NORTH CAROLINA JOURNAL OF LAW & TECHNOLOGY
VOLUME 24, ISSUE 3: APRIL 2023

CYBERFLASHING: PUBLIC INDECENCY IN THE DIGITAL AGE

Sophia M. Vouvalis*

Cyberflashing is an emerging cybercrime not yet widely recognized. As new technology provides perpetrators the guise of anonymity, regulators should consider using a broad definition of cyberflashing to encapsulate the increasing number of ways to flash victims with lewd images. This Article discusses the various approaches taken in the United States and internationally to address this newly emerging cybercrime. This Article exposes the shortcomings of these approaches, and provides recommendations for drafting laws in the future to support the best interests of victims and address the social media platforms on which these crimes often occur. This Article recommends key factors for consideration in drafting future cyberflashing legislation, including: (1) classifying cyberflashing as a criminal offense, (2) removing specific motivation requirements for culpability, (3) encompassing both a larger variety of content depicted within media and kinds of media sent in such acts, and (4) omitting age requirements for both perpetrators and victims.

TABLE OF CONTENTS

* J.D. Candidate, University of North Carolina School of Law, 2024. The Author would like to thank Professor Deborah Gerhardt for her guidance and support, and all of the NC JOLT editors and staff, particularly Arianna Pearson, Ellenor Brown, and Jared Mark, for their assistance throughout the editorial process. The Author would also like to thank her family and friends for their unwavering support throughout the publication process.

I. INTRODUCTION

A woman sits on the L train, heading home after a long day of work, when suddenly, her phone vibrates. She looks down, hoping it is not another email from work and is genuinely relieved to see only an AirDrop request. *An AirDrop request?* The notification piques her interest, as she thinks someone must have sent it by accident. She swipes her phone open to view the request, and before she can decline it, she is met with the thumbnail preview of an erect penis. She quickly glances to her left and right, hoping the people sitting next to her did not see the image. She then looks around the rest of the train car, searching for any indication of who could have sent it to her. For the rest of the ride home, she remains paranoid, as she tries to forget the image engrained in her head.

This hypothetical is the harsh reality of the crime, "cyberflashing." Cyberflashing can generally be defined as "the act of using digital means (such as a messaging app or social media platform) to send sexual or pornographic images (such as a nude photo of oneself) to someone without their consent."[1] This is the newest form of "image-based sexual abuse," which is an umbrella term referring "to the non-consensual taking, making[,] and/or sharing of intimate images."[2]

This Article will proceed in four Parts. Part II distinguishes cyberflashing from other common cybercrimes, methods, victims, motivations, and statistics to emphasize the pervasiveness and harmful effects of this crime, as well as bring awareness to cyberflashing and its victims. Part III describes existing and proposed cyberflashing laws in the United States ("U.S.") and abroad, discussing the pros and cons of each. Part IV highlights the critical roles technology and social media have played in instigating cyberflashing, and how the companies running these platforms can harness their powers to mitigate this cybercrime. Finally, Part V identifies key issues that lawmakers should consider when creating laws to criminalize cyberflashing, based on weaknesses in current law and the roles technology and social media companies currently play.

---

[1] *Cyberflashing*, DICTIONARY.COM, https://www.dictionary.com/e/tech-science/cyberflashing/ [https://perma.cc/Z4QF-AX7G] (last visited Aug. 31, 2022). A less formal term often used to describe cyberflashing is "unsolicited dick pics." Morten Birk Hansen Mandau, *'Directly in Your Face': A Qualitative Study on the Sending and Receiving of Unsolicited 'Dick Pics' Among Young Adults*, 24 SEXUALITY & CULTURE 72 (2020). However, using this informal term as a synonym for cyberflashing can minimalize the seriousness of the crime and the victim's trauma. Rachel Thompson, *It's Time to Stop Saying 'Unsolicited Dick Pics.' Here's Why.*, MASHABLE (July 19, 2019), https://mashable.com/article/cyberflashing-unsolicited-dick-pics-terminology [https://perma.cc/SB87-SF2H]. Therefore, this Article will predominantly use the term "cyberflashing," and will only use alternative language to identify this cybercrime as it is used in mentioned literature.

[2] Clare McGlynn et al., *'It's Torture for the Soul': The Harms of Image-Based Sexual Abuse*, 30 SOC. & LEG. STUD. 541 (2020).

II. THE FIVE WS OF CYBERFLASHING

A. What: Distinguishing Cyberflashing from Revenge Porn and other Cybercrimes Involving Imaged-Based Sexual Abuse

Given the multitude of sexually-based crimes transpiring on the internet, it is important to clarify their differences to avoid conflation and account for their distinct treatment by the law. "Revenge porn," formally referred to as nonconsensual pornography, is the distribution of sexually graphic images or videos of individuals without their consent.[3] Although cyberflashing could arguably be described as a type of revenge porn, because a perpetrator could send explicit images of someone else (rather than themselves) to commit the act, their offenders' objectives differentiate the two crimes.[4] Unlike revenge porn, cyberflashing does not involve exposing sexual material to the general public.[5] Although cyberflashing may involve the use of some public forum (i.e., a dating app), cyberflashers tend to target specific individuals.[6] Further, revenge porn offenders may be motivated by a variety of factors (vengeance, money, notoriety, entertainment) or by no particular reason at all.[7] By contrast, cyberflashers may desire to invite flirting, solicit sexual favors, or simply harass people.

Another cybercrime that could be confused with cyberflashing is sextortion. Sextortion occurs when a perpetrator obtains or claims to have obtained an individual's private and sensitive material and threatens to harm loved ones or distribute the material unless the individual "provide[s] them images of a sexual nature, sexual favors, or money."[8] While both offenses involve sexual images, unlike sextortion, cyberflashing does not involve threatening or

---

[3] Danielle Keats Citron & Mary Anne Franks, *Criminalizing Revenge Porn*, 49 WAKE FOREST L. REV. 345, 346 (2014).

[4] *See, e.g.*, DEAN FIDO & CRAIG A. HARPER, NON-CONSENSUAL IMAGE-BASED SEXUAL OFFENDING, 37–45 (Jens Binder ed., 2020).

[5] *Id.*

[6] *Id*.

[7] Mary Anne Franks, *"Revenge Porn" Reform: A View From The Front Lines*, 69 FLA. L. REV. 1251, 1257–58 (2017).

[8] *What is Sextortion?*, FED. BUREAU INVESTIGATION, https://www.fbi.gov/video-repository/newss-what-is-sextortion/view [https://perma.cc/3QHW-K67H] (last visited Mar. 27, 2023).

distributing a victim's sexual images. Moreover, the offenders of these crimes also have different agendas: the objective of sextortion is typically to obtain sexual material or money.[9]

B. When/Where: Various Methods of Cyberflashing

Because of the omnipresent nature of technology and social media in people's everyday lives, cyberflashing can occur anywhere, anytime, and anyplace. Women have reported being cyberflashed in a variety of public places, including restaurants, airports, bus and train stations, libraries, as well as on buses, planes, and trains.[10] When cyberflashing occurs in these locations, it is usually via AirDrop, a feature of Apple electronic devices. A Wi-Fi and Bluetooth-based technology, AirDrop allows perpetrators to anonymously send lewd photos to other Apple Wi-Fi and Bluetooth-enabled devices within thirty feet of one another; both the sender and receiver of AirDrop content can only be identified by a self-chosen name or pseudonym.[11] Although AirDrop provides individuals the option to accept or deny the photos they are sent, even if they click "decline," a thumbnail[12] of the photo is displayed on an individual's screen. Unfortunately, the sender can repeatedly resend the previously declined content, which must be continuously

---

[9] *Id*.

[10] Sophie Gallagher, *Cyber Flashing: 70 Women on What It's Like to Be Sent Unsolicited Dick Pics*, HUFFPOST (July 12, 2019), https://www.huffingtonpost.co.uk/entry/cyberflashing-70-women-on-what-its-like-to-be-sent-unsolicited-dick-pics_uk_5cd59005e4b0705e47db0195?guce_referrer=aHR0cHM6Ly93d3cuZ29vZ2xlLmNvbS8&guce_referrer_sig=AQAAAFZD_TUs--qICwvyN2E5vHocyBZoHbfQInB83QHMxNUXDJbwAGlaM1vICgQ-Tn41jxpgvLY9h100RV3leO4Hhn01I_7C6SxyLSgYMGCGRD-1pKs8JJloNh8q63HNN44UM7uAojLb3UXEVvEiP6jPLumVXJNzjkuupTgSyzB2dSYs&guccounter=2 [https://perma.cc/5HKT-EVHD].

[11] AirDrop settings must be placed on "Everyone" to receive media from individuals not on a person's contact list.

[12] A thumbnail is "a small copy of a larger picture on a computer [or other device], shown in this way to allow more to be seen on the screen." *Thumbnail*, CAMBRIDGE DICTIONARY, https://dictionary.cambridge.org/us/dictionary/english/thumbnail [https://perma.cc/SJ7A-LMEA] (last visited Mar. 27, 2023).

declined. Consequently, there are no means for people to avoid viewing the explicit photos sent by cyberflashers.[13]

AirDrop is not the only way that cyberflashing occurs. Perpetrators also use dating websites and applications, among other social media platforms, to cyberflash innocent victims.[14] When using these platforms to conduct their crimes, offenders rely on the private messaging features of these platforms.[15] In other words, perpetrators send non-consensual lewd photos through the direct message feature present on many social media platforms, including Facebook, Twitter, Instagram, and Snapchat.[16] Because these social media platforms have default settings that allow users to receive messages or message requests from accounts they do not follow, offenders can send lewd content to virtually every user on these platforms.[17] Although some platforms, like Instagram, provide users the option to accept or deny message requests, a thumbnail of the message is displayed on an individual's screen, regardless of whether it was accepted or declined.[18]

---

[13] This is only the case for individuals with their Airdrop settings placed on "Everyone." Individuals who place AirDrop settings on "Contacts Only," or turn AirDrop off entirely, cannot be cyberflashed via AirDrop. *See* discussion *infra* Part IV.

[14] *See generally* Gallagher, *supra* note 10 (recounting the experiences of 70 women cyberflashed on a variety of platforms, including Facebook, Instagram, Snapchat, and Twitter).

[15] Shannon Flynn, *What is Cyberflashing? Is it Illegal?*, MAKE USE OF (Jan. 28, 2022), https://www.makeuseof.com/what-is-cyberflashing/?newsletter_popup=1 [https://perma.cc/PS5X-BU5G].

[16] *See* Gallagher, *supra* note 10.

[17] *Id*.

[18] "On social media, it's often possible to opt out of receiving direct messages from strangers or users you don't follow. You may also be able to disable direct messaging entirely. Many platforms also allow you to limit comments or interactions from accounts you don't follow. You can also make your account private to be fully protected. Depending on the platform, strangers won't be able to view your account or message you, preventing them from sending you images, comments, or files." *Id*.

Finally, cyberflashers also commit their crimes through video conferencing applications like Zoom and Skype.[19] Specifically, uninvited perpetrators barge into online meetings on these applications, and either expose themselves or display unsolicited pornographic images to everyone in the meeting. Because anyone who has a link to a public meeting can join, offenders are easily able to gain access to these meetings. Similarly, because some video conferencing applications have default settings that allow any meeting participant "to share their screen without permission from an event's host," perpetrators have little difficulty sharing lewd content.[20]

C. Who: Victims and Survivors of Cyberflashing

Most victims of cyberflashing are women.[21] Indeed, "women—and especially young women—encounter sexualized forms of abuse at much higher rates than men."[22] According to a U.S. study of online harassment conducted in 2017,

> 31% of Americans say that someone has sent them explicit images that they did not ask for, . . . [b]ut young women in particular encounter this behavior at exceptionally high rates. About half (53%) of women ages 18 to 29 have had someone send them explicit content without their consent.[23]

The percentage of women who have reported being sexually harassed online has doubled since this study was published.[24] In a study conducted in 2018 by and on the users of the dating app Bumble, the company found that 33% of "women reported having received unsolicited lewd photos from someone they hadn't yet met

---

[19] Taylor Lorenz, *'Zoombombing': When Video Conferences Go Wrong*, N.Y. TIMES (Apr. 7, 2020), https://www.nytimes.com/2020/03/20/style/zoombombing-zoom-trolling.html [https://perma.cc/6JAR-EW77].

[20] *Id*.

[21] Maeve Duggan, *Online Harassment 2017*, PEW RSCH. CTR. 1, 7 (July 11, 2017).

[22] *Id*.

[23] *Id.* at 6.

[24] Emily A. Vogels, *The State of Online Harassment*, PEW RSCH. CTR. 1, 17 (Jan. 13, 2021).

in person," and that "[a]n overwhelming number of these women—96%—were unhappy to have been sent these images."[25]

Similar survey results have occurred overseas. A survey conducted on British millennials revealed that out of 46% of female millennials who received nude pictures, nearly 90% of them received the pictures without soliciting receipt of the images.[26] According to the same study, 53% of the women who received lewd pictures were between eighteen and twenty-four years old.[27]

Although the overwhelming majority of cyberflashing victims have been women, cyberflashing does not discriminate based on gender or sexual identity. 90% of participants in a 2021 study "reported having received an *unsolicited* dick pic," which included "90.7% of women—90.7% of heterosexual, 91.3% of lesbian, and 90.8% of bisexual women—and 87.1% of men—88.1% of gay men and 82.1% of bisexual men."[28]

While cyberflashing has seemingly become commonplace, this does not mean that its impacts on victims should go unrecognized. Victims of cyberflashing often report "feeling scared, violated, embarrassed, uncomfortable[,] and lacking control."[29] For instance, one victim who was cyberflashed via AirDrop reported being "so shocked to be sent those kind of images whil[e] [she] was in such a public and safe setting."[30] In an attempt to combat this perceived erosion of safety, some women have opted to take evasive measures, such as locking down their phones and social media applications.

---

[25] *Why Bumble Backed a New Law to Curb Online Sexual Harassment*, BUMBLE, https://bumble.com/en-us/the-buzz/lewd-photo-texas-law [https://perma.cc/84QY-HQCC] (last visited Mar. 27, 2023).

[26] Matthew Smith, *Four in Ten Female Millennials Have Been Sent an Unsolicited Penis Photo*, YOUGOV (Feb. 15, 2018), https://yougov.co.uk/topics/politics/articles-reports/2018/02/16/four-ten-female-millennials-been-sent-dick-pic [https://perma.cc/AE7B-QTJA].

[27] *Id.*

[28] Alexandra S. Marcotte et al., *Women's and Men's Reaction to Receiving Unsolicited Genital Images from Men*, 58 J. SEX RSCH. 512, 516 (2021).

[29] Vasia Karasavva et al., *Putting the Y in Cyberflashing: Exploring the Prevalence and Predictors of the Reasons for Sending Unsolicited Nude or Sexual Images*, 140 COMPUTERS IN HUM. BEHAV. 1, 2 (2022).

[30] Gallagher, *supra* note 10.

On the other hand, a significant number of women have chalked up cyberflashing as part "of the experience of being a woman online," and therefore, "something that they could do little about and . . . something that they just had to deal with online."[31] In other instances, some women do not even know that receiving unsolicited lewd photos is a crime. Even those who are aware of its illegality often choose not to report it because they are convinced that nothing will be done.[32] Regardless of how women choose to handle cyberflashing, they should not have to accept the reality of and endure the feelings that come with this cybercrime.

D. Why: The Disconnect Between Cyberflashers and Their Victims

Inherent in the prevalence of cyberflashing is the discrepancy between the expectations of its perpetrators and the reactions of its victims. This disparity can likely be attributed to the multiple theorized motivations male cyberflashers have for sending lewd photos of themselves. Three theories attempt to characterize the reasons people cyberflash: positive, strategic, and deviant motivations.[33] Positive motivations describe cyberflashing as a method of flirtation.[34] Strategic reasons describe cyberflashing as a way to receive reciprocation; that is, by sending photos of themselves, men hope to receive nude images in return.[35] Deviant motivations describe cyberflashing as a way for men to exert power over women, acting with aggression, coercion, and force, which is sometimes attributed to narcissism.[36]

---

[31] Rikke Amundsen, *'A Male Dominance Kind of Vibe': Approaching Unsolicited Dick Pics as Sexism*, 23 NEW MEDIA & SOC'Y 1465, 1471–72 (2021).

[32] *See* Sophie Gallagher, *Would Making Cyber Flashing Illegal Stop People Sending Dick Pics?*, HUFFPOST (July 12, 2019, 8:45 AM), https://www.huffingtonpost.co.uk/entry/would-making-cyberflashing-illegal-stop-people-sending-dick-pics_uk_5c50674fe4b0d9f9be6951ce [https://perma.cc/Z2TJ-YL46].

[33] Flora Oswald et al., *I'll Show You Mine so You'll Show Me Yours: Motivations and Personality Variables in Photographic Exhibitionism*, 57 J. SEX RSCH. 597, 599 (2019).

[34] *Id.*

[35] *Id.*

[36] *Id.*

A different motivation for cyberflashing may be characterized as pranking or tomfoolery. Under this motivation, cyberflashing is just another form of high jinks. For example, many teens use AirDrop for mass image sharing amongst friends, classmates, and even strangers. While they typically bombard phones by sending memes, selfies, photos, and more, "[i]t's not unheard of for kids to blast out nudes (of themselves or others) and porn."[37] One man who fell victim to such cyberflashing recounted his experience:

> [W]hile checking my Twitter feed on the train commute home, my phone was bombarded for a solid five minutes with random dick pics. [Realizing] it wasn't someone's embarrassing mistake and thinking it might have been a friend who had seen me on the same train, I was in fact, the subject of a 'Cyber-flash.' I went into stealth mode and subtly scanned the carriage for a familiar face who might have thought it was a funny way to get my attention with pictures of penises (Because hahaha). What surprised me is that sure enough, a couple of seats down, it was actually a group of schoolgirls in uniform, who were giggling as they sent the adult images to different phones in the carriage that had the AirDrop feature switched on.[38]

The overall reaction to cyberflashing also differs amongst genders. Results from a 2021 study examining the impact that receiving unsolicited nude photos has on recipients showed that women generally exhibited negative reactions to receiving such images, while men generally exhibited more positive reactions.[39] More specifically, the most commonly endorsed reactions by women were "grossed out" (50%) and "disrespected" (46%); the most commonly endorsed reactions by men were "entertained" (44%) and "curious" (41%).[40] Given that men predominantly

---

[37] Taylor Lorenz, *When Grown-Ups Get Caught in Teens' AirDrop Crossfire*, ATLANTIC (June 5, 2019), https://www.theatlantic.com/technology/archive/2019/06/why-teens-try-airdrop-you-memes-concerts/591064/?utm_source=facebook&utm_medium=social&utm_campaign=share&fbclid=IwAR3HpYpaJQQ4tr9oZ67s7nY7JV1EhhEUgovfHHh8wGW5v9gWRL2fNBtV4c0 [https://perma.cc/4PBV-W3XL].

[38] Tom Livingstone, *School Kids Putting Themselves at Risk 'Pranking' Strangers with AirDrop Porn,* NEWS.COM.AU (May 14, 2018, 2:01 PM), https://www.news.com.au/technology/school-kids-putting-themselves-at-risk-pranking-strangers-with-airdrop-porn/news-story/8f65a97dbb9bc70709a18a6b64ee5320 [https://perma.cc/T7EZ-UGZ9].

[39] Marcotte et al., *supra* note 28, at 516–17.

[40] *Id.*

comprise the perpetrators of cyberflashing,[41] these gender-based differences in reactions to cyberflashing are likely a contributing factor to the differing motivations of cyberflashers and the expectations of their victims.

III. CYBERFLASHING LAWS & THEIR PITFALLS

Currently, there is a lack of legislation worldwide addressing cyberflashing. Contributing to this deficiency is the absence of awareness of cyberflashing and a lack of knowledge regarding punishment for offenders under existing laws. Despite these circumstances, some countries have identified the troubling presence of cyberflashing within their communities and the need for action. In India, for example, cyberflashing perpetrators can be charged under either Section 509 of the Indian Penal Code ("IPC"), which penalizes any "*gesture or act intended to insult the modesty of a woman,*"[42] Section 268 of the IPC, which penalizes public nuisance, or Section 67 of the Information Technology Act, which penalizes "transmitting or publishing '*obscene material in electronic form.*'"[43]

Like India, other countries have seemingly opted to shoehorn cyberflashing into existing laws, rather than create laws specific for cyberflashing.[44] While these countries should be applauded for their

---

[41] *See* Andrea Waling & Tinonee Pyn, *'C'mon, No One Wants a Dick Pic': Exploring the Cultural Framings of the 'Dick Pic' in Contemporary Online Publics*, 28 J. GENDER STUD. 70, 70 (2019).

[42] Mansi Jain, *Cyber Flashing: A "Big Deal,"* JURIS CTR. (July 3, 2022), https://juriscentre.com/2022/07/03/cyber-flashing-a-big-deal/#:~:text=However%2C%20cases%20of%20Cyber%2DFlashing,IPC%2C%20that%20penalize%20public%20nuisance [https://perma.cc/AZ8Q-JTQZ].

[43] *Id.*

[44] *See* Jake Adelstein, *Japan's Police Crack Down on 'AirDrop' Dick Pics*, DAILY BEAST (Aug. 23, 2019, 5:06 AM), https://www.thedailybeast.com/japans-police-crack-down-on-airdrop-dick-pics?ref=scroll [https://perma.cc/3PXN-5JJN]; Asher Flynn, *Cyberflashing—Old-Style Sexual Harassment for the Digital Age*, MONASH UNIV. (Sept. 6, 2019), https://lens.monash.edu/@politics-society/2019/09/06/1376441/cyberflashing-the-latest-form-of-digital-sexual-harassment [https://perma.cc/T33K-DYXA]; Samantha Beattie, *Canada's Laws Can't Handle 'Cyberflashing,' A New Type Of Sexual Harassment*, HUFFPOST (Dec. 13, 2018, 1:03 PM), https://www.huffpost.com/archive/ca/entry/

proactive responses, embedding cyberflashing into preexisting laws is quite arduous and often fails to deter perpetrators, provide victims with redress, or yield a clear-cut method for prosecuting cyberflashing. Instead, legislators should choose to create cyberflashing-specific provisions to address the cybercrime; indeed, multiple jurisdictions in the U.S. and abroad have enacted such laws. The proceeding Sections analyze proposed and enacted U.S. and international provisions geared directly toward cyberflashing and highlight the pros and cons of each approach.

A. Domestic Approaches

Currently, there is no federal law criminalizing cyberflashing. Fortunately, state legislatures have begun to recognize the prevalence of this cybercrime. Four states have enacted state-specific laws to combat cyberflashing: Texas,[45] Virginia,[46] California,[47] and New Hampshire.[48] While each state-based approach focuses on punishing cyberflashing offenders,[49] each accomplishes this objective by different means.

1. Criminal Law Approaches

Some states that have already enacted or are in the process of enacting cyberflashing-specific laws have criminalized

cyberflashing-canada-airdrop-dick-pics-subway-sexual-harassment_ca_5cd57db3e4b07bc729789100 [https://perma.cc/9LCY-H2YR].

[45] *See* TEX. PENAL CODE § 21.19(b) (2019).

[46] *See* VA. CODE ANN. § 8.01-46.2(B) (2022).

[47] *See* CAL. CIV. CODE § 1708.88(a) (2023).

[48] *See* N.H. REV. STAT. § 645:1(I)(b) (2023).

[49] *See* Cristiano Lima, *States Are Moving to Penalize 'Cyber-Flashing,'* WASH. POST (Sept. 27, 2022, 9:00 AM), https://www.washingtonpost.com/politics/2022/09/27/states-are-moving-penalize-cyber-flashing/ [https://perma.cc/5PNN-2AMY]. In contrast, bills previously introduced in Congress have focused on punishing the platforms which enable such harassment. *Id.* ("Sens. Mark Warner (D-Va.), Mazie Hirono (D-Hawaii) and Amy Klobuchar (D-Minn.) last year proposed legislation that would open digital platforms to civil liability in cases related to harassment, "cyberstalking" or "cyberharassment," which could encompass cyberflashing.").

cyberflashing. In 2019, Texas became the first state to enact a law directed at cyberflashing.[50] Texas law reads:

> A person commits an offense if the person knowingly transmits by electronic means visual material that:
>
> (1) depicts:
>
> (A) any person engaging in sexual conduct or with the person's intimate parts exposed; or
>
> (B) covered genitals of a male person that are in a discernibly turgid state; and
>
> (2) is not sent at the request of or with the express consent of the recipient.[51]

The statue also defines "intimate parts,"[52] "sexual conduct,"[53] and "visual material."[54] This offense is a misdemeanor, which carries a maximum penalty of a $500 fine.[55]

The Texas statute is broadly constructed in a victim-friendly manner, providing an excellent blueprint for states looking to create similar laws. One beneficial component of this law is its *mens rea*[56]

---

[50] *See* Clarice Silber, *Texas Teams with Bumble to Crack Down on 'Cyber Flashing,'* AP NEWS (Aug. 30, 2019), https://apnews.com/article/austin-laws-wa-state-wire-ca-state-wire-pa-state-wire-7e6192f8c06a4b36acdcc705a76b2fdb [https://perma.cc/C7PY-EZRP].

[51] TEX. PENAL CODE § 21.19(b) (2019).

[52] *Id.* § 21.19(a) (incorporating the definition of "intimate parts" provided in section 21.16(a)(1)); *Id.* § 21.16(a)(1) (defining "intimate parts" as "the naked genitals, pubic area, anus, buttocks, or female nipple of a person.").

[53] *Id.* § 21.19(a) (incorporating the definition of "sexual conduct" provided in section 21.16(a)(3)); *Id.* § 21.16(a)(3) (defining "sexual conduct" as "sexual contact, actual or simulated sexual intercourse, deviate sexual intercourse, sexual bestiality, masturbation, or sadomasochistic abuse.").

[54] *Id.* § 21.19(a) (incorporating the definition of "visual material" provided in section 21.16(a)(5)); *Id.* § 21.16(a)(5) (defining "visual material" as "any film, photograph, videotape, negative, or slide or any photographic reproduction that contains or incorporates in any manner any film, photograph, videotape, negative, or slide; or . . . any disk, diskette, or other physical medium that allows an image to be displayed on a computer or other video screen and any image transmitted to a computer or other video screen by telephone line, cable, satellite transmission, or other method.").

[55] *Id.* §§ 21.19(c), 12.23.

[56] *Mens rea* is "[t]he state of mind that the prosecution, to secure a conviction, must prove that a defendant had when committing a crime." *Mens rea*, BLACK'S LAW DICTIONARY (11th ed. 2019).

requirement. Because the law describes *mens rea* simply as "knowingly" transmitting without consent, there is no specific intent requirement, meaning less work will be required for the prosecution to render a guilty verdict in favor of the victim.[57] Likewise, using "transmits" bases the offense on distribution rather than forced viewing, once again avoiding an onerous evidentiary burden for victims.[58]

Additional useful components of the Texas statute include its definitions of visual material and what that material depicts. By including both an extensive list of mediums within the meaning of visual material and a variety of scenarios of what this material could depict, this statute ensures that virtually all forms of sexually explicit visual material are punishable. Because of its broad, inclusive language, the Texas statute is likely to capture a majority of its intended offenders.[59]

Following in Texas's footsteps, New Hampshire also opted to criminalize cyberflashing. Effective as of January 1, 2023, New Hampshire law makes it a crime for a person to "knowingly transmit[] to another, who is 16 years of age or older, an image of himself or herself fornicating, exposing his or her genitals, or performing any other act of gross lewdness, when the recipient does not consent to receipt of the image."[60] This offense is a misdemeanor,[61] which carries a maximum penalty of a $1,200 fine.[62] At first glance, this statute fails to consider minors under sixteen as either perpetrators or victims. However, this exclusion is partially reconciled, as New Hampshire has a preexisting law in place which

---

[57] TEX. PENAL CODE § 21.19(a) (2019).

[58] *Id*.

[59] This breadth may come back to haunt Texas lawmakers. Many legal scholars worry the Texas law might not withstand First Amendment scrutiny. *See* Troy Closson, *A New Texas Law Criminalizes Sending Unwanted Nudes. Lawyers Say It Might Be Difficult to Enforce.*, TEX. TRIB. (Aug. 14, 2019, 12:00 AM), https://www.texastribune.org/2019/08/14/Texas-new-law-sending-unwanted-nudes-dating-apps-texts/ [https://perma.cc/8N8D-GNH7].

[60] N.H. REV. STAT. § 645:1(I)(b) (2023).

[61] *See id.* § 625:9(IV)(c) ("Any crime designated within or outside this code as a misdemeanor without specification of the classification shall be presumed to be a class B misdemeanor . . . .").

[62] *Id*. § 651:2(IV)(a).

criminalizes sending intimate images to children under 16. The "older" New Hampshire statute makes it a crime for a person to

> purposely transmit[] to a child who is less than 16 years of age, or an individual whom the actor reasonably believes is a child who is less than 16 years of age, an image of himself or herself fornicating, exposing his or her genitals, or performing any other act of gross lewdness.[63]

This offense is a felony, carrying a maximum penalty, exclusive of fine, of "imprisonment in excess of one year but not in excess of 7 years."[64]

Compared to Texas's cyberflashing statute, New Hampshire's cyberflashing laws are less likely to capture offenses for several reasons. First, both New Hampshire statutes employ considerably narrower language in their description of images and what sexually explicit scenarios contained within those images are. Further, neither of these statutes provides explanation as to what is meant by "image." This ambiguity leaves room for narrow construction of this terminology by courts. Likewise, "an image of himself or herself fornicating, exposing his or her genitals, or performing any other act of gross lewdness," leaves too much open to interpretation.[65] Unless "other act[s] of gross lewdness" are construed to exclude more illicit behaviors, such as images of clothed, erect penises and other forms of sexual activity, these laws could fail to encapsulate a significant number of offenders.[66] Another glaring issue with these statutes is that they fail to recognize a significant population of juvenile offenders. As these statutes currently operate, juvenile offenders under the age of sixteen cannot be prosecuted for cyberflashing, regardless of whether the victims are minors or adults under New Hampshire law. Consequently, these statutes fail to provide recourse for a large demographic of both offenders and victims.

There are also quite a few differences between the two New Hampshire statutes. Pertinently, the older New Hampshire statute omits non-consensual receipt from its definition and creates a specific intent requirement (i.e., "purposely"). As a result, the older New Hampshire statute is more stringent, and therefore less likely

---

[63] *Id*. § 645:1(II)(c).
[64] *Id*. § 625:9(III)(a)(2).
[65] *Id.* § 645:1(I)(b).
[66] N.H. REV. STAT. § 645:1(I)(b) (2023).

to capture the cyberflashing offenses falling under its domain (e.g., adults cyberflashing those under the age of sixteen) than its newer counterpart.

In addition to Texas and New Hampshire enacting cyberflashing-specific criminal laws, several other states have introduced similar bills in their legislatures.[67] Moreover, some cities have also introduced and/or enacted cyberflashing-specific laws. For example, Chicago has criminalized cyberflashing, making the act punishable by a fine up to $500 for the first offense and $1,000 for the second offense, as well as punishable as a misdemeanor with a prison term of up to 90 days.[68] However, the crime is limited to AirDrop-based cyberflashing; the Municipal Code of Chicago defines cyberflashing to mean "knowingly and without lawful justification send an intimate image to another person *through the use of data-dropping technology* without the request or express consent of the person."[69] Because of its narrow scope, the Chicago law fails to capture other prevalent forms of cyberflashing discussed above, which may ultimately result in an abundance of unhampered transgressions.

2. Civil Law Approaches

On the other hand, some states that have already enacted or are in the process of enacting cyberflashing-specific laws have stopped short of criminalizing cyberflashing and have instead created a different vehicle for victims to seek redress. In July 2022, Virginia became the second state to enact a cyberflashing law, and the first

---

[67] *See* Assemb. 5041, 220th Leg., Reg. Sess. (N.J. 2023); Assemb. 319, 2023 Leg., Reg. Sess. (N.Y. 2023).

[68] MUN. CODE CHI. § 8-4-127(d) (2022).

[69] *Id.* § 8-4-127(a)(5) (emphasis added). *See also id.* § 8-4-127(a)(6) ("'Data-dropping technology' means technology that enables the transfer of files, including, but not limited to, pictures, videos, or texts, using wireless local area networking devices to cellular telephone users located within close proximity with the sender. The term 'data-dropping technology' does not include transferring of files through e-mail, telephone text messaging, or by posting on social media networks.").

state to utilize a civil action approach.[70] The Virginia statute, in pertinent part, reads:

> Any person 18 years of age or older who knowingly transmits an intimate image by computer or other electronic means to the computer or electronic communication device of another person 18 years of age or older when such other person has not consented to the use of his computer or electronic communication device for the receipt of such material or has expressly forbidden the receipt of such material shall be considered a trespass and shall be liable to the recipient of the intimate image for actual damages or $500, whichever is greater, in addition to reasonable attorney fees and costs. The court may also enjoin and restrain the defendant from committing such further acts.[71]

Additionally, the statute defines an "intimate image" as "a photograph, film, video, recording, digital picture, or other visual reproduction of a person 18 years of age or older who is in a state of undress so as to expose the human male or female genitals."[72]

Although the Virginia statute prevails by encompassing all forms of media in which cyberflashing can be accomplished and does not require specific intent, these victories are overshadowed by multiple defects that hamper victims' relief. One shortcoming of the Virginia statute is its failure to include minors as both perpetrators and victims. As it currently stands, juvenile offenders cannot be held liable for cyberflashing, regardless of whether the victims are minors or adults under Virginia law. Likewise, adult offenders cannot be held liable for cyberflashing when their victims are minors.[73] Therefore, this statute fails to account for a significant body of offenders and victims. An additional deficiency in this

---

[70] *See* Saleen Martin, *Thinking About Sending Unsolicited Nudes? It'll Be Illegal in This State Starting July 1*, USA TODAY (Apr. 14, 2022, 4:02 PM), https://www.usatoday.com/story/news/nation/2022/04/14/unsolicited-nudes-illegal-virginia/7317178001/ [https://perma.cc/HP8T-QX4A].

[71] VA. CODE ANN. § 8.01-46.2(B) (2022).

[72] *Id.* § 8.01-46.2(A).

[73] The Virginia cyberflashing law was designed to be cumulative and not restrict remedies available under another Virginia law that may apply to this offense. *Id.* § 8.01-46.2(B). Therefore, adult offenders cyberflashing minors could possibly be held criminally liable under § 18.2-374.3. *See id*. § 18.2-374.3. However, classifying certain instances of cyberflashing under different offenses could lead to confusion and/or difficulties for victims seeking redress. *See* discussion *infra* Section V(D).

statute is the images it includes. Under the language of the statute, only images of male or female genitals "in a state of undress" are included within the offense.[74] Limiting the offense to these kinds of images fails to acknowledge the emotional distress that victims may endure from receiving unsolicited pictures of a clothed, erect penis, as well as other forms of sexual imagery. Unfortunately, these issues can go unnoticed and are likely to impede a victim's legal recourse.

In January 2023, California became the second state to create a civil means of recourse for cyberflashing.[75] Coined the FLASH (Forbid Lewd Activity and Sexual Harassment) Act, the California measure creates a "private cause of action . . . against a person 18 years of age or older who knowingly sends an image, that the person knows or reasonably should know is unsolicited, by electronic means, depicting obscene material."[76] The Act provides a comprehensive description of its cyberflashing offense by not only defining "obscene material,"[77] but also defining an "image"[78] and when an image is "unsolicited."[79] Under the FLASH Act, victims may recover "[e]conomic and noneconomic damages proximately caused by the receipt of the image, including damages for emotional distress," statutory damages "of a sum of not less than one thousand five hundred dollars ($1,500) but not more than thirty thousand dollars ($30,000)," and punitive damages.[80]

---

[74] *Id.* § 8.01-46.2(A).

[75] *See Bumble-Backed Anti-Cyberflashing Bill Passes in California*, BUMBLE, https://bumble.com/en-us/the-buzz/bumble-california-cyberflashing-bill-law [https://perma.cc/55W8-EGDC] (last visited Apr. 4, 2023).

[76] CAL. CIV. CODE § 1708.88(a) (2023).

[77] *Id.* § 1708.88(b)(2) ("'Obscene material' means material, including, but not limited to, images depicting a person engaging in an act of sexual intercourse, sodomy, oral copulation, sexual penetration, or masturbation, or depicting the exposed genitals or anus of any person, taken as a whole, that to the average person, applying contemporary statewide standards, appeals to the prurient interest, that, taken as a whole, depicts or describes sexual conduct in a patently offensive way, and that, taken as a whole, lacks serious literary, artistic, political, or scientific value.").

[78] *Id.* § 1708.88(b)(1) ("An 'image' includes, but is not limited to, a moving visual image.").

[79] *Id.* § 1708.88(b)(3) ("An image is 'unsolicited' if the recipient has not consented to or has expressly forbidden the receipt of the image.").

[80] *Id.* §§ 1708.88(c)(2)(A)-(C).

In general, California's FLASH Act falls short of vindicating victims of cyberflashing. Like Virginia's civil action statute, the FLASH Act fails to capture a considerable demographic of perpetrators and victims because it excludes minors from its provisions. While the statute's definition of "obscene material" covers a vast array of mediums and sexual scenarios, it contradicts this with its conclusion: "taken as a whole, that to the average person, applying contemporary statewide standards, appeals to the prurient interest, that, taken as a whole, depicts or describes sexual conduct in a patently offensive way, and that, taken as a whole, lacks serious literary, artistic, political, or scientific value."[81] By incorporating this language into the definition, the statute turns what was a clear-cut definition of obscene material into an obfuscated standard that could potentially be narrowly construed by the courts. Collectively, these deficiencies fail to keep victims' best interests in mind and are likely to mangle the efficacy of civil recourse.

B. International Approaches

Cyberflashing is not a crime exclusive to the United States. Indeed, what may have been the first ever reported cyberflashing offense occurred in England.[82] As it currently stands, only two countries have enacted cyberflashing-specific laws: Singapore[83] and Scotland.[84] However, some countries, such as England and Wales,[85] are in the process of developing cyberflashing-specific legislation.

1. Singapore

In January 2020, Singapore criminalized cyberflashing.[86] Singapore's provision holds a person guilty of "sexual exposure" if:

---

[81] *Id.* § 1708.88(b)(2).

[82] *See* Sarah Bell, *Police Investigate 'First Cyber-flashing' Case*, BBC (Aug. 13, 2015), https://www.bbc.com/news/technology-33889225 [https://perma.cc/CQX9-9XSZ].

[83] *See* SING. PENAL CODE § 377BF(1)-(2).

[84] *See* Sexual Offences (Scotland) Act 2009, (ASP 9) § 6, ¶¶ 1–2.

[85] *See* Online Safety Bill 2022-3, HL Bill [87] cl. 167 (UK).

[86] Staff Writer, *Cyber-flashing, Voyeurism, Doxing Criminalised from 1 Jan 2020*, YAHOO! NEWS (Dec. 27, 2019), https://sg.news.yahoo.com/cyberflashing-voyeurism-criminalised-from-1-january-2020-103908757.html?guccounter=1&guce_referrer=aHR0cHM6Ly93d3cuZ29vZ2xlLmNvbS8&guce

(1) they intentionally expose or distribute their own genitals or an image of their or any other person's genitals for the purpose of obtaining sexual gratification or of causing another person humiliation, alarm, or distress; (2) intend for that person to see their or someone else's genitals; and (3) do so without that person's consent.[87] Individuals found guilty of sexual exposure can face imprisonment for up to a year, a fine, or both.[88] However, the punishment is heightened when victims are less than 14 years old. In such cases, guilty individuals can "be punished with imprisonment for a term which may extend to 2 years, and shall also be liable to fine or to caning."[89]

Overall, Singapore's cyberflashing law contains both pros and cons. One positive aspect of this provision is its focus on distribution rather than receipt, as it removes the burden on victims to prove that they received or viewed the image. Another valuable component of Singapore's law is its inclusion of images of another person's genitals, in addition to the perpetrator's genitals, in the images covered. This incorporation is emblematic of the nature of the harm cyberflashing victims experience, as an image of genitals is an image of genitals, regardless of whose genitals are actually depicted.

However, given that this law only covers images of genitals, it fails to account for other lewd content that victims could be harmed by. Similarly, because this law does not provide any definition of "image," it is unclear whether videos or other forms of media that can be used to cyberflash would fall within its provisions. While its intent requirement (i.e., "intentionally") "is at least broader than only requiring proof of sexual gratification, . . . it remains limited."[90] For instance, situations where individuals were cyberflashing with the intention of pranking others will not fall within the bounds of

---

_referrer_sig=AQAAAAF5VDMlxa3auNHCfeM3Lr87574MFVOdCLBh3Zdh CW3EjF3Ksh6vwNo9_uirCPUCjOypGiGRTJKUraT7R38X5lIm4Md6KTaPedl 2ohVHJcYipR979bWk1GELzxqERg2v-9ye9N-jG-7KHVjYf4z1TN7lHl6iAVJoZ-TTFUu4apBP [https://perma.cc/K83F-HXRN].

[87] SING. PENAL CODE § 377BF(1)-(2).

[88] *Id*. § 377BF(3).

[89] *Id*. § 377BF(4).

[90] Clare McGlynn & Kelly Johnson, *Criminalising Cyberflashing: Options for Law Reform*, 85 J. CRIM. L. 171, 182 (2020).

this law. Although Singapore's cyberflashing law has some shortcomings, it is sufficient to capture a substantial amount of cyberflashing offenses.

2. Scotland

The Sexual Offences (Scotland) Act of 2009 makes it an offense to coerce a person into looking at a sexual image. More specifically, an individual commits this crime if they "intentionally and for a purpose [of obtaining sexual gratification, humiliating, distressing, or alarming another person] cause another person ("B") . . . to look at a sexual image . . . without B consenting, and . . . without any reasonable belief that B consents."[91] This law also provides a definition of "sexual image."[92] This offense carries a penalty of imprisonment for a term up to ten years, a fine, or both.[93]

The Sexual Offences (Scotland) Act of 2009 also makes it an offense to cause a young child to look at a sexual image. An individual commits this crime if they "intentionally and for a purpose [of obtaining sexual gratification, humiliating, distressing, or alarming a child] cause[] a child . . . who has not attained the age of 13 years to look at a sexual image."[94] Like its adult counterpart, this law also provides a definition of "sexual image."[95] This offense carries a penalty of imprisonment for a term up to ten years, a fine, or both.[96]

Because of the language used, Scotland's laws are not likely to capture the majority of cyberflashing cases, if any at all.[97] Indeed, these are the only cyberflashing-specific laws that require proof of

---

[91] Sexual Offences (Scotland) Act 2009, (ASP 9) § 6, ¶¶ 1-2.

[92] *Id.* ¶ 3 ("[A] sexual image is an image (produced by whatever means and whether or not a moving image) of—(a) A engaging in a sexual activity or of a third person or imaginary person so engaging, (b) A's genitals or the genitals of a third person or imaginary person.").

[93] *Id.* § 48, sch. 2.

[94] *Id.* § 23 ¶¶ 1–2.

[95] *Id.* ¶ 3.

[96] *Id.* § 48, sch. 2.

[97] *See generally* Constance Kampfner, *More Than 95% of Cyberflashing Goes Unpunished in Scotland*, SUNDAY TIMES (Mar. 14, 2022, 12:01 AM), https://www.thetimes.co.uk/article/more-than-95-of-cyberflashing-goes-unpunished-in-scotland-2d9vjvx3t [https://perma.cc/5EAU-VUDK].

an offender "causing" another person or child to look at a lewd image without their consent, in contrast with the "distributing, transmitting, or sending" graphic images language utilized elsewhere. Scotland's laws also attach specific intent requirements, including obtaining sexual gratification, humiliating, distressing, or alarming another person. Like Singapore's law, situations where cyberflashing occurs with the intention of pranking would likely not be captured under Scotland's laws. Still, both of Scotland's laws contain broad definitions of "sexual images" that are inclusive of multiple forms of images and what those images depict.

It is also important to note the difference between the Scottish statutes. Notably, the Scottish offense that is geared towards protecting children omits non-consensual receipt from its definition. However, it maintains an identical specific intent requirement. As a result, both laws operate identically and will be limited to capturing offenses in which cyberflashers "caused" their victims to look at sexually graphic images.

3. England and Wales

While there is no existing law specifically dealing with cyberflashing in England and Wales, laws criminalizing cyberflashing have been included in the United Kingdom's (UK) Online Safety Bill, which is currently making its way through Parliament. The proposed Online Safety Bill aims "to protect children and adults online," as well as "make social media companies more responsible for their users' safety on their platforms."[98] If passed, this bill will create an "[offense] of sending . . . photograph or film of genitals," which reads:

> (1) A person (A) who intentionally sends or gives a photograph or film of any person's genitals to another person (B) commits an [offense] if—
>
> > (a) A intends that B will see the genitals and be caused alarm, distress[,] or humiliation, or

[98] Dep't for Digital, Culture, Media & Sport, *A Guide to the Online Safety Bill*, GOV.UK (Dec. 16, 2022), https://www.gov.uk/guidance/a-guide-to-the-online-safety-bill#types-of-content-that-will-be-tackled [https://perma.cc/67TH-8CAX].

> (b) A sends or gives such a photograph or film for the purpose of obtaining sexual gratification and is reckless as to whether B will be caused alarm, distress[,] or humiliation.[99]

The bill goes even further, providing definitions for references to "sending or giving"[100] and "photograph or film."[101] If convicted, offenders can face fines, imprisonment for up to two years, or both.[102]

Despite its aspirations, England and Wales's proposed cyberflashing provision in the Online Safety Bill has a glaring flaw that could render this legislation virtually useless to victims: it fails to include lack of consent as an element of the crime. Central to any image-based sexual abuse is the absence of consent. By not including a consent requirement, this proposed law holds cyberflashing to a higher standard of proof than that of other sexually-based crimes. Moreover, this proposed law requires additional elements necessary to satisfy the crime in addition to "intentionally" sending an explicit photo, creating more hurdles for prosecutors to prove such cases. The mental states attached to these additional elements (e.g., "intent," "purpose," and "recklessness") compound the problem, as the subjective nature inherent in these requirements of culpability effectively excludes certain cases of cyberflashing from punishment. For example:

> [I]f D believes [cyberflashing] will sexually thrill the receiver as he thinks he is very attractive, D will not be liable for this new [offense] because D will lack the intention to cause or recklessness as to causing the receiver any alarm, distress[,] or humiliation . . . . Where D sends such image or video to V having [realized] that it might cause V alarm, distress[,] or humiliation, he will not be liable if his purpose is not to

---

[99] Online Safety Bill 2022-3, HL Bill [87] cl. 167 (UK).

[100] *Id*. ("References to sending or giving such a photograph or film to another person include, in particular—(a) sending it to another person by any means, electronically or otherwise, (b) showing it to another person, and (c) placing it for a particular person to find.").

[101] *Id*. ("References to a photograph or film also include—(a) an image, whether made by computer graphics or in any other way, which appears to be a photograph or film, (b) a copy of a photograph, film or image within paragraph (a), and (c) data stored by any means which is capable of conversion into a photograph, film or image within paragraph (a).").

[102] *Id*.

> obtain sexual gratification. This could be a case where D sends such photo or video to make fun of V.[103]

Because this law defines cyberflashing as more than just sending a lewd photo, it "leaves victims vulnerable, exposed, and without recourse to justice."[104] Thus, despite its broadly inclusive definitions of the meanings of transmission and kinds of images, the cyberflashing provision of the UK's Online Safety Bill is likely to limit victims' abilities to seek redress.

IV. THE ROLE OF TECHNOLOGY & SOCIAL MEDIA COMPANIES IN CYBERFLASHING

Before considering recommendations to improve current and future cyberflashing legislation, it is important to recognize the unique role technology and social media companies play in the proliferation—and in few instances, prevention—of this cybercrime. It is indisputable that technology is a breeding ground for cyberflashing and cybercrimes alike. Thanks to the anonymity the internet offers, perpetrators can get away with crimes more easily than ever before. New York City Councilman Joseph Borelli, a co-sponsor of a failed citywide anti-flashing bill,[105] shared this same sentiment: "In the old days, you had to have a long trench coat and good running shoes, . . . Technology has made it significantly easier to be a creep."[106]

Unfortunately, U.S. federal and state legislators are likely to have a hard time imposing any form of liability on technology and social media companies and their platforms on which cyberflashing occurs. Section 230 of the Communications Decency Act holds that "[n]o provider or user of an interactive computer service shall be

---

[103] Bo Wang, *A Critical Analysis of the Law Commission's Proposed Cyberflashing Offence*, 87 J. CRIM. L. 39, 42 (2022).

[104] Sophie Gallagher, *The Cyber Flashing Law Remains Inadequate and it's too Soon to Celebrate its Criminalization*, INEWS (Mar. 17, 2022, 5:23 PM), https://inews.co.uk/opinion/cyberflashing-law-remains-inadequate-too-soon-celebrate-criminalisation-1523383 [https://perma.cc/KBX6-4UKS].

[105] *See* N.Y.C. Council Int. No. 1244 (2018).

[106] Sharon Otterman, *Sending Lewd Nudes to Strangers Could Mean a Year in Jail*, N.Y. TIMES (Nov. 30, 2018), https://www.nytimes.com/2018/11/30/nyregion/airdrop-sexual-harassment.html [https://perma.cc/X68T-44AH].

treated as the publisher or speaker of any information provided by another information content provider."[107] In other words, social media platforms cannot be held liable for any user-posted illegal content.[108] Similarly, social media platforms cannot be held liable for any self-imposed, good-faith efforts to moderate content (the Good Samaritan provision).[109] Therefore, unless another exception is made to Section 230 that would hold social media companies liable for enabling (or failing to police) cyberflashing on their platforms, it will remain virtually impossible to hold these companies accountable for their role in cyberflashing.[110] However, it is not impossible. In theory, the Good Samaritan provision *should* inadvertently encourage platforms to voluntarily block and screen abhorrent content; therefore, social media companies *could* attempt to filter out cyberflashing, *if they so choose*.

Some technology and social media companies are taking measures to protect their users from cyberflashing. In particular, the dating app Bumble[111] has been instrumental in increasing the discourse surrounding cyberflashing both in the U.S. and abroad. Bumble has successfully advocated for cyberflashing laws, with its efforts directly helping to pass the cyberflashing laws in Texas, Virginia, and California.[112] In addition to its lobbying efforts,

---

[107] 47 U.S.C. § 230(c)(1).

[108] There are few exceptions to Section 230, specifically for copyright violations, content related to sex trafficking, and other violations of federal criminal law. *See* VALERIE C. BRANNON & ERIC N. HOLMES, CONG. RSCH. SERV., R46751, SECTION 230: AN OVERVIEW 24–29 (2021).

[109] 47 U.S.C. § 230(c)(2).

[110] Interestingly enough, California and Virginia accounted for Section 230 within their cyberflashing statutes. *See* CAL. CIV. CODE § 1708.88(d)(1); VA. CODE ANN. § 8.01-46.2(C).

[111] "Bumble was first founded to challenge the antiquated rules of dating. Now, Bumble empowers users to connect with confidence whether dating, networking, or meeting friends online. We've made it not only necessary but acceptable for women to make the first move, shaking up outdated gender norms. We prioritize kindness and respect, providing a safe online community for users to build new relationships." *Why Bumble?*, BUMBLE, https://bumble.com/en-us/ [https://perma.cc/2U5A-2YN3] (last visited Apr. 4, 2023).

[112] *Bumble Releases Open-Source Version of Private Detector A.I. Feature to Help Tech Community Combat Cyberflashing*, BUMBLE, https://bumble.com/en-

Bumble has also created and implemented in its application a safety feature called "Private Detector."[113] This feature works "by using [artificial intelligence] to automatically blur a potential nude image shared within a chat on Bumble. It'll then notify you that you've been sent something that's been detected as inappropriate; it's up to you to decide whether to view or block the image."[114] Bumble has also released an open-source version of this feature on GitHub, in the hopes that others in the technology community will utilize this feature to "work in tandem to make the internet a safer place."[115] Instagram is also working on its own version of the Private Detector, which the company has dubbed as the "nudity protection" filter.[116] This feature will function almost identically to Bumble's, with one extra benefit: Instagram will not view the actual messages or share them with third parties.[117] If these efforts are a sign of things to come,

---

us/the-buzz/bumble-open-source-private-detector-ai-cyberflashing-dick-pics [https://perma.cc/Z37Z-5AWE] (last visited Apr. 4, 2023).

[113] "The Private Detector feature will also be added to global dating apps Badoo, Chappy, and Lumen," which, alongside Bumble, are all owned by parent company MagicLab. Sarah Ashley O'Brien, *Bumble Says it Will Soon Detect Lewd Images Sent on its App*, CNN BUS. (Apr. 24, 2019, 2:28 PM), https://www.cnn.com/2019/04/24/tech/bumble-lewd-images-private-detector/index.html [https://perma.cc/86G7-AHGH].

[114] *With Bumble's Private Detector, You Have Control Over Unsolicited Nudes*, BUMBLE, https://bumble.com/en/the-buzz/privatedetector [https://perma.cc/26MS-CMVM] (last visited Apr. 4, 2023).

[115] *Bumble Releases Open-Source Version of Private Detector A.I. Feature to Help Tech Community Combat Cyberflashing*, *supra* note 112; *see also* Bumble-Tech, *Private-Detector*, GITHUB, https://github.com/bumble-tech/private-detector [https://perma.cc/M5A4-TTJA] (last visited Apr. 4, 2023).

[116] Todd Spangler, *Instagram Developing 'Nudity Protection' Feature to Block Unsolicited Nude Photos in DMs,* VARIETY (Sept. 22, 2022, 6:55 AM), https://variety.com/2022/digital/news/instagram-nudity-protection-block-photos-dms-1235380379/ [https://perma.cc/4P5U-377S].

[117] Sheena Vasani, *Instagram's Finally Working on Protecting Users From Unsolicited Nude Photos*, VERGE (Sept. 21, 2022, 4:20 PM), https://www.theverge.com/2022/9/21/23365079/instagram-meta-cyberflashing [https://perma.cc/C2ZY-HBWQ]. Unlike Instagram, Bumble has not explicitly stated that it does not view the actual messages that depict nude imagery or share them with third parties. However, its privacy policy implies that it does view and share such images. *See Bumble Privacy Policy*, BUMBLE, https://bumble.com/privacy [https://perma.cc/2YG9-8QL9] (last visited Mar. 9, 2023).

a widespread adoption of similar filtering features on social media platforms could eventually curb this outlet for cyberflashing.

While efforts on the social media front are starting to gain traction, Apple has yet to directly address cyberflashing offenses related to its AirDrop.[118] Admittedly, there are preventative measures iPhone users themselves can take to minimalize vulnerability. By default, an iPhone's AirDrop settings permit users to receive content via AirDrop only from devices already stored in an iPhone's contacts list.[119] Yet, for various reasons, people change these settings, and without realizing it, many have left themselves vulnerable to being cyberflashed. Although adjusting an iPhone's AirDrop settings from "Everyone" back to "Contacts Only" does solve the problem, it should not be the only solution.[120] People who want or need to use the "Everyone" setting should be able to do so,

---

[118] With its release of iOS 16.2 in December 2022, Apple swapped the previous "Everyone" option out for a "Everyone for 10 Minutes" setting. When selected, this option allows users to receive AirDrop requests from any Apple device for up to 10 minutes. Once 10 minutes have elapsed, AirDrop will automatically return to the "Contacts Only" default option, with users having to manually select the "Everyone for 10 Minutes" option every time they want to receive new AirDrop requests from anybody, regardless of whether that individual is listed in their "Contacts" list. Tom Sykes, *iOS 16.2 Adds "Everyone for 10 Minutes" AirDrop Setting, Replacing Previous "Everyone" Option*, APPLE POST (Dec. 13, 2022), https://www.theapplepost.com/2022/12/13/ios-16-2-adds-everyone-for-10-minutes-airdrop-setting-replacing-previous-everyone-option/ [https://perma.cc/NJN4-DV8X].

[119] "The Contacts Only option is available on devices that support iOS 10 and later, iPadOS, or macOS Sierra 10.12 and later. If AirDrop is set to Contacts Only on your device with an earlier software version, you'll need to adjust AirDrop settings to the Everyone option in Settings or from Control Center. You can select the Everyone option while using AirDrop and disable it when not in use." *How to use AirDrop on Your iPhone or iPad*, APPLE SUPPORT (Dec. 13, 2022), https://support.apple.com/en-us/HT204144 [https://perma.cc/GJ35-K5EU]. *See also AirDrop Security*, APPLE SUPPORT (Feb. 18, 2021), https://support.apple.com/guide/security/airdrop-security-sec2261183f4/web [https://perma.cc/ARW4-T6ZH].

[120] Admittedly, the AirDrop settings update included in iOS 16.2 looks promising for minimizing occurrences of cyberflashing via AirDrop. Given its novelty, no studies regarding this feature's effectiveness in curbing cyberflashing are currently known to exist; only time will tell whether this feature curtails cyberflashing incidents.

without feeling the need to take extra precautions to avoid being cyberflashed.[121] Instead, Apple could blur or restrict preview images sent from iPhones not listed in a person's contacts, giving the person the option to decline or accept the AirDrop.[122] Or, Apple could remove the preview altogether. At a minimum, the company could provide a warning when a person switches AirDrop into the "Everyone" setting.[123] There are a number of ways that Apple can solve this problem without constraining people's use of AirDrop.

Like with other forms of image-based sexual abuse, it is indisputable that technology facilitates cyberflashing. And with the way the majority of these platforms are designed to operate,[124] they are only adding to these victims' troubles. However, given the reactionary nature of U.S. state and federal legislators, technology and social media companies themselves are, in fact, best positioned to put an end to cyberflashing. More of an emphasis should be placed on these companies' capabilities to protect their users, instead of forcing victims to rely on legal recourse.

V. COMBATTING CYBERFLASHING: RECOMMENDATIONS FOR DOMESTIC LEGAL REFORM

Given the lack of federal cyberflashing laws, coupled with the fact that many states do not address cyberflashing within existing cybercrime statutes, most victims have been left with little means of legal recourse. Further, when victims do have the ability to pursue legal action, the standard of proof is not always clear.[125] Drawing on the pros and cons of both state and international laws surrounding cyberflashing, this Section highlights important components of

---

[121] In one instance, a women changed her iPhone's name "to John's work phone and the dick pics stopped immediately." Gallagher, *supra* note 10.

[122] Charlotte Palermino, *The Airdropped Dick Pic Epidemic is Upon Us*, ELLE (Mar. 21, 2018), https://www.elle.com/culture/tech/a19549140/the-airdropped-dickpic-epidemic-is-upon-us/ [https://perma.cc/A5TF-FDFM].

[123] Mark Sullivan, *How Apple Could Easily Fix the iPhone's "Cyber Flashing" Problem*, FAST CO. (Nov. 20, 2018), https://www.fastcompany.com/90275095/how-apple-could-easily-fix-the-iphones-cyber-flashing-problem [https://perma.cc/Q99W-E638].

[124] *See* discussion *supra* Section II(B).

[125] *See, e.g.*, CAL. CIV. CODE § 1708.88(b)(2).

these existing laws that should be considered by U.S. legislators in drafting future federal and state cyberflashing statutes.

A. Cyberflashing Should Be a Criminal Offense

Jurisdictions take two different approaches when it comes to crafting cyberflashing laws.[126] Some jurisdictions have opted to criminalize cyberflashing, while others have opted to make it a cause of action for a civil suit.[127] Regardless of the benefits associated with a civil action, framing cyberflashing as a civil, rather than criminal, offense fails to acknowledge the nature of the crime and invalidates the experiences of its victims. At its core, cyberflashing is sexual harassment and a digitized form of public indecency: both of which are criminal offenses. Similarly, this crime is not rooted in innocence. Cyberflashing perpetrators generally have either a desire to harm or a disregard for the welfare of others.[128] Cyberflashing is an intentional, harmful crime; it meets the textbook definition of a criminal act[129] and therefore should be treated as such.

B. Cyberflashing Should Not Require Specific Intent for Culpability

At a minimum, all of the existing cyberflashing laws describe the crime as a person sending an image of their own or someone else's genitals. However, jurisdictions differ as to whether they also require the perpetrator to commit a further act (e.g., causing the recipient emotional distress). Approximately half of jurisdictions characterize cyberflashing simply as the action of sending the lewd photo; the other half of jurisdictions prescribe additional components to that action.[130] For example, they may require proof that, when the perpetrator sends such photos, they do it for the

---

[126] *See* discussion *supra* Section III(A).

[127] *Id*.

[128] *See* discussion *supra* Section II(D).

[129] A crime is "[a]n act that the law makes punishable." *Crime*, BLACK'S LAW DICTIONARY (11th ed. 2019). "[T]he constituent parts of a crime—usu[ally] consisting of the actus reus, mens rea, and causation—that the prosecution must prove to sustain a conviction." *Elements of Crime*, BLACK'S LAW DICTIONARY (11th ed. 2019).

[130] *See* discussion *supra* Part III.

purpose of sexual gratification or to cause the recipient alarm, humiliation, or distress.[131]

On its face, these differences may seem insignificant. But in reality, if the latter construction is used, there is a notably higher evidentiary burden for prosecutors to overcome. This is because when a specific intent provision (for example, intent to cause alarm) is added to the definition of the crime, it turns cyberflashing into a specific-intent offense, meaning more than conduct alone is required to form the basis for intent of the crime. Characterizing cyberflashing in this manner is problematic because it portrays cyberflashing as a crime "perpetrated only for specific motives, as if being cyberflashed for reasons of status-building or [humor] reduce the harm experienced."[132]

Instead, cyberflashing should be construed as a general-intent crime, in which the conduct alone serves as the basis for intent to commit the crime. As a result, prosecutors will not have the onerous task of proving that perpetrators had some sort of ill intent when sending images. Crafting statutes in this way is ideal because it does not detract from one of the fundamental components of cyberflashing: the lack of consent. In doing so, cyberflashing is not conflated with other cybercrimes like sextortion, which is always specifically motivated. Therefore, cyberflashing does not discriminate by quantifying its victims' harms by its perpetrators' motivations.

C. Cyberflashing Should Not Be Limited to Photos of Male Genitalia

While cyberflashing is typically committed by men, women may be perpetrators as well. Cyberflashing statutes should apply to all lewd content, not merely to male genital photos. In fact, cyberflashing should not be limited to photos or images, generally. Different jurisdictions define the details of cyberflashing differently, including the types of media used for transmission and kinds of content depicted.[133]

---

[131] *See, e.g.*, Sexual Offences (Scotland) Act 2009, (ASP 9) § 6, ¶¶ 1–2.
[132] McGlynn & Johnson, *supra* note 90, at 186.
[133] *See* discussion *supra* Part III.

In both the U.S. and other countries, legislators have predominantly chosen to incorporate several kinds of media that are used to cyberflash within their laws.[134] Types of media used to transmit lewd content can include photographic images, videos, GIFs, and more.[135] It is important that the law acknowledges and includes the various forms of media perpetrators use within the legal definition of cyberflashing, as this will assure that all—or at least most—offenses fall under the statute. Jurisdictions also vary as to the sexual material covered under their statutes. While some statutes focus solely on male and female genitals, others cover a wider variety of content and include other sexual acts.[136] Of these two approaches, the latter is preferrable for constructing future legislation for a few reasons.

First, a broader definition clarifies under the law that sending lewd content beyond the generic genital picture can also constitute harassment and sexual abuse. Second, a broader definition of sexual acts is preemptive because it anticipates future categories of explicit content that offenders could use to circumvent anti-cyberflashing laws.[137] While a wide definition of sexually explicit content can be viewed as turning cyberflashing laws into "sending pornography without consent" laws, it describes and thus recognizes cyberflashing for what it is at its core: digitalized sexual harassment.[138] Embracing such a definition is likely to invoke arguments over its enforceability, viability (regarding First Amendment concerns), and functionality (i.e., its capacity for overcriminalization). However, anticipating these concerns is half the battle; legislators must craft future statutes to withstand judicial scrutiny.

Similarly, legislators should avoid fusing standards into the definitions of the sexual conduct depicted, as is done in California's FLASH Act.[139] Including such standards in the definitions of

---

[134] *Id*.

[135] *See supra* notes 54, 69, 78, 100 and accompanying text.

[136] *Compare* VA. CODE ANN. § 8.01-46.2(A)-(B) (2022), *with* TEX. PENAL CODE § 21.19(b) (2019).

[137] *Id*. at 187.

[138] *Id*. at 183.

[139] *See* discussion *supra* Section III(1)(B).

sexually explicit content tends to muddy their understanding, leaving it up to the judiciary to construe these definitions to its liking. For example, consider a cyberflashing case involving a picture of a clothed, erect penis. With a standard in place that includes language like

> taken as a whole, that to the average person, applying contemporary statewide standards, appeals to the prurient interest, that, taken as a whole, depicts or describes sexual conduct in a patently offensive way, and that, taken as a whole, lacks serious literary, artistic, political, or scientific value[,][140]

a judge or jury may not view such an image as falling within the definition of "sexually explicit content" of the implicated cyberflashing statute, and ultimately rule in favor of the defendant. Holdings of this sort could have drastic ramifications on victims' cases, and subsequently, their overall likelihood of reporting these crimes.

D. Cyberflashing Should Have No Age Requirement

Another pertinent feature of existing cyberflashing laws is the inclusion of an age requirement. Interestingly enough, the jurisdictions that do include this component have all failed to some extent to acknowledge a large body of perpetrators and victims: juveniles.[141] Indeed, in some of these jurisdictions, juvenile cyberflashers can evade conviction for flashing fellow juveniles or even adults.[142] What is arguably worse is the fact that some jurisdictions fail altogether to punish adults for cyberflashing minors.[143] While other provisions may exist to punish adults for behaviors aimed at minors on a broader level (i.e., state statutes criminalizing transmitting harmful materials to a child through electronic means), categorizing cyberflashing in such a way leaves an undesirable amount of breathing room for courts in their decision-making, uncertainty for law enforcement officers attempting to apprehend perpetrators, and may create more confusion and difficulty for victims seeking redress. Future

---

[140] CAL. CIV. CODE § 1708.88(b)(2).
[141] *See* discussion *supra* Part III.
[142] *See, e.g.*, VA. CODE ANN. § 8.01-46.2(B) (2022).
[143] *See, e.g.*, CAL. CIV. CODE § 1708.88(a) (2023).

lawmakers should avoid making the same mistake; they can do so by forgoing the age requirement altogether.

VI. CONCLUSION

Cyberflashing is the newest cybercrime to impact the Digital Age and seems to be the least discussed. Anyone with a Wi-Fi and Bluetooth-enabled device or who uses social media is at risk of being cyberflashed, and the repercussions on victims of this crime are real. As history has shown, perpetrators who once relied on exposing themselves in person will continue in increasing numbers to adapt to perpetration via the digital domain. Given the fact that the technological advancements which heavily enable such behavior are increasing and transforming every day, it is only going to become more difficult to stop this crime.

The U.S. has only just begun to address the issues surrounding cyberflashing. Several states have taken the lead by enacting their own cyberflashing legislation. While these initiatives are a step in the right direction, they are riddled with intricacies that have only created more hurdles for victims to overcome on their journey to justice. Thus, federal law is needed to provide clarity and a uniform approach to combat this crime.

While lawmakers scramble to address cyberflashing, the role of technology and social media companies as not-so-innocent bystanders in these transgressions has become more apparent. Indeed, they have proven their abilities to harness their powers for combatting this crime, yet seldom choose to. Ultimately, it will take the combined efforts of lawmakers and technology and social media companies to stop cyberflashing. While the U.S. may have lost the battle, there is still time to win the war against cyberflashing.