Original Manuscript

The Journal of Criminal Law

A Critical Analysis of the Law Commission's Proposed Cyberflashing Offence

The Journal of Criminal Law
1–14

DOI: 10.1177/00220183221125873
journals.sagepub.com/home/clj

Bo Wang
School of Law, University of Sheffield, UK

Abstract

The Law Commission has proposed a new offence of cyberflashing to combat the problem of sending unsolicited images or videos of human genitals to others. It seems that what the Law Commission has in mind is not flashing *per se*, but cyber-nudity. Its proposal fails to comprehensively evaluate the adequacy of existing law and fails to balance the harm of a criminal conviction against the potential harm of cyberflashing. It shall be argued that the Law Commission seems to have conflated wrong with harm and that its harm claim is supported only by anecdotal evidence. The vast majority of cyberflashing cases, including most Airdropping and Bluetoothing cases, are already covered by existing law, leaving untouched only a handful of one-off Airdropping or Bluetoothing cases where the flasher did not intend to cause distress or anxiety and the victim did not apprehend imminent unlawful force. Thus, it is argued that this very narrowly tailored cyberflashing offence adds very little and that amending existing communication offences or harassment offences would provide more protection to victims as such offences could apply to a wide range of sexually harassing content, not just images or videos of human genitals.

Keywords

Cyberflashing, Communication Offences, Sexual Offences, Harassment, Harm, Wrong

Introduction

The common use of smartphones and wireless technologies makes communication between people more efficient and easier, and online communication has become an almost indispensable part of people's daily life. But such technological and societal change has caused many new problems, one of which is the prevalence of cyberflashing. Cyberflashing can encompass a number of different behaviours, from the sending of self-produced sexual images or videos to the non-consensual transfer of pornographic media via digital means.[1] It is stated that women frequently experience cyberflashing in public places

1. Craig A Harper, Dean Fido and Dominic Petronzi, "Delineating Non-consensual Sexual Image Offending: Towards an Empirical Approach" (2021) 58 (1015347*) Aggression and Violent Behaviour* 1, 6.

Corresponding author:
Bo Wang, School of Law, University of Sheffield, Bartolome House, Winter Street, Sheffield S3 7ND, UK.
E-mail: b.v.wang@sheffield.ac.uk

as well as on various online platforms.[2] Receiving an unsolicited sexually explicit image or video could impact the victim in various ways such as causing them disgust, anger, annoyance or fear.[3] In certain contexts, cyberflashing also has the potential to communicate that physical contact including violent and sexual contact might follow the communication. Cyberflashing thus is seen as part of a wider pattern of everyday sexual harassment and has attracted considerable public attention lately. New offences have been introduced in some parts of the world to tackle cyberflashing.[4]

As part of a larger project to combat harmful online communications, the Law Commission of England and Wales has proposed a new independent offence of cyberflashing.[5] The harm caused by cyberflashing, the prevalence of cyberflashing and the inadequacy of the current law are said to be the three rationales for proposing this new offence.[6] The Law Commission suggests that cyberflashing causes harm as it causes serious mental distress, but the Law Commission does not make this a result crime requiring it to cause actual bodily (mental) harm. Thus, it seems not convinced that in practice evidence of harm will be forthcoming in the majority of cases. The scope of conduct this new offence aims to criminalise is very narrow in that it merely covers sending the image or video of human genitals to another. Other forms of sexually harassing communication such as sending a foul text message without any imagery of genitalia and sending a nude photo of the recipient to the recipient, are not covered by this new offence. If this offence aims to tackle sexual harassment, then it would have made sense to cover other forms of grossly offensive material that aims to harass, and it would also have made sense to introduce "a course of conduct" test like that in the Protection from Harassment Act 1997 to prevent overcriminalisation. The Law Commission seems to be fixated with nudity *per se*, but other sexually harassing content in a message need not contain any nudity[7] and can cause equal mental distress to the recipient.

In this article, it will be submitted that the proposed cyberflashing offence is unsatisfactory and may add to the overcriminalisation crisis if all it adds is to catch a very small number of one-off Airdropping and Bluetoothing[8] cases where the flasher did not intend to cause distress or anxiety and the victim did not apprehend imminent unlawful force. Criminalisation of such one-off flashing conduct is not supported by sound empirical evidence, especially when the proposed offence carries a two-year custodial sentence and the sex offender registration. This is not to say that cyberflashing does not need criminalising or

2. Clare McGlynn and Kelly Johnson, "Criminalising Cyberflashing: Options for Law Reform" (2020) *The Journal of Criminal Law* 1, 3.
3. Brenna C Miller, "Fact or Phallus? Considering the Constitutionality of Texas's Cyber-Flashing Law under the True Threat Doctrine" (2021) *8 Texas A&M Law Review* 423, 427.
4. For example, S.21.19 of the Texas Penal Code makes it an offence if one, without the request or express consent of the recipient, knowingly transmits by electronic means visual material that depicts any person engaging in sexual conduct or with the person's intimate parts exposed or depicts covered genitals of a male person that in a discernibly turgid state. Similarly, S.377BF of the Singapore Penal Code makes it an offence if one, for the purpose of obtaining sexual gratification or of causing the recipient humiliation, alarm or distress, intentionally exposes his or her genitals to the recipient or distributes an image of any person's genitals, without the recipient's consent.
5. Law Commission, *Modernising Communications Offences: A Final Report* (Law Com 399, 2021) chap. 6.
6. Ibid, para. 6.11.
7. For example, one newspaper columnist received a message stating "it doesn't say much for her… that with 3.4 billion rapists on earth, she hasn't had a cock near her in decades". Another sexually harassing comment states: "if u were beaten to death i would laugh then id find the pics of ur bloody, bruised body & jack off to them". Jessica Megarry, "Online Incivity or Sexual Harassment? Conceptualising Women's Experiences in the Digital Age" (2014) 47 *Women's Studies International Forum* 46, 49.
8. AirDrop is a feature on Apple devices which enables the user to share information with other nearby Apple devices using Wi-Fi and Bluetooth. Caroline Knorr, "What's AirDrop and Why Are Kids Using It?"<https://www.commonsensemedia.org/blog/whats-airdrop-and-why-are-kids-using-it> accessed 15 October 2021; Bluetooth devices can be connected to each other and exchange information if they are within a distance of 10 meters. Mark Taylor and Victoria Coombs, "Wi-Fi, WiMax and Bluetooth" (2006) 12(7*) Computer and Telecommunications Law Review* 257, 257. Bluetooth technology enables the creation of an *ad hoc* network between devices, which is taken as an electronic communications network because it permits the conveyance of signals. Eleni Kosta, Peggy Valcke and David Stevens, "'Spam, Spam, Spam, Spam…Lovely Spam!' Why is Bluespam Different?" (2009) 23 (1-2) *International Review of Law, Computers and Technology* 89,92.

that the victim's sexual autonomy does not deserve protection. Rather, this paper aims to examine whether it is worth all the legislative resources to have such a narrowly tailored offence and all the judicial resources in the future to enforce this offence if it only covers one of many forms (human nudity) of online sexual harassment.

This paper begins by setting out the constituent elements of this proposed cyberflashing offence. It then examines if existing offences in English law are sufficient for dealing with cyberflashing as defined in the Law Commission report. It will be argued that the vast majority of cyberflashing cases can be caught by existing offences making the contribution of this new offence limited to the tackling of one-off cyberflashing done by means of a non-public communication network where the recipient suffers only ephemeral distress but does not apprehend imminent unlawful force. Starting from this premise, the article moves on to the harm analysis assessing if this narrowly tailored cyberflashing offence is well supported by criminalisation theory and sound empirical evidence. It is submitted that the Law Commission seems to have confused harm with wrong and fails to carry out a nuanced ethical and social evaluation of the harm that is likely to be caused by cyberflashing. It is bad enough Parliament blindly adding law on top of law without seeing that the conduct is already adequately criminalised in existing offences without the Law Commission adding to that problem.[9]

The Proposed Cyberflashing Offence

The Law Commission contends that the current law cannot provide a satisfactory solution to cyberflashing and proposes a cyberflashing offence reads as follows:

> (1) The defendant (A) intentionally sent an image or video recording of any person's genitals to another person (B), and
> (2) either- (a) A intended that B would see the image or video recording and be caused alarm, distress or humiliation, or (b) A sent the image or video recording for the purpose of obtaining sexual gratification and was reckless as to whether B would be caused alarm, distress or humiliation.

The conduct element of this proposed cyberflashing merely requires the defendant sends an image or video of any person's genitals to the victim regardless the way how it is sent. It is not limited to electronic communication, and thus it also covers situations such as where the defendant slips a printed photograph of human genitals into the victim's bag.[10] This conduct element mirrors that of S.1 of the Malicious Communications Act 1988. The Law Commission proposes this offence to be a sexual offence, yet the conduct element does not reflect a typical feature of sexual offences that the conduct is done without the victim's consent.[11] Consent is described as "moral magic" which can transform the moral quality of a conduct.[12] Taking property from another with their consent is not theft, and adults' having sex consensually is not rape and so forth. Those who attend a nude strip show will not be wronged even if they become alarmed or distressed by the show, because they consented to its

9. See Andrew Ashworth, "Is the Criminal law a Lost Cause?" (2000) 116 LQR 225.
10. Law Com 399, 2021, para. 6.54.
11. The newly enacted cyberflashing offence under S.21.19 of the Texas Penal Code has "not sent at the request of or with the express consent of the recipient" as one of the conduct elements. S.6 of the Sexual Offences Act 2009 (Scotland) has "without B's consenting" as one of the conduct elements and "without any belief that B consents" as one of the *mens rea* elements. McGlynn, who is a strong advocate of having a new cyberflashing offence, argues that the cyberflashing offence should be consent-based rather than motive-based so that it can cover all kinds of non-consensual sending of image or video of human genitals. Clare McGlynn, "Cyberflashing: Consent, Reform and the Criminal Law" (2022) 18 Jan. *The Journal of Criminal Law* 1-17.
12. Heidi M. Hurd, "The Moral Magic of Consent" (1996) 2 *Legal Theory* 121.

content and chose to see it. There is scarcely any denying of the centrality of the consent threshold in contemporary sexual offences legislation and policy.[13]

The reason for not adopting non-consent as an element in the proposed offence is that the Law Commission is concerned that too many non-consensual communications without fault will be caught by the offence.[14] It is suggested by the Law Commission that accidentally sending nudity would be criminalised if consent were required. Suppose a person sends a picture of himself fully clothed on a nudist beach without realising a nude person is showing in the background; it is said that if lack of consent is an element this person would be liable as his friend did not consent to see the nude person in the background.[15] This argument is hollow, since the *mens rea* element would protect the sender from criminal liability. The sender's mistake about the fact that he is sending nude images rather than simply an image of him clothed would negate the mental element concerning an intention to send nudity with the ulterior intention or ulterior recklessness that it will cause alarm and distress.

Another situation may arise after lovers have just ended their relationship and had a history of sexting each other nude images. D genuinely believes that he can seduce V to take him back by sending her nude images: the context here would give the factfinder sufficient evidence to infer that D genuinely believed he was acting with V's implied consent. Of course, if V has already expressed her dissent in receiving any of D's nude photos, the factfinder could infer the opposite. In the vast majority of cyberflashing cases, where images or videos of human genitals are sent to strangers, the factfinder most likely would infer that sender's mistaken belief in consent was so unreasonable that he could not have held such a belief. Similarly, where police officers send child pornography to a specialist colleague so that it can be catalogued in evidence for use in a trial, they will not only have a statutory defence but will be able to assert that the colleague impliedly consented to receive the communication. It seems contradictory that the Law Commission takes cyberflashing as a sexual offence[16] while at the same time arguing that a lack of consent element is unnecessary for this offence.[17]

The *mens rea* element of this proposed cyberflashing offence can be satisfied in two alternative ways. One is that the defendant intends to cause alarm, distress or humiliation. The other is that the defendant has a purpose of obtaining sexual gratification and is also reckless as to whether the receiver will suffer alarm, distress or humiliation. But if D believes it will sexually thrill the receiver as he thinks he is very attractive, D will not be liable for this new offence because D will lack the intention to cause or recklessness as to causing the receiver any alarm, distress or humiliation. Such a delusional sender subjectively believes there is no risk of causing alarm, distress or humiliation because he believes the image will thrill the recipient. Objectively, his conduct may cause, or will cause, alarm, distress or humiliation to the recipient; however, the test for recklessness is a subjective one looking at what the defendant has foreseen rather than what he should or could have foreseen.[18] Where D sends such image or video to V having realised that it might cause V alarm, distress or humiliation, he will not be liable if his purpose is not to obtain sexual gratification. This could be a case where D sends such photo or video to make fun of V.

This offence aims to preserve the sexual autonomy and dignity of potential victims.[19] However, it is odd that it does not cover the act of sending other sexually harassing content, such as pornographic novels and stories, cartoon images of a penis, a comic strip of a woman being raped, gang rape jokes, etc. It is not

13. Tom O'Malley and Elisa Hoven, "Consent in the Law Relating to Sexual Offences" in Kai Ambos and others (eds) *Core Concepts in Criminal Law and Criminal Justice* Vol. 1 (CUP 2019) 136; Vanessa E Munro, "Shifting Sands? Consent, Context and Vulnerability in Contemporary Sexual Offences Policy in England and Wales" (2017) 26(4) *Social and Legal Studies* 417, 418.
14. Law Com 399, 2021, para. 6.81.
15. Ibid, para. 6.112.
16. Ibid, para. 6.51.
17. Ibid, para. 6.108.
18. *R v G and Another* [2003] UKHL 50.
19. Law Com 399*,* 2021, para. 6.108.

clear why the Law Commission prefers to have an independent offence for the sending of image or video of human genitals but not for the sending of other sexually harassing materials, if this offence needs marking out as a sexual offence to make the sexual offenders registration scheme applicable. It seems that this offence is not targeting flashing *per se* but the transfer of sexual images or videos containing nudity. The publication of obscene materials has traditionally been treated as a pornography offence, but those offences are rarely prosecuted in twenty-first century[20] as nudity *per se* is no longer so taboo and frightening as it was in the 1950s.[21] Paternalistic conceptions of women fainting at the sight of nudity and needing to be brought back to consciousness with "smelling salts" is not reflective of 21st century Britain. If nudity itself is not the problem, then it has to be the sexually harassing nature of cyberflashing that provides the justification for criminalising it. If it is sexual harassment that is essentially being criminalised, then it is best done under the Protection from Harassment Act 1997, which could be amended (e.g. making the sexual nature of the conduct an aggravating factor) so that the notification provisions in Ss.80-81 of the Sexual Offences Act 2003 can apply in serious cases.

Is the Current Law Sufficient for Combating Cyberflashing?

The Law Commission contends that the current English criminal law is inadequate to combat cyberflashing.[22] In the following discussions, I will examine if the current criminal law can effectively deal with cyberflashing and whether it is worth all the effort and legislative as well as judicial resources to have such a narrowly tailored offence.

The common law offence of outraging public decency is committed where one does an act which is of such a lewd, obscene or disgusting character that it outrages public decency and the act is done in a place to which the public has access or in a place where the act done is capable of public view.[23] Cyberflashing on certain social media such as Twitter will be caught by this offence because it is done in a public online space and the image or video sent is capable of being seen by other users. The public element of this offence is satisfied as long as the act is capable of being seen by two or more persons who are actually present, even if they do not actually see it.[24] But not all cyberflashing cases can be caught by this offence. A great deal of cyberflashing involves person to person communications which will not be capable of being seen by others other than the recipient and thus will not satisfy the public element of the offence of outraging public decency.

Section 66 of the Sexual Offences Act 2003 is another offence which can cover some of the cyberflashing cases. The offence has an *actus reus* requirement that D exposes himself or herself at the time of the offence. The provision itself does not limit the exposure to in-person exposure.[25] In the case of *R v Alderton*,[26] the defendant made Facetime calls to his victims and showed himself masturbating, as a result of which he was held liable for S.66.[27] But the reach of S.66 does not extend to digital images and videos as opposed to live conduct.

Although sending image or video of another's genitals cannot be dealt with by the exposure offence, it may well fall into the ambit of the communication offences as prescribed in the Malicious

20. Peter Beaumont and Nichi Hodgson, "Obscenity law in doubt after jury acquits distributor of gay pornography" (The Guardian, 7 Jan 2012) < https://www.theguardian.com/law/2012/jan/07/obscene-publications-act-future-doubt > accessed 2 August 2022.
21. For a background of the Obscene Publications Act 1959, see Norman St. John-Stevas, *Obscenity and the Law* (Secker & Warburg 1956).
22. Law Com 399, 2021, paras. 6.26-6.31.
23. *R v Hamilton* [2007] EWCA Crim 2062 [31].
24. Ibid [39]; *Rose v DPP* [2006] EWHC 852 (Admin) [24].
25. In person exposure has a wide range of impact on the victim ranging from disturbing, sinister to frightening. *R v Ferguson* [2008] EWCA Crim 2940.
26. [2014] EWCA Crim 2204.
27. Section 21.19 of the Texas Penal Code treats non-live streamed exposure (i.e., still images and video recordings) as a form of online indecent exposure. Miller (n 3) 439.

Communications Act 1988 and the Communications Act 2003. S.1 of the Malicious Communications Act 1988 provides for the offence of sending materials or communication with intent of causing distress or anxiety. The *actus reus* of this offence can be committed if (a) the defendant sends a letter, electronic communication or article of any description which conveys a message that is indecent or grossly offensive, a threat or information that is false or believed to be false by the defendant or (b) the defendant sends an article or electronic communication which is, in whole or in part, of an indecent or grossly offensive nature. Cyberflashing easily satisfies the *actus reus* of this offence because images or videos of human genitals are sent to the recipient by means of an electronic communication network. Cyberflashing done by using the Internet or other instant communication technologies such as Airdrop and Bluetooth is electronic communication. Moreover, the image or video of one's genitals would surely be indecent or grossly offensive when it is sent to non-consensual recipient. "Grossly offensive" indicates a high threshold of offensiveness and "indecent" conveys the idea of offending against the recognised standards of propriety.[28] The *mens rea* of S.1 requires that the purpose or one of the purposes of the defendant in sending such material is to cause distress or anxiety to the intended recipient.[29] The Law Commission believes this offence is insufficient to cover cyberflashing cases due to its restricted *mens rea* requirement.[30] If there is a case for criminalising reckless acts of cyberflashing, then why not amend S.1 of the Malicious Communications Act 1988 so that reckless acts of sending other grossly offensive messages are also criminalised? It is not clear why the Law Commission feels that image or video of human genitals is worse than other forms of sexually explicit messaging (which could equally make a person apprehend imminent sexual violence or feel sexually harassed) and therefore needs a separate offence. For example, sending someone a picture containing pornographic cartoons or pornography quotes from poetry or elsewhere without consent can also cause alarm or distress, if sent in a harassing context. S.1 of the Malicious Communications Act 1988 catches the full range of materials that might be used to harass the victim and can be easily amended by adding recklessness as an alternative *mens rea* element.

What's more, the vast majority of reckless cyberflashing cases will be covered by S.127(1)(a) of the Communications Act 2003. The *actus reus* of S.127(1)(a) requires the defendant sends by means of a public electronic communications network a massage or other matter that is grossly offensive or of an indecent, obscene or menacing character. The *mens rea* of S.127(1)(a) is proved if the defendant intends or is reckless as to whether the communication will be grossly offensive,[31]indecent, obscene or menacing.[32] The purpose of the S.127(1)(a) is to protect the integrity of public communication networks rather than to protect individual from receiving unsolicited messages which they may find seriously objectionable.[33] When a person sends image or video of human genitals to another without consent, it is not difficult to find them liable for S.127(1)(a), because such image or video will be grossly offensive to the non-consenting recipient and the sender intends it be so or is reckless as to it being so. "Public electronic communications network" means an electronic communications network provided wholly or mainly for the purpose of making electronic communications services available to members of the public.[34] Where the communication is sent through websites (e.g. Facebook and Twitter) or on applications (e.g. WhatsApp, Snapchat and Zoom) which operate through the Internet,

28. *Connolly v DPP* [2008] EWHC 237 (Admin) [8]. In this case, the defendant sent close-up colour photographs of dead foetuses to the victim, which was regarded as grossly offensive or indecent by the court. The photographs were described by the court as "shocking and disturbing". Image or video of one's genitals that is sent to a non-consensual recipient clearly share such characteristic of being shocking and disturbing.
29. Malicious Communications Act 1988, s 1 (1); *DPP v Bussetti* [2021] EWHC 2140 (Admin) [26].
30. Law Com 399, 2021, para. 6.29.
31. *DPP v Collins* [2006] UKHL 40 [10]-[11].
32. *Chambers v DPP* [2012] EWHC 2157(Admin) [38].
33. *Collins* (n 31) [7]; *Bussetti* (n 29) [27].
34. Communications Act 2003, s 151(1).

it will be regarded as sent by means of a public communication network.[35] The fact that the defendant may only want the communication to reach a limited class of people who would be neither fearful nor apprehensive is irrelevant.[36] In addition, S.127(2)(c) of the Communications Act 2003 is established when a person persistently makes use of a public electronic communication network for the purpose of causing annoyance, inconvenience or needless anxiety to another. When one keeps sending unsolicited images or videos of human genitals or any other annoying materials to another, this would be persistent use of public electronic communication network, which would cause annoyance or inconvenience, if not needless anxiety. Such persistent conduct would also be harassment contrary S.2 of the Protection from Harassment Act 1997.

The Law Commission's concern is that cyberflashing done through peer-to-peer communication technologies such as Airdrop and Bluetooth falls outside the purview of S.127. Given that S.1 of the Malicious Communications Act 1988 can cover Airdropping or Bluetoothing cases where the defendant intends to cause the recipient distress or anxiety by sending an image or video of human genitals, the appropriate solution would be to expand the mental element for that offence, not to layer up with another narrowly tailored crime carving out "image or video of human genitals" for treatment while leaving all other forms of sexually explicit and sexually harassing content to be dealt with in the existing law. The Law Commission seems to be fixated with nudity at the cost of considering all sexual content that might be used to violate the sexual autonomy of others by sexually harassing them.

Among those Airdropping and Bluetoothing cases that are not covered by existing communication offences, many of them will be easily caught by the offences of common assault and statutory harassment. According to the Law Commission report, one of the rationales for making an independent cyberflashing offence is that many victims of cyberflashing suffer harm that stems from a well-founded fear that a sexual assault might follow the communication.[37] It is true that when the sender is within physical proximity and the recipient knows this or believes this to be the case, the recipient may genuinely feel that an assault is imminent. However, the offence of common assault is sufficient to cover such cases. The *actus reus* of common assault is easily satisfied in such cases if the flashing makes the recipient fear that any physical contact is imminent.[38] The *mens rea* of common assault requires the defendant intends to cause or is reckless as to causing V to apprehend imminent unlawful force.[39] The threshold for recklessness is pretty low, and even if the defendant foresaw a consequence as unlikely to happen they could still be regarded as being reckless as to causing such consequence as long as the defendant foresaw it and chose to unreasonably risk it.[40] Where flashers Airdropped or Bluetoothed stranger images or videos of human genitals on public transport, it will not be hard to prove that they foresaw that this might make the recipient fear imminent sexual contact, given the physical proximity and non-consensual circumstance.

Moreover, if one cyberflashes multiple times, he could be caught by S.2 of the Protection from Harassment Act 1997. The *actus reus* of S.2 requires that the defendant's conduct on at least two occasions in relation to a single person amounts to harassment or that the defendant's conduct on at least one occasion in relation to each of the persons, if there are two or more persons, amounts to harassment.[41] "Harassment" refers to a course of conduct targeted at an individual that is oppressive in nature.[42]

35. *Chambers v DPP* [2012] EWHC 2157(Admin), where messages were sent on Twitter; *R v Watts* [2017] EWCA Crim 1009, where film of threatening behaviour was posted on Snapchat; *R v Walker* [2016] EWCA Crim 2053, where messages were sent on WhatsApp.
36. *Chabloz v DPP* [2019] EWHC 3094 (Admin) [16].
37. Law Com 399, 2021, paras. 6.19-6.20.
38. *R v Constanza* [1997] 2 Cr App R 492.
39. *R v Venna* [1976] QB 421.
40. *G and Another* (n 18). The degree of risk foreseen by the defendant is irrelevant. *R v Brady* [2006] EWCA Crim 2413.
41. Protection from Harassment Act 1997, ss 1(1)(a), 1(1A) (a) and 7(1).
42. *R v Smith* [2012] EWCA Crim 2566 [24]; *R v N* [2016] EWCA Crim 92 [38].

Although S.7(2) states that references to harassment include alarming the person or causing the person distress, alarm or distress is not what defines harassment. S.7(2) is inclusive rather than exhaustive, and what defines the essential nature of harassment is not alarm or distress but oppression and unacceptableness.[43] Harassing someone may cause mental suffering such as alarm and distress, but a course of conduct can be harassment without causing alarm or distress in fact.[44] Other mental suffering such as embarrassment[45]and humiliation[46]can also be the consequence of harassment. When a person Airdrops or Bluetoothes image or video of human genitals to a victim more than once without consent, this will easily satisfy the *actus reus* of S.2 because repeatedly sending another such content without consent is a course of conduct that is oppressive and unacceptable in nature. The *mens rea* of this offence requires that the defendant knows or ought to know that the course of conduct amounts to harassment.[47] The "ought to know" alternative has in effect made the *mens rea* of harassment an entirely objective one. The defendants ought to know their course of conduct amounted to harassment if a reasonable person in possession of the same information would have.[48] Airdropping or Bluetoothing another images or videos of human genitals twice or more without consent will likely be taken by a reasonable person as harassing because it is coercing the recipient to see something he or she does not want to see. Thus, cyberflashing twice or more is sufficiently covered by existing law, even if it is done through peer-to-peer communication network. The "course of conduct" requirement will guard against over-criminalisation.

In addition, where such repeated cyberflashing against the same victim causes the victim to fear that violence will be used, the sender will be caught by S.4 of the Protection from Harassment Act 1997, if the sender knows or ought to know such course of conduct will cause V so to fear each time. It is true that the offences in the Protection from Harassment Act 1997 require a course of conduct, but that is a reasonable constraint against overcriminalisation. One's subjective belief about what might happen to him or her in the future is not current action and care needs to be taken not to extend the criminal law too far. There is no empirical evidence or actual cases reported of cyberflashing leading to sexual assaults or bodily contact of any kind; and without that, one wonders if it is justifiable to categorise cyberflashing, especially the one-off Airdropping or Bluetoothing, as such a serious offence that would need to be subject to the sex offenders register.

Another concern raised by the Law Commission is that without a new offence the prevalence of cyberflashing will subject children to harmful content.[49] However, sending children sexual images or videos is already caught by S.12 and S.15(A) of the Sexual Offences Act 2003. S.12 makes it an offence to intentionally cause a child to watch a third person engaging in a sexual activity or to look at an image of any person engaging in a sexual activity, for the purpose of obtaining sexual gratification. S.15(A) is committed if, for the purpose of obtaining sexual gratification, one intentionally communicates with a child and the communication is sexual or is intended to encourage the child to make a sexual communication.[50] It is argued that S.12 may not cover cyberflashing where a picture of flaccid

43. *R v Curtis* [2010] EWCA Crim 123 [29].
44. *Majrowski v Guy's and St Thomas's NHS Trust* [2007] 1 AC 224, 225.
45. *Lang v CPS* [2017] EWHC 3639 (Admin) [13]. In this case, the defendant sent his ex-wife numerous texts intending to undermine her and her new relationship with another man, and his such conduct caused his ex-wife embarrassment, alarm and distress.
46. *R v Lewis* [2003] EWCA Crim 395. In this case, the defendant did a series of conduct harassing the victim, including sending her obscene and aggressive Valentine's card, putting the victim's name on a poster of a naked woman offering sexual service and arranging for suitors in a lonely heart column to contact the victim. D's such conduct caused V mental suffering including humiliation and distress. Dennis J Baker, *Glanville Williams and Dennis Baker Treatise of Criminal Law* (5th edn, LexisNexis 2021) 547.
47. Protection from Harassment Act 1997, s 1(2); *R v Pelham* [2007] EWCA Crim 1321.
48. *R (Aylesbury Crown Court) v CPS* [2013] EWHC 3228.
49. Law Com 399, 2021, para. 6.24.
50. Sexual Offences Act 2003, s 15(A).

penis is sent to the victim because such image in itself cannot be regarded as an image of a person engaging in sexual activity.[51] Even if this is true, such an act can easily satisfy the *actus reus* of S.15(A). Where the sender, for the purpose of obtaining sexual gratification, sends a picture of a penis, erect or flaccid, to a non-consensual child, such a communication is sexual because any reasonable person will consider this to be sexual.[52] Unless the defendant can produce evidence of some legitimate purpose such as a medical or educational purpose, it will be nigh impossible for that defendant to convince a jury that sending such material to a child was not sexual. S.12 and S.15(A) only require that an intentional conduct is done with the purpose of obtaining sexual gratification, but the second alternative *mens rea* for the proposed cyberflashing offence will require not only a purpose of obtaining sexual gratification but also recklessness as to causing alarm, distress or humiliation. Relying on the proposed cyberflashing offence to deal with the sending of image or video of human genitals to children will in effect limit the protection of children compared to relying on these two existing offences. It is therefore unconvincing to say that the protection of children adds to the necessity of having such a separate narrow offence of cyberflashing.

Considering the above analyses, it seems that the only contribution the new cyberflashing offence would make would be to criminalise the one-off conduct of cyberflashing an adult through non-public communication network, such as Airdropping or Bluetoothing image or video of human genitals, where the sender seeks sexual gratification and is aware of the risk of causing alarm, distress or humiliation, but the recipient does not apprehend imminent unlawful force. But one would be free to use Airdrop or Bluetooth to send other sexually harassing content, as the new offence only criminalises a narrowly defined form of offensive content—that is, image or video of human genitals. As already noted, if there was any case for distinguishing sexual communications for the purpose of making them sexual offences to allow for offenders to be put on the sex offenders register, then why did the Law Commission leave out other sexually harassing communications such as pornographic stories and violent rape cartoons? If other forms of sexually harassing communications are taken as being properly dealt with by the existing law, why is the act of sending of image or video of human genitals so special that it deserves such a narrowly tailored offence? If we are to criminalise a single act of peer-to-peer sexual harassment through the electronic communication of human nudity, why not just amend the communication offences to cover all sexually explicit content that objectively judged might cause alarm or distress? In the following section, I will examine the Law Commission's harms analysis to further demonstrate that having such a narrowly tailed offence of cyberflashing is unnecessary.

A Harm Analysis: Harm to the Defendant From Criminalisation Versus Harm to the Victim

One of the greatest penal theorists of the last century drew a distinction between causing others disgust and causing them harm. Feinberg notes:

> A grating noise or evil smell is just an unpleasant sensation to be put up with grudgingly, irritating to be sure, but not harmful or injurious; but if it keeps one awake all night, then it interferes with one's interest, in the way ill health might, by making it impossible to work efficiently the next day. Similarly, an affront or an insult normally causes a momentary sting; we wince, suffer a pang or two, then get on with our work, unharmed and whole. But if the experience is severe, prolonged, or constantly repeated, the mental suffering it causes may become obsessive and incapacitating, and therefore harmful.[53]

51. McGlynn and Johnson (n 2) 7.
52. According to section 15(A)(2), a communication is sexual if any part of it relates to sexual activity or if a reasonable person would, in all the circumstances but regardless of any person's purpose, consider any part of the communication to be sexual.
53. Joel Feinberg, *Harm to Others* (OUP 1984) 46.

Feinberg's works[54] have been accepted by appellate courts around the world, cited by numerous law reform bodies, and almost all the leading criminal law scholars of this century have treated his analysis of harm and offence as conceptually sound. If the Law Commission wants to go beyond the remit of making existing offences fairer and more efficient to engage in proposing the criminalisation of new areas of conduct that are not currently criminalised properly, then it ought to at least engage with the philosophical and criminological literature—not merely present anecdotal views of stakeholders, who are not representative of the border electorate, without empirically verifying such views.

The Law Commission report works from a presumption that cyberflashing is harmful but fails to supply sufficient empirical or scientific evidence to demonstrate that cyberflashing can cause an adult of normal sensibility actual harm, even though it might cause ephemeral distress.[55] There is no doubt that cyberflashing is wrongful and I take no issue with that. But we also need to know why it is harmful and how harmful it is if we are to justify a jail sentence as long as two years. Wrongful harms are usually punished more severely than wrongs that merely cause disgust,[56] so it is important to ensure any harm claim is normatively and empirically sound. Reference is made to a YouGov poll at para 6.24 of the Law Commission report, but that is about incidents of cyberflashing rather than the extent of harm cyberflashing causes. This YouGov survey involved 2021 women and 1738 men aged between 18 and 36.[57] The sample size is relatively small if its result is to be used to justify a new offence which will affect all citizens (population size of England and Wales is 62,704, 800). We are not told what selection criteria they used to select the sample either. Its representativeness of the British citizens' experiences with cyberflashing is questionable, given that the sample was very small and did not include anyone over the age of 36. According to this survey, women who have ever received a penis picture are most likely to describe them as gross (58%) or stupid (54%).[58] Such data, even if reliable, shows that cyberflashing causes disgust rather than any actual harm as the Law Commission claims it does. It seems that the Law Commission takes any ephemeral mental distress as harm;[59] however, according to Feinberg's abovementioned harm analysis such ephemeral mental distress clearly is not sufficient to pass the standard for harmful wrongs. It is also claimed in the Law Commission report that 76% of victims of cyberflashing are under the age of 18,[60] but this data comes from a research sample of a mere 144 young people aged between 11 and 18.[61] It is not methodologically convincing, and it does not focus on harm, but just on incidents of such imagery being sent. Even if such data can reliably show how prevalent cyberflashing is in the UK, it cannot support the Law Commission's claim that cyberflashing causes harm if we are to adopt Feinberg's harm analysis.

54. Joel Feinberg, *Harm to Others* (OUP 1984), *Harmless Wrongdoing* (OUP 1988) and *Offense to Others* (OUP 1985).
55. The only study cited is from Alexandra S Marcotte, Amanda N Gesselman, Helen E Fisher and Justin R Garcia, "Women's and Men's Reactions to Receiving Unsolicited Genital Images from Men" (2021) 58 (4) *The Journal of Sex Research* 512. The research outcome of this paper is based on 2,045 Americans using a singles dating site, and its authors stated clearly the study is based on anecdotal evidence.
56. For detailed discussion about wrong and harm, see A P Simester and Andrew von Hirsch, *Crimes, Harms, and Wrongs: On the Principles of Criminalisation* (Hart Publishing 2011); Andrew von Hirsch and Andrew Ashworth, *Proportionate Sentencing – Exploring the Principles* (OUP 2005).
57. YouGov 'Four in ten female millennials have been sent and unsolicited penis photo' (2018) <https://yougov.co.uk/topics/politics/articles-reports/2018/02/16/four-ten-female-millennials-been-sent-dick-pic> accessed 18 July 2022.
58. Ibid.
59. A layperson may call any wrong a harm, just like they would call any physical threat or attack an assault. Legislative processes should be careful not to use the concept "harm" in a way that refers to any infringement or violation of rights. It is true that victims who are cyberflashed feel they are violated, but this is different from saying they have suffered longer-term actual mental harm that requires longer-term treatment.
60. Law Com 399*,* 2021, para. 6.24.
61. Jessica Ringrose, Kaitlyn Regehr and Sophie Whitehead, "Teen Girls' Experiences Negotiating the Ubiquitous Dick Pic: Sexual Double Standards and the Normalization of Imaged Based Sexual Harassment" (2021)85 Sex Roles 558-576 <https://doi.org/10.1007/s11199-021-01236-3> accessed 25 July 2022.

The Law Commission's conclusions concerning the harmfulness of cyberflashing are asserted rather than argued for and are not evidence based. The Law Commission presents a range of subjective and anecdotal views that have been expressed by the employees consulted from the campaign organisations and thinktanks that the Law Commission consulted, but has not pointed to any large-scale empirical studies. The problem with subjective and anecdotal views is that while they may be well intended, they can be skewed by the aims of the particular campaign group or thinktank being consulted. The small-scale empirical studies[62]cited by the Law Commission are not sufficiently robust to justify the harm element for making cyberflashing an offence carrying with it a maximum sentence of two-year imprisonment and sex offender registration. It would have been helpful for the Law Commission to make it clear that offence to others (rather than harm to others) is the rationale it relies on for criminalisation.

Nearly everyone in Britain would agree that cyberflashing is wrong, but that is different from everyone agreeing it is so harmful that the criminal law, police and prisons are required to prevent it. What the Law Commission needs is two or three large-scale gender neutral and randomised empirical studies to ascertain what percentage of victims are left so traumatised from this sort of sexual harassment that they are suffering mentally a day later, a week later or a month later. This is important mainly because the Law Commission wants this conduct separated from other communication wrongs so that offenders will be put on the sex offender register. The damage to the offender will be a loss of employment opportunities and the hardship of time in jail, and thus it would be helpful to know whether this conduct is sufficiently harmful to warrant special treatment. A stint in prison is likely to cause PTSD,[63] but seeing a nude human in an electronic film or photograph is not likely to cause any recognised mental illness, even if it might cause ephemeral shock and offence. If it causes a person to fear imminent violence, then that is common assault and already a crime. It ought to be demonstrated that cyberflashing causes actual bodily (mental) harm. If the majority of respondents were to report that while they felt harassed upon receiving such an image, they suffered no more than ephemeral annoyance, then the fact that an overly sensitive minority suffered longer term mental distress might suggest the harm is too soft for full criminalisation. That in a few extreme cases more serious harm is caused such as where V's PTSD is trigged cannot be used as a rationale for making all cyberflashing harmful wrongdoings, if a person of ordinary sensibility would not have suffered such harm. Feinberg rightly points out: "It seems clear, however, that the more fragile our sensitive sufferer's psyche, the less protection he can expect from the criminal law."[64] If it is true that cyberflashing is objectively harmful in that it can cause more than ephemeral mental distress such as days and weeks of mental anguish, then the Law Commission needs to prove that before pushing for a new criminal offence.

Back in the 1960s, Kadish penned his famous essay titled: "The Crisis of Overcriminalization."[65] Much of what Kadish wrote then about moral panics still applies. The situation is much worse now as the panic is usually about a wrong, but the wrong is blown out of all proportion resulting in a criminal trial, jail time and criminal labelling being resorted to as a first resort remedy, instead of a last resort remedy. Emotive language such as the term "survivor" has the effect of augmenting the harm involved beyond the reality of that actual harm suffered. A person who has avoided being murdered is rightly termed a survivor. To the contrary, cyberflashing itself does not threaten one's physical safety,

62. Clare McGlynn, who was consulted, in her research cited other research data, but such data sample is still relatively small compared to the population size. For example, Oswald's research involved 1087 heterosexual males aiming to find the motivations behind cyberflashing, and Ringrose's research involved 144 young people. McGlynn also made it clear that there is a shortage of data identifying the extent of cyberflashing and it is important not to generalise across all populations. Clare McGlynn and Kelly Johnson, *Cyberflashing: Recognising Harms, Reforming Laws* (Bristol University Press 2021) 12.
63. Alison Liebling and Maruna, Shadd (eds) *The Effects of Imprisonment* (Oxford: Routledge, 2013); Mika'il DeVeaux, 'The Trauma of the Incarceration Experience' (2013) 48 Harvard CR-CL L Rev 257.
64. Feinberg, *Offense to Others* (n 54) 34.
65. See generally, Sanford H Kadish, "The Crisis of Overcriminalization" (1968) 7 Am Crim L Q 17.

let alone one's life, and thus there is no chance of a person not surviving it. Cyberflashing is a wrong that is worthy of deterrence, but to overstate its harmfulness mislabels it. The serious harm label needs to be applied appropriately to the sorts of wrongs that cause serious harm such as rape. Rape is appropriately labelled a "survivor" crime because it has the potential to mentally cripple its victims for decades, if not for life. Whether cyberflashing has the potential to cause lasting actual mental harm as opposed to transient discomfort and disgust needs solid evidence based on large-scale empirical research such as national surveys. The Law Commission could have carried out a harms analysis by balancing the harm of criminalisation against any potential harm to the victim.[66]

Criminalisation involves the defendant being searched, arrested, put on trial with the stress of fearing prison, suffering the stigmatisation of arrest and the loss of a career even from mere accusation, let alone conviction. "Even one day in prison would be a cruel and unusual punishment for the 'crime' of having a common cold."[67] The Law Commission report is victim-centric, which is welcomed. But what is needed is a gender-neutral account that balances the harm of a criminal conviction against the potential harm of the defendant's conduct. A person is unlikely to recover for years from even one month in prison, but a person of normal sensibility would probably recover from seeing a nude image within a day, if not in minutes. Given the very limited contribution of this proposed cyberflashing offence is to catch the one-off Airdropping or Bluetoothing situations which cannot be covered by existing offences, it would be helpful if the Law Commission made efforts to show why amending the communication offences is not a good way or why fixed penalty notice might not be a good way to deal with such one-off cyberflashing.

The proposed new communication offence is set to replace the existing offences in S.127(1) of the Communications Act 2003 and the Malicious Communications Act 1988, but this new offence does not extend to harmful communications that are sent recklessly.[68] The Law Commission believes regulatory measures such as duty of care imposed on organisations hosting user-generated content would be a better tool than criminal law to prevent such communication.[69] Recklessly sending the victim sexually harassing images or videos other than those containing human genitals are therefore not within the remit of the new communication offence. Why the image or video of human genitals is so special that it deserves a narrowly tailored offence compared to other similarly sexually harassing content? If regulatory measures work perfectly well for other sexually harassing content, why cannot it work for images or videos of human genitals?

The image of a dead person on a battlefield is likely to cause most people far greater distress than seeing a human's genitalia. The image of seeing the ice sheets disappearing under the feet of polar bears also is likely to cause most people far greater distress than seeing a human's genitalia. What is it about cyberflashing that makes it worse than the evening news flashing images of dead people in war zones? It is submitted that cyberflashing is best conceptualised as a form of harassment: it is sexual harassment because the flasher is trying to make another look at a sexual image. It is not clear whether flashers internalise cyberflashing as a form of flirting,[70] or as a form of sexually motivated exhibitionism.[71] But is this sort of one-off sexual harassment worse than workplace harassment and bullying which is not criminalised? An employee under the constant fear of unfair dismissal is likely to suffer far greater distress than a person enduing a one-off incident of cyberflashing. For instance, a single parent of three children, who is threatened with unfair dismissal from a job for no other reason than her line manage

66. Andrew von Hirsch, "Extending the Harm Principle: 'Remote' Harms and Fair Imputation" in Andrew Simester & Tony A. H. Smith (eds) *Harm and Culpability* (OUP 1996) 259.
67. *Robinson v California* [1962] 360 US 660, 667.
68. Law Com 399, 2021, chap.2.
69. Ibid, para. 2.157.
70. Cf Kari A Walton & Cory L. Pedersen "Motivations behind Catcalling: Exploring Men's Engagement in Street Harassment Behaviour" (2021) *Psychology & Sexuality*, DOI: 10.1080/19419899.2021.1909648 (accessed 10 July 2021).
71. Ibrahim Arpaci et al, "The Moderating Role of Exhibitionism in the Relationship between Psychological Needs and Selfie-posting Behavior" (2021) *Current Psychology* <https://link.springer.com/article/10.1007/s12144-021-01732-5> accessed 20 July 2022; Harper et al (n 1).

is a power-hungry bully, [72] suffers greater distress than a person who is sent a nude photo without consent. The parent might fear not being able to pay the rent, feed her children and so on; yet this sort of workplace bullying is not a crime. Feinberg writes:

> There is a more general reason, however, why legal coercion should not be used to prevent minor harms, even though in theory it would be morally legitimate to do so: namely that chances are always good that such a use of power would cause harm to wrongdoers out of all proportion both to their guilt and to the harm they would otherwise cause, even when the priority of innocent interests is taken into account. Moreover, such an interference with liberty would frequently do more indirect harm to the innocent parties themselves than the conduct it constrains might have done.[73]

There is no doubt that it is wrong to cyberflash people, but we need to consider whether using the criminal law to prevent it is to use a sledgehammer to crack a walnut. On its own, a single act of cyberflashing seems insufficiently serious to warrant a criminal law response. As mentioned previously, only a handful of one-off flashing sent through Airdrop or Bluetooth is left untouched. In addition to the option of simply amending the harassment offences or the communication offences which can apply to all sexually harassing content, we still have regulatory measures as well as practical technological solutions (e.g., changing the phone settings to "receiving off" or "contacts only"). This is not to say that victims whose phone settings is set to "everyone" should not be protected from cyberflashing, nor is it to say that more serious forms of cyberflashing should be left untouched such as where the victim apprehends imminent unlawful force coming from the flasher or where the victim is repeatedly flashed. One wonders if it is really necessary to have such a narrowly tailored cyberflashing offence, the actual contribution of which is so limited and the custodial sentence and sex offender registration of which is not properly justified by principles of criminalisation[74] and sound empirical evidence. Criminal law should not be used as a first resort; rather, it should only be used if non-criminal means are not enough to prevent the conduct in question.[75] By keeping prison, the court and police investigation system unclogged with trivial wrongs, the police and prisons will be left better resourced to tackle harmful wrongs, such as rape which has appallingly low conviction rates and other technology enhanced crimes which cost markets billions.[76]

Conclusion

The Law Commission is right to state that cyberflashing is an increasingly common phenomenon and thus needs tackling. There is no doubt that legal measures are in need to deal with cyberflashing, but whether and how criminal law should be involved is something that needs to be looked at very carefully. The vast majority of

72. *D v Defence Unlimited International Ltd (London) and others*: 2206723/2018, where the victim was unfairly dismissed for objecting to sexual harassment and demands for intercourse. She was only given compensation, when having her job back would have been much better for her in the long term.
73. Feinberg (n 38)189-190.
74. Causing PTSD and making a person unemployable by listing them as a sex offenders seems disproportionate criminalisation and punishment. On dangerousness and the need to put certain individuals on sex offender registers, see John C. Navarro *et al*., "Revisiting sex offender registration and notification: Does awareness differ across community type?" (2022) 47(1) *Criminal Justice Review* 34; Ji Seun Sohn and Soo Jung Lee, "Revisiting the Relationships between Psychopathy Checklist-Revised (PCL-R) Facets and Sexual Recidivists versus Nonsexual Recidivists" (2022) *Journal of Forensic Psychology Research and Practice* 1; Patrick Lussier *et al*, "Psychopathy and the prospective prediction of adult offending through age 29: Revisiting unfulfilled promises of developmental criminology" (2022) 80 *Journal of Criminal Justice* 101770; Dennis J. Baker, "Punishment without a Crime: Is Preventive Detention Reconcilable with Justice" (2009) 34 *Austl J Leg Phil* 120; On proportionate punishment, see Andrew von Hirsch, *Censure and Sanctions* (Clarendon Press 1996).
75. Douglas Husak, "The Criminal Law as Last Resort" (2004) 24(2) OJLS 207, 217.
76. The Rt Hon Lord Hodge, "Financial Technology: Opportunities and Challenges to Law and Regulation" in Dennis J Baker and Paul H Robinson (eds), *Artificial Intelligence and the Law: Cybercrime and Criminal Liability* (Routledge 2021); Joseph Zabel, "Rethinking Open- and Cross-Market Manipulation Enforcement" (2021) 15 Va. L. & Bus. Rev. 417, 431; Blake Hamil, "Eu Crypto Currency Regulation: Creating A Haven for Businesses or for Criminals? (2020) 48 Ga. J. Int'l & Comp. L" 833, 834.

cyberflashing cases can be dealt with by current criminal law, including common law offences of outraging public decency and common assault, sexual offences under the Sexual Offences Act 2003 (Ss. 66, 12 and 15(A)), harassment offences under the Protection from Harassment Act 1997 (Ss.2 and 4) and communication offences under the Malicious Communications Act 1988 (S.1) and Communications Act 2003 (S.127). It is claimed the loophole in the current law is that cyberflashing through non-public communications network, such as Airdrop and Bluetooth, is not properly covered. However, most such Airdropping or Bluetoothing cases can be covered by existing offences. Where D Airdrops or Bluetoothes images or videos of human genitals twice or more, D is liable for harassment. Where D Airdrops or Bluetoothes such image or video intending to cause distress or anxiety, he will be liable for S.1 of the Malicious Communications Act 1988, even if it is only a one-off act. If such conduct, once or more, causes the victim to apprehend imminent unlawful force, D could be liable for common assault if D is intentional or reckless as to causing such apprehension. As a result, it will only be a very handful of one-off Airdropping or Bluetoothing cases where the sender did not intend to cause distress or anxiety and the victim did not apprehend imminent unlawful force that are left untouched.

It is submitted that having a very narrowly tailored cyberflashing offence is unsatisfactory. Proposing new offence should be done with great caution by conducting a nuanced ethical and social evaluation of the harm that is likely to be caused by cyberflashing and by carefully examining the adequacy of the existing law. The Law Commission's basing its harm-analysis on anecdotal evidence is problematic, so is its succinct evaluation of the effectiveness of existing law. Other sexually harassing content seems not to bother the Law Commission so much that it would propose a separate offence for such content. The Law Commission has failed to demonstrate why conceptually images or videos of human genitals are so special as to deserve a separate offence.

Horder has observed: "When evaluating law reform proposals, it is wrong to suggest that judges and scholars are unaffected by (to use Raz's phrase) 'passing fashions', and it is insulting to politicians, civil servants, and the public to suggest that they cannot rise above such fashions, blind zeal, the rough-and-tumble of politics, and so on."[77] It would be beneficial if the Law Commission could provide a balanced examination of the harmfulness of criminalisation against the harmfulness of cyberflashing, which is supported by gender-neutral large-scale empirical studies. The proposal has failed to weigh the harm of cyberflashing against the harm for defendant when the defendant is tried and jailed or fined and put on the sex offenders register. The mental distress of being tried, jailed and put on the sex offenders register far outweighs the ephemeral distress caused by a one-off cyberflashing. It is hoped that the Parliament rejects this very narrowly tailored offence and amends the communications offences or harassment offences, so that they can be applied to all forms of sexually harassing communications to protect the sexual autonomy and dignity of people from cyber-sexual harassment. Such an offence should require a course of conduct to prevent overcriminalisation of intimate human relations.

Declaration of Conflicting Interests

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

Funding

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

ORCID iD

Bo Wang https://orcid.org/0000-0001-8947-8526

77. Jeremy Horder, *Homicide and the Politics of Law Reform* (OUP 2012) 30.