AUTOMATING HARM: FEDERAL PRIVACY FAILURES AND THE AI PRODUCTION OF IMAGE-BASED SEXUAL ABUSE

A Policy Paper

by

Taylor Michele McRho

California State University, Sacramento

May 7, 2026

Executive Summary

of

AUTOMATING HARM: FEDERAL PRIVACY FAILURES AND THE AI PRODUCTION OF IMAGE-BASED SEXUAL ABUSE

by

Taylor Michele McRho

This paper examines the history and current legislation of non-consensual pornography and image-based sexual abuse (IBSA), and how these have evolved with the evolution of artificial intelligence and deepfakes. The goal is to evaluate whether states are equipped to regulate emerging forms of AI-generated IBSA. This paper conducts a comparative policy analysis of statutes across all 50 states, as well as federal statutes and legal cases. States currently have three forms of IBSA law: traditional "revenge porn" statutes, expanded digital manipulation frameworks, and emerging AI-specific regulations.

The data of all 50 states show that most states continue to rely on intent-based dissemination-focused IBSA models that are poorly suited to address AI-generated harms, which involve anonymous creation, mass production, and decentralized distribution. While a number of states have tried to incorporate AI-specific language, significant gaps remain in regulating the creation of synthetic imagery, providing civil remedies, and assigning responsibilities to platforms and technology developers. Congress has attempted several federal policies, including the Intimate Privacy Protection Act, Stopping Harmful Image Exploitation and Limiting Distribution Act, Violence Against Women Reauthorization Act, and the Take It Down Act, but these laws continue to fall flat and demonstrate a fragmented approach that separates criminal, civil, and platform-based solutions.

In this paper, I argue that effective IBSA regulation must shift towards consent-based frameworks that explicitly criminalize the creation of AI-generated imagery, including expanding civil remedies for victims, and adopt distributed responsibility models that address the technical systems that are currently enabling harm.

Acknowledgements

Thank you to my mom, Monica, for always being there for me and providing an endless amount of love and support, late-night ramblings and all.

Thank you to my friends and family for their support, getting me out of the house for breaks, and checking on me to make sure I haven't lost my mind.

Thank you to Shane, my wonderful advisor, who has shown nothing but patience with me, evening ramblings and all.

I don't think I can put into words how much all of you, my community, means to me. I could not have done this without you.

Thank you,

Taylor McRho

Table of Contents

Introduction: From Revenge Porn to AI-Generated Abuse

Scholars and media have traditionally referred to image-based sexual abuse (IBSA) as "revenge porn," which is characterized as the dissemination of a real intimate image, often by a former intimate partner acting with malicious intent. In response to this issue, states across the United States enacted statutes primarily focused on regulating the distribution of such images, frequently requiring proof of intent to harm and an underlying expectation of privacy. While these laws addressed early forms of IBSA, they were built on the assumption that IBSA would always require an original image, which is no longer applicable in the current digital age.

The emergence of artificial intelligence has transformed the IBSA landscape by removing the need for an original image, enabling the rapid and inexpensive creation of synthetic intimate content, and facilitating mass dissemination across digital and online platforms. AI-generated deepfake pornography allows perpetrators to create highly realistic images of individuals without their consent, often targeting women, children, and LGBTQ+ individuals. Unlike traditional IBSA, the harms of AI-generated IBSA do not require a prior relationship between perpetrator and victim, an original image, or a clear intent to harm. As a result, the existing legal frameworks are inadequate.

In this paper, I examine how state and federal IBSA laws have addressed AI-generated intimate imagery and identify the policy changes needed to ensure victims are able to receive support and restitution. I use qualitative data from public legal records and statutes to compare policies across all 50 states, examining statutory language, enforcement mechanisms, and policies to assess how IBSA laws have evolved and where they still fall short. I find that while many states have begun to adapt their legal frameworks, the majority still rely on outdated, intent-based approaches that fail to capture the realities of AI-generated abuse. Furthermore,

federal efforts, including the Intimate Privacy Protection Act, Stopping Harmful Image Exploitation and Limiting Distribution Act, Violence Against Women Reauthorization Act, and Take It Down Act remain fragmented in addressing criminalization, civil remedies, and platform accountability.

Today, non-consensual intimate imagery no longer needs an original image. In January 2024, this was realized when non-consensual pornographic images of Taylor Swift were created and spread around the internet, and were viewed 45 million times in 17 hours (James, 2025). There are other examples of this, and the impacts are life-altering:

"In 2020, Breeze Liu, who had never consensually appeared in a pornographic film, was informed by a friend that videos of her were on a popular pornography website. The creator of the videos used a nude video recorded without Liu's consent to fabricate videos of her performing sex acts. As a result, Liu contemplated suicide" (James, 2025).

In 2021, the Department of Homeland Security reported that there were "over 100,000 computer-generated fake nude images of women created without their consent and knowledge" on the internet (James, 2025; Department of Homeland Security, 2021). Like with IBSA, women and girls are particularly at risk for deepfake pornography (Łabuz, 2025), with estimates that 96% of all artificial videos and images online are pornography, and up to 100% of those videos and images are of women (James, 202). One website, DeepNude, only creates images of women (James, 2025). Deepfake images are defined as "false images created using artificial intelligence that include the likenesses of real people, usually by mapping the face or body of one individual onto the face or body of another individual" (James, 2005; Suslavich, 2023). This means that any individual who has pictures on the internet is at risk of becoming a victim of nonconsensual deepfake pornography (James, 2025; Viola & Voto, 2023). This ability to create deepfake

pornography without the consent of the individual in the image and video can be used as revenge, to hurt or embarrass someone, or even to generate monetary gain.

Besides the emotional harm that is caused by deepfake pornography (Łabuz, 2025), deepfakes have the potential to erase sexual privacy and perceived autonomy (James, 2025). Kugler and Pace (2019) argue that while "deepfakes do not depict the naked bodies of the deepfake subject – only the subject's face is taken – they still impinge on sexual autonomy by repurposing the subject's identity". In this space where sexual privacy and autonomy are not guaranteed, women are viewed as objects and not individuals with the ability to make choices about how they will express their own sexuality (James, 2025).

Technology and generative artificial intelligence companies are responsible for creating an ecosystem of sexual violence... (Łabuz, 2025). An example of this is the growing number of tools and services that can create deepfakes, whether or not they were explicitly developed to do so. This means that almost anyone can quickly and at low cost create an AI-generated IBSA of another person and disseminate it to thousands of people through social media and other online platforms.

Literature Review: The Social and Legal Architecture of Image-Based Sexual Abuse

Revenge Porn and Image-Based Sexual Abuse

Non-consensual pornography can be traced back to the nineteenth century when New York-based photographer Le Grange Brown was "accused of showing and selling photographs of 'undraped women' in local saloons" (Lake, 2021). We know these picutres were not consensual because he cut and pasted the heads of young, high society women onto the images of naked women. As technology progressed, so did the dissemination of non-consensual pornography. Search engines, social networking, artificial intelligence, and other advancements

(Henry et al., 2021; Walker & Sleath, 2017; Paradiso et al., 2023), led to an increase in the prevalence and types of non-consensual pornography, including “revenge pornography” and “image-based sexual abuse” (Henry et al., 2021, pg.1).

The term revenge porn is defined as “sexually explicit images of a person posted online without that person’s consent, especially as a form of revenge or harassment” (Henry et al., 2021). Researchers coined the term in the mid-2000s due to the rise in images shared without consent, some of which were uploaded to websites (Henry et al., 2021; Walker & Sleath, 2017). While the term “revenge porn” has given a name to the act of sharing images without consent, it has some inherent issues. It infers that all forms of non-consensual sharing include some level of revenge or hatred motivation, ignores other reasons one might disseminate non-consensual intimate imagery, does not include other forms of intimate imagery abuse, places the inherent blame on the victim, conflates the term “pornography” with consensual pornography, and focuses the attention on the content of the image instead of on the abusive actions (Henry et al., 2021). Attitudes towards intimate imagery myths, such as that dissemination should be a form of flattery, are also associated with the dissemination of intimate imagery without consent (Paradiso et al., 2023). In various studies looking at the dissemination of intimate imagery, one of the primary reasons was for social rewards or individual benefits, followed by amusement, gossiping, a want to control the person in the photograph, or believing others wanted to see it (Hanson, 2022; Henry and Beard, 2024; Barrense-Dias et al., 2020, Henry et al., 2020, Clancy et al., 2020, Powell et al., 2019). Very few respondents in these studies cited revenge or hatred as a reason for wanting to disseminate the intimate imagery (Clancy et al., 2020).

Revenge porn also does not take into consideration other forms of image-based sexual abuse, such as non-consensual filming, that can be perpetuated by either people the victim

knows or by unknown individuals (Henry et al., 2021). Common forms of this include “upskirting” (taking an image up someone’s skirt), “downblousing” (taking an image down someone’s shirt), blackmail, sextortion (Henry et al., 2021; McGlynn & Rackley, 2017; McGlynn, Rackley, & Houghton, 2017; Powell & Henry, 2017; Powell, Henry, & Flynn, 2018, Paradiso et al., 2022), or sexualized photoshopping (Paradiso et al., 2022). These forms of non-consensual intimate imagery do not fall into the “revenge porn” definition because they do not necessarily meet the benchmark for being done out of revenge or hate. Abuse does not necessarily need to come from a place of revenge, but can rather be from a place of power, control, or just because it benefits the individual.

Since he term “revenge porn” is a narrow term that does not include other forms of abuse (Henry et al., 2021),the term “image-based sexual abuse” (IBSA) broadens the scope of the harm being done to include not only non-consensual intimate imagery in the case of revenge or hatred, but also the collection and dissemination of imagery in the cases of social rewards, individual benefits, amusement, and control. IBSA makes it clear that any form of non-consensual intimate imagery is a form of abuse that can impact the life of an individual. As such, IBSA will is defined as “the taking, sharing, creating, pressuring, coercing, and threatening of non-consensual intimate images” (Henry et al., 2021; Henry & Beard, 2024; Henry & Flynn, 2019; Powell et al., 2018; Paradiso et al., 2023; Karasavva & Forth, 2021).

Two forms of IBSA exist in online material.[1] The first kind of IBSA is when images are distributed onto public sites, where harassment and humiliation of the victim take place (Henry & Flynn, 2019; Fernet et al., 2019). Researchers consider these sites as public shaming sites, and

[1] Other studies, such as Fernet et al., 2019, list different types of IBSA, but they all fall under the two general classifications listed below.

fall under the conventional definition of "revenge porn" more than IBSA because the images posted are often ex-lovers for the purposes of vengeance, relationship violence, stalking, control, abuse, or humiliation (Henry & Flynn, 2019). Victims and survivors often become aware of images posted onto public shaming sites because they often find the image themselves, or someone in their extended social network might alert them to it (Henry & Flynn, 2019). The second category of IBSA involves sharing images on private sharing sites, including image boards, community forums, and less viable online communities (Henry & Flynn, 2019). IBSA disseminated to private sharing sites is less linked to revenge, but instead linked to a desire for peer bonding and esteem building with other like-minded peers who use sexual objectification and humiliation as an instrument for sexual gratification and status building (Henry & Flynn, 2019). Victims and survivors are less likely to find out that their image has been disseminated when perpetrators use these types of private sharing sites (Henry & Flynn, 2019).

There is a common thread between both public and private sharing sites, and that is that users across both sites were interested in shaming and humiliating women through misogynistic internet objectification (Nussbaum, 2010; Henry & Flynn, 2019). This objectification is fueled by a form of "ressentiment" that is projected onto "blameworthy" and "gendered" others that they believe are the objects of governance and regulation (Foucault, 1990; Nussbaum, 2010; Henry & Flynn, 2019).

Feminist Theory and Gendered Harm

Gender and IBSA are fundamentally intertwined, as IBSA is predominantly used to harm women (Fernet et al., 2019). The gender dynamics that both men and women engage in are "shaped and governed by culturally constructed norms, conventions, and power relations that are highly regulatory and reiterative" (Henry & Flynn, 2019). Heteronormative gender beliefs serve

to legitimize patriarchal behavior and male dominance, which often upholds the idea of violence against women (Connell & Messerschmidt, 2005; Henry & Flynn, 2019), in addition to men feeling a sense of entitlement over women's bodies (Hargreaves, 2018; Henry & Flynn, 2019). Men who participate in IBSA have a belief that they are entitled to access to women's bodies against their will with impunity, legitimizing the systematic tolerance of sexual violence against women (Tran, 2015; Henry & Flynn, 2019). This belief that some men have about women is why women are more vulnerable to IBSA violence (Chan, 2011; Sinha, 2013; Fernet et al., 2019).

Victimization, Perpetration, Motives, and Prevalence

Although IBSA can impact anyone, clear trends emerge regarding which populations are disproportionately victimized and the frequency at which these harms occur. A 2016 study by Lenhart, Ybarra, and Price-Feeney found that one in 25 Americans who are active online had someone threaten to post or did post their nude image or nearly nude image without their consent (Lenhart, Ybarra, and Price-Feeney, 2016, pg.4). However, the issue with this study is it only considered motivations fueled by embarrassing or harming the victim (Ruvalcaba & Eaton, 2020). As previously discussed, only including non-consensual intimate imagery disseminated from a want to embarrass or harm does not fully capture the scope of IBSA (Henry et al., 2021; Paradiso et al., 2023; Hanson, 2022; Henry and Beard, 2024; Barrense-Dias et al., 2020; Clancy et al., 2020; Powell et al., 2019). When using the definition of IBSA, studies have found that women are more likely to be victims than men (Branch et al., 2017; Henry et al., 2017; Lenhart et al., 2016) , and IBSA perpetrators are more likely to be men (Branch et al., 2017).

In the study conducted by Ruvalcaba and Eaton (2020), out of 3,044 participants in the United States, 53.8% were female, with 9.21% reporting IBSA victimization, and men reported a

victimization rate of 6.61%. The majority of victimization took place between the ages of 18 and 29 for the victim, with a mean age of 25.99 (Ruvalcaba & Eaton, 2020). When factoring in sexuality, bisexual men (17.19%) and bisexual women (12.82%) have the highest victimization rates, but it should be noted that the sample size for lesbian women, gay men, bisexual women, and bisexual men was relatively small compared to the sample size of heterosexual men and women (Ruvalcaba & Eaton, 2020). When looking at perpetuation, women are often less likely than men to disseminate non-consensual intimate imagery (Ruvalcaba & Eaton, 2020).

Methods and Limitations:

In this study I use primary sources, legal and doctrinal analyses, and descriptive qualitative content analysis. I primarily used C.A. Goldberg's "Revenge Porn Laws: State by State" tracker to see which states had some form of regulation on the books. Once I identified the statutes, I checked whether any bills had failed or whether any recent legislative amendments were available to include in the results. This created a state-by-state qualitative comparative analysis of IBSA statutes across all 50 states, which is included in Table 1 in the Appendix. Table 1 includes statutory language, definitions, and enforcement mechanisms. I subsequently categorized each state's approach by key features, including intent requirements, civil remedies, AI coverage, and responsibility structures. Beyond the IBSA statutes listed in Table 1, I have also included background information on foundational legal cases and federal statutes to provide the legal context for regulating AI-generated IBSA.

There are limitations to this study. One challenge I encountered in data collection was that information on this subject is often decentralized. The second challenge in data collection is the speed at which both technology and the regulatory environment changed over the course of

this paper. There is always the possibility that any analysis of a state mentioned has become outdated by the time this paper is written. Additionally, each state, federal law, and legal case needs to be reviewed in the context of the time it was decided and the existing laws that may have influenced the decision. For example, a law in California cannot be evaluated on the same basis as laws in Texas because the social norms and legislative history differ between the two states.

In addition to the limitations, it should be noted that I was the only one reading the statutes and deciding whether they lend themselves to AI-generated IBSA laws, meaning there is potential for personal subjectivity. The interpretation of state statutes, intent, and scope comes from my personal experience working in California. However, as mentioned above, each state is unique in how they handle legislation and legal interpretation.

Results: The Fragmented Landscape of Image-Based Sexual Abuse Law

Legal Remedy

Prior to the introduction of the Intimate Privacy Protection Act (IPPA), the only legal remedy for victims of non-consensual pornography was civil litigation by citing a "tort remedy of breach of confidentiality, intentional or reckless infliction of emotional distress, the privacy tort of public disclosure of private facts, and the copyright law as avenues of redress for the wrongs committed against them" (Mitchell, 2019, p.581). This is an issue for victims because it creates a disparity between those who have the resources to seek legal help and those who do not. While there are issues with the state failing marginalized communities when they are harmed (such as whom the state takes seriously or who it lends more power to), there needs to be an avenue for individuals to seek redress, regardless of their financial well-being.

Federal Legislation

Intimate Privacy Protection Act of 2016

The Intimate Privacy Protection Act (IPPA) was introduced by California Congresswoman Jackie Speier in 2016 with the goal of criminalizing the unlawful and knowing distribution of photographs, film, or video of a nude depicted individual or an individual engaging in sexually explicit acts (Mitchell, 2019). The IPPA was created and modeled after increasing concern over traditional revenge porn, gaps in state-by-state laws, and a lack of federal protection. At the time, there was no federal law directly addressing IBSA, and state laws were inconsistent, lacked civil remedies, and made enforcement regarding interstate distribution difficult.

The original 2016 version of the IPPA created a federal criminal offense for disseminating IBSA, standardized IBSA-related definitions across states, and addressed interstate image distribution. This was done through its core provisions, which criminalized the nonconsensual dissemination of intimate images and required a lack of consent, expectation of privacy, and intent to harm. However, the 2016 version of the IPPA failed and was later reintroduced in 2019. The 2019 version of the IPPA improved the original definitions of consent and intimate images and expanded the coverage of digital distribution and online platforms. However, the 2019 version still primarily focused on real images and did not address deepfakes and AI-generated content. The 2019 version also did not pass through the legislature. Both the 2016 and 2019 versions of the IPPA faced pushback over First Amendment concerns, intent-versus-consent requirements, federal-versus-state authority, and rapid technological change. Regarding the First Amendment, opponents such as the American Civil Liberties Union argued that the IPPA could be used to criminalize protected speech and had a lack of clear limits. The

intent-versus-consent issue arose because the IPPA required an intent to harm, and some proponents of the bill wanted to remove that requirement. This created tension between enforceability and constitutionality. The federal-versus-state issue was primarily due to some lawmakers questioning whether IBSA should be handled at the state level and whether federal law was duplicating existing statutes and creating jurisdictional conflicts. Lastly, rapid technological changes also created issues for the passage of the IBSA because, as AI and deepfakes emerged, the earlier versions of the IPPA became outdated, and lawmakers struggled to future-proof the bill and define synthetic imagery in a way that would stand the test of time. The repeated failure of the IPPA illustrates the difficulty of establishing a federal criminal framework for IBSA that balances both First Amendment concerns with evolving technological harms, particularly in the context of AI-generated imagery.

Stopping Harmful Image Exploitation and Limiting Distribution Act (SHIELD) of 2019

Lawmakers introduced the SHIELD Act in YEAR. It was designed to create uniform federal baselines, cover interstate and online distribution, and close enforcement gaps where state jurisdiction is weak. The core provisions of the SHIELD Act included creating a federal crime for the nonconsensual disclosure or dissemination of an intimate image of a person who had a reasonable expectation of privacy. Additionally, the SHIELD Act also targets threats and coercion to use intimate images, which are defined as images including nudity, sexual activity, and images where a person is identifiable. The language of the bill requires a lack of consent and either knowledge or reckless disregard of that lack of consent, meaning the SHIELD Act is a modern version of strict “intent to harm” laws, but is still not a pure, strict-liability law. Similar to the IPPA, the SHIELD Law is centered on dissemination rather than creation. Senator

Klobuchar, one of the authors of the Act, noted that the purpose of the bill is to "provide victims of online abuse with the legal protection they deserve, and to hold their exploiters accountable".

While the SHIELD Act was aimed at closing loopholes in IBSA, it had limitations that may explain why it was never passed and signed into law. One of these limitations is that the Act would not have stood the test of time because it did not cover AI-generated deepfakes or synthetic images. The second limitation is that it targeted only the dissemination or the threat of dissemination, not the creation of deepfakes or the production of AI-generated intimate images. Third, the SHIELD Act was a criminal provision only and did not include any mechanism for private lawsuits, damages, or injunctions for victims. Lastly, the Act raised First Amendment issues due to the risk of overbreadth and the need for a more narrow tailoring of the definitions While the SHIELD Act represents an early federal attempt to criminalize nonconsensual intimate image distribution, its focus on dissemination and lack of explicit AI coverage illustrate the limitations of traditional legal frameworks in addressing emerging forms of IBSA.

Violence Against Women Reauthorization Act of 2022

In 2022, the Violence Against Women Reauthorization Act (VAWRA) included the first federal law allowing an individual to file a federal lawsuit against another individual for disclosing intimate images without the individual's consent, known as the Intimate Imagery and Privacy Protection Act (IIPPA) (Ballotpedia, n.d.). This law allows the depicted individual to bring a civil claim in federal court for up to $150,000. Additionally, the courts are authorized to provide other forms of legal relief, such as temporary restraining orders, preliminary injunctions, or permanent injunctions (American Bar Association, 2022). What this law means for victims of IBSA is that they can file a lawsuit against the person who disseminated intimate images, regardless of their state's laws. This marked a significant shift in federal response to IBSA

regulation. Prior to 2022, IBSA protection depended entirely on state law, which meant uneven regulations for victims of IBSA.

The language used in the VAWRA also created federal definitions for terms such as "intimate visual depiction", "consent", "depicted individual", and "disclosure/" Creating federal definitions helps standardize how IBSA is understood not only within the federal government but also across states. One of the most important definitions is consent, which the VAWRA notes that consent to take an intimate image does not mean consent to distribute it. This closed a common defense often used in IBSA cases. VAWRA's language also covers internet-based and interstate harm, meaning that the law applies when dissemination occurs using the internet and across state lines through any interstate communication system. This includes social media, messaging apps, and websites.

While the VAWRA created civil remedies for victims, it has limitations; most glaringly, it does not federally criminalize IBSA. Instead, it provides only civil remedies for victims, leaving criminal prosecution to state discretion. While every state does have some form of criminal statute regarding IBSA, successful prosecution and investigation vary by state. Even if a state criminalizes an action, that does not mean it takes the action and the victims seriously. Another issue with the VAWRA is that it focuses only on dissemination, not creation, meaning the creation of IBSA (including deepfakes and AI-generated images) is not explicitly illegal. Lastly, VAWRA does not explicitly address AI-generated images or deepfakes; instead, it primarily focuses on traditional, real-image-based IBSA.

Take It Down Act

Senator Ted Cruz introduced the Take It Down Act in January 2025 with the goal of fixing the issue of intimate images remaining online even when IBSA is illegal. Victims can still

struggle with getting non-consensual content removed from pornography sites, social media, and anonymous platforms, even when criminal laws have punished the individuals who disseminate the image. At the time, lawmakers were noticing a gap between image removal and criminal enforcement, and AI-generated deepfakes were increasing in volume, becoming harder to track, yet easier to spread. Due to this shift in the issue of IBSA image removal, the policy focus shifted from punishment to removal and prevention. The Take It Down Act's policy goal was to create a federal takedown requirement for nonconsensual intimate images. This is evident in the Act's core provision, which focuses on platform responsibility rather than individual wrongdoing. The Act requires platforms to provide a way for victims of both traditional IBSA and AI-generated images and deepfakes to report such images and have the content removed within a specified timeframe. The Act's model is similar to copyright takedown systems and content moderation rules, in which victims must submit a request along with proof of identity and harm. Companies that fail to comply can receive regulatory penalties and enforcement actions.

The role of the Act in relation to VAWRA and the IPPA is that while VAWRA provides civil remedies and the IPPA attempted to focus on criminalization, but not platform responsibility, the Act carved out new obligations within its framework to bridge an enforcement gap and meet the rapid growth and mass distribution of AI-generated IBSA and deepfakes. Additionally, the Act prioritizes the speed of content removal over mere legal punishment. However, the Act is not perfect and still has its issues. Mary Anne Franks, President of the Cyber Civil Rights Initiative (CCRI), noted in a statement that the Act's takedown provision is highly susceptible to misuse and could be counterproductive for victims (Franks, 2025). One specific provision that CCRI's notes identifies is the following exception to the Act: "a person who possesses or publishes an intimate visual depiction of himself or herself". This exception could

create a loophole that would allow a person to disseminate intimate images without consent as long as that person also appears in the image (Franks, 2025). Additionally, the CCRI noted concerns with the "constitutionality, efficacy, and potential misuse" of the Act's notice and removal provision because the language of the provision is unlikely to accomplish the goals of the Act and could likely be selective and improperly misused for political or ideological purposes that endanger communities most affected by IBSA (Franks, 2025). Specifically, the language in that provision is vague and overbroad, making it difficult for individuals and platforms to understand which conduct is prohibited. The broad language could also risk bad-faith reports and protected speech. For example, the notice-and-removal provision was modeled after the Digital Millennium Copyright Act (DMCA) but did not include any of the DMCA's safeguards against false or malicious reports (Franks, 2025). CCRI notes that there could be instances in which individuals and organizations inundate platforms with notice-and-takedown requests about explicit content simply because they morally disapprove of it, rather than because it is IBSA.

While the CCRI notes several other issues with the Act, one important critique is that it can give victims false hope by presenting the removal provision as a guarantee that the image will be removed within 48 hours. Due to the language of the law and the broad enforcement discretion given to the Federal Trade Commission, the chances of victims seeing redress are slim. If platforms are flooded with false reports, authentic complaints can be drowned out, preventing the platform from operating. While the Act improves victim protection through rapid takedown mechanisms and addresses a critical gap in IBSA enforcement, it also raises significant concerns about free speech, due process, platform burden, and the failure to regulate the rapid creation and dissemination of AI-generated IBSA.

The Big, Beautiful Bill (H.R.1.)

On May 22, 2025, Congress passed H.R.1. which, among other things, covered taxes and immigration. However, the original version included §43201, which prohibited any state from regulating artificial intelligence for the next 10 years (Hou, 2025). While this portion of H.R.1. was fully removed in July of 2025, the original goal of §43201 was to support the growth of artificial intelligence by creating a singular set of national rules. In addition to accelerating innovation, proponents of this provision argued that it will "help businesses save time and money by avoiding the need to comply with different laws in every state" and create a shift toward centralized federal oversight for artificial intelligence. This is important because, currently, each state has different regulations governing artificial intelligence companies, which can create inconsistent and contradictory rules across the country. It's important to note that a week before the passage of H.R.1, the National Governors Association held a discussion regarding the ongoing legal and regulatory challenges surrounding artificial intelligence. Critics of §43201. argued that as artificial intelligence has continued to advance at a high pace, ethical concerns and user safety have taken a back seat. Local regulations are a way to ensure that artificial intelligence companies follow rules regarding important user safeguards.

It's important to note that §43201 did not include any regulation regarding the creation or dissemination of AI-generated IBSA and could have impeded any future legislation that states may introduce to regulate it.

Data Analysis: From Individual Liability to System Responsibility

Table 1, included in the Appendix, provides each state's existing statute, attempted regulation, and court case. From there, if there was successful regulation, bill numbers and years are listed. Next, the target population is either noted as "perpetrator" (meaning person who disseminated the image) or "depicted individual" (meaning the statute is aimed at providing a

remedy for the victim). The next column defines what IBSA means in each state for the specific statute. The last column is an analysis of whether the current statute lends itself to AI-generated IBSA regulation, and if not, how far away the state is from implementing it. Looking at data from all 50 states and their current legislation, some trends emerge regarding the development of legislation, access to civil remedies for victims, and the scope of the statute.

Legislation

When looking at current statutes and legislation, the first category that emerges is states with some level of IBSA legislation, but far from having strong AI-generated IBSA statutes. These states have statutes in which the current framework is built around harassment, voyeurism, or older privacy concepts rather than modern, consent-based IBSA models. These models could be amended to include AI-generated IBSA, but the statutes would also require additional structural amendments to be fully applicable in the modern day. Some examples of these states include Alaska, Iowa, Massachusetts, Montana, and Wisconsin. Alaska and Iowa's laws are essentially harassment statutes that focus on digital conduct, rather than statutes that address identity consent, permanence, and IBSA. Massachusetts' law remains rooted in a voyeurism-and-unlawfully-obtained-image framework, which is too narrow for an AI-generated IBSA statute because synthetic images do not require an original image. Montana and Wisconsin are closer to where they need to be to enact AI-generated IBSA laws because their statutes are more closely aligned with privacy-in-communications laws, but they still have a voyeurism workaround that can hinder AI-IBSA laws.

The second category is that states that do not yet have AI-generated IBSA laws are primed to add them. This means that they already have robust IBSA laws, and adding an amendment to include AI-generated IBSA would be relatively simple (such as updating

definitions rather than redesigning the whole statute). Some examples of these states include Alabama, Arizona, Connecticut, Delaware, Florida, Kentucky, Maine, Michigan, Mississippi, Missouri, Nebraska, Nevada, New Mexico, Vermont, West Virginia, and Wyoming. A majority of these states already have the core pieces of modern IBSA regulation, including a recognizable victim, lack of consent, expectation of privacy, and dissemination of sexual images. However, the problem with these statutes is that they still operate on real, original images or require a traditional intent-to-harm narrative. To bring these states up to the level at which AI-generated IBSA could be enforced, terms such as synthetic image, computer-generated depiction, digitally altered image, or artificially generated intimate image need to be added. These terms would ensure that AI-generated intimate images could also be regulated in the same way as traditional "original image" IBSA is. In this category, some standout states include Florida, Arizona, and Kentucky. Florida currently has a functioning sexual cyber harassment law that includes civil relief. While Florida did have a bill specifically aimed at AI-generated IBSA that died in committee, it shows that the legislature has identified this as an issue and is primed to consider it. Arizona is similar to Florida, where they have statutes that criminalize traditional IBSA, but there is ongoing legislative efforts to criminalize synthetic depictions and online publishers. Kentucky is a unique state where they have a traditional IBSA law, but they also have a takedown-style mechanism for website operators that includes civil remedies tied to the nonremovable of images.

The third category is states that already have AI-generated or inclusive IBSA statutes, which can be separated into two groups: states that have explicitly regulated AI-IBSA and states that regulate digitally altered images, but do not specifically call out AI-generated IBSA. The first group is strongest, and they have already moved beyond the traditional IBSA laws that

explicitly regulate deepfakes, synthetic depictions, computer-generated images, and digitized depictions. Some examples of these states include Arkansas, Idaho, Illinois, Kansas, Louisiana, Maryland, and Minnesota. Arkansas, in particular, has one of the strongest AI-generated IBSA statutes because it criminalizes the creation or distribution of AI-generated IBSA, such as deepfake visual material, and gives victims the ability to seek a civil cause of action against both the creator of the IBSA and technology providers. Idaho, Illinois, and Maryland all created separate statutes for explicit synthetic media and sexually explicit digitized depictions. Like Idaho, Illinois, and Maryland, Louisiana has a separate AI-generated IBSA statute, but they also have an additional statute that criminalizes the dissemination or sale of AI-generated IBSA. Maryland is another state with a notable AI-generated IBSA statute because its definition of visual representation includes computer-generated images, so any AI-generated images are already covered by its Criminal Law section. The second group of states is those with functionally AI-ready statutes, but the language does not specifically call out AI-generated IBSA. Instead, statutory language usually covers digitally altered, computer-generated, synthetic, fake, or intimate digital depictions. These terms can provide lawmakers and courts with a clear path for applying their laws to AI-generated imagery; however, these states can also benefit from definitional clarification to ensure they cover AI-generated IBSA. These states include California (civil law), Colorado, Georgia, Hawaii, Indiana, New Hampshire, New Jersey, New York, North Carolina, Pennsylvania, Rhode Island, South Carolina, Tennessee, Utah, Virginia, and Washington.

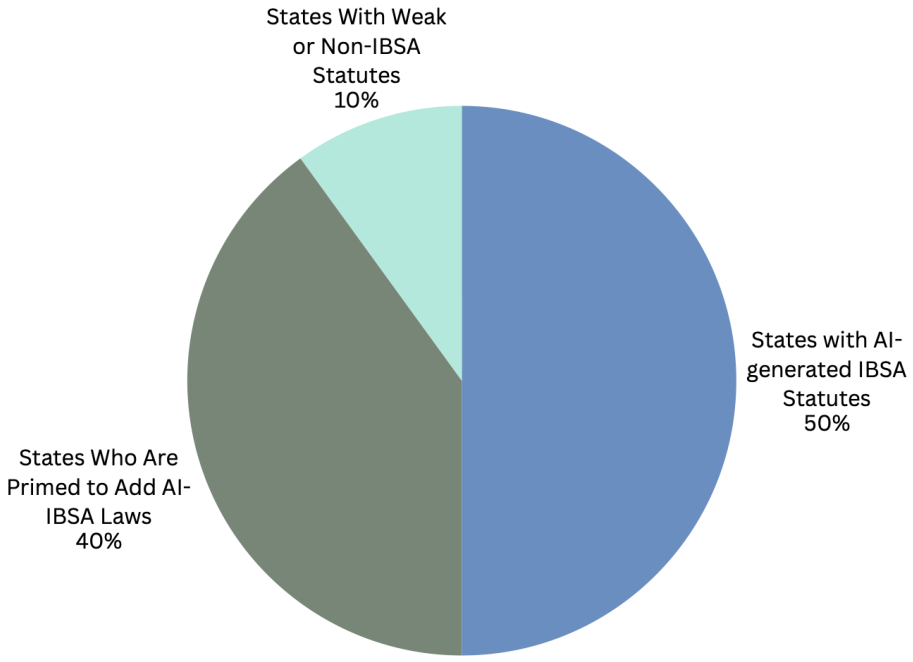

Figure 1: Distribution of Legislation

Access to Civil Remedies

When looking at states that include civil remedy statutes, what is important is that the language allows victims to seek injunctions, damages, or take-down related relief. Currently, 18 states have civil remedy statutes, and 32 do not. States with strong civil remedies include Arkansas, California, Delaware, Florida, Illinois, Indiana, Kentucky, Maryland, Minnesota, Missouri, Nebraska, New Jersey, Pennsylvania, Tennessee, Vermont, and Virginia. These states allow victims to sue perpetrators, seek damages, request injunctions, force the removal of images (in some cases), and recover attorneys' fees (in some cases). Unique states in this area include Arkansas, California, Delaware, Illinois, Minnesota, and Kentucky. Arkansas' civil law is unique because the victim can seek damages not only from the creator, but also from the developer or provider of the underlying image-generation technology if safeguards were missing. California's civil statute allows a victim to seek relief for altered or synthetic material. Delaware and Illinois

both have strong tracks for civil remedies that extend to AI-generated imagery. Minnesota is another state with a unique civil statute that provides parallel civil remedies for both real-image and AI-generated IBSA. Lastly, Kentucky not only addresses the act of disseminating AI-generated IBSA but also allows civil remedies that address the failure to remove sexually explicit images from websites. This model gives victims a targeted post-distribution remedy. However, just because a state has a mechanism for civil remedies does not mean the state relies primarily on prosecutors. 32 out of 50 states (64%) require a police report, prosecutor discretion, and a criminal case. This means that victims cannot act directly when they experience IBSA.

Civil remedies are an important component in ensuring that victims of IBSA can seek relief. However, AI statutes are growing faster than civil remedies, and while many states may criminalize deepfakes, they do not allow victims to sue. This creates gaps in enforcement, takedown, and compensation. Additionally, states with some form of civil remedy do not always include language allowing the victim to have their image removed. While civil remedies might already include this alongside financial compensation, there must be explicit language that allows victims to ensure that images of them are not public without their consent.

Language

IBSA statutory language falls into three categories. The first category is language that created classic "revenge porn" laws that existed before AI and deepfakes became common and focused on the distribution of real intimate images with the intent to harm, harass, intimidate, or coerce (such as an ex-partner sharing a real image). These laws were often in response to cases such as Hunter Moore v. the U.S. District Court for the Central District of California and FTC v. Craig Brittain. These laws tended to be easier to pass politically due to the intent-to-harm clause, but they are narrower and harder to enforce against AI-generated IBSA because they assume a

real image existed and had an expectation of privacy, someone disseminated the image with malicious intent, a traditional privacy breach occurred, and the victim suffered emotional distress. As such, the language of these laws often includes terms such as “image obtained under circumstances of privacy”, “photograph of another person”, or “captured image”. The reason this legislative model struggles with AI-generated IBSA is that with AI-generated imagery, no real image existed, there was no original breach of privacy, and the harm may occur without malicious intent (such as being done as a joke, anonymously, for sexual gratification, or for profit). Additionally, these laws criminalize only sharing, posting, and distributing, not creating, generating, or possessing. With these statutes, someone could technically create a large number of AI deepfakes, keep them, and send them privately. States with this form of language include Alabama, Arizona, California, Connecticut, Florida, Kentucky, Maine, Michigan, and Vermont. These states are the most vulnerable to AI abuse and make it harder to prosecute deepfakes and protect victims.

The second language category includes broader consent-based or digitally altered image frameworks that extend beyond real photos but do not yet fully regulate AI-generated imagery. These laws usually cover digitally altered images, false or manipulated depictions, still require distribution and an intent to harm, do not regulate creation, and do not mention AI explicitly. The terms used in this form of language include intimate digital depiction, digitized depiction, visual representation, or falsely created image. These terms cover Photoshop edits, face swaps, and partial deepfakes, but may not fully cover AI-generated images. These terms can reduce the amount of future legislative work needed, but they may still not recognize AI-generated IBSA as a distinct problem requiring specific statutory language. Additionally, these laws remain dissemination-focused and intent-based, meaning they cover only the distribution, publication, or

posting of images with the intent to harass, harm, or intimidate. This means these laws do not cover the creation, generation, or possession of AI-generated IBSA for other purposes, such as content created as a joke, for sexual gratification, or for profit. Like with the first category of classic revenge porn laws, individuals could technically create a deepfake and keep it private. For this classification of language to meet the needs of modern AI-IBSA laws, they would need to add civil remedies, terms like "computer-generated" or "synthetic depiction" and remove the intent requirement. States with this form of language include Colorado, Delaware, Georgia, Illinois, Indiana, Maryland, New Hampshire, New Jersey, New York, and North Carolina.

The third language category includes the direct regulation of deepfakes or AI-generated intimate imagery. These statutes are no longer updating older "revenge porn" statutes but instead are beginning to treat AI-generated abuse as a distinct problem that requires specific statutory language. This can be seen by the use of language such as "AI-generated images", "deepfakes", "synthetic media", and "computer-generated depictions". These terms remove ambiguity from civil and criminal cases by ensuring that courts do not have to interpret whether AI-generated IBSA is included in the statute. This form of language also allows for more than the criminalization of sharing. It also includes the criminalization of creation, generation, possession, and distribution. This means an individual can be held liable, even if they never posted, distributed, or shared the image, reflecting that the harm begins at creation, not just dissemination. Additionally, this kind of language focuses more on the lack of consent rather than an intent to harm, recognizing that harm extends beyond emotional distress and can extend into economic and psychological harms and sexual exploitation. One of the benefits of this form of language is that it recognizes that AI depictions of an individual do not need to be perfect but only believable. This consent and "believable image"-based structure allows victims to seek civil

remedies, hold platforms or developers liable, and issue takedown requests outside of the DMCA process. This form of language will most likely prove adaptable to new technology, less reliant on intent, provide broader protection for victims, continue to recognize AI-specific harms, and address the creation and distribution of images. These states include Arkansas, Idaho, Illinois, Louisiana, Maryland, Minnesota, and Tennessee.

While there has been headway on regulatory language regarding AI-generated IBSA, there are still a few key areas that could be improved across the board. Regulatory language, whether civil or criminal, still needs to completely remove intent requirements. As long as the law requires some level of intent, the burden falls onto the victim to prove the motive of the disseminator, even if there is no clear one. This can lead to gaps in enforcement and allow for users to continue creating and disseminating AI-generated IBSA. In this same vein, there needs to be stronger regulation of platforms. This regulation could look like ensuring that AI companies include coding language that prevents AI-generated IBSA images from even being created. Of course, there will always be outlier cases where an individual knows how to work the system to circumvent these safeguards, but what matters is that AI companies demonstrate their commitment to ending this issue by preventing the creation of these images. Lastly, while many states include a path for civil remedies, this needs to be consistent across the country so that anyone whose image is disseminated without their consent can seek both criminal and civil liability. Any civil law also needs to extend to AI companies that violate regulations. Many states are in a “hybrid” phase of legislative development, where they have real-image, revenge-porn statutes codified but are expanding traditional laws to cover altered and digitized images and plan to add AI- and deepfake-specific statutes later. This creates layered and inconsistent legal frameworks that make it hard to enforce any regulation. However, when looking at the language

across the United States, the data show that states are largely moving beyond traditional real-image, revenge-porn laws and are rapidly transitioning their regulatory frameworks to address altered and digitized image coverage and AI- and deepfake-specific statutes. Only a small minority of states remain structurally outdated.

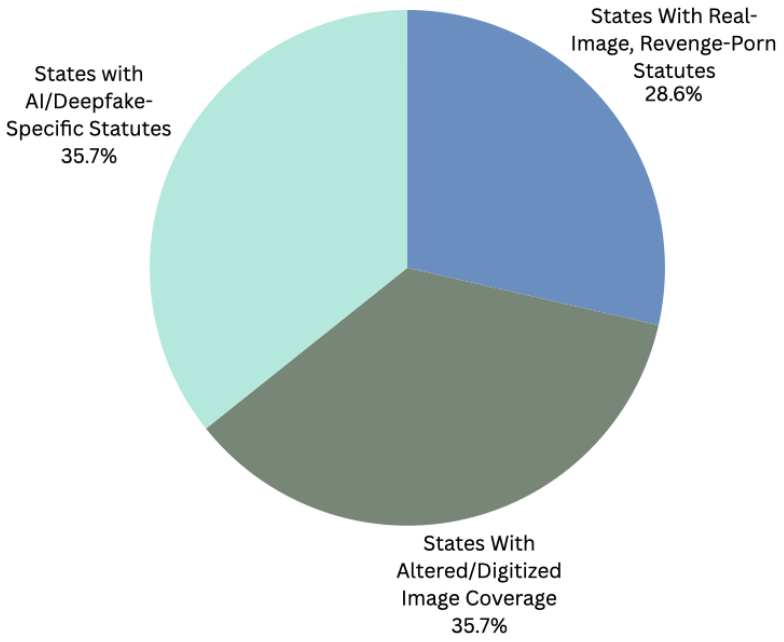

Figure 2[2]: Distribution of states with different kinds of language, taking into consideration that a state can have two different forms of language.

Regulatory Responsibility

Another way to analyze and evaluate a state's laws regarding AI-generated IBSA is to consider whether the statute includes an intent-to-harm requirement and who bears responsibility when someone is the victim of AI-generated IBSA. Intent-to-harm requirements were first introduced through harassment and stalking laws, but they quickly found their way into IBSA

[2] It should be noted that some states can have two different forms of language, and these categories are not mutually exclusive. For example, a state many have an older revenge porn law and a separate newer deepfake law.

laws to address First Amendment concerns, since sharing images is a form of free speech and courts tend to be wary of laws that restrict speech. Originally, IBSA was a form of harassment and was born from the prevalent stalking and cyberbullying that victims experienced, which did have an intent to harass, threaten, and cause distress. Intent-to-harm requirements allowed for IBSA laws to pass while also meeting the strict scrutiny of the courts by ensuring the laws were narrow, targeted, and did not criminalize protected expression. Additionally, lawmakers could argue that they are not banning speech but rather abusive conduct, as the common story at the time was one where an ex-partner posted intimate images to get revenge. Ultimately, the intent-to-harm requirement allowed IBSA laws to pass without groups like the ACLU raising concerns or blocking legislation. However, with the cases of Hunter Moore v. U.S. District Court for the Central District of California and the Federal Trade Commission v. Craig Brittain, along with the development of AI-generated IBSA, the intent-to-harm requirements quickly became a roadblock in expanding IBSA laws and combating deepfakes. Currently, 34 states have some form of an intent to harm, harass, intimidate, coerce, or cause emotional distress requirement, while 16 states do not. States that do not have an intent-to-harm requirement focus their statutory language on consent, knowledge, or recklessness standards, strict liability, and AI-specific statutes that remove the requirement of motive. When looking at the intent-to-harm requirement, along with the kind of statutory language, traditional revenge porn laws are more likely to require an intent-to-harm, while updated AI/deepfake-specific statutes are less likely to require an intent-to-harm due to the nature of the act itself.

When looking at regulatory responsibility, it could be understood in three phases. The first is individual responsibility, which focuses on the person who posts or distributes the image and is liable. This phase is often seen in criminal law and focuses on individual punishment. The

second phase is victim and perpetrator, along with limited intermediaries, which still focuses on the disseminator but begins to recognize websites, publishers, and hosting services. In this phase, the outcome remains reactive, but responsibility begins to expand. The third phase is distributed responsibility, which includes the creator, distributor, platform, AI developer, and hosting service. In this phase, the responsibility is system-wide, allowing victims to hold several actors liable. AI changed the scope of responsibility by altering how states thought about and regulated IBSA. As mentioned before, traditional IBSA statutes assumed a one-person, one-image, one-victim model. However, AI has created a model in which a single tool can mass-produce thousands of images, the creators of those images are anonymous, and the distribution is decentralized. In this instance, the harm is not caused by a single person taking a non-consensual photo – it is enabled and created by systems, even when no actual relationship between the perpetrator and victim exists. In this instance, punishing a single individual does not stop the harm created by AI-generated IBSA. Once a victim realizes a non-consensual picture has been created, it has often been spread throughout a social media platform and cannot be easily contained. This is not to say that non-consensual real photos cannot be spread with ease (as seen on Hunter Moore's website, IsAnyoneUp?), but modern-day technology has made mass dissemination easier. This is where the regulatory responsibility on AI companies and platforms comes in. If an AI platform were required to prevent the creation of an image, it would also prevent its dissemination. Additionally, required platform moderation and take-down notices would allow victims to prevent mass dissemination of non-consensual images. Currently, only Arkansas, Kentucky, and Arizona have full phase three, distributed responsibility statutes. Tennessee is moving toward system-level responsibility and has broader regulation of digital depictions, but it is not as explicit as the states mentioned. Most states are either still in phase one

(individual responsibility) or in phase two (expanded individual responsibility). This creates a regulatory gap where AI tools are largely unregulated, platforms are lightly regulated, and developers are almost never regulated. While many states have begun to recognize AI-generated IBSA in their statutory language, only a small number have moved toward creating distribution regulations by including a distributed responsibility model that requires not only disseminators but also the technology companies and systems to be held accountable for enabling harms caused by AI-generated IBSA.

Policy Implications: Closing the AI Governance Gap

As technology continues to advance and states update existing statutes, several policy considerations should be taken into account.

Intent-to-harm

The first of these policy considerations is to remove any requirements to remove any intent to harm, harass, intimidate, or cause distress from statutes. As mentioned in the data analysis section, intent-to-harm requirements are outdated and were often included in traditional real-image IBSA laws because they made the laws politically feasible and prevented large stakeholders from advocating against them. However, in a world where a real image doesn't need to exist for a non-consensual image to be created, intent to harm may not exist. Individuals who create AI-generated IBSA may do it out of sexual gratification, as a joke, for profit, or for use in pornography markets.

For states to ensure that victims of AI-generated IBSA can seek both criminal and civil liability, the intent-to-harm requirement needs to be removed. This would make prosecution and civil liability easier to achieve. Additionally, states should move towards a "lack of consent" model, which will give victims and prosecutors broad authority to enforce AI-generated IBSA

statutes. The combination of removing intent-to-harm requirements and adopting consent-based models will allow states to keep pace with the advancements in AI deepfakes. Regardless of the disseminator's intent, laws should criminalize the nonconsensual creation, possession, and dissemination of both intimate images and AI-generated IBSA to protect the potential victims

Expanding Civil Remedies for Victims

Currently, only 18 states offer mechanisms for civil remedies associated with IBSA, and most rely solely on criminal enforcement. While criminal enforcement is a crucial piece of AI-generated IBSA regulation, victims cannot be made whole without a civil component. For states to ensure that victims can obtain compensation for harms caused by AI-generated IBSA, the statutes need to include a private right of action, injunctions, takedown mechanisms, and damages. An important yet overlooked component of this is rapid takedown mechanisms. While some states do allow a claim for civil liability, not every one includes specific language allowing the victim to request that the image be removed from a website and destroyed by the creator. Without this mechanism, websites like "IsAnyoneUp" are not necessarily required to remove images, unless the victim seeks a costly DMCA takedown. Image takedowns need to be equitable, fast, and accessible for everyone to ensure that vulnerable populations are protected. Additionally, to deter websites from continuing to host images, penalties for noncompliance need to be imposed. In the Hunter Moore case, while he did accept takedown requests, they were often not honored, or he charged victims a fee to remove the image. Effective AI-generated IBSA policy must prioritize rapid content removal mechanisms to mitigate ongoing harm.

Civil remedies are essential to provide victims with timely and direct avenues for relief that criminal justice alone cannot offer, and this can only be done by having a robust civil statute that

ensures victims can not only seek financial compensation but also have all images removed in a timely manner.

Criminalizing Creation

Currently, most states regulate only the dissemination of AI-generated IBSA, and only four address full-scale liability by extending regulation to platforms, developers, and publishers. This leaves the creation and possession of AI-generated IBSA legal. For states to ensure they have a well-rounded AI-generated IBSA statute, they need to apply regulatory pressure on AI programs and developers to prevent the creation of such images. This is because the harm does not begin only at dissemination but at the creation of the image without the depicted individual's consent. Creating these images constitutes a breach of intimate privacy and should require consent, regardless of whether a real image exists. Additionally, there's always the risk that images may be circulated later, and private sharing can still harm the depicted individual. For a state's AI-generated IBSA laws to be robust, regulation must target the full lifecycle of harm, including the creation and possession of synthetic images. In this way, AI-generated IBSA laws should be modeled after child pornography laws, which criminalize every part of child pornography.

Recognizing IBSA as a Structural Harm

The perception of both real image IBSA and AI-generated IBSA harms is focused on revenge, and few states have made the effort to shift the perception to systemic abuse. As discussed in the literature review, women are more likely to be victims of IBSA, and most states are still not taking a tailored approach to meeting this structured harm. In other words, they are treating AI-generated IBSA as a criminal issue and not a public policy, safety, and well-being issue. Continuing to treat AI-generated IBSA in this way will further exacerbate gender inequality, political participation, and digital safety. AI-generated IBSA must be addressed as a systemic form of harm requiring coordinated legal, technological, and policy responses, rather

than relying on outdated perceptions of IBSA and the harms it creates. Additionally, by reframing AI-generated IBSA harms from individual revenge to systemic abuse, policymakers can ensure that new laws better protect individuals as the technology continues to improve. This can include using broader language such as "created by any means", "synthetic or manipulated", or "emerging technologies". Language such as this ensures that statutes withstand rapidly evolving technology and that laws do not need to be constantly amended or rewritten. In light of this, policymakers must adopt technology-neutral language to ensure AI-generated IBSA statutes remain effective, even as digital tools continue to evolve.

Discussion/Conclusion: Beyond Intent: Regulating Structural Harm

On September 10, 2022, Audrie Pott took her own life in her mother's home in Saratoga (Burleigh, 2013). Audrie had been the victim of sexual assault while she was unconscious from being inebriated. Her assailants then drew on her body with Sharpies, took photos of her without clothes on, and distributed the pictures. Audrie was fifteen years old at the time of her death.

> "After she got drunk and passed out, three boys, who had been her friends since middle school, undressed her, sexually assaulted her, wrote all over her body with permanent marker…Throughout the assault, they took pictures on their cell phones. When she woke up, Audrie had no idea why her body was covered in marker. Her Facebook messages in the aftermath show her desperate attempts to piece together what happened. She pleaded with one of the boys to delete the photos…Her peers taunted and bullied her…Eight days after the assault, Audrie hanged herself" (Democracy Now!, 2016).

Audrie's story is sadly not uncommon. Savannah Dietrick was sixteen when she was raped by two men who later distributed the video of her assault (Burleigh, 2013). In 2011, Rehtaeh was raped by four men who also took pictures of her and distributed them. Her classmates harassed her for two years before she took her life. She would pass away at 17 once she was taken off life support (Burleigh, 2013). While these cases occurred over a decade ago, the inherent evil of IBSA has persisted, even as lawmakers have attempted to regulate it.

In the early stages of this paper, I decided to focus only on information and legislation prior to January 2026. This was done because the AI landscape is rapidly evolving, and this paper would not have been completed if I kept updating it every time new information emerged. What I've learned is that states are moving in the right direction and trying to regulate AI-generated IBSA. However, the real world doesn't work as neatly as bureaucracy intends. Ashley St. Clair's story demonstrates the true vitriol of this issue. Ashley, Elon Musk's former partner and the mother of one of his children, is one of the many victims of AI-generated IBSA. Users on X found images of her as a 14-year-old and asked Grok to undress her, put her in a bikini, and generate graphic content of her (Black, 2026). When Ashley filed complaints about these images, she not only lost access to her premium subscription, but X also kept some of her images up for more than seven days. In response to the image creation and lack of takedown, Ashley filed a lawsuit against X, alleging that the AI tool created sexually explicit images (McMahon, 2026). In retaliation, the parent company of X and Grok has counter-sued Ashley for violating its terms of service (McMahon, 2026). Ashley's lawyer, Carrie Goldberg, has stated in interviews that they "intend to hold Grok accountable and help establish clear legal boundaries for the entire public's benefit to prevent AI from being weaponized for abuse...By manufacturing nonconsensual sexually explicit images of girls and women, xAI is a public nuisance and a not reasonably safe product" (Goldberg, 2026). Goldberg also stated that the images created of Ashley were "de facto non-consensual", and Grok's developers had explicit knowledge that Ashley did not consent to the image creation. Even while Ashley and X's court cases are still ongoing and news of Grok's image creation has been brought to light, the social media and artificial intelligence platform is still showing willful negligence regarding the abuse it is creating and fanning the flames of.

Ashley is not the first person to have AI-generated IBSA created of them. This started in 2025 when xAI released a new generative AI tool called Imagine (Ingram, 2026). Unlike other generative AI tools, this one included a "spicy" mode, which allowed users to create AI-generated not-safe-for-work content. This led to the creation and dissemination of topless deepfakes of Taylor Swift without her consent. In December of 2025, users began to complain about large amounts of sexualized deepfakes (primarily of women and girls), whose photos were digitally edited to make them appear naked or nearly naked (Ingram, 2026). Instead of Elon or another X employee making a statement, Grok itself said it "deeply regretted" what it had done, and these images were "isolated cases where users promoted for and received AI images depicting minors in minimal clothing". Grok's statement shows that X wanted to place full responsibility on the user and avoid any accountability for allowing the image to be created in the first place. An NBC News article by David Ingram shows that while the company pledged to halt abusive deepfakes, AI-generated sexual images and videos depicting real people still proliferated the app, sometimes thousands per hour. In response to the backlash, Elon Musk announced that AI image generation would only be open to paying customers starting January 9, 2026, and announced a more comprehensive crackdown on January 14, 2026. Even after January 14th, when I scrolled through X, I was inundated with AI-generated images of celebrities, accompanied by the user's Grok command. These commands usually follow the same format, such as "put Billie Eilish in this dress" or "remove Alyssa Liu's shirt". As seen in Ashley's case, these images do not stop with adults. X users are also using Grok's image creation to create fake, sexual images of children.

While Elon Musk and X have pledged to curb AI-generated deepfakes, the stark reality is that AI-generated IBSA is not slowing down. Elon Musk has even made statements that he is

"not aware of any naked underage image generated by Grok". However, a 2026 study by the Center for Countering Digital Hate estimated that Grok produced 3 million sexualized images in an 11-day period, 23,000 of which appeared to depict children. Additionally, as of April 2026, the California Attorney General's office, Australia's eSafety office, the Privacy Commissioner of Canada, the European Commission, Ireland's Data Protection Commission, the Paris public prosecutor, and the British Office of Communications and Information Commissioner's Office have opened investigations into Grok. xAI is also facing several lawsuits over Grok's generation of sexualized images, including two class action lawsuits in California brought by women and girls whose likenesses were edited by Grok, and a lawsuit by the city of Baltimore alleging violations of its consumer protection code. Simply putting up flimsy barriers to prevent the creation of nude images is not enough, and it seems as if Elon and X's pledges are but a show of smoke and mirrors to appease the government and consumers. While the images Grok and its users create are fake, the pain and harm they cause are very real. What gives me hope is that IBSA is one of the few issues that doesn't have a partisan divide. Both Democratic- and Republican-led states are making progress in regulating AI-generated IBSA through collaboration across the aisle. I hope that state lawmakers continue their steadfast regulation of both original image and AI-generated IBSA, and begin to realize that industry will not regulate itself before we have more Audrie's and Savannah's.

Table 1 in Appendix A

State	**Existing Statute/Attempted Regulation/ Court Case**	**Successful Regulation**	**Target Population**	**IBSA definition**	**Can it be amended to include AI?**
Alabama	Alabama Code Title 13A. Criminal Code Section 13A-6-240: Distributing a Private Image; Creating a Private Image	SB 301(2017) SB 35(2025)	Perpetrator	Distribution: Knowingly posts, emails, texts, transmits, or otherwise distributes a private image when the depicted individual has not consented in writing to the dissemination and had a reasonable expectation of privacy. Creation: Knowingly creates, records, or alters a private image when the depicted individual has not consented to the creation, recording, or alteration and the depicted individual had a reasonable expectation of privacy against the creation, recording, or alteration of the private image. Extortion: Knowingly causes or attempts to cause another person to engage in sexual acts or to produce any photograph, digital image, video, film, or other recording by communicating any threat to injure the body, property, or reputation of the person.	It is unclear if the creation portion of the statute applies to AI-generated images, so an amendment that specifically calls that out would be ideal to ensure the creation of AI-generated images is enforceable. Additionally, Alabama does not have civil code allowing for injunctions for financial remedy or to have the image taken down.
Alaska	Alaska Statutes 11.61.120: Harassment in the second degree	HB 14(2003) HB 326(2006)	Perpetrator Perpetrator	Publishing, producing, or distributing electronic or printed photographs, pictures, or films that show a person in a state of nudity or engaged in a sexual act	No, because this bill focuses on digital conduct and communication behavior as harassment, not necessarily focusing on image distribution, identity, consent, and permanence. Substantial amendments would be needed to make this statute widely enforceable. There is no statute that allows for an injunction to take down the image.
Arizona	HB 2515(2014)	No. After HB 2515's passage, the ACLU filed a lawsuit (Antigone Books v Horne) arguing that the bill was unconstitutional and violated First Amendment rights. The bill was	Perpetrator	Intentionally disclosing, displaying, distributing, publishing, advertising, or offering a photograph, videotape, film, or digital recording of another person in a state of nudity or engaged in a sexual activity if the person knows or should have known that the depicted person has not consented to the disclosure.	If HB 2515 were still enforceable, then AI amendments could be easily added.

	ultimately blocked because it did not include an intent to harm.			
Antigone Books v. Horne (2014)	Challenged the passage of HB 2515 based on the bill going beyond criminalizing revenge prn and straying into the territory of criminalizing the dissemination of historic, artistic, educational, and newsworthy images.	N/A	The case of Antigon Books v Horne began with the passage of Arizona House Bill 2515 (HB 2515), which made it a class five felony to knowingly disclose, display, distribute, publish, advertise, or offer any form of media that includes an individual in a state of nudity or engaged in a sexual act without obtaining written consent of the depicted individual (Arizona Legislature, Chapter 14, Statutes of 2014). The intent of this bill was to prevent and stop revenge porn, but in response to HB 2515, the Freedom to Read Foundation, along with the American Booksellers Foundation for Free Expression, Association of American Publishers, five Arizona bookstores, and other individuals, filed a suit against the State of Arizona for infringing on the First Amendment (Freedom to Read Foundation, 2014). The plaintiffs in this Antigone Books v. Horne argue that while revenge porn is a "malicious invasion of privacy", HB 2515 goes beyond criminalizing revenge porn and strays into the territory of criminalizing the dissemination of historic, artistic, educational, and newsworthy images (Freedom to Read Foundation, 2014). Additionally, the plaintiffs noted that HB 2515 does not require the distributor to have the intent to harm (Freedom to Read Foundation, 2014), a point of contention among stakeholders in favor of IBSA regulation.	N/A
Arizona Revised Statutes 13-1425: Unlawful disclosure of images depicting states of nudity or specific sexual activities; classification; definitions	HB 2001(2016) SB 1426(2025)	Perpetrator	Intentionally disclosing of an image of another person in a state of nudity or engaged in specific sexual activities, and if the person has a reasonable expectation of privacy. This statute also has an intent to harm, harass, intimidate, threaten, or coerce.	Amendments to include AI-generated images is in process through HB 2133 (2026). There is no statute that allows for an injunction to take down the image.

	Arizona Revised Statutes 13-1425: Unlawful disclosure of images depicting states of nudity or specific sexual activities; classification; definitions	HB 2133(2026)	Uploaders of sexual material	Knowingly and intentionally publishing, distributing, or allowing the publishing or distribution of sexual material on an internet website without reasonable consent verification and proof the identifiable person is at least 18 years old. Additionally, commercial entities cannot publish or disseminate sexual material without obtaining verified consent from a depicted individual. This bill includes synthetic depictions, which is defined as visual depictions that are created or altered through the use of artificial intelligence, digital manipulation, or other technology, in its regulations regarding sexually explicit material.	Yes. If the Arizona legislature wanted to take IBSA protections one step further, they can include a way for IBSA victims to submit complaints for investigation. There is no statute that allows for an injunction to take down the image.
Arkansas	Arkansas Code §5-26-314: Unlawful distribution of an intimate image	SB 156 (Act 304). (2015) HB 1967 (Act 981) (2025)	Perpetrators	Distributing sexual images or recordings of an individual who is 18 years or older without the consent of the identifiable person.	A simple amendment is needed to include AI-generated imagery. There is no statute that allows for a civil injunction to take down the image.
	Arkansas Code §5-14-139: Unlawful creation or distribution of deepfake visual material	HB 1529 (Act 827) (2025)	Perpetrator	Makes it unlawful to create or distribute deepfake visual material without consent, including a photograph, image, video, or other visual depiction that: appears to be authentic to the ordinary person, is generated; is generated, modified, or adapted using technology to falsely depict an individual's appearance, voice, or conduct; has the individual in a state of nudity or engaging in sexual contact, intercourse, or activity. Lastly, this bill places responsibility on technology companies for implementing safeguards to prevent the generation of AI IBSA.	This bill already covers AI-generated IBSA and does not have an intent to harass requirement.
	Arkansas Code §16-118-119: Civil action for unlawful creation of deepfake visual material	HB 1529 (Act 827) (2025)	Depicted Individual	Same definition as Arkansas Code §5-14-139, but this code section allows the depicted individual to bring civil action against the provider or developer of the image generation technology if they did not have reasonable safeguards in place to protect against the generation of deepfake visual material and the person who created the deepfake visual material.	This statute already covers AI-generated IBSA and provides civil injunctive relief.
California	Penal Code §647	SB 255 (2013) SB 1255 (2014) AB 379 (2026)	Perpetrator	Distributing photographs or recordings of an identifiable individual's intimate body parts under the circumstances where both parties agree or understand the image shall remain private. This statute also protects individuals	An amendment to include AI-generated imagery could be easily added. Additionally, any amendments should include a mechanism for the victim to seek civil injunctive relief.

			who share their own sexually explicit image with the expectation it would remain private with its intended party. Additionally, this bill requires an intent to cause serious emotional distress, and the depicted person does suffer emotional distress.	
Civil Code §1708.86	AB 602 (2019)	Depicted Individual	Creating and intentionally disclosing sexually explicit material of a depicted person who did not consent to the material's creation or disclosure.	While not specifically called out, this bill includes AI-generated imagery and creates a private right of action for depicted individuals to seek civil injunctive relief and damages.
Hunter Moore v U.S. District Court for the Central District of California (2013-2014)	N/A	Perpetrator	In 2010, Hunter Moore was the operator of a pornographic website called "Is Anyone Up?" (IAU), which featured non-consensual intimate images that were either hacked, stolen, or used without the individual's consent (Sangster, 2022). As IAU gained traction, Moore allowed users to anonymously submit sexually explicit images to the site along with the person's name and links to their social media accounts. According to Bazaar, IAP received thirty million monthly page views at the height of its popularity (Sangster, 2022). Moore stated in interviews that if an individual wanted their image removed, he would take it down (Hill, 2011). However, pleas for removals often went unheard, and at the time, one of the only ways individuals could have their images removed was through the Digital Millennium Copyright Act (DMCA), which states that an individual who takes a photo owns the copyright to it. The issue with this is that the image was not removed from the website itself, only the website result is removed from the internet search results. Removal of IAU images was particularly difficult because the website was protected by the Communications Decency Act (CDA), which "protects publishers from the content that the people they serve post" (Hill, 2011; Williams, 2015). Essentially, since IAU is composed of images and information provided by its users, Moore would be protected by the CDA (Hill, 2011; Williams, 2015).	N/A

				In October of 2013, a grand jury for the United States District Court for the Central District of California indicted Moore and his associate, Charlie Evans, for "accessing a protected computer without authorization to obtain information for private financial gain, and later formally charged Moore and Evans in 2014 (United States v Hunter Moore and Charles Evans, 2013). This occurred after forty victims came forward to the Federal Bureau of Investigation with proof of hacking by Moore and Evans. Moore pleaded guilty and was sentenced to 2.5 years in federal prison, followed by 3 years of probation and a $145.70 payment to a victim (Williams, 2015). At the time of the IAU's creation, the website was not considered illegal. This is why Moore went to prison for hacking into victims' computers and stealing photos, not disseminating non-consensual pornography.	
Colorado	Colorado Revised Statutes §18-7-107 & 18-7-108	HB 1378 (2014) HB 1264 (2018)	Perpetrator	Criminal: Disclosing or threatening to disclose an intimate image or an intimate digital depiction without the depicted individual's consent. The criminal statute requires either an intent to harass, intimidate, or coerce the depicted individual; or, the disclosure or physical, emotional, or reputational harm. Civil: Disclosing a private intimate image or intimate digital depiction for pecuniary gain without consent of an individual. Additionally, this statute can hold a disseminator civilly liable if they reasonable should have known that the original intent of the image or digital depiction should have remained private or would cause financial harm to the depicted individual.	This statute already includes AI-generated images by using the language "intimate digital depiction"; however, specifically calling out "images generated with artificial intelligence" would make the statute clear. Additionally, language to limit AI programs from creating the image in the first place would strengthen the law. This statute does not include language that creates a private right of action for depicted individuals to seek civil Cp;injunctive relief and damages.
	Colorado Revised Statutes 18-7-107 & 18-7-108	SB 100 (2019)	Perpetrator	Same definition as HB 1264 (2018)	No. This bill creates loopholes for perpetrators by creating an exception to the civil action under prior statutes if the disclosure was made in good faith under various circumstances, such as if the perpetrator disclosed the image as a parent or guardian, or did not disclose the image for the purposes of sexual arousal, sexual

				gratification, humiliation, degradation, or monetary or commercial gain.
Federal Trade Commission (FTC) v. Craig Brittain (2015)	N/A	Perpetrator	Craig Brittain was the owner and operator of a website called "isanybodydown.com", where he posted intimate images of individuals obtained by either requesting submissions that included the individual's personal information and image, posing as a woman on Craigslist and either advertising or soliciting photographs after sending his own, and instituting a "bounty system" on his website where users could request images of a specific person for a $100 reward (Federal Trade Commission, 2015). In all of these methods, the individual whose image was used did not consent to its dissemination and Brittain had images of approximately 1,000 individuals on his website, a majority of whom were women. If an individual wanted their image removed, they could use services on Brittain's website, such as the "Takedown Hammer" and "Takedown Lawyer," provided they paid a fee (Federal Trade Commission, 2015). However, whether or not the individuals who requested their images be removed knew it, Brittain owned these takedown services and was essentially paid to remove the same photos he posted (Federal Trade Commission, 2015). In 2015, the FTC filed two counts against Brittain for violating sect. 5(a) of the FTC Act (Federal Trade Commission, 2015), which prohibits "unfair or deceptive acts or practices in or affecting commerce" (15 U.S.C. Sec. 45), such as causing substantial injury to consumers (Federal Reserve, 2008). The first count alleged that Brittain disseminated both intimate images of individuals and their personal information for commercial gain without their consent and the second count alleged that Brittain deceptively solicited images from individuals by stating he would only use those images fro his personal private use.. In this complaint, the FTC notes that Brittain either knew or should have known that the individuals had a "reasonable	N/A

				expectation their image would not be disseminated in that manner". In addition to the two counts against Brittain, the FTC included the following prohibitions: first, Brittain cannot disseminate intimate images and videos through a website or online service without written consent that the image is being used for commercial gain; second, Brittain cannot misrepresent his collection, use, disclosure, or deletion of personal information; his identity; or the identity of those providing content or sponsoring advertising on a website when offering any good or service for sale; and third, Brittain cannot benefit from the images and personal information he obtained from his website and required him to destroy any images and personal information of individuals within 30 days of the order's entry. In 2015, Brittain entered into an Agreement Containing Consent Order (Order) with the FTC in which Brittain neither admitted nor denied any of the FTC's allegations, and it was approved in 2016.	
Connecticut	Connecticut General Statutes 53a-189c: Unlawful dissemination of an intimate image	SB 489 (2014) HB 6594 (2021) HB 5421 (2024) SB 1440 (1440)	Perpetrator	Dissemination by electronic or other means of an intimate image when intimate areas are exposed, the person is engaged in sexual intercourse, and the image is disseminated without the consent or knowledge of the individual in the image. This statute also requires that the depicted individual must suffer physical, financial, psychological, or emotional harm.	Yes, but the harm element should be removed. An amendment to this statute should include provisions that make it impossible to generate the image. However, it does not include a statute authorizing an injunction to take down the image.
Delaware	Delaware Code Title 11, 1335: Violation of Privacy	HB 306 (2013) HB 194 (2019) HB 322 (2024)	Perpetrator	Knowingly reproduces, distributes, exhibits, publishes, transmits, or otherwise disseminates a visual depiction of a person who is nude or engaging in sexual conduct when the disseminator should have known that the image was created with the reasonable expectation of privacy. This statute also criminalizes dissemination for profit and/or harm.	Yes, an AI amendment would be easy to add. However, it does not include a statute that allows for an injunction to take down the image.
	Delaware Uniform Civil Remedies for	SB 169 (2020) SB 353 (2024)	Depicted Individual	Same definition as Title 11, Violation of Privacy, but allows a depicted individual who suffers harm from an image that was taken	This is a well-rounded statute that includes AI-generated imagery, but this only applies to Civil remedies. Further amendments are needed for

	Unauthorized Disclosure of Intimate Images Act			without consent and had a reasonable expectation the image was private. This statute also includes deepfakes where an individual is identifiable.	Criminal remedies. However, it does not include a statute that allows for an injunction to take down the image.
Florida	Bollea v. Gawker	Yes	Depicted Individual	In 2012, Gawker Media released a video of Terry Bollea having intercourse with a woman by the name of Heather Clem (Somaiya, 2016) after Heather's husband, Todd Clem, convinced Bollea to engage in sexual activities with Heather (Morin, 2017). After several years, it was discovered that there was a camera in the room where the sexual encounter took place (Somaiya, 2016; Morin, 2017). When Gawker Media LLC released a short segment of the recording, Todd claimed it was taken from the home and sent to Gawker by an anonymous source (Morin, 2017; Somaiya, 2016). With the release of the tape, Bollea sued Todd for recording the interaction without his consent (Somaiya, 2016). Todd would end up paying Bollea $5,000 and testify in a suit that Bollea filed against Gawker. Bollea sued Gawker Media and was awarded $140 million in damages for various infractions, such as invasion of privacy and the intent to inflict emotional distress (Morin, 2017). This case between Bollea, Todd, and Gawker is an example of the publication of non-consensual pornography, but on a nationwide scale. Bollea was able to utilize the only means of legal remedy	N/A
	Florida Statutes 784.049: Sexual cyberharassment	HB 1501 (2015) HB 1451 (2025) – signed by Governor on 5/23/2025	Perpetrator	Intentionally publishing or disseminating a sexually explicit image of a person without their consent and contrary to the depicted person's reasonable expectation that the image would remain private, and if the image contains or conveys personal identification information	This statute could include AI-generated imagery, but the intent to harm needs to be removed. This statute does include the ability for a depicted person to seek injunctive relief and monetary damages.
	SB 1084 (2025)	No – died in Committee	Perpetrator	Publishing an intimate image that has been created, altered, adopted, or modified by electronic, mechanical, or other computer-generated means that depicts nudity of an identifiable individual and appears to a	This bill was specifically targeting the dissemination of AI-generated images. However, it did not target the creation of AI-generated images. This bill also included civil remedy for punitive damages and reasonable

				reasonable person to be indistinguishable from an authentic visual depiction of the individual, regardless of whether the image makes a distinction that it is not authentic.	attorney's fees for the depicted individual against the creator of the image.
Georgia	GA Code 16-11-90: Prohibition on nude or sexually explicit electronic submission	HB 838 (2014) SB 78 (2021)	Perpetrator	Knowingly transmits or posts a photograph or video that depicts nudity or sexually explicit conduct of an adult, including falsely created a videographic or still image.	This statute already includes false imagery, but it is unclear if it also applies to AI-generated images. An explicit AI statute should be added to create clarity. Additionally, this statute applies when the dissemination causes harassment or financial loss, but is unclear if these are a requirement for enforcement. It does not include a statute that allows for an injunction to take down the image.
Hawaii	Criminal section 711-1110.9 Violation of privacy in the first degree	Act 278 (1999) Act 48 (2003) Act 83 (2004) Act 116 (2014) Act 114 (2018) SB 309 (2021)	Perpetrator	Intentionally or knowingly installs or uses any device for observing, recording, amplifying, or broadcasting another person or recognizable fictitious person in a stage of undress or sexual activity without their consent. This statute also includes knowingly disclosing or threatening to disclose an image or video of another identifiable person or fictitious person either in the nude or engaged in sexual conduct without the consent of the depicted person with the intent to harm. This statute also includes sexual extortion with the intent to harm.	This statute seems to include AI-generated imagery in its language, but specifically calling it out would better. It does not include a statute that allows for an injunction to take down the image.
Idaho	Idaho Code 18-6605 Video Voyeurism	HB 528 (2002) HB 509 (2006) HB 498 (2015) HB 727 (2026) - pending	Perpetrator	Installing or permitting the use or installation of an imaging device at a place where a person would have a reasonable expectation of privacy, without the knowledge or consent of the person using a place. This statute also includes intentionally disseminating, publishing, or selling/conspiring to disseminate either an intimate image of an identifiable person or the identifiable person engaged in a sexual act. This statute is a voyeurism law, and only applies if there is an intent to harm or arousal.	An amendment to include AI-generated images could be added to 18-6605, but Idaho added a separate statute for synthetic media (18-6606). The current statute requires an intent to harm and/or arouse, and does not include civil reliefs.
	Idaho Code 18-6606 Disclosing Explicit Synthetic Media	HB 575 (2024) HB 391 (2024) – replaced and refined	Perpetrator	Knowingly disclosing explicit synthetic media and knows that the identifiable person portrayed in the media did not consent to such disclosure and the media would cause substantial emotional distress.	The state of Idaho did not take a "traditional IBSA law to amendment" path. The definition of synthetic media in the statute does not clearly call out AI-generated media. An amendment to make this clear would clarify the statute and its enforcement powers. Additionally, this statute does not include any civil injunctive reliefs for the individual.

Illinois	720 ILS 5/11-23.5 Non-consensual dissemination of private sexual images	HB 4970 (2014) SB 2129 (2016) People v Austin (2019) SB 1716 (2023)	Perpetrator	Intentionally disseminating an intimate image of an identifiable person. Intimate image is defined as an image that shows the identified individual engaged in a sexual act or whose intimate parts are exposed, when the individual had a reasonable expectation the image would remain private and/or the individual did not consent to the image's dissemination.	Amendments are unneeded to this section because 720 ILCS 5/11-23.7 covers AI-generated images. This statute seems to imply that a person cannot be found guilty for being in possession of IBSA, only for dissemination. Civil remedies are located in 740 ILCS 190/.
	People v Autin (2019)	Yes	Perpetrator	In 2016, Austin was engaged to a man named Matthew W. Rychlik and later found nude images and text messages with another woman by the name of Elizabeth Dreher on Rychlik's phone (Global Freedom of Expression, n.d.). Austin called off her engagement to Rychlik and later sent Rychlik's cousin a package that contained a four-page letter along with the text messages between Rychlik and Dreher and nude images of Dreher after Rychlik made comments about Austin. Two days later, Rychlik contacted the Crystal Lake Police Department to report that Austin had mailed copies of nude images of Dreher to his family, and an officer named Ryan Coutre confirmed that the images Dreher took were only intended for Rychlik. Austin was subsequently charged with the "non-consensual dissemination of private sexual images". The Circuit Court in Illinois determined that the charges against Austin violated her First Amendment rights and dismissed them because Section 11-23.5(b) of the Criminal Code imposes content-based restrictions on speech only when there is a compelling government interest. Additionally, the Circuit Court argued that since Dreher sent a nude photo to Rychlik, she had sent it to a third party and therefore had no expectation of privacy. This case ended up in the Supreme Court of Illinois, where the initial Circuit Court decision was overruled, and the Supreme Court observed that Rychlik was not a third party but rather a second party when he received the nude image. Therefore, Dreher did not relinquish her expectation of privacy, and consensually sending a photo cannot be	N/A

				equated with consent to its distribution to others outside the private relationship (Global Freedom of Expression, n.d.). Additionally, the Supreme Court ruled that protecting privacy rights was in the government's interest, and that the dissemination of nonconsensual pornography did not burden more speech than necessary (Sandoval, 2019). The Supreme Court's final ruling was that Criminal Code section 11-23.5(b) does criminalize the dissemination of sexual images without consent.	
	720 ILCS 5/11-23.7 Non-consensual dissemination of sexually explicit digitized depictions	HB 2123 (2023) SB 1716 (2023)	Perpetrator	An image, photograph, film, video, digital recording, or other depiction or portrayal that has been created, altered, or otherwise modified to realistically depict sexual activity or intimate parts of another human being as the intimate parts of the computer-generated individual, when the depicted individual did not consent to the dissemination of the image.	This statute most likely covers AI-generated images, although this is not specifically called out. Additionally, this statute does not prevent the creation of these images, nor does it make it illegal to posses it. Civil remedies are located in 740 ILCS 190/.
	740 ILCS 190/1-35	SB 1657 (2019) HB 2123 (2023) SB 1716 (2023)	Depicted Individual	This statute is the civil component to both 720 ILCS 5/11-23 and 720 ILCS 5/11-23.7, and allows a depicted individual that suffers harm from the intentional dissemination or threatened dissemination of a private or intentionally digitally altered sexual image without the depicted individual's consent to bring forth a cause of action.	This statute most likely includes civil remedies for AI-generated images, but only finds the individual responsible for dissemination liable. It does not allow for an individual to hold the platform that allowed for the creation to be held liable.
Indiana	IC §35-45-4-8 Distribution of an Intimate Image	SB 243 (2019) HB 1047 (2024)	Perpetrator	Distributes an intimate image (photograph, digital image, computer generated image, or video) that depicts an individual engaged in sexual intercourse, sexual conduct, or exhibiting intimate areas when the disseminator knows or reasonably should have known that the depicted individual did not consent to the distribution of the intimate image.	This bill includes AI-generated images in its language, but it should be noted that this statute seems to only criminalize the distribution of an intimate image, not the possession or creation of one. Section 8(a)(d)(i-ii) includes an exception to the law for images that are located in an area intended solely for the storage or backup of personal data and is password protected. Civil action is located in IC 34-21.5-3-1
	IC Code §34-21.5-3-1	SB 243 (2019) HB 1047 (2024)	Depicted Individual	A depicted individual who is identifiable and suffered harm from the creation or disclosure of nonconsensual pornography, disclosing the intimate image to a third party with the intent to harass, and knowing or acting with reckless disregard for whether the depicted individual	This statute does not include AI-generated IBSA, but since it is a counterpart to IC §35-45-4-8, it seems like an individual can be held civilly liable for the dissemination of AI-generated IBSA. Additionally, this statute does include the creation of nonconsensual pornography, which may mean creation can be

				was identifiable or did not consent to the image's disclosure.	held civilly liable, but not criminally. This statute does not contain language that allows for the deleted individual to request for the deletion of the image.
Iowa	§708.7 Harassment	Iowa does not have a standalone IBSA law. SF 2166 (2017) added IBSA to the existing harassment statute.	Perpetrator	Disseminating, publishing, distributing, posting, or causing to be disseminated, published, distributed, or posted a visual depiction of another person in a state of full or partial nudity or engaged in a sex act, to which the depicted individual has not consented to the dissemination, publication, distribution, or posting.	This is a bare-bones IBSA law. For robust enforcement, a separate statute is needed along with an amendment to include AI-generated IBSA. A civil statute is also needed so the depicted individual can seek restitution.
Kansas	Kansas Statutes Annotated 21-6101(8) Breach of Privacy	HB 2062 (2015) SB 186 (2025) SB 205 (2025): proposed	Perpetrator	Disseminating any videotape, photograph, film or image of another person who is nude or engaged in sexual activity and under circumstances in which such indefinable person had a reasonable expectation of privacy, with the intent to harass, threaten, or intimidate, and the identifiable person did not consent to such dissemination. This statute includes disseminating any videotape, photograph, film or image that has been created, in whole or part, altered or modified by artificial intelligence or any digital means to appear to depict or purport to depict an identifiable person, regardless of whether they were involved in creating the original image.	Kansas has included AI-generated images into its IBSA statute, but it is unclear if there is a requirement to harass for the AI-generated portion like there is for the original image portion.
Kentucky	Kentucky Revised Statute Section 531.120 Distribution of sexually explicit images without consent	HB 98 (2018) SB 73 (2025)	Perpetrator	Intentionally distributing to any third party private erotic matter without the consent of the person depicted, and do so with the intent to profit, or to harm, harass, intimidate, threaten, or coerce the person depicted, and the disclosure would cause a reasonable person to suffer harm. This statute also requires a person who maintains an Internet Web site, online service, online application, or mobile application that distributes private erotic matter to remove any such image if requested by a person depicted, and shall not solicit or accept a fee or tother consideration to remove the visual image.	This statute could easily be amended to include AI-generated IBSA. Kentucky is unique in the fact they also include a section that requires website holders to take down images upon request, without charging a fee. To improve this statute, the intent to harm should be removed when adding an AI-generated IBSA statute. Additionally, there should be restrictions on creating and/or being in possession of IBSA.
	Kentucky Revised Statute Section 411.215 Action for failure to remove sexually explicit image	HB 296 (2018)	Depicted Individual	An individual in violation of KRS 531.120(3) who does not remove a sexually explicit image upon the request of the person depicted in the image. Damages include $1,000 for	An amendment would allow depicted individuals of AI-generated IBSA to seek civil remedy under this statute, as it is tied to KRS

	from Web site, online service or application, or mobile application upon request – Damages – Statute of Limitations			each sexually explicit image for each day the image remains on the Web site after receipt of the request.	531.120, which sets the requirements for nonconsensual pornography.
Louisiana	Revised Statutes §283.2 Nonconsensual disclosure of a private image	Acts 2015, No. 231 Acts 2024, No. 11 Acts 2024, No.64 Acts 2024, No. 431	Perpetrator	Requires all of the following: 1. Intentionally disclosing an image of another person who identifiable from the image or information displayed in connection with the image and wither whose intimate parts are exposed in while or in part or who is engaged in sexual conduct 2. The person who discloses the image obtained it through unauthorized access or under circumstances in which a reasonable person would know or understand that the image was to remain private. 3. The person who discloses the image knew or should have known the person in the image did not consent to the disclosure of the image. 4. The person who discloses the image knew or should have known that the disclosure could harass or cause emotional distress to the person in the image.	AI-generated IBSA was added in Revised Statutes §14:73.14 but this statute needs additional work to make it properly enforceable, such as the intent to harm. This statute should also include language that makes it illegal to create or possess nonconsensual pornography. This statute also does not include any mechanism for civil remedy or to have the pictures taken down/destroyed.
	Revised Statutes §14:17.13 Unlawful deepfakes	SB 175 (2023)	Perpetrator	Knowingly advertises, distributes, exhibits, exchanges with, promotes, or sells deepfake material without the consent of the depicted individual	This is a well-rounded deepfake statute but it does not criminalize possession or creation of deepfake material unless the depicted individual is under 18 years of age. Additionally, there is no mechanism for civil remedies.
	Revised Statutes §14:73.14 Unlawful dissemination or sale of images of another created by artificial intelligence	SB 6 (2024)	Perpetrator	With the intent to coerce, harass, intimidate, or maliciously disseminate or sell any video or still image created by artificial intelligence that depicts another person who is totally nude or in a state of undress so as to expose intimate areas, when the person disseminating the video or still image knows or has reason to know that the person is not licensed or authorized to disseminate or sell such video or still image.	This amendment does include AI-generated IBSA, but more work needs to be done, like removing the intent to harm and removing the ability to create and possess an AI-generated nonconsensual pornographic image or video. Additionally, there is no mechanism for civil remedy.
Maine	Criminal Code 17-A, §511-A	LD 1047 (2015) LD 1020 (2019)	Perpetrator	With the intent to harass, torment or threaten the depicted person or another person, intentionally or knowingly disseminates, displays, or publishes an image of another person in a state of nudity or engaged in a sexual act or engaged in sexual contact, when the depicted person has not consented to the	This statute seems to include images created through AI, but it would be helpful for AI-generaed images to be specifically called out. Additionally, the intent to harm should be removed, and a section that specifies that the picture was taken when a reasonable person would have the expectation of privacy should

				dissemination, display, or publication of the image. This statute includes images that have been created or modified.	be included. Any future amendments should also include a mechanism for civil remedy.
Maryland	Criminal Law §3-809	HB 43 (2014) HB 917/SB 1007 (2017) HB 145 (2024) SB 360 (2025)	Perpetrator & Depicted Individual	Knowingly distributing a visual representation of another identifiable person that displays the other person with intimate parts exposed or while engaged in an act of sexual activity with the intent to harm, harass, intimidate, threaten, or coerce the depicted individual, under the circumstances in which the person knew that the depicted individual did not consent to the distribution, or with reckless disregard as to whether the depicted individual consented to the distribution, under circumstances in which the depicted individual had a reasonable expectation that the image would remain private.	This statute includes both original images and AI-generated images because the definition of "visual representation" includes both computer-generated images and unaltered images. Improvements to this statute could include criminalizing the creation and possession of IBSA and placing regulations on AI companies to prevent AI-generated IBSA from even being created. This statute does include civil remedies for depicted individuals.
Massachusetts	General Law Chapter 272 Section 105	St. 2004, c. 266 St. 2014, c.43	Perpetrator	Willfully disseminating the visual image of another person, with knowledge that such visual image was unlawfully obtained through either photographing videotaping, or electronically surveilling, with the intent to secretly conduct or hide such activity, the sexual or other intimate parts of a person under or around the person's clothing to view or attempt to view the person's sexual or other intimate parts when a reasonable person would believe the depicted individual had a right to privacy and did not consent to the photographing, videotaping, or electronic surveilling.	For an AI amendment to be added, several changes need to occur to make this statute smoother and more enforceable. The current statute as written does not include regulations on companies that allow for the creation of AI-generated IBSA, nor websites that that knowingly host it. Additionally, it does not regulate the creation or possession of IBSA, just its dissemination.
Michigan	Criminal Law 750.145e: Dissemination of sexually explicit visual material of another person	PA 389 (1978) PA 84 (2000) PA 281 (2018)	Perpetrator	Intentionally and with the intent to threaten, coerce, or intimidate, disseminate any sexually explicit visual material of another person is all the following conditions apply: 1. the other person is not less than 18 years of age 2. the other person is identifiable from the sexually explicit visual material itself or information displayed in connection with the sexually explicit visual material. This subdivision does not apply if the identifying information is supplied by a person other than a disseminator. 3. the person obtains the sexually explicit visual material of the other person under	Amendments to include AI-generated IBSA could be added when additional clean-up is done. Amendments should include removing the intent to harm and removing the portion that requires identifying information to only be supplied by the disseminator. Additional amendments should include a mechanism for civil remedy and regulations regarding the creation and possession of both original and AI-generated IBSA.

				circumstances in which a reasonable person would know or understand that the material was to remain private 4. the person knows or reasonably should know that the other person did not consent to the dissemination of the sexually explicit material.	
Minnesota	617.261 Nonconsensual Dissemination of Private Sexual Images	Laws 2016, Ch. 126	Perpetrator	Intentionally disseminating an image of another person who id depicted in a sexual act or whose intimate parts are exposed, in whole or in part when the person is identifiable, the disseminator knows or reasonably should know that the person depicted in the image does not consent to the dissemination, and the image was obtained or created under circumstances in which the disseminator knew or reasonably should have known the depicted individual had a reasonable expectation of privacy	This is a standard IBSA statute. Regulations on AI-generated IBSA are located in 617.262. Civil remedy mechanisms are located in 604.31
	617.262 Nonconsensual Dissemination of a Deep Fake Depicting Intimate Parts or Sexual Acts	HF 1370 (2023) SF 1394 (2023)	Perpetrator	Intentionally disseminating a deep fake when the disseminator knows or reasonably should know that the depicted individual did not consent to the dissemination, the intimate parts/artificially generated intimate parts of another individual are presented as the intimate parts of the depicted individual, the depicted individual is engaging in a sexual act, and the depicted individual is identifiable.	This is a well-rounded basic AI-generated IBSA law. Civil remedies are located in 604.31.
	604.31 Cause of Action for Nonconsensual Dissemination of Private Sexual Images; Sexual Solicitation	SF 2713 (2016)	Depicted Individual	The dissemination of an image of an identifiable person without the consent of the person depicted in the image and who is engaged in a sexual act or whose intimate parts are exposed.	Civil remedy for AI-generated deepfakes is located in 604.32.
	604.32 Cause of Action for Nonconsensual Dissemination of a Deep Fake Depicting Intimate Parts or Sexual Acts	HF 1370/SF 1394 (2023)	Depicted Individual	The dissemination of a deep fake with the knowledge that the depicted individual did not consent to its public dissemination, and the deepfake realistically depicts the intimate parts/artificially generated intimate parts presented as the intimate parts of the depicted individual or the depicts the individual engaged in a sexual act.	
Mississippi	MS Code §97-29-64.1	SB 2121 (2021) HB 1115 (2026 – proposed)	Perpetrator	Disclosing visual material of another's intimate parts/sexual conduct without to consent, with the intent to harm, where the image was private, causes harm, and reveals	Yes, but the current real-image statute is intent- and harm-heavy; a cleaner AI amendment should remove the harm element and expressly cover creation/possession, not just disclosure/promotion.

				the identity of the depicted individual. This statute also covers	
	SB 2437 (2026)	Died on Calendar	N/A	Defined artificial intelligence.	It is unknown whether this bill would have an impact on AI-generated IBSA because it died early on in the legislative process.
Missouri	Mo. Rev. Stat. §573.110	HB 1558 (2018) HB 243 (2019) HB 544 (2019)	Perpetrator & Depicted Individual	Intentional dissemination of a private sexual image of an identifiable adult, obtained under circumstances showing it was to remain private, knowing nonconsent; includes a private cause of action in the statute itself.	Yes. Missouri's core law is still real-image focused; an amendment could add synthetic/AI images fairly easily, but the intent to harass/threaten/coerce requirement would still limit reach.
Montana	Mont. Code Ann. §45-8-213	HB 192 (2019) HB 514 (2025) HB 178 (2025)	Perpetrator	Publishing/distributing printed or electronic photos/images/films of an identifiable person showing genitals/anus/buttocks/female breast or a real/simulated sexual act, without consent and with purpose to terrify, intimidate, threaten, harass, or injure.	Yes, but only with substantial cleanup. The statute already references real or simulated sexual acts, but it is still fundamentally a privacy in communications / harassment model rather than a modern consent-based IBSA scheme.
Nebraska	Neb. Rev. Stat. §28-311.08	LB 903 (1006) LB 61 (2021) LB 998 (2014) LB 605 (2015) LB 603 (2019)	Perpetrator	Criminally covers distribution of an intimate-area/sexually explicit image without consent, where the person had a reasonable expectation of privacy and dissemination serves no legitimate purpose; also covers threats.	Yes. Nebraska has a strong consent/privacy structure and a civil remedy already; adding AI/deepfake language would be straightforward.
	Neb. Revised. Stat §25-3503	LB 680 (2019) LB 371 (2025)	Depicted Individual	Civil law gives a cause of action for intentional/threatened disclosure of a private intimate image	Yes. Nebraska has a strong consent/privacy structure and a civil remedy already; adding AI/deepfake language would be straightforward
Nevada	Nev. Rev. Stat. §200.780	AB 49 (2015) SB 213 (2025)	Perpetrator	Electronic dissemination or sale of an intimate image without prior consent, where the person expected privacy and was at least 18 when created, with intent to harass, harm, or terrorize	Yes, but the current law is narrow: electronic dissemination/sale only, adult images only, and intent-heavy. A good AI amendment should expressly add synthetic images and remove the motive bottleneck.
New Hampshire	N.H. Rev. Stat. §644:9-a	HB 1260 (2024) HB 1319 (2024) SB 464 (2024)	Perpetrator	Purposeful dissemination of a private sexual image of an identifiable person, obtained under private circumstances, knowing nonconsent, with intent to harass/intimidate/threaten/coerce; effective 2025 language also covers synthetic images that realistically but falsely depict intimate parts, sexual acts, or sexual activity	Already includes AI/deepfakes. The weakness is not AI coverage but the continued intent-to-harm framing.
New Jersey	Title 2C: 14-9	S2366 (2003) A343 (2023) A1892 (2024) S3344 (2026 – Introduced)	Perpetrator & Depicted Individual	Observing, recording, or disclosing intimate images without consent under circumstances where a reasonable person would not expect to be observed; now also covers deceptive audio or visual media in the disclosure subsection, with civil damages available	Already substantially AI-ready. New Jersey is one of the stronger states because it expressly folds deceptive media into the disclosure framework and already has civil relief.

New Mexico	N.M/ Code §30-37A-1	HB 0142 (2015) HB 530 (2025)	Perpetrator	Distributing/publishing/making available "sensitive images" without consent, with intent to harass, humiliate, intimidate, incite harassment, cause fear, injury, or substantial emotional distress, and where the conduct would cause a reasonable person substantial emotional distress	Yes, but not cleanly. The statute is broad enough that AI language could be added, but right now deepfake creation/dissemination is not explicitly covered, and the emotional-distress framework is heavy.
New York	N.Y. Penal Law §245.15	S1042/A06338 (2023-24) S7202/A7855 (2025-26) A00318/S03202 (2025-26)	Perpetrator	Intentional dissemination/publication of a still or video image of another person's intimate parts or sexual conduct, including an image created or altered by digitization, with intent to cause emotional, financial, or physical harm	Largely yes already. New York is one of the clearer states for AI amendment because the statute already mentions images "created or altered by digitization." A targeted amendment could just define AI/deepfake expressly.
North Carolina	N.C. Gen. Stat. §14-190.5A	SL 2015-250 SL 2017-93 SL 2024-37	Perpetrator	Knowingly disclosing an image of another person with intent to coerce, harass, intimidate, demean, humiliate, or cause financial loss; the image can show intimate parts or sexual conduct that are realistically depicted, and the law also covers images obtained, created, adapted, or modified without consent or under private circumstances; "digitization" includes AI/machine learning.	Already includes AI-ready language. North Carolina is one of the strongest examples because the definition of digitization explicitly includes software, machine learning, artificial intelligence, or other computer-generated means.
North Dakota	N.D. Cent. Code §12.1-17-07.2	SB 2357 (2015) SB 20037 (2025)	Perpetrator	Real-image law covers distribution without consent where the image was private and actual emotional distress/harm is caused. HB 1351 adds production, possession, distribution, promotion, advertising, sale, exhibition, broadcast, or transmission of a sexually explicit deepfake plus civil damages and injunctions	Already includes AI/deepfakes via HB 1351. North Dakota is strong because the newer law goes beyond dissemination and adds possession/production plus civil relief.
	N.D. Cent. Code §12.1-27.1	SB 2360 (2023) - failed HB 1333 (2023) HB 1205 (2023) SB 2307 (2025) HB 1351 (2025)	Perpetrator	Acquires and knowingly distributes any sexually expressive image that was created without the consent of the subject of the image.	This statute needs significant amendments to include AI-generated images.
Ohio	Ohio Rev. Code §2917.211	HB 497 (2018)	Perpetrator	Knowingly disseminating an image of another adult, identifiable from the image or attached info supplied by the offender, in a state of nudity or sexual act, without consent, with intent to harm	Yes, but amendment needed. Ohio's new real-image law is not yet AI-specific, and the offender-supplied identifying information plus intent-to-harm elements may make deepfake enforcement awkward unless amended.

	Ohio Rev. Code §2307.66	HB 497.66 (2018) HB 96 (2025)	Depicted Individual	This is the civil component of Ohio Rev. Code §2307.66	The civil component includes a provision which defines "fabricated sexual image" as an image that is created, adapted, or modified.
Oklahoma	Oklahoma Stat. §1040.13b	SB 1257 (2016) HB 3639 (2024) HB 1364 (2025)	Perpetrator	Covers both (1) traditional nonconsensual dissemination of private sexual images and (2) dissemination of an artificially generated sexual depiction with intent or reckless disregard to harass, annoy, threaten, alarm, or cause physical, emotional, reputational, or economic harm	Already includes AI-generated sexual depictions. Oklahoma is a good model because it separates the real-image and artificial-image theories in one statute.
Oregon	Oregon Revised Statutes 163.472	HB 2596 (2015) HB 4146 (2024) HB 2299 (2025)	Perpetrator	Knowingly causing disclosure of an identifiable image of intimate parts or sexual conduct, without consent, with intent to harass, humiliate, or injure	Yes, and Oregon is already moving there. The statute is still motive-based, but the CAG page notes HB 2299 explicitly includes AI-generated content in the image definition.
Pennsylvania	18 Pa.C.S §3131	Act 115 (2014) Act 125 (2024)	Perpetrator	Dissemination of a current/former sexual or intimate partner's nude/sexual image or an artificially generated sexual depiction of an individual, with intent to harass, annoy, or alarm.	Already includes artificially generated sexual depictions. The main weakness is that the "real image" subsection is still partner-framed, while the AI subsection is broader.
	42 Pa.C.S. §8316.1	Act 115 (2014)	Depicted Individual	Civil component to 18 Pa. C.S. §3131	Since it is the civil component of the criminal statute, this statute would most likely apply to artificially generated sexual depictions.
Rhode Island	R.I. Gen. Laws §11-64-3	HB 7452 (2018) SB 2581 (2018)	Perpetrator	Intentional dissemination/publication/sale of a sexually explicit visual image of an identifiable adult, including an image created by a digital device or altered by digitization, when it was private or created without consent, disseminated without consent, and with knowledge/reckless disregard of likely harm or intent to harass/intimidate/threaten/coerce; threats and pay-to-remove extortion also covered	Largely yes already. Rhode Island already references digital creation and digitization; a future AI amendment would mainly be a clarity amendment.
South Carolina	S.C. Code §16-15-332	HB 3058 (2025)	Perpetrator	Intentional dissemination of an intimate image or digitally forged intimate image without effective consent, where the actor knows the image was obtained or created under circumstances showing a reasonable expectation of privacy	Already includes digitally forged intimate images. This is one of the cleaner recent statutes for AI/deepfake inclusion.
South Dakota	S.D. Codified Laws §22-21-4	HB 1158 (2004) SB 35 (2011) HB 1243 (2016) SB 47 (2020) HN 1204 (2021) SB 120 (2022)	Perpetrator	Criminal law covers use/disclosure/dissemination of illicit recordings and the knowing intentional dissemination or sale of an image/recording intentionally manipulated to create a realistic but false image, without consent or	Already includes deepfake-style manipulated images. The main weakness is the motive requirement and the fact that the statute is still framed partly through voyeurism/self-gratification.

		SB 41 (2026) - proposed		knowledge, with intent to self-gratify, harass, or embarrass and invade privacy.	
	S.D. Codified Law §21-67-3	SB 1108 (2020)	Depicted Individual	This statute is the civil mechanism related to S.D. Codified Laws §22-21-4	
Tennessee	Title 39, Chapter 17	HB 222/SB 466 (2025)	Perpetrator	It is an offense to disclose, threaten to disclose, or solicit disclosure of an intimate digital depiction with intent to harass/annoy/threaten/alarm or cause substantial reputational/financial harm, or with actual knowledge/reckless disregard that physical, emotional, reputational, or economic harm will result.	Already very AI-capable. Tennessee's use of "intimate digital depiction" plus civil equitable relief makes it one of the stronger AI-era frameworks.
Texas	Texas Penal Code §21.165	SB 1135 (2015) HB 2252 (2017) HB 98 (2019) SB 1361 (2023) SB 441 (2025) SB 1621 (2025)	Perpetrator	Criminal law covers knowingly producing or distributing by electronic means a deep fake video appearing to show intimate parts or sexual conduct without effective consent.	Already includes AI/deepfake video on the criminal side. A broader amendment would be needed if Texas wants the criminal law to cover more than deepfake videos.
	Texas Civil Prac. & Rem. Code §98B.002	SB 1135 (2015) HB 98 (2019)	Depicted Individual	Unlawful disclosure or promotion of intimate visual material, with damages, fees, and injunctions.	
	Ex parte Jones (Texas Court of Criminal Appeals, 2021)	N/A	Perpetrator	In Ex parte Jones, Jordan Barlett Jones had met a woman named Ashley Boykin on Tinder and subsequently exchanged sexual messages and videos after Jones requested them (State v Jones, 2023). After Jones and Boykin had sex, Boykin decided to end the relationship, but failed to communicate it to Jones. In retaliation, Jones sent Boykins' sexual video to 84 people, including her mother, ex-husband, and former brother-in-law. Boykin asked Jones to stop sharing the video and later filed a police report, in which she told the detective that she had sent the video only to Jones, expecting it to remain private. Jones was subsequently charged with violating Texas Penal Code Section 21.16(b), which specifies, among other things, that a person commits an offense if they disclose intimate imagery of another person without their consent with the intent to harm, and if the other person has a reasonable expectation that the visual material would remain private at the time of disclosure. Before Jones went to trial, he filed a petition for writ of habeas corpus, alleging that the	N/A

				Texas Penal Code statute was unconstitutional under the First Amendment (State v Jones, 2023). The trial court denied the petition, but on appeal, stated that the statute was a content-based restriction that was overbroad under the First Amendment (State v Jones, 2023). The Court of Criminal Appeals disagreed with the Trial Court and held the Texas Penal Code constitutional (State v Jones, 2023). Jones pleaded not guilty, but the jury found him guilty and charged him with violating the Texas Penal Code. When Jones appealed, he argued that the State failed to prove Boykin had a reasonable expectation of privacy because she sent the sexually explicit video to a man she had never met in person, along with admitting she sent similar sexual videos to other individuals, including her ex-husband (Hoyle, 2023). The Justice overseeing the case, Brian Hoyle, argued that Jones knew the video was meant to remain private because Jones disseminated the videos only after Boykin failed to communicate that their relationship was over (Hoyle, 2023). Jones' actions showed that he knew that disseminating the sexual video was wrong, and his guilty verdict remained after appeal.	
Utah	Utah Code §76-5b-203	HB 71 (2014) HB 147 (2021) HB 59 (2021) HB 18 (2022)	Perpetrator	Knowing/intended distribution/duplication/copying of an intimate image without consent where privacy existed and actual harm resulted.	Already includes counterfeit intimate images. Utah's gap is not AI coverage so much as the continued actual harm requirement in the real-image section.
	Utah Code §76-5b-205	HB 193 (2021) HB 18 (2022) HB 148 (2024)	Perpetrator	Distribution of a counterfeit intimate image without consent where the image was created/provided without the depicted individual's knowledge and consent.	
Vermont	13 V.S.A §2606 H.105 (2015)	H.626 (2026) - introduced	Depicted Individual	Knowingly discloses a visual image of an identifiable person who is nude or engaged in sexual conduct, without the depicted person's consent, with the intent to harm, harass, intimidate, threaten, or coerce. This statute also applies to individuals who maintain an internet website, online service, online	This statute includes civil remedy only, and does not include any language that would lend itself to modern-day AI-generated IBSA.

				application, or mobile application that contains a visual image of an identifiable person who is nude or engaged in sexual conduct.	
	State v. VanBuren	Yes	Perpetrator	The case of State v. VanBuren revolves around a woman named Dana who sent nude photos of herself via Facebook Messenger to her ex-boyfriend, Andrew Coon, in October of 2015 (Harvard Law Review, 2020). Similar to People v. Austin, Coon, at the time, was involved with a woman named Rebekah VanBuren. VanBuren accessed Coon's phone and saw the photos, prompting her to post the photos of Dana on Coon's public Facebook page the next day and tag Dana in the photos. After seeing the photos, Dana left a voicemail on Coon's phone and asked him to delete the photos. However, VanBuren called Dana back, called her a "moraless [sic] pig and said she was going to "ruin" her by calling her employer, a childcare facility, and telling them "what kind of person worked there". After this threat, Dana contacted the police to report the incident, and VanBuren was later charged with Virginia's revenge porn statute. This statute makes it a Class 1 misdemeanor to coerce, harass, intimidate, or maliciously disseminate an image or video that depicts another person who is, among others, totally nude, or in a state of undress which exposes the genitals, public area, buttocks, or female breast (Code of Virginia, § 18.2-386.2).	N/A
Virginia	Va. Code §18.2-386.1-386.2	H.499 (1994) H.844 (2004) H.1741 (2005) H.995 (2008) H.326 (2014) H.2678 (2019) S.1736 (2019) H.926 (2024)	Perpetrator	Malicious dissemination or sale, with intent to coerce/harass/intimidate, of any still or video image "created by any means whatsoever" depicting another person nude/undressed/obscene, where the actor knows or has reason to know they are not authorized; "another person" includes a person whose image was used in creating/adapting/modifying the image and who is recognizable	Already very AI-friendly. Virginia's "created by any means whatsoever" plus recognizable-person language makes it one of the most amendment-light states.
	Va. Code §8.01-40.4	S.1210 (2017)	Depicted Individual	N/A	This is the civil component to Virginia's criminal law.

Washington	RCW 9A.86.010	HB 1272 (2015) HB 2384 (2016) HB 1999 (2024)	Perpetrator	Knowing disclosure of a private intimate image without consent where the actor knows or should know disclosure would cause harm.	AI-generated IBSA is covered in RCW 9A.86.030. To improve this statute, a mechanism for civil remedy should be included.
	RCW 9A.86.030	HB 1999 (2024)	Perpetrator	Knowing disclosure of fabricated intimate images, including computer-generated intimate body parts or fabricated sexual activity.	This statute covers AI-generated IBSA. To improve this statute, a mechanism for civil remedy should be included.
West Virginia	W. Va. Code §61-8-28a	HB 3282 (2005) – died in Committee SB 240 (2017) HB 2017 (2021) – died in Committee SB 198 (2025)	Perpetrator	Knowingly and intentionally disclosing, causing disclosure of, or threatening to disclose a private intimate image, with intent to harass/intimidate/threaten/humiliate/embarrass/coerce, where the image was captured under circumstances of expected privacy	Yes, but a separate AI amendment is needed. The current statute is classic real-image IBSA and not yet synthetic-image focused. A mechanism for civil remedy should also be added.
Wisconsin	Wis. Stat. §942.09	AB 841 (1995) SB 55 (2001) SB 60 (2001) AB 1 (2002) AB 8 (2007) SB 367 (2013) AB 521 (2015) AB 566 (2015) SB 300 (2017) AB 846 (2017) SB 33 (2025)	Perpetrator	Capturing, reproducing, possessing, distributing, or exhibiting intimate representations captured without consent and under private circumstances; also separately posting/publishing a "private representation" knowing the depicted person does not consent	Maybe, but it would need real drafting work. Wisconsin is still a voyeurism/private-representation framework; it could be amended, but an explicit AI/deepfake statute would be cleaner. A mechanism for civil remedy should also be included.
Wyoming	Wyo. Stat. §6-4-306	HB 0085 (2021)	Perpetrator	Disseminating an intimate image of another person where the actor knew or should have known the person expected privacy and did not expressly consent, and the actor intended to humiliate, harm, harass, threaten, coerce, or obtain sexual gratification/arousal	Yes, but it is still a first-generation real-image law. Wyoming would need explicit synthetic-image language and would likely benefit from removing the motive requirement if it wants broader AI enforcement. A mechanism for civil remedy should also be included.

Table of Contents

12VAC5-340-20. (Repealed.). (n.d.). Retrieved March 11, 2026, from https://law.lis.virginia.gov/vacode/title18.2/chapter8/section18.2-386.2/

AB-602 Depiction of Individual Using Digital or Electronic Technology: Sexually Explicit Material: Cause of Action., 1708.86 Civil Code § 1 (2019). https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201920200AB602

Action for Disclosure of Nonconsensual Pornography, Pub. L. No. P.L.185-2019, 34 Civil Law and Procedure (2019). https://iga.in.gov/laws/2025/ic/titles/34#34-21.5 P.L.29-2019, SEC.4.

Action for Failure to Remove Sexually Explicit Image from Web Site, Online Service or Application, or Mobile Application upon Request -- Damages -- Statute of Limitations., 411 Rights of Action and Survival of Actions § 411.215 (2018). https://apps.legislature.ky.gov/law/statutes/statute.aspx?id=47657 Created 2018 Ky. Acts ch. 50, sec. 3, effective July 14, 2018.

AG Marshall, Office of Prosecution Services Praise Bipartisan New Sex Offense Legislation Signed by Governor Ivey—Alabama Attorney General's Office. (2017, May 31). https://www.alabamaag.gov/ag-marshall-office-of-prosecution-services-praise-bipartisan-new-sex-offense-legislation-signed-by-governor-ivey/

Agrawal, A. (n.d.). *Social Construction of Gender*.

Alabama SB35 | 2025 | Regular Session. (n.d.). LegiScan. Retrieved March 21, 2026, from https://legiscan.com/AL/text/SB35/id/3227063

Alaska SB247 | 2025-2026 | 34th Legislature. (n.d.). LegiScan. Retrieved March 29, 2026, from https://legiscan.com/AK/text/SB247/id/3366263

Alaska: Statutory Criminal Law | Without My Consent. (n.d.). Retrieved March 29, 2026, from https://withoutmyconsent.org/50state/state-guides/alaska/statutory-criminal-law/?utm_source=chatgpt.com

Antigone Books L.L.C. v. Horne. (n.d.). *Global Freedom of Expression*. Retrieved March 4, 2026, from https://globalfreedomofexpression.columbia.edu/cases/antigone-books-l-l-c-v-horne/

Antigone update: Judge stays enforcement of AZ "nude image" law—Freedom to Read Foundation. (n.d.). Retrieved March 29, 2026, from https://www.ftrf.org/blogpost/852091/204140/Antigone-update-Judge-stays-enforcement-of-AZ-nude-image-law

Arizona Criminal Law Banning Nude Images Violates First Amendment. (n.d.). *ACLU of Arizona*. Retrieved March 28, 2026, from https://www.acluaz.org/press-releases/arizona-criminal-law-banning-nude-images-violates-first-amendment/

Arizona HB 2133 Sexual Material; Consent; Synthetic Depiction, Chapter 13, Article 1425; Chapter 44, Article 7302 Arizona Revised Statutes §§ 13-1425.

Arizona HB2001 | 2016 | Fifty-second Legislature 2nd Regular. (n.d.). LegiScan. Retrieved March 28, 2026, from https://legiscan.com/AZ/text/HB2001/id/1368420

Arizona HB2515 | 2014 | Fifty-first Legislature 2nd Regular. (n.d.). LegiScan. Retrieved March 29, 2026, from https://legiscan.com/AZ/text/HB2515/id/1012671

Arkansas Code of 1987 (2024): Title 5 - CRIMINAL OFFENSES (§§ 5-1-101 — 5-79-101) :: Subtitle 3 - OFFENSES INVOLVING FAMILIES, DEPENDENTS, ETC. (§§ 5-25-101 — 5-29-205) :: Chapter 26 - OFFENSES INVOLVING THE FAMILY (§§ 5-26-201 — 5-26-503) :: Subchapter 3 - DOMESTIC BATTERING AND ASSAULT (§§ 5-26-301 — 5-26-314) :: Section 5-26-314 - Unlawful distribution of sexual images or recordings. (n.d.). Justia Law. Retrieved March 31,

2026, from https://law.justia.com/codes/arkansas/title-5/subtitle-3/chapter-26/subchapter-3/section-5-26-314/

Artificial intelligence, deepfakes, and the uncertain future of truth. (n.d.). *Brookings*. Retrieved February 25, 2026, from https://www.brookings.edu/articles/artificial-intelligence-deepfakes-and-the-uncertain-future-of-truth/

Ashley St Clair, mother of Elon Musk's child, sues xAI over Grok deepfakes. (2026, January 16). https://www.bbc.com/news/articles/cp37erw0zwwo

Black, J. (2026, January 15). *Ashley St. Clair Sues Elon Musk's xAI, Alleging His Company Uses "AI to Undress, Humiliate, and Sexually Exploit Victims."* Vanity Fair. https://www.vanityfair.com/news/story/ashley-st-clair-elon-musk-lawsuits

Breach of Privacy, 21 Crimes and Punishments §§ 21-6101. Retrieved April 5, 2026, from https://www.ksrevisor.gov/statutes/chapters/ch21/021_061_0001.html L. 2010, ch. 136, § 171; L. 2011, ch. 63, § 1; L. 2016, ch. 96, § 5; L. 2024, ch. 96, § 5; L. 2025, ch. 120, § 3; July 1.

Brittain, C. (n.d.). *Decision and Order*.

Burleigh, N. (2013, September 17). Sexting, Shame and Suicide. *Rolling Stone*. https://www.rollingstone.com/culture/culture-news/sexting-shame-and-suicide-72148/

Carrie A. Goldberg, Esq. (n.d.). *C.A. Goldberg*. Retrieved April 26, 2026, from https://www.cagoldberglaw.com/our-crew/carrie-a-goldberg/

Central District of California | Operator of 'Revenge Porn' Website Sentenced to 2½ Years in Federal Prison in Email Hacking Scheme to Obtain Nude Photos | United States Department of Justice. (2015, December 3). https://www.justice.gov/usao-cdca/pr/operator-revenge-porn-website-sentenced-2-years-federal-prison-email-hacking-scheme

Chapter 106, Senate Bill 1462. (2025, April 21). [PDF]. Arizona Senate. https://apps.azleg.gov/BillStatus/BillOverview/82886

Civil Remedies for Nonconsensual Dissemination of Private Sexual Images Act., 740 Civil Liabilities § 740 ILCS 190/1-35. Retrieved April 5, 2026, from https://www.ilga.gov/Legislation/ILCS/Articles?ActID=4035&ChapterID=57&Chapter=CIVIL%20LIABILITIES&MajorTopic=RIGHTS%20AND%20REMEDIES P.A. 103-294, eff. 1-1-24; 103-571, eff. 12-8-23.

Clancy, E. M., Klettke, B., & Hallford, D. J. (2019). The dark side of sexting – Factors predicting the dissemination of sexts. *Computers in Human Behavior*, *92*, 266–272. https://doi.org/10.1016/j.chb.2018.11.023

Clancy, E. M., Klettke, B., Hallford, D. J., Crossman, A. M., Maas, M. K., & Toumbourou, J. W. (2020). Sharing is not always caring: Understanding motivations and behavioural associations with sext dissemination. *Computers in Human Behavior*, *112*, 106460. https://doi.org/10.1016/j.chb.2020.106460

Coursey, M. (2025, June 23). Image-Based Sexual Abuse Laws: Combat Nonconsensual AI Deepfakes. *RAINN*. https://rainn.org/rainns-recommendations-for-legislators/image-based-sexual-abuse-laws-combat-nonconsensual-ai-deepfakes/

Criminal Law, 3 Criminal Law § 809. Retrieved April 5, 2026, from https://mgaleg.maryland.gov/2026RS/Statute_Web/gcr/3-809.pdf

CRIMINALIZING REVENGE PORN | Secondary Sources | National | Westlaw. (n.d.). Retrieved February 16, 2026, from https://1-next-westlaw-com.proxy.lib.csus.edu/Document/I0765856b067911e498db8b09b4f043e0/View/FullText.html?navigationPath=Search%2Fv1%2Fresults%2Fnavigation%2Fi0a89a3780000019c6869b69c6884

7f6b%3Fppcid%3D72fa84f26af24a05948fedc839b2961c%26Nav%3DANALYTICAL%26fragmentIdentifier%3DI0765856b067911e498db8b09b4f043e0%26parentRank%3D0%26startIndex%3D1%26contextData%3D%2528sc.Search%2529%26transitionType%3DSearchItem&listSource=Search&listPageSource=e3c68ea0dd7e773b29218db90a60d71c&list=ANALYTICAL&rank=1&sessionScopeId=231c44414532c4b89e6d760131383dc252260a42e8032546f4cdd1a24d785185&ppcid=72fa84f26af24a05948fedc839b2961c&originationContext=Search%20Result&transitionType=SearchItem&contextData=%28sc.Search%29

Dekker, A. & Thula Koops. (2017). Sexting als Risiko? *Bundesgesundheitsblatt - Gesundheitsforschung - Gesundheitsschutz*, *60*(9), 1034–1039. https://doi.org/10.1007/s00103-017-2595-9

developer. (2025, April 28). CCRI Statement on the Passage of the TAKE IT DOWN Act (S. 146). *Cyber Civil Rights Initiative*. https://cybercivilrights.org/ccri-statement-on-the-passage-of-the-take-it-down-act-s-146/

Disclosing Explicit Synthetic Media, 18–6606 Crimes and Punishments: Sex Crimes. Retrieved April 4, 2026, from https://legislature.idaho.gov/statutesrules/idstat/Title18/T18CH66/SECT18-6606/ [18-6606, added 2024, ch. 105, sec. 1, p. 472.]

Disorderly Conduct: Invasion of Privacy, Section 647 Penal Code § 647 (2013). https://leginfo.legislature.ca.gov/faces/billCompareClient.xhtml?bill_id=201320140SB255&showamends=false

Disorderly Conduct: Unlawful Distribution If Image, Penal Code § 647 (2014). https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201320140SB1255

Dissemination of Sexually Explicit Visual Material of Another Person; Prohibition; Exceptions; Other Violations of Law; Violation; Penalty; Definitions, 750 Michigan Penal Code § 750.145e.

Retrieved April 5, 2026, from https://www.legislature.mi.gov/Laws/MCL?objectName=MCL-750-145E Add. 2016, Act 89, Eff. July 25, 2016

Distribution of an Intimate Image, 35 Criminal Law and Procedure §§ 35-45-4-8. Retrieved April 5, 2026, from https://iga.in.gov/laws/2025/ic/titles/35#35-45-4 .L.185-2019, SEC.3. Amended by P.L.79-2024, SEC.4.

Distribution of Sexually Explicit Images without Consent., 531 Pornography § 531.120 (2018). https://apps.legislature.ky.gov/law/statutes/statute.aspx?id=47656 Created 2018 Ky. Acts ch. 50, sec. 2, effective July 14, 2018.

Divito, N. (2013, March 12). Revenge Porn King Owes $250K for Defamation. *Courthouse News Service*. https://www.courthousenews.com/revenge-porn-king-owes-250k-for-defamation

Ex parte Jones, NO. 12-17-00346-CR | Tex. App., Judgment, Law, casemine.com. (n.d.). Https://Www.Casemine.Com. Retrieved March 9, 2026, from https://www.casemine.com/judgement/us/5e5d4ec64653d05304cf1521

Federal HR1 regulations on AI - Google Search. (n.d.). Retrieved May 6, 2026, from https://www.techpolicy.press/tracker/artificial-intelligence-and-information-technology-modernization-initiative-hr-1/

Federal Trade Commission. (2015, January 29). *Analysis of Proposed Consent Order to Aid Public Comment In the Matter of Craig Brittain* [Analysis]. Federal Trade Commission. https://www.ftc.gov/system/files/documents/cases/150129craigbrittainanalysis.pdf

Flynn, A., Powell, A., Eaton, A., & Scott, A. J. (2025). Sexualized Deepfake Abuse: Perpetrator and Victim Perspectives on the Motivations and Forms of Non-Consensually Created and Shared Sexualized Deepfake Imagery. *Journal of Interpersonal Violence*, 08862605251368834. https://doi.org/10.1177/08862605251368834

FTC Approves Final Order In Craig Brittain 'Revenge Porn' Case. (2016, January 8). Federal Trade Commission. https://www.ftc.gov/news-events/news/press-releases/2016/01/ftc-approves-final-order-craig-brittain-revenge-porn-case

Gassó, A. M., Forero, C. G., Piqueras, J., & Gómez-Durán, E. L. (2022). Psychopathological aspects of sexting and IBSA perpetrators: A brief research report. *Frontiers in Psychiatry*, *13*. https://doi.org/10.3389/fpsyt.2022.983881

Grok floods X with sexualized images of women and children. (n.d.). *Center for Countering Digital Hate | CCDH*. Retrieved April 26, 2026, from https://counterhate.com/research/grok-floods-x-with-sexualized-images/

Hall, M., & Hearn, J. (2019). Revenge pornography and manhood acts: A discourse analysis of perpetrators' accounts. *Journal of Gender Studies*, *28*(2), 158–170. (133897610). https://doi.org/10.1080/09589236.2017.1417117

Hanson, S. (2022). *"Weaponized sexuality" to the normalization of sexual violence: Rape culture and the nonconsensual distribution of intimate imagery (NCDII)* [Master of Arts in Criminal Justice, University of Winnipeg]. https://doi.org/10.36939/ir.202208251629

Harassment, 708 Assault § 708.7. Retrieved https://www.legis.iowa.gov/publications/search/document?fq=id:1592545&pdid=1545636#708.7

HB 1264 Concerning Measures to Clarify the Scope of Revenge Porn Criminal Offenses, 18-7–107, 18-7-108, Colorado Revised Statutes §§ 1, 2, 3, and 4 (2018). https://leg.colorado.gov/bills/hb18-1264

HB 1378 Concerning Prohibiting the Posting of a Provate Image on Social Media Without Consent to Cause Serious Emotionao Distress, 18-7–107, 18-7–108, 24-72-308.4, 24-72-709, Colorado Revised Statutes §§ 1, 2, 3, and 4 (2014). https://legiscan.com/CO/text/HB1378/id/1023230

HB2515—512R - I Ver. (n.d.). Retrieved March 4, 2026, from https://www.azleg.gov/legtext/51leg/2r/bills/hb2515p.htm

Henry, N., & Beard, G. (2024). Image-Based Sexual Abuse Perpetration: A Scoping Review. *Trauma, Violence, & Abuse*, *25*(5), 3981–3998. https://doi.org/10.1177/15248380241266137

Henry, N., & Flynn, A. (2019). Image-Based Sexual Abuse: Online Distribution Channels and Illicit Communities of Support. *Violence Against Women*, *25*(16), 1932–1955. https://doi.org/10.1177/1077801219863881

Henry, N., McGlynn, C., Flynn, A., Johnson, K., Powell, A., & Scott, A. J. (2020). *Image-based Sexual Abuse: A Study on the Causes and Consequences of Non-consensual Nude or Sexual Imagery* (1st ed.). Routledge. https://doi.org/10.4324/9781351135153

Hill, K. (n.d.). *How Hunter Moore Could Get Into Legal Trouble For The Revenge Porn On IsAnyoneUp*. Forbes. Retrieved March 7, 2026, from https://www.forbes.com/sites/kashmirhill/2011/11/22/how-hunter-moore-could-get-into-legal-trouble-for-the-revenge-porn-on-isanyoneup/

hlr. (2020, May 10). State v. VanBuren. *Harvard Law Review*. https://harvardlawreview.org/print/vol-133/state-v-vanburen/

Hou, Y. (2025, June 5). The H.R.1 Act and AI Regulation: Opportunities and Risks [News Website]. *The Medium*. https://medium.com/@lextrackai/the-h-r-1-act-and-ai-regulation-opportunities-and-risks-e6f5c1761e9c

House Bill 1967, Arkansas Code §§ 5-26-314 (2025). https://arkleg.state.ar.us/Home/FTPDocument?path=%2FBills%2F2025R%2FPublic%2FHB1967.pdf

Hu, Y., Clancy, E. M., & Klettke, B. (2023). Understanding the Vicious Cycle: Relationships between Nonconsensual Sexting Behaviours and Cyberbullying Perpetration. *Sexes*, *4*(1), 155–166. https://doi.org/10.3390/sexes4010013

Hulk Hogan won one of his most notable victories in a Florida courtroom. | AP News. (n.d.). Retrieved March 3, 2026, from https://apnews.com/article/hulk-hogan-gawker-lawsuit-sex-tape-9e0034fdbbaf8d0a60ee19acab49ec80

Invasions of Privacy; Transmission of Photography or Video Depicting Nudity or Sexually Explicit Conduct of an Adult under Certain Circumstances; Prohibit, HB 838, House 2013–14, Official Code of Georgia (2014). https://www.legis.ga.gov/legislation/40810

James, T. P. (2025). Not Her Fault: AI Deepfakes, Nonconsensual Pornography, and Not Her Fault: AI Deepfakes, Nonconsensual Pornography, and Federal Law's Current Failure to Protect Victims Federal Law's Current Failure to Protect Victims. *BRIGHAM YOUNG UNIVERSITY LAW REVIEW*.

Jeong, S. (2015, December 3). Hunter Moore Revenge Porn Victim Got a Whopping $145.70 in Restitution [News Website]. *Vice News*. https://www.vice.com/en/article/hunter-moore-revenge-porn-victim-got-a-whopping-14570-in-restitution/

Jones v. State, No. 12-22-00306-CR | Tex. App., Judgment, Law, casemine.com. (n.d.). Https://Www.Casemine.Com. Retrieved March 9, 2026, from https://www.casemine.com/judgement/us/6520df842cec034620addaf2

Judge Halts Enforcement of Unconstitutional Nude Photo Law in Arizona. (n.d.). *ACLU of Arizona*. Retrieved March 4, 2026, from https://www.acluaz.org/press-releases/judge-halts-enforcement-unconstitutional-nude-photo-law-arizona/

Kang, M., Lessard, D., Heston, L., & Nordmarken, S. (2017). *Social Constructionism*. https://openbooks.library.umass.edu/introwgss/chapter/social-constructionism/

Karasavva, V., & Forth, A. (2022). Personality, Attitudinal, and Demographic Predictors of Non-consensual Dissemination of Intimate Images. *Journal of Interpersonal Violence*, *37*(21–22), NP19265–NP19289. https://doi.org/10.1177/08862605211043586

Karasavva, V., Swanek, J., Smodis, A., & Forth, A. (2023). From myth to reality: Sexual image abuse myth acceptance, the Dark Tetrad, and non-consensual intimate image dissemination proclivity. *Journal of Sexual Aggression*, *29*(1), 51–67. https://doi.org/10.1080/13552600.2022.2032430

Kira, B. (2024). When non-consensual intimate deepfakes go viral: The insufficiency of the UK Online Safety Act. *Computer Law & Security Review*, *54*, 106024. https://doi.org/10.1016/j.clsr.2024.106024

Lake, J. (2021, September 23). *In the 19th century, a man was busted for pasting photos of women's heads on naked bodies … sound familiar?* The Conversation. https://doi.org/10.64628/AA.ew6m3je9g

Lefco, R. W. (2019, October 29). *People v. Austin: Is Revenge Porn Constitutionally Protected Speech?* Harvard Journal of Law & Technology. https://jolt.law.harvard.edu/digest/people-v-austin-is-revenge-porn-constitutionally-protected-speech

Leibert, D. (2025, August 26). Congress's Attempt to Criminalize Nonconsensual Intimate Imagery: The Benefits and Potential Shortcomings of the TAKE IT DOWN Act. *National Association of Attorneys General*. https://www.naag.org/attorney-general-journal/congresss-attempt-to-

criminalize-nonconsensual-intimate-imagery-the-benefits-and-potential-shortcomings-of-the-take-it-down-act/

Lenhart, A., Ybarra, M., & Price-Feeney, M. (n.d.). *Nonconsensual Image Sharing*.

Levendowski, A. (2022). Defragging Feminist Cyberlaw. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.4208296

Lorber, J. (2018). *The Social Construction of Gender* (pp. 318–325). https://doi.org/10.4324/9780429494468-36

Maas, M. K., Cary, K. M., Clancy, E. M., Klettke, B., McCauley, H. L., & Temple, J. R. (2021). Slutpage Use Among U.S. College Students: The Secret and Social Platforms of Image-Based Sexual Abuse. *Archives of Sexual Behavior*, *50*(5), 2203–2214. https://doi.org/10.1007/s10508-021-01920-1

maintenance. (n.d.). Image-based sexual abuse. *Victim Support*. Retrieved February 16, 2026, from https://www.victimsupport.org.uk/crime-info/types-crime/image-based-sexual-abuse/

Man Who Operated 'Revenge Porn' Website Pleads Guilty in Hacking Scheme That Yielded Nude Photos from Google E-Mail Accounts—FBI. (n.d.). [Press Release]. Retrieved March 7, 2026, from https://www.fbi.gov/contact-us/field-offices/losangeles/news/press-releases/man-who-operated-revenge-porn-website-pleads-guilty-in-hacking-scheme-that-yielded-nude-photos-from-google-e-mail-accounts

McGibney v. Moore | Digital Media Law Project. (n.d.). Retrieved March 7, 2026, from https://www.dmlp.org/threats/mcgibney-v-moore

McGlynn, C., Johnson, K., Rackley, E., Henry, N., Gavey, N., Flynn, A., & Powell, A. (2021). 'It's Torture for the Soul': The Harms of Image-Based Sexual Abuse. *Social & Legal Studies*, *30*(4), 541–562. https://doi.org/10.1177/0964663920947791

Mental health correlates of sexting coercion perpetration and victimisation in university students by gender. (n.d.). *Journal of Sexual Aggression*. Retrieved February 16, 2026, from https://www.tandfonline.com/doi/abs/10.1080/13552600.2021.1894493

Mithani, J. (2026, January 13). Senate moves to let victims of sexually explicit deepfakes sue for damages. *The 19th*. https://19thnews.org/2026/01/senate-defiance-act-nonconsensual-images-deepfakes/

Morin, A. (n.d.). *Hoganv.Gawker: AA LLeegg—DDrroopp oonn tthhee FFiirrsstt AAmmeennddmmeennttt*.

Moseley, B. (2017, June 1). Ivey signs new sex offense Legislation. *Alabama Political Reporter*. https://www.alreporter.com/2017/06/01/ivey-signs-new-sex-offense-legislation/

Musk's Grok AI chatbot is still making sexual deepfakes, despite X's promise to stop it. (2026, April 14). NBC News. https://www.nbcnews.com/tech/tech-news/musks-ai-chatbot-grok-xai-making-sexual-deepfakes-imagine-rcna265855

Non-consensual deepfakes, consent, and power in synthetic media | Digital Watch Observatory. (2026, January 28). https://dig.watch/updates/non-consensual-deepfakes-consent-and-power-in-synthetic-media

Nonconsensual Disclosure of a Private Image, 283 Revised Statutes § 283.2. Retrieved April 5, 2026, from https://www.legis.la.gov/legis/Law.aspx?d=963342 Acts 2015, No. 231, §1; Acts 2024, No. 11, §1; Acts 2024, No. 65, §1; Acts 2024, No. 431, §1.

Nonconsensual Dissemination of Private Sexual Images, 671 Crimes; Expungement; Victims § 261. Retrieved https://www.revisor.mn.gov/statutes/cite/617.261 2016 c 126 s 9

Non-Consensual Dissemination of Private Sexual Images., 720 Criminal Code § 5/11-23.5 (2012). https://www.ilga.gov/legislation/ILCS/details?MajorTopic=RIGHTS%20AND%20REMEDIES

&Chapter=CRIMINAL%20OFFENSES&ActName=Criminal%20Code%20of%202012.&ActID=1876&ChapterID=53&ChapAct=720+ILCS+5%2F&SeqStart=19100000&SeqEnd=20300000

P.A. 103-825, eff. 1-1-25.

Non-Consensual Dissemination of Sexually Explicit Digitized Depictions., 720 Criminal Code § 5/11-23.7 (2012). https://www.ilga.gov/legislation/ILCS/details?MajorTopic=RIGHTS%20AND%20REMEDIES&Chapter=CRIMINAL%20OFFENSES&ActName=Criminal%20Code%20of%202012.&ActID=1876&ChapterID=53&ChapAct=720+ILCS+5%2F&SeqStart=19100000&SeqEnd=20300000

P.A. 103-825, eff. 1-1-25; 104-417, eff. 8-15-25.

Nonconsensual Distribution of Intimate Imagery. (n.d.). Retrieved April 26, 2026, from https://www.americanbar.org/advocacy/governmental_legislative_work/publications/washingtonletter/june-22-wl/intimate-imagery-0622wl/

Okolie, C. (2023). Artificial Intelligence-Altered Videos (Deepfakes), Image-Based Sexual Abuse, and Data Privacy Concerns. *Artificial Intelligence*, *25*.

Paradiso, M. N., Rollè, L., & Trombetta, T. (2024). Image-Based Sexual Abuse Associated Factors: A Systematic Review. *Journal of Family Violence*, *39*(5), 931–954. https://doi.org/10.1007/s10896-023-00557-z

Penzo, S. C. (n.d.). *5 By: Representative K. Brown*.

People v. Austin. (n.d.). *Global Freedom of Expression*. Retrieved March 9, 2026, from https://globalfreedomofexpression.columbia.edu/cases/people-v-austin/

Photographing, Videotaping or Electronically Surveiling Partially Nude or Nude Person or the Sexual or Other Intimate Parts of a Person around the Person's Clothing; Exceptions; Punishment, 272

Crimes Against Chasity, Morality, Decency and Good Order § 105. Retrieved https://malegislature.gov/Laws/GeneralLaws/PartIV/TitleI/Chapter272/Section105

Pierce, J. J., Siddiki, S., Jones, M. D., Schumacher, K., Pattison, A., & Peterson, H. (2014). Social Construction and Policy Design: A Review of Past Applications. *Policy Studies Journal*, *42*(1), 1–29. https://doi.org/10.1111/psj.12040

Pina, A., Holland, J., & James, M. (2017). The Malevolent Side of Revenge Porn Proclivity: Dark Personality Traits and Sexist Ideology. *International Journal of Technoethics*, *8*(1), NA-NA. https://doi.org/10.4018/IJT.2017010103

Powell, A., Henry, N., Flynn, A., & Scott, A. J. (2019). Image-based sexual abuse: The extent, nature, and predictors of perpetration in a community sample of Australian residents. *Computers in Human Behavior*, *92*, 393–402. https://doi.org/10.1016/j.chb.2018.11.009

Prohibition on Nude or Sexually Explicit Electronic Transmissions., 16-11–90 Invasion of Privacy. Retrieved https://advance.lexis.com/documentpage/?pdmfid=1000516&crid=3a5e496d-09a8-48b8-8f0d-cadcbe57b9a9&nodeid=AAQAAMAAEAAEAAB&nodepath=%2FROOT%2FAAQ%2FAAQAAM%2FAAQAAMAAE%2FAAQAAMAAEAAE%2FAAQAAMAAEAAEAAB&level=5&haschildren=&populated=false&title=16-11-90.+Prohibition+on+nude+or+sexually+explicit+electronic+transmissions.&config=00JAA1MDBlYzczZi1lYjFlLTQxMTgtYWE3OS02YTgyOGM2NWJlMDYKAFBvZENhdGFsb2feed0oM9qoQOMCSJFX5qkd&pddocfullpath=%2Fshared%2Fdocument%2Fstatutes-legislation%2Furn%3AcontentItem%3A65DR-WD13-GXF6-83DD-00008-00&ecomp=6gf59kk&prid=088ae9ba-aa58-4616-98a6-2ad4a0c5c3a4 Code 1981, § 16-11-90, enacted by Ga. L. 2014, p. 220, § 1/HB 838; Ga. L. 2015, p. 5, § 16/HB 90; Ga. L. 2020, p.

579, § 1/SB 337; Ga. L. 2021, p. 442, § 1/SB 78; Ga. L. 2021, p. 922, § 16/HB 497; Ga. L. 2022, p. 352, § 16/HB 1428.

Renner, N. (2016, April 27). How Hulk Hogan v. Gawker May Change the Face of Journalism. *JSTOR Daily*. https://daily.jstor.org/journalism-in-age-of-hulkamania/

Revenge Porn Laws: State by State. (n.d.). *C.A. Goldberg*. Retrieved March 15, 2026, from https://www.cagoldberglaw.com/resources/states-with-revenge-porn-laws/

"Revenge porn" site owner Hunter Moore sued for defamation. (2013, March 11). *BBC News*. https://www.bbc.com/news/technology-21740386

Revenge-Porn King Hunter Moore Indicted on Federal Charges. (2014, January 23). TIME. https://time.com/1703/revenge-porn-king-hunter-moore-indicted-by-fbi/

Ringrose, J., Regehr, K., & Whitehead, S. (2022). 'Wanna trade?': Cisheteronormative homosocial masculinity and the normalization of abuse in youth digital sexual image exchange. *Journal of Gender Studies*, *31*(2), 243–261. https://doi.org/10.1080/09589236.2021.1947206

Rogers, M. M., Fisher, C., Ali, P., Allmark, P., & Fontes, L. (2023). Technology-Facilitated Abuse in Intimate Relationships: A Scoping Review. *Trauma, Violence, & Abuse*, *24*(4), 2210–2226. https://doi.org/10.1177/15248380221090218

Ruvalcaba, Y., & Eaton, A. A. (2020). Nonconsensual pornography among U.S. adults: A sexual scripts framework on victimization, perpetration, and health correlates for women and men. *Psychology of Violence*, *10*(1), 68–78. https://doi.org/10.1037/vio0000233

Said, I., & McNealey, R. L. (2023). Nonconsensual Distribution of Intimate Images: Exploring the Role of Legal Attitudes in Victimization and Perpetration. *Journal of Interpersonal Violence*, *38*(7–8), 5430–5451. https://doi.org/10.1177/08862605221122834

Sangster, E. (2022, August 2). Is Anyone Up?: Who is Hunter Moore, AKA The Most Hated Man On the Internet [News Website]. *Harper's Bazaar Australia*. https://harpersbazaar.com.au/hunter-moore-is-anyone-up/

SB 100 Concering the Creation of the "Uniform Civil Remedies for Unauthorized Disclosure of Intimate Images Act," 13-21–1401, 13-21–1402, 13-21–1403, 13-21–1404, 13-21–1405, 13-21–1406, 13-21–1407, 13-21–1408, 13-21–1409, 18-7–107, 18-7–108 Colorado Revised Statutes §§ 1-4 (2019). https://leg.colorado.gov/bill_files/65273/download

Schneider, A., & Sidney, M. (2009). What Is Next for Policy Design and Social Construction Theory?1. *Policy Studies Journal*, *37*(1), 103–119. https://doi.org/10.1111/j.1541-0072.2008.00298.x

Sexual Cyberharassment, HB 1451, House 2025, Florida Statutes (2025). https://www.flsenate.gov/Session/Bill/2025/1451/?Tab=BillHistory

Somaiya, R. (2016, March 17). Hulk Hogan v. Gawker: A Guide to the Trial for the Perplexed. *The New York Times*. https://www.nytimes.com/2016/03/18/business/media/hulk-hogan-v-gawker-a-guide-to-the-trial-for-the-perplexed.html

Sparks, B. (2022). A Snapshot of Image-Based Sexual Abuse (IBSA): Narrating a Way Forward. *Sexuality Research & Social Policy*, *19*(2), 689–704. https://doi.org/10.1007/s13178-021-00585-8

Take It Down Act, addressing nonconsensual deepfakes and "revenge porn," passes. What is it? (n.d.). U.S. Senator Amy Klobuchar. Retrieved February 25, 2026, from https://www.klobuchar.senate.gov/public/index.cfm/2025/4/take-it-down-act-addressing-nonconsensual-deepfakes-and-revenge-porn-passes-what-is-it

TFGBV: Deepfakes and Image-Based Abuse. (n.d.). Office for the Prevention of Domestic Violence. Retrieved February 25, 2026, from https://opdv.ny.gov/tfgbv-deepfakes-and-image-based-abuse

Træen, B., & Kvalem, I. L. (2023). Gender Differences in Sending Nude Pictures and Videos Across Multiple Relationship Contexts in the Adult Norwegian Population. *Sexuality & Culture*, *27*(2), 570–590. https://doi.org/10.1007/s12119-022-10028-0

Transcript—How Grok Filled X With Deepfake Porn. (n.d.). Slate Magazine. Retrieved April 26, 2026, from https://slate.com/transcripts/TUJpdEozYTlob2JhcDBUQk51bUU5WU5FbjlyZVNpU0ZiS2taMjB6U2ZWVT0=

Unauthorized Dissemination of Certain Private Images, 17-A Maine Criminal Code §§ 511-A. Retrieved April 5, 2026, from https://legislature.maine.gov/statutes/17-a/title17-Asec511-A.html PL 2015, c. 339, §1 (NEW). PL 2015, c. 394, §5 (AMD). PL 2015, c. 410, Pt. A, §1 (AMD). PL 2025, c. 400, §§2, 3 (AMD).

Unlawful Dissemination or Sale of Images of Another Created by Artificial Intelligence, 14 Revised Statutes § 73.13 (2024). https://www.legis.la.gov/legis/Law.aspx?d=1388452 Acts 2024, No. 142, §1

Video Voyeurism, 18–6605 Crimes and Punishments. Retrieved April 4, 2026, from https://legislature.idaho.gov/statutesrules/idstat/Title18/T18CH66/SECT18-6605/ [(18-6605) 18-6609, added 2004, ch. 122, sec. 1, p. 410; am. 2014, ch. 173, sec. 1, p. 477; am. 2018, ch. 256, sec. 1, p. 606; am. and redesig. 2022, ch. 124, sec. 9, p. 438.]

Viola, M., & Voto, C. (2023). Designed to abuse? Deepfakes and the non-consensual diffusion of intimate images. *Synthese*, *201*(1), 30. https://doi.org/10.1007/s11229-022-04012-2

Violation of Privacy; Class A Misdemeanor; Class G Felony., Title 11, Chapter 5 Crimes and Criminal Procedure—Special Offenses § 1335. Retrieved April 5, 2026, from https://delcode.delaware.gov/title11/c005/sc07/index.html#1335 11 Del. C. 1953, § 1335; 58 Del. Laws, c. 497, § 1; 67 Del. Laws, c. 130, § 8; 70 Del. Laws, c. 186, § 1; 72 Del. Laws, c. 180, §§ 1-3; 73 Del. Laws, c. 172, §§ 1, 2, 3; 75 Del. Laws, c. 341, §§ 1, 2; 79 Del. Laws, c. 415, § 1; 81 Del. Laws, c. 79, § 11; 84 Del. Laws, c. 42, § 1; 84 Del. Laws, c. 479, § 2;

Violation of Privacy in the First Degree, 711 Offenses Against Public Order §§ 711-1110.9. Retrieved April 4, 2026, from https://www.capitol.hawaii.gov/hrscurrent/Vol14_Ch0701-0853/HRS0711/HRS_0711-1110_0009.htm Act 278, Session Laws 1999, Act 48, Session Laws 2003, Act 83, Session Laws 2004, Act 116, Session Laws 2014, Act 114, Session Laws 2018, Act 59, Session Laws 2021

Vivek, D. (n.d.). *Deepfakes and AI-Generated Intimate Images Involving Minors*.

Wagner, T., & Blewer, A. (2019). "The Word Real Is No Longer Real": Deepfakes, Gender, and the Challenges of AI-Altered Video. *Open Information Science*, *3*, 32–46. https://doi.org/10.1515/opis-2019-0003

Walker, K., & Sleath. (2017). A systematic review of the current knowledge regarding revenge pornography and non-consensual sharing of sexually explicit media. *Aggression and Violent Behavior*, *36*, 9–24. https://doi.org/10.1016/j.avb.2017.06.010

Walker, K., Sleath, E., Hatcher, R. M., Hine, B., & Crookes, R. L. (2021). Nonconsensual Sharing of Private Sexually Explicit Media Among University Students. *Journal of Interpersonal Violence*, *36*(17–18), NP9078–NP9108. https://doi.org/10.1177/0886260519853414

Williams, G. (2015, December 4). How "the godfather of revenge porn" rose, and fell, on the internet. *Wired*. https://www.wired.com/story/hunter-moore-revenge-porn-ruling/

WION. (2026, January 14). *Elon Musk In Trouble? | Ashley St. Clair Accuses Grok Of AI Deepfake Abuse | WION* [Video recording]. https://www.youtube.com/watch?v=y7pInYPSbm8

Zhong, L. R., Kebbell, M. R., & Webster, J. L. (2020). An exploratory study of Technology-Facilitated Sexual Violence in online romantic interactions: Can the Internet's toxic disinhibition exacerbate sexual aggression? *Computers in Human Behavior*, *108*, 106314. https://doi.org/10.1016/j.chb.2020.106314

(N.d.-a). Alaska State Legislature. Retrieved March 29, 2026, from https://www.akleg.gov/basis/Bill/Text/24?Hsid=HB0326A

(N.d.-b). Alaska Statutes 2024. Retrieved March 29, 2026, from https://www.akleg.gov/basis/statutes.asp#11.61.110