Asma Masude

November 25, 2024

INFO 498

Final Project

## I. Introduction

In the last decade, the intersection of privacy rights and technology-facilitated abuse has become a critical concern, particularly in cases of emotional abuse and intimidation. Victims of emotional abuse and intimidation are often left vulnerable due to outdated or inadequate policies while technology continually evolves. This is especially true in the context of a government that celebrates and guarantees the right to free speech online, potentially at the expense of people's privacy and safety. By outlining limitations of current legislation and advocating for reform, this project will highlight what changes need to be made. This project will analyze current policies surrounding technology facilitated emotional abuse and intimidation, particularly in the context of involuntary exposure of private information through doxxing and revenge porn, to identify gaps in the legal framework and to propose new policy recommendations to protect populations from experiencing this in a country that does not explicitly guarantee privacy through its constitution.

## II. Types of Relevant Technology-Facilitated Abuse

Doxxing, the act of publicly revealing or publishing private personal information such as an individual's home address, phone number, or workplace details without consent, is one of the most prevalent forms of technology-facilitated abuse. This often looks like someone's personal information posted on a public platform as a form of retaliation or intimidation to cause emotional distress and reputational damage (MacAllister 2016).

Nonconsensual pornography (NCP), also referred to as revenge porn, is the unauthorized sharing or dissemination of explicit images or videos without the consent of the subject. The rise of AI technology such as deepfakes has further complicated the issue, as perpetrators can now use AI tools to create fake explicit content, increasing the difficulty of addressing the problem (Rogers 2023).

## III. Current Policy

### A. Doxxing

While doxxing, the act of publicly releasing someone's personal information with the intent to harm or harass, is recognized as harmful, legal protections against it vary across jurisdictions. On the federal level, the Interstate Doxxing Prevention Act (H.R.6478), was introduced in 2016 but it did not pass. This bill would have criminalized using "any means of interstate commerce" to engage in doxxing, with violators being subject to criminal penalties. No federal bill directly addressing doxxing has been proposed since. Some states have enacted laws targeting doxxing, though they often apply to specific groups such as public health workers, judges, or law enforcement officers. For example, Colorado's law provides protection to a narrow range of public employees, while Minnesota's law focuses on law enforcement and their families (*50-state survey* 2021). States like Washington have taken a broader approach, criminalizing the unauthorized publication of personal identifying information under RCW 4.24.792, making it illegal even if the information was voluntarily disclosed (*Unauthorized publication of personal identifying information.* 2023).

### B. NCP and Deepfakes

NCP is illegal in nearly all U.S. states, though there is no single federal law specifically criminalizing it (Cyber Civil Rights Initiative 2019). However, the unanimity of state law gets murkier when we take into account the integration of evolving technology such as AI. Many state laws addressing NCP are rooted in the idea that taking someone's personal and sensitive photos and sharing them publicly is immoral, but with the introduction of deepfakes, it's not technically someone's personal photographs that they own, but rather is something that the perpetrator has created themselves. Some recent legislation on the state level has broadened the definition of NCP to include digital manipulations such as deepfake pornography. States like Indiana, New York, and Virginia have expanded their revenge porn statutes to include deepfakes, while Georgia and Hawaii have incorporated deepfake protections into broader privacy laws. Others, such as Florida, South Dakota, and Washington, have updated child pornography laws to include deepfake created content depicting minors. For instance, Washington's HB 1999 explicitly criminalizes the creation and distribution of fabricated sexually explicit images, providing both civil and criminal remedies for victims. Similarly, laws in Louisiana and South Dakota have targeted deepfakes involving minors by expanding definitions within child pornography statutes. However, some states, like Mississippi and Tennessee, have passed broader deepfake laws that may include NCP but lack specificity, leaving their applicability open to interpretation (Fitzgerald 2024). These legislative updates reflect some

progress in combatting the harms of AI in the realm of technology-facilitated abuse, but questions remain about the consistency and effectiveness of these measures to address this rapidly advancing form of abuse.

## IV. Holes And Limitation

### A. Vagueness and Limitations on who's Protected

The primary limitations in the legal response to doxxing, NCP, and deepfakes lie in the vagueness and inconsistency of laws across states, as well as the evolving nature of technology. For example, the definition of "doxxing" or "nonconsensual pornography" can vary, leading to challenges in enforcement. The lack of a cohesive federal framework leaves many victims relying on fragmented state laws, which may not provide adequate recourse for those harmed by digital abuse. Terms like "harm," "malicious intent," and "consent" are difficult to define and apply, particularly in digital spaces where content spreads rapidly and anonymously. Moreover, the effectiveness of these laws is often undermined by the lack of cooperation from digital platforms in removing harmful content or assisting in investigations.

The absence of a uniform federal policy leaves victims vulnerable, especially as these crimes often involve cross-state or international online platforms. This gap creates difficult legal loopholes where victims must navigate varying state laws, making it more difficult to seek justice. Additionally, many state and federal laws addressing technology-facilitated abuse suffer from vague language that complicates enforcement.

The legal landscape regarding doxxing varies widely from state to state. Many existing state laws are narrow in scope, often targeting specific groups of individuals such as public officials or workers in certain professions. For example, while some states, like Washington, offer more robust legal protections against doxxing, many other states apply their laws too narrowly. Laws in Colorado and Minnesota limit protections to certain public employees or officials, meaning private citizens remain vulnerable to doxxing without recourse. The narrow focus of many state laws means that several vulnerable groups, including private citizens, activists, and journalists, are left unprotected. The impact of doxxing on marginalized or vulnerable groups can be especially severe, as these individuals may face heightened risks of harassment, violence, or discrimination as a result of their personal information being shared online.

There is similar inconsistent protection offered by laws attempting to control NCP. While some states, such as Washington, provide broader protections, many others have narrowly tailored laws that only apply to specific groups or fail to account for the full scope of harm caused by doxxing. State laws addressing NCP have been implemented with varying scope. For example, California's law makes it a criminal offense to distribute intimate images without consent, with penalties that include fines and imprisonment. Similarly, New York's law, passed in 2019, allows victims to pursue civil lawsuits for the distribution of intimate images, and Texas has a law with both criminal and civil remedies for victims of nonconsensual image-sharing (Cyber Civil Rights Initiative 2019) . However, these laws differ in their penalties, coverage, and processes for victims seeking redress. This inconsistency across states complicates enforcement and justice for victims, particularly in cases involving multiple jurisdictions. Many state laws focus primarily on the dissemination of images through digital platforms, but they may not address the more complex issue of deepfake pornography, a growing concern fueled by artificial intelligence.

Laws that protect against the unauthorized creation and distribution of adult deepfake NCP are still in their infancy, and the legal framework remains inadequate to comprehensively address the harms caused by deepfakes in this context. Many deepfake NCP laws focus primarily on child pornography, which overlooks the violation of privacy rights for adults. This exclusion is concerning because it implies that there is no privacy violation issue with NCP created by deepfakes and there is no harmful behavior that needs regulation and protection besides the potential for child pornography. Where such content involves adults, it may fall under broader NCP laws or existing fraud and harassment statutes, but these laws were not designed to address the unique challenges posed by deepfake technology. Regular revenge porn laws are inadequate to address deepfake NCP because they require that the individual be engaged in a sexual act, so a digitally altered piece of media flies under the radar while still imposing harm on the depicted individual (Pritts 2024).

### B. Free Speech

In an attempt to alleviate the previously discussed issue of inconsistent laws regarding doxxing, there have been attempts to address the issue at the federal level, but ultimately their inability to balance privacy protections with First Amendment concerns led to the bill's death. The U.S. Constitution guarantees the freedom of speech, which has been included the right to share information, even if it may be harmful or distasteful. Opponents of doxxing legislation argue that the act of disclosing personal information, even with malicious intent, is a form of protected speech.

Courts may be hesitant to endorse broad doxxing laws because they could inadvertently suppress free expression or punish speech that is deemed offensive but not unlawful. The Interstate Doxxing Prevention Act (H.R. 6478) introduced in 2016, aimed to criminalize doxxing on a federal level by making it illegal to knowingly disclose personal information with the intent to cause harm, harassment, or incite violence (*Summary: H.R.6478 — 114th Congress* 2016). However, the bill did not pass, largely due to opposition over concerns about the vagueness of the proposed language and its potential to infringe on free speech rights. Critics of this kind of legislation argue that the law could be misused to stifle legitimate expression, especially when the disclosure of information is framed as part of political discourse or public criticism (MacAllister 2016). The inability to reconcile doxxing protection with First Amendment protections contributed to the failure of this legislative effort.

The tension between protecting free speech and an individual's right to privacy is a significant challenge in developing effective laws against NCP and deepfakes (Waldstricher 2020). First Amendment concerns often arise when perpetrators argue that their actions fall under protected speech, particularly if the content is intended as satire, parody, or artistic expression. This is often the case in deepfake NCP where the digital creation of an individual engaged in a sexual act is not technically intruding on the privacy of anyone's reality, and can be argued to be a piece of artistic expression on the perpetrators part (Pritts 2024).

### C. Technological Challenges in Enforcement

Enforcement of laws addressing NCP and doxxing faces significant challenges due to technological and jurisdictional limitations. Online platforms often operate across state and national borders, making it difficult for law enforcement to track and prosecute offenders. As mentioned previously, states vary on how they approach the criminalization of doxxing and deepfake NCP, which can make the process of seeking justice more convoluted and difficult. Furthermore, the anonymity of the internet complicates the identification of perpetrators, and perpetrators can easily circumvent traditional law enforcement methods. The existing laws are also difficult to enforce in practice, as proving intent or harm in doxxing cases can be challenging. (Eckert & Metzger-Riftkin 2020) Victims may face difficulties gathering evidence, particularly when personal information is shared across multiple platforms or in a way that is designed to be anonymous or temporary.

### D. Inadequate Victim Support

Despite growing awareness of technology-enabled abuse, there remain significant gaps in providing comprehensive support to victims of crimes of technology-facilitated abuse such as doxxing and NCP. Proposed legislation, such as the Tech Safety for Victims of Domestic Violence, Sexual Assault, and Stalking Act of 2023, illustrates the urgent need for targeted resources to address this issue (*Reps. Eshoo, Lesko Introduce Bill* 2023). This bipartisan bill intended to combat technology-facilitated abuse but failed to pass, leaving its initiatives and potential fruits unrealized.

The Act proposed two critical measures to enhance victim support. First, it aimed to establish 15 technology-facilitated abuse clinics under the Department of Justice's Office on Violence Against Women. These clinics would provide various forms of assistance to victims experiencing this abuse. With grants of $2 million per clinic, this program could have offered a strong framework to help victims navigate the complex and often traumatic implications of technology-facilitated abuse.

Second, the Act proposed an additional grant program to develop and implement training and educational initiatives. These programs, also overseen by the Office on Violence Against Women, would empower nonprofit organizations and educational institutions to equip victim support providers with the knowledge and tools needed to address technology-facilitated abuse effectively. This would have expanded the capacity of service providers to support victims in overcoming the challenges posed by these crimes.

The failure to pass such legislation underscores the inadequacy of current victim support systems. Victims of doxxing and NCP often face unique hurdles, such as the inability to see their perpetrator face legal consequences due to the reasons mentioned previously, which are not adequately addressed by traditional support services. Without federal action to implement innovative and targeted solutions like those proposed in the Tech Safety for Victims Act, victims remain underserved and vulnerable to continued harm.

## V. Policy Recommendations

Given the list of limitations and holes in current policy addressing these forms of technology-facilitated abuse, there are multiple courses of action that should be enacted to strengthen the protection of those afflicted by the abuse. First, there must be federal policies standardizing the criminalization and coverage of doxxing and NCP in order to be clear what the repercussions would be for engaging in this behavior online across state lines, such as if the perpetrator and victim were living in different states. This policy would override any state law that applies protection from

doxxing only to specific classes of employees, and state law that applies protection from the use of deepfakes for NCP only for young children.

In terms of doxxing, this could look like a federal law similar to the Washington State one, which criminalizes the unauthorized publication of personal identifying information with the intent to cause harm or harassment. This law is broader than those in many other states because it does not limit its protections to specific groups but instead applies to any individual whose personal information is shared without consent. The law also includes a critical provision stating that it is not a defense if the information was voluntarily provided or previously disclosed, closing a potential loophole where doxxers might argue that the information was publicly available or given by the victim willingly. Washington's law serves as a stronger model for protecting individuals from online harassment and threats resulting from doxxing. In terms of NCP and deepfakes, the federal law must consistently and explicitly criminalize the use of deepfakes to create NCP for beings of all ages, not just children.

To maximize the effectiveness of standardized federal policy, a key step is refining legislative language to provide greater specificity and clarity. Current laws often suffer from vague definitions that leave room for inconsistent interpretation. Clearer definitions can help distinguish between illegal behavior, such as the malicious distribution of intimate images or personal information, and protected speech. By emphasizing the intent behind the action and the harm it causes, lawmakers can create policies that are more targeted and less likely to be struck down. For example, defining "malicious intent" and clarifying what constitutes "harm" can reduce the risk of vague legal language being misinterpreted and ensure that the laws are both enforceable and constitutionally sound. To avoid policies being struck down for overbreadth or vagueness, lawmakers should focus on defining the intent behind the action and the resulting harm caused to victims. Laws that center on malicious intent or the clear harm inflicted on individuals would be less likely to infringe on protected speech. Additionally, establishing clear guidelines about what constitutes illegal behavior, without overly restricting free speech, would help strike a balance between protecting privacy and safeguarding First Amendment rights.

Beyond strengthening current policy that criminalizes the perpetrator of technology-facilitated abuse, there is a need for external resources to support victims. The resources outlined in the failed 2023 Tech Safety for Victims Act are vital in the sense that they have the potential to provide support and serve as a resource to people who likely may not receive closure or

justice from the legal system due to the current vague nature of policies. One of the key proposals within the act is the creation of programs to provide dedicated resources for victims of NCP, doxxing, and other forms of digital abuse. These programs could offer support, counseling, and financial assistance to help victims recover. Additionally, law enforcement agencies should be provided with education and training programs to better understand the complexities of digital abuse and equip them with the tools needed to investigate and correctly prosecute these crimes.

In summary, the legislative landscape surrounding NCP and doxxing is still evolving, and current laws are insufficient to fully protect victims in a world that is continually expanding in its ways to perpetuate harm on vulnerable populations through tools such as deepfakes. Key gaps in current policy include vague language, inconsistent state laws, and the lack of a unified federal approach. The proposed solutions, refining legislative language, prioritizing victim support programs, and advocating for standardized federal legislation, address these challenges while being mindful of the need to balance First Amendment concerns and overcome technological and jurisdictional barriers. To protect each and every individual from the harms associated with technology-facilitated abuse, it is essential for lawmakers to create clear, targeted, and enforceable laws that evolve with emerging technologies while staying in the lines of constitutional rights.

WORKS CITED

*50-state survey: Doxing - legal protections for ...* (2021) *The Network for Public Health*. Available at: standwithpublichealth.jhsph.edu/wp-content/uploads/2022/02/Doxing-50-State-Survey-December-Final.pdf (Accessed: 26 November 2024).

Cyber Civil Rights Initiative. (2019). 46 states + DC + one territory have revenge porn laws. https://www.cybercivilrights.org/revenge-porn-laws/

Eckert, S., & Metzger-Riftkin, J. (2020). Doxxing, privacy and gendered harassment. The shock and normalization of veillance cultures. *M&K Medien & Kommunikationswissenschaft*, *68*(3), 273-287.

Fitzgerald, M. (2024) *States race to restrict deepfake porn as it becomes easier to create* • *Washington State Standard*, *Washington State Standard*. Available at: https://washingtonstatestandard.com/2024/04/11/states-race-to-restrict-deepfake-porn-as-it-becomes-easier-to-create/ (Accessed: 25 November 2024).

MacAllister, Julia M. "The doxing dilemma: seeking a remedy for the malicious publication of personal information." Fordham L. Rev. 85 (2016): 2451.

Pritts, B. (2024) *Combatting deepfake pornography: The Battle for Digital Decency*, *Ave Maria School of Law*. Available at: https://www.avemarialaw.edu/combatting-deepfake-pornography/#:~:text=1%20However%2C%20deepfake%20pornography%20is,satisfy%20current%20revenge%20pornography%20laws. (Accessed: 25 November 2024).

'Reps. Eshoo, Lesko Introduce Bill to Combat Tech-Enabled Domestic Violence' (2023) *Eshoo.House.Gov* [Preprint]. US House. Available at: https://eshoo.house.gov/media/press-releases/reps-eshoo-lesko-introduce-bill-combat-tech-enabled-domestic-violence.

*Summary: H.R.6478 — 114th Congress (2015-2016)* (2016) *Congress.gov*. Available at: https://www.congress.gov/bill/114th-congress/house-bill/6478#:~:text=This%20bill%20amends%20the%20federal,and%20as%20a%20result%2C%20place (Accessed: 26 November 2024).

*Unauthorized publication of personal identifying information.* (2023).

Rogers, Michaela M., et al. "Technology-facilitated abuse in intimate relationships: A scoping review." *Trauma, Violence, & Abuse* 24.4 (2023): 2210-2226.

Waldstricher, Bradley. "Deeply Fake, Deeply Disturbing, Deeply Constitutional: Why the First Amendment Likely Protects the Creation of Pornographic Deepfakes." *Cardozo L. Rev.* 42 (2020): 729.