It must also be proven that the defendant intends that their words or behaviour is threatening or abusive, or is aware that it may be. Accordingly, it is not obvious that this offence would cover cyberflashing. While the use of Bluetooth or Airdrop might be 'within the hearing or sight' of a person likely to be caused harassment, alarm or distress, that would require prosecutors to take a more innovative approach to prosecutions under this legislation. It also requires recognition that the conduct itself is 'threatening or abusive' which may also require persuasion of criminal justice personnel. Therefore, while the public order offences might provide some means by which police could challenge cyberflashing behaviours, successful prosecutions seem unlikely. Further, as these are 'public' order offences, they do not apply to conduct occurring exclusively in private, further limiting their scope.[54]

Accordingly, while many victim-survivors describe their experience of cyberflashing as one of sexual harassment, there is little scope under current criminal laws covering harassment to prosecute cyberflashing.

Cyberflashing as a Problematic Communication?

This leads us to the final option for the current criminal law and to what are known as communications offences which were first introduced in the 1980s to criminalise 'poison pen' letters and other communications which were abusive and threatening.[55] There are two possible offences that might cover cyberflashing, namely s 1 of the Malicious Communications Act 1988 and s 127 of the Communications Act 2003. In essence, cyberflashing will only come within these provisions if it can be shown that at least one of the purposes in sending the penis image was to cause distress or anxiety to the recipient and that the message was indecent or grossly offensive.

While there may be some debate about whether an accused intended to cause distress or anxiety, for example if they claim that they acted for a sexual purpose or for amusement, as the required intention need only be *one of* the purposes, then this element is going to be more easily satisfied. More open to debate is whether a penis image will pass the threshold of being indecent, grossly offensive, menacing or obscene. These are malleable concepts whose meaning shifts over time. Grossly offensive requires some 'added value'[56] over and above offence, with CPS guidance stating that the behaviour must be more than 'offensive, shocking or disturbing'.[57] Judicial guidance does little to help with Lord Bingham in *DPP v Collins* [2006] stating: 'There can be no yardstick of gross offensiveness otherwise than by the application of a reasonably enlightened, but not perfectionist, contemporary standards to the particular message sent in its particular context'.[58] The law on 'indecency' is similarly vague. Indecency in some contexts includes nudity, particularly in relation to child sexual abuse images, but it is less certain whether adult nudity satisfies such a test.[59] It may be that a particularly problematic distinction could arise between an erect or not penis, with the former being classed grossly offensive and indecent, but not the latter as it is 'simple nudity'.

The communications offences, therefore, have a potentially broad reach meaning that they could encompass some forms of cyberflashing. However, the vagueness and potential breadth of these offences means that their use is often controversial, with concerns raised regarding the over-use of the criminal law. Further, if there is a public or prosecutorial belief that cyberflashing is not serious or unlikely to cause significant harm, such behaviours may not be characterised as 'grossly offensive' or indecent and

54. Law Commission (n 43) para 8.108.
55. Ibid para 4.10.
56. Ibid para 5.43.
57. As stated in Crown Prosecution Service Guidance, 'Stalking and Harassment' <https://www.cps.gov.uk/legal-guidance/stalking-and-harassment> accessed 25 August 2020.
58. [2006] UKHL 40 para 9.
59. Law Commission (n 43) para 6.85.

are more likely to be dismissed as just annoying or shocking, but not of a criminal standard of harm. Finally, because these offences are designed around specific forms of communications, some means of cyberflashing, such as using Bluetooth, cannot be prosecuted under the Communications Act as it is designed to protect only a 'public communications network'.

Taking these complications and concerns together, securing a prosecution under the communications offences is likely to be a challenge; albeit still more likely than the other potential offences discussed above. Therefore, while the idea of cyberflashing being characterised as a 'problematic communication' fails to recognise the nature and harms of these behaviours, it provides one potential avenue for criminalisation under current English criminal laws.

Learning Lessons: Law Reform in Texas, Singapore and Scotland

English law, therefore, is struggling to cope with advances in technology and new ways of perpetrating harassment and abuse. It is not alone, with other common law jurisdictions such as Canada,[60] New Zealand and Australia[61] and many of the US states, also having a range of harassment and communications provisions which could be used, in some circumstances, to prosecute cyberflashing. However, as in England and Wales, the law is not clear and it is difficult to shoehorn cyberflashing into existing criminal offences. Other countries are seeking to use provisions in their general laws to cover this phenomenon, with India, for example, making imaginative use of laws against pornography and 'insulting the modesty of a woman' to successfully prosecute cyberflashing.[62] While these countries, including England and Wales, fail to provide a clear deterrent and avenue for victim-survivors to take redress, other jurisdictions have either recently introduced specific offences to cover cyberflashing or, in the case of Scotland, have a sufficiently broad sexual offence which covers this conduct. This section analyses these provisions to identify the key elements necessary to craft a specific criminal law in England and Wales targeting cyberflashing.[63]

Singapore: New Offence of Sexual Exposure

Since January 2020, cyberflashing has constituted a specific criminal offence in Singapore, with a maximum prison sentence of one year. Introduced following concern over both 'emerging crime trends'[64] and the 'pervasive' nature of 'digital sexual violence',[65] the new offence is committed where a person intentionally distributes to another an image of their or another's genitals, intending that the

60. Beattie (n 19).

61. *The Sydney Morning Herald* (n 18); *Gizmodo* 'Australian Man Jailed for Unsolicited Sexting' (12 September 2014) <https://www.gizmodo.com.au/2014/09/australian-man-jailed-for-unsolicited-sexting/> accessed 25 August 2020.

62. *Times of India*, 'Mumbai: Man Makes Video Call to Scriptwriter and Flashes Her' (14 July 2019) <https://timesofindia.indiatimes.com/city/mumbai/mumbai-man-makes-video-call-to-scriptwriter-and-flashes-her/articleshow/70211023.cms?utm_source=contentofinterest&utm_medium=text&utm_campaign=cppst> (accessed 21 August 2020).

63. We focus on Singapore, the US and Scotland, but there is also specific legislation in Denmark where the government recently raised the penalty for sending penis images without consent, with the maximum fine now being 5000 DKK (approx. 760 USD) Mandau (n 9). Another example can be found in Japan where local areas are also taking action where they can against cyberflashers; *Asia Times*, 'Mobile Penis Flashers on the Rise in Japan' (25 August 2019) <https://asiatimes.com/2019/08/mobile-penis-flashers-on-the-rise-in-japan/> accessed 25 August 2020.

64. PCRC, *Penal Code Review Committee Report* (2018) <https://www.reach.gov.sg/-/media/reach/old-reach/2018/public-consult/mha/annex–pcrc-report.ashx> accessed 25 August 2020; *Today*, 'Explainer: How the Criminal Law Reform Bill Aims to Fight Crimes of the Internet Age' (13 February 2019) <https://www.todayonline.com/singapore/explainer-how-criminal-law-reform-bill-aims-fight-crimes-internet-age> accessed 25 August 2020.

65. *Thomson Reuters Foundation* '"Pervasive" Digital Sexual Violence against Women Skyrockets in Singapore' (25 November 2019) <https://www.reuters.com/article/us-singapore-crime-technology-women/pervasive-digital-sexual-violence-against-women-skyrockets-in-singapore-idUSKBN1XZ1NB> accessed 25 August 2020; L Vitis. 'Private, Hidden and Obscured: Image-Based Sexual Abuse in Singapore' 15 Asian J Criminol 25.

victim see the image and that the offender does so for the purpose of obtaining sexual gratification or of causing the victim humiliation, distress or alarm.[66] Crucially, the offence is labelled 'sexual exposure' and included as a new sexual offence in the Penal Code. The Penal Code Review Committee had noted that existing offences which covered some forms of exposure did not capture sexual or malicious motives, nor did they capture the 'essence' of the wrongdoing and were not characterised as a 'sexual offence'.[67]

This provision has many important elements which will be valuable to replicate. In terms of the images covered, it includes an image of either the perpetrator's genitals, or another person's, removing a burdensome evidential requirement to prove the image to be of the perpetrator's penis. This is also a welcome recognition of the nature of the harm experienced by the victim, as it matters not whether she is sent an image of the perpetrator's penis or another person's. In addition, the offence is one of distribution, rather than receipt; removing any requirement to prove that the victim received the image or viewed it. The requirement to prove that the offender intends that the victim sees the image is drawn from the provisions on physical exposure, instituted to ensure that careless exposure of genitals (such as public toileting) is not included. In terms of motive requirements, the offence is at least broader than only requiring proof of sexual gratification, though it remains limited. It precludes instances of cyberflashing which may be carried out for the purpose of status-building, humour, or as a 'prank' by other young people.[68] Overall, these provisions demonstrate a welcome recognition of the problem of cyberflashing and introduce a measure which is sufficiently broad to capture a wide range of behaviours.

Texas: Criminalising Cyberflashing as Sexual Harassment

In 2019, Texas became the first US state to introduce a new, specific state law criminalising cyberflashing. The sponsors of the legislation noted that the current law 'addresses the physical act of indecent exposure, but is silent to the increasingly prevalent occurance [sic] of individuals sending sexually explicit images to an individual without their consent'.[69] The aim of the legislation was to 'offer a clear deterrent to those considering this and similar inappropriate conduct'.[70] Thus, since September 2019, there has been a criminal offence of 'unlawful electronic transmission of sexually explicit visual material', with a maximum penalty of a $500 fine, included in the sexual offences chapter of the Penal Code.[71]

The offence is one of knowing transmission of visual material depicting images of any person engaging in sexual conduct, the intimate parts of a person exposed, as well as the 'covered genitals of a male person that are in a discernably turgid state'. This broad provision means that not only are images of penises included, but also of other forms of sexual activity, as well as clothed penises. The distribution of the sexual images must have been made without the 'express consent of the recipient'. The mens rea is straightforward in requiring only intentional distribution without consent of the sexual image. There is, therefore, no specific motive requirement in this provision.

The Texan law will cover almost all instances of cyberflashing as it is not restricted in terms of motive, is an offence of distribution, and covers an extensive range of images. Indeed, it is this latter

66. Section 377BF of Singapore Penal Code.
67. PCRC (n 64) 86.
68. See our above discussion on cyberflashing motivations; also *News.com.au,* 'School Kids Putting Themselves at Risk "Pranking" Strangers with AirDrop Porn' (14 May 2018) <https://www.news.com.au/technology/school-kids-putting-themselves-at-risk-pranking-strangers-with-airdrop-porn/news-story/8f65a97dbb9bc70709a18a6b64ee5320> accessed 25 August 2020.
69. *Texas Tribune,* 'A New Texas Law Criminalizes Sending Unwanted Nudes. Lawyers Say It Might Be Difficult to Enforce' (14 August 2019) <https://www.texastribune.org/2019/08/14/Texas-new-law-sending-unwanted-nudes-dating-apps-texts/> accessed 25 August 2020.
70. Ibid.
71. Section 21.19 of Texas Penal Code.

element which makes this provision particularly interesting. The wide definition of sexually explicit visual material means that this provision becomes, in effect, an offence of sending pornography without consent. This may well give rise to challenges in terms of enforcement and debates regarding over-criminalisation. But it does underline that this is an offence of sexual harassment where it has long been recognised that unwelcome displays of pornography constitute a hostile environment.

Following the Texan lead, similar law reforms are now being considered in California where what is being called the FLASH Act (Forbid Lewd Activity and Sexual Harassment) was introduced into the Senate in February 2020.[72] The offence provides for a maximum fine of $500 for a first-time offence, rising to $1000 thereafter, where an individual knowingly transmits unsolicited lewd or sexually explicit material by electronic means. While an earlier draft of this legislation only included images of the perpetrator's penis, the most recent proposal includes images of various forms of sexual activity, or the 'exposed genitals or anus' of any person. In terms of consent, the Californian drafts provide interesting opportunities to clarify consent requirements. The current draft refers to the requirement to have 'expressly requested the image' or that the victim 'has not expressly consented to its transmittal' and this is explained to be satisfied if 'the request or consent is communicated in writing, including, but not limited to, a writing communicated by electronic means'.

These proposed reforms are interesting for a number of reasons. First, there is a clear focus on the activity constituting sexual harassment and being linked to physical exposure. The offence, therefore, is clearly framed as an issue of harassment of women, and the need for the law to catch up with technological developments. The focus is also on all forms of cyberflashing, including in dating apps and other forms of social media, beyond some of the paradigmatic examples of harassment on public transport. The images included are broad, though not as extensive as in Texas, with detailed demands to prove consent and no motive requirement. Prosecution for this offence should, therefore, be more straightforward than in relation to many other provisions.

Scotland: Coercing a Person to Look at a Sexual Image

While the jurisdictions discussed above have recently adopted specific laws on cyberflashing, there are also countries where the existing sexual offence laws are sufficiently broad to cover some instances of cyberflashing.[73] In Scotland, for example, the Sexual Offences (Scotland) Act 2009 includes the offence of 'coercing a person into looking at a sexual image' (s 6). What is interesting about this provision is that it was not introduced to specifically tackle cyberflashing, but as part of a broader understanding of the breadth and nature of sexual offending and need to ensure that laws covered as many eventualities as possible. It is now being used to prosecute cyberflashing.[74] Crucially, under this legislation, cyberflashing is framed as a sexual offence and the potential penalties are serious, with up to a maximum term of imprisonment of 10 years.

The Scottish provision was introduced in the 2009 Act following a Scottish Law Commission consultation that considered the sexual offence in English law of 'causing a person to engage in sexual activity' (s 4 Sexual Offences Act 2003). It was recognised on both sides of the border that sexual offending can include non-contact activities and behaviour, characterised by the Scottish Law

72. Measures are also being put forward in Pennsylvania, *Infosecurity,* 'Pennsylvania Might Be Second State to Criminalise Cyber Flashing' (30 September 2019) <https://www.infosecurity-magazine.com/news/pennsylvania-might-criminalize/>, and New York city introduced in 2019 an amendment to its City Code to make it 'unlawful for a person, with the intent to harass, annoy or alarm another person, to send by electronic device an unsolicited intimate image'; *New York Times,* 'Sending Lewd Nudes to Strangers Could Mean a Year in Jail' (30 November 2020) <https://www.nytimes.com/2018/11/30/nyregion/airdrop-sexual-harassment.html> (accessed 22 August 2020).

73. See also s 45 of the Irish Criminal Law (Sexual Offences) Act 2017, discussed in McGlynn and Johnson (n 4).

74. See, eg, S Gallagher, 'Would Making Cyberflashing Illegal Stop People Sending Dick Pics?' *The Huffington Post* (10 June 2019) <https://www.huffingtonpost.co.uk/entry/would-making-cyberflashing-illegal-stop-people-sending-dick-pics_uk_5c50674fe4b0d9f9be6951ce> (accessed 22 August 2020).

Commission as 'coercive'. However, while English law only provides for the offence of causing another to *engage in* sexual activity, the Scottish Law Commission recognised that coercive and offending behaviour is more complex and varied and includes the use of images and written materials. It noted that 'just as being forced to participate in sexual activity is an invasion of a person's sexual autonomy so is being forced to watch such activity'.[75]

Accordingly, the Scottish Law Commission recommended introducing an offence of making a sexual communication without consent.[76] It noted that while English law had offences of engaging in sexual activity in the presence of a child and causing a child to watch sexual activity (ss 11 and 12 of the Sexual Offences Act 2003), both offences only applied to children and sexual gratification was a required motive.[77] The Scottish Law Commission rejected both limitations as being too constraining and not covering all types of offending behaviour. The result was s 6 of the Sexual Offences (Scotland) Act 2009 which created the offence of 'coercing a person into looking at a sexual image' covering adults and children. The offence is one of intentionally causing another to look at a sexual image without their consent for the purposes of sexual gratification or humiliating, distressing or alarming the victim.

Unfortunately, this provision is more limited than that proposed by the Law Commission, as the conduct required to be proven is that of 'causing' another to look at a sexual image without their consent, rather than the more straightforward distribution of the image or making the communication. For example, if the victim did not view the image, the offence is not made out. Specific motives must also be proven, though this at least includes humiliating, distressing or alarming the victim, as well as the more commonly introduced purpose of sexual gratification. Nonetheless, 'sexual image' is broadly defined, covering images of the genitals or other 'sexual activity' of the offender, another or an 'imaginary person'. This provision, therefore, extends beyond cyberflashing to include images of other sexual activity, as well as fake and photoshopped images.

There are many lessons to be learned from this analysis of Scots law. Being framed as a sexual offence means that the nature and harms of the conduct is suitably acknowledged and, in applying to adults and children, the rights of all individuals whose sexual autonomy has been breached is recognised. Further, this provision was not originally introduced with cyberflashing in mind, but with a focus on the wide range of ways in which sexual harms are perpetrated such that the range of images covered is not unduly restricted. This highlights the importance of trying, as much as possible, to 'future-proof' the law. Further, the coverage of 'imaginary' people has particular resonance and value today, as technology is making it ever more straightforward to manipulate and fake images and videos.

The introduction of this measure has proved prescient in light of the emergence of cyberflashing: the more generic focus on coercive and non-consensual activity led to the drafting of a broad provision which is able to be used in rapidly changing circumstances, such as the technical revolution that has enabled cyberflashing. It is for those reasons that the provision is wider ranging than simply covering penis images; its scope includes images of all forms of sexual activity, meaning that causing a person to look at pornographic images without their consent is covered. Nonetheless, the provision is limited in only applying where the offender has caused another to look at the image.

Options for Law Reform: Drafting a Specific Law Criminalising Cyberflashing

As English criminal law does not clearly cover cyberflashing, and in view of the significance of the harms and impacts experienced by victim-survivors, we suggest that a new offence is introduced which

75. Scottish Law Commission, *Report on Rape and Other Sexual Offences* (Scottish Law Commission, Edinburgh 2007) para 3.55.
76. Ibid para 3.62.
77. Ibid para 3.58.

can provide a clear foundation for prosecutions and victim redress. This section outlines some of the key issues to be considered in drafting such a law, drawing on the discussion above both of the harms and nature of the conduct, as well as the lessons to be learned from other jurisdictions.

Cyberflashing as a Sexual Offence

The critical feature of each of the laws in Singapore, Texas and Scotland is that they frame cyberflashing as a sexual offence and form of sexual harassment. This ensures proper recognition of the experiences of victim-survivors and dictates the nature and scope of the offence. It is also crucial to the development of appropriate prevention and education programmes. Further, characterisation as a sexual offence brings with it vital protections for victims and witnesses such as automatic anonymity for complainants and special protections in court. Accordingly, any future provision on cyberflashing must form part of the Sexual Offences Act 2003. This could be achieved by amending s 66 of the Sexual Offences Act 2003 so that it extends to cyberflashing, as well as physical exposure, following the approach of Singapore.

Criminalise Distribution Not Viewing

Two different approaches emerge from the jurisdictions analysed above: the Scottish approach which bases the offence on causing the victim to view the image, compared with the Singaporean and Texan focus on distribution. The Scottish approach is more challenging to evidence, requiring not only a causal connection between the sending of the image and its viewing, but also that the actual image was viewed. The more straightforward focus on distribution is to be preferred, therefore, to reduce the evidential burden on prosecution and the victim-survivor.

Distribution Without Consent

The core wrong is non-consensual conduct, with any provision therefore requiring that the intended distribution is without the agreement of the victim-survivor. Determining what constitutes consent then becomes the key issue. The most straightforward approach would be to adopt the definition of consent in existing laws, in England and Wales, s 74 of the Sexual Offences Act 2003. Nonetheless, that definition has been widely critiqued as vague and unhelpful.[78] What is key in these situations of online harassment and abuse is that consent is not implied or assumed. Explicit consent, therefore, could be included as a requirement, such as the Texan law which requires 'express consent'. Further, consideration could be given to measures such as those proposed in California where current proposals are that consent to receive images must be in writing.

Intend the Victim to See the Image

To avoid criminalising accidental distribution of images, Singaporean law provides that the offender must have intended the victim to see the image. This means that were the accused to intend to distribute the image to A (perhaps with consent), but in fact sent it to B (who did not consent), the offence would not be made out, as the accused did not intend B to see the image. While in such a situation, B may well experience the harms and adverse impacts of others who are sent sexual images without their consent, there is no malice or 'guilty mind' of the person sending the image. The criminal law, therefore, is not to be engaged

78. V Munro, 'Shifting Sands? Consent, Context and Vulnerability in Contemporary Sexual Offences Policy in England and Wales' (2017) 26(4) Soc Leg Stud 417.

No Requirement to Prove Particular Motives

Texan law focuses on the key wrong of cyberflashing: non-consensual conduct which interferes with an individual's right to sexual autonomy and dignity. The offence is not characterised, therefore, as one perpetrated only for specific motives, as if being cyberflashed for reasons of status-building or humour reduce the harm experienced. This approach, therefore, best ensures that all forms of cyberflashing are covered, the victim-survivor experiences are appropriately recognised, and enables the most straightforward prosecutions. We know from studies into the prosecution of non-consensual sharing of intimate images that the requirement to prove intention to cause distress inhibits prosecutions and reports to the police.[79]

Nonetheless, if there are to be motive requirements included, they should at least cover both sexual gratification and causing harm, distress or humiliation, as in the relevant Scots and Singaporean laws. In addition, this threshold should be met where reckless intention is evidenced, as in the Scots law on non-consensual distribution of intimate images.[80] This would help to ensure that where, for example, a perpetrator is acting in order to impress or humour his friends, awareness that his actions could cause distress to the victim, even if not his direct motive, would be sufficient to satisfy the provision.

All the Penises: Not Limited to Images of the Perpetrator's Genitals

If the offence is limited to only covering images of the perpetrator's penis, we will be left with a practically impossible offence to prosecute. Police and prosecutors would be required to prove that the offending image was of the accused's penis, which raises a wealth of challenges—including a likely unattainable evidential burden, especially because the current status and scope of forensic penile identification is limited and insufficient for a criminal justice setting.[81] It is also not difficult to anticipate that such a requirement will make victim-survivors less likely to report the offence and the police less willing to pursue investigations. Law makers should be ready to straightforwardly follow the example of other jurisdictions and include all penis images.

Fake Images and Imaginary People

Scots law on causing someone to look at a sexual image ensures broad applicability by providing that the sexual image can be of the offender, another person or an 'imaginary person'. Similarly, Scots law on the non-consensual sharing of intimate images covers images altered by digital or other means meaning that images and videos amended using developing technology, and often referred to as 'deepfakes', are covered.[82] These provisions ensure that the law is keeping pace with digital technologies which are making it easier and easier to create images where it is almost impossible to tell whether they are 'real' or 'faked'. English law lags far behind in this regard and future laws must ensure that they apply to altered images, as it is perhaps not surprising that photoshopping technology is used to alter penis images.

Criminalising Non-Consensual Distribution of Sexual Images

A final question to consider is whether material other than genital images are to be included. Many of the proposals and laws in the US, for example, extend to a wide range of images of sexual activity, as well as images of genitals, as does Scots law. Texan law also includes a 'covered' penis, if erect. In practice,

79. McGlynn and others (n 3).
80. Section 2 of Abusive Behaviour and Sexual Harm (Scotland) Act 2016.
81. See McGlynn and Johnson (n 4); also *Irish Legal News,* 'Forensic Expert Moots Penile Database to Tackle Sex Crime' (3 September 2018) <https://irishlegal.com/article/forensics-expert-moots-penile-database-to-tackle-sex-crime> accessed 14 August 2020.
82. Section 3 of Abusive Behaviour and Sexual Harm (Scotland) Act 2016.

these provisions amount to an offence of distributing pornography without consent. One advantage of such breadth is that it ensures that we do not end up adopting a law that covers sending penis images without consent, only to find that perpetrators start harassing and abusing with some other type of image. It would also ensure that we see the links between cyberflashing and other forms of sexual harassment. However, rather than merely developing a broad definition for a cyberflashing offence, it may be that developing legislation to target the underlying wrong of sexual harassment would be more advantageous for 'future-proofing the law', against men's various, ever-evolving practices that sexually harass and abuse women.[83]

Conclusions

The criminal law is failing victim-survivors as there is no clear means by which to prosecute cyberflashing. The law is simply failing to recognise, understand and tackle an alarmingly commonplace form of coercive sexual intrusion experienced by women. Cyberflashing, as with so many harms experienced predominantly by women, falls between the gaps and categories of English criminal law. As seen with other forms of abuse that have thrived with developing technology, such as forms of image-based sexual abuse such as 'upskirting' and the non-consensual sharing of sexual images, these experiences defy existing categories and provide a headache for victims and the criminal justice system in trying to fit them within existing laws. Partly, this is because technology is advancing and perpetrators are finding new ways of harassing and abusing women, with the law notoriously slow to catch up.

But this is not the whole story. Feminist lawyers have long argued that the law fails to understand and reflect women's experiences of harm,[84] with some scholars developing whole new ways of categorising and understanding the law with women's experiences at the fore.[85] The challenge is that while it is right to recognise that there are 'no clearly defined and discrete analytic categories' into which 'men's behaviour can be placed',[86] to provide some remedy via the criminal law, we must work to organise the law such that it reflects, supports and then challenges the harms experienced by women.

A first step towards remedying this situation is to introduce a specific law criminalising cyberflashing. This approach has some advantages including that the behaviours would clearly be criminal, deploying the expressive power of the criminal law to signal to society that this is unwanted and unacceptable conduct. In this way, any new law may support educational and other prevention initiatives by recognising cyberflashing as a form of sexual harassment and abuse. Moreover, prosecution and convictions would enable some victim-survivor to secure some measure of justice for the harms they have experienced.

Nonetheless, while welcome, the disadvantages of a specific law only covering cyberflashing is that it may provide a remedy for identified behaviours in the short-term, but does not 'future-proof' the law to cover the new, but as yet unimaginable, ways that offenders will inevitably perpetrate abuse and harassment. Accordingly, therefore, as well as adopting a specific measure, we must think more deeply about measures to criminalise broader forms of sexual intrusions which may, in the longer term, provide women more general protection against abuse.

Acknowledgements

The authors owe considerable thanks to Magdalena Furgalska for her excellent research assistance in the preparation of this article.

83. See McGlynn and Johnson (n 4).
84. See, eg, R Graycar and J Morgan, *The Hidden Gender of Law* (Federation Press, Alexandria 2002); J Conaghan, *Law and Gender* (OUP, Oxford 2013).
85. TS Dahl, '*Women's Law: An Introduction to Feminist Jurisprudence* (Scandinavian University Press, Oslo 1987).
86. Kelly (n 29) 7.

Declaration of Conflicting Interests

The author(s) declared no potential conflicts of interest with respect to the research, authorship and/or publication of this article.

Funding

The author(s) received no financial support for the research, authorship and/or publication of this article.