September 2025

A Weapon Against Women in Politics: Reining in Nonconsensual Synthetic Intimate Imagery

Adriana Stephan

Future Security
Last edited on September 17, 2025 at 1:52 p.m. EDT

Acknowledgments

The author thanks Helen Margetts for her support; Lauren Zabierek, Camille Stewart Gloster, Peter W. Singer, Bridget Chan, Pavlina Pavlova, Ben Polsky, and Paul B. Stephan for their feedback on this report; and the many experts who contributed their time to be interviewed. Their valuable insights inform this work.

Editorial disclosure: The views expressed in this report are solely those of the author and do not reflect the views of New America, its staff, fellows, funders, or board of directors.

About the Author

Adriana Stephan is a 2025 #ShareTheMicInCyber Fellow.

About New America

We are dedicated to renewing the promise of America by continuing the quest to realize our nation's highest ideals, honestly confronting the challenges caused by rapid technological and social change, and seizing the opportunities those changes create.

About Future Security

Future Security is a partnership between New America and Arizona State University. It reconceptualizes U.S. security policy towards a holistic engagement with current and future challenges including domestic terrorism, armed drones, climate change, pandemics, rising authoritarianism, and new and emerging technologies.

About #ShareTheMicInCyber Fellowship

The #ShareTheMicInCyber Fellowship invests, grows, and platforms emerging cybersecurity and technology leaders from traditionally underrepresented backgrounds in support of strengthening our nation's resilience to digital threats.

Contents

Contents Cont'd

Introduction

When asked about experiencing abuse, including online abuse, for a 2016 global study on harassment against women members of parliament, several participants expressed resignation: "It is the norm. If you react, everyone says, 'So what? Big deal!'" Another parliamentarian from sub-Saharan Africa described these attacks as part of "the political culture," stating, "You have to get used to it."[1] This normalization of abuse reveals a troubling acceptance of incidents that should be recognized as a serious threat to democratic participation.

Nonconsensual synthetic intimate images (NSII) pose a documented threat to women in politics. Yet this form of image-based abuse remains largely overlooked in discussions of the impact of artificial intelligence (AI) on democratic processes. A 2016 survey of 55 women parliamentarians from 39 countries revealed that 42 percent of respondents had encountered "extremely humiliating or sexually charged" images of themselves shared on social media, including doctored images depicting them nude.[2] Since easily accessible AI-based tools to generate images were introduced in 2022, the problem for women political leaders has likely become much worse. Despite extensive media attention on the potential for AI-generated impersonations to disrupt elections, NSII targeting individuals in the political sphere, including candidates as well as elected and unelected public officials (hereafter collectively referred to as "public officials"), remains vastly underreported and underresearched.[3]

This report aims to address this critical gap in research by examining how NSII is weaponized against public officials across countries and varying political contexts. Through exploratory analysis of 100 documented cases in 14 countries, this study investigates which public officials are targeted globally, documents the specific tactics and internet ecosystems enabling these attacks, and examines their impact on victims. These documented cases likely represent only the visible portion of a much larger phenomenon. The findings presented here inform evidence-based recommendations designed to prevent NSII creation and limit its spread, and ultimately to protect democratic participation from this evolving technological threat.

Defining Nonconsensual Synthetic Intimate Imagery

Artificial intelligence (AI) revolutionizes the creation of nonconsensual synthetic intimate imagery (NSII) by increasing the scale and speed with which perpetrators can create explicit images. Using computer vision and generative AI techniques, "nudification" applications can digitally remove clothing from photographs or videos of real people. These tools enable users without technical or even photo editing skills to generate intimate imagery of an individual without their consent.

NSII encompasses any digitally altered intimate images of a person created without the consent of the image subject.[4] NSII falls under the broader category of synthetic media, which refers to any form of media that has been digitally manipulated or created to represent something that does not exist in reality.[5] These images or videos are created using technologies from traditional photo editing software to sophisticated AI algorithms. NSII represents a form of image-based sexual abuse involving the nonconsensual creation or distribution of nude or sexual imagery, or the threat to do so, often as a form of control, power, or harassment.[6]

NSII is produced through several methods: face-swapping technology that replaces someone's face onto existing adult content or live sexual videos; digital image manipulation that alters photographs to make clothed individuals appear undressed; or artificial intelligence generation that creates completely new images depicting people in nude or sexual situations.[7] The technologies can be used for creative and positive purposes. For example, educators can use AI image generators to create infographics and other instructional material.[8] However, the availability of these tools makes their use more widespread and the potential for harm significant, transforming what was once a technically complex process requiring specialized skills into something virtually anyone with internet access can do.

The term "deepfake" is commonly used to describe digitally altered content to make it appear that a person is doing or saying something that they never actually did or said. The history of deepfakes is firmly rooted in the harassment of women: The term itself was coined in 2017 by a Reddit moderator who created a now-removed subreddit for users to exchange nonconsensual, falsified sexual videos of female celebrities.[9] Survey data suggested a serious problem back in 2019; 14.1 percent of 864 total respondents in a nonrepresentative survey across the United Kingdom, Australia, and New Zealand reported experiencing the creation, distribution, or threat of distributing a digitally altered sexualized image of them.[10] By 2023, the top 10 explicit deepfake websites attracted over 34 million monthly visitors. An oftcited 2023 report estimated that 98 percent of deepfake videos online were "pornographic" and 99 percent of those pornographic deepfake videos targeted women, the vast majority of which were prominent actresses and musicians.[11]

An Enabling Ecosystem

Both the creation and distribution of NSII are facilitated by a complex internet infrastructure encompassing payment providers, search engines, app stores, AI model-hosting platforms, and mainstream social media sites. This ecosystem has commercialized the nonconsensual sexualization of women's bodies, with numerous "nudify" applications operating as profitable businesses that monetize gender-based abuse.[12]

Historically, combating NSII has been complicated by fragmented approaches across the internet ecosystem, including divergent platform policies.[13] While some platforms proactively banned the sharing of sexual deepfakes and digitally altered content, many others were slow to respond, or required victims to self-identify and report the imagery for it to be removed, placing the enforcement burden on those being harmed.[14]

NSII is, by definition, nonconsensual. While deepfake technology has applications protected by free speech laws in many countries, such as in entertainment and parody, these same tools become harmful when used to generate intimate imagery without consent. The technology serves both legitimate and harmful purposes. This creates enforcement challenges for technology companies that enable deepfake creation and must distinguish between legitimate and harmful uses of the same underlying tools.

As governments increasingly enact legislation to address NSII, such as the TAKE IT DOWN Act, enacted May 2025 in the United States, platforms face increasing legal pressure to remove such content. For example, a provision of the TAKE IT DOWN Act requires removal of nonconsensual intimate imagery (AI-generated or otherwise) within 48 hours of a verified request.[15] The distributed nature of the internet creates multiple intervention points where different stakeholders, from AI developers to payment processors, can disrupt the NSII pipeline. Despite this, significant challenges to curbing the creation and spread of NSII remain due to the financial incentives driving this ecosystem.

Creation Infrastructure

AI Developers: AI models power nudification websites. Historically, AI developers have made open-source models that offer the functionality to create deepfake nudes, including popular image generators like Stable Diffusion and Flux. These models require limited technical expertise from users, who can easily deploy them to create AI nudification websites or apps.[16] A 2023 Graphika report estimates that the increasing capability and accessibility of open-source AI image diffusion models are the primary driver of growth in NSII services.[17]

Apps: The proliferation of bad-faith "nudify" applications, which allow users to upload a photo and receive back a "nude" version of the subject, has fueled a market based on exploiting women's images. These apps typically sell various nudification features with very limited free functionality.[18] One popular app has an annual budget of $3.5 million, according to a whistleblower.[19] Nudify apps advertise their services as creating fake nonconsensual nude or sexually explicit images of women, in some cases specifically marketing to young men and boys.[20]

Most of these apps use a machine learning model trained to predict how an image subject would look naked and then alter the image to represent their as-predicted nude bodies. Other apps leverage AI face-swapping to morph the subject's face onto another person's body. Additional features of applications allow a user to put a subject in sexual scenes. One study found that the vast majority of the apps studied (19 out of 20) explicitly specialize in the undressing of women, while only half mention that they expect the user to have the image subject's consent, and fewer ask for affirmation that consent has been obtained.[21]

Model and App Hosting Platforms: The proliferation of AI tools capable of creating NSII has created enforcement challenges across two key channels: model-hosting platforms and mobile app stores.

Model-hosting platforms like Civitai, Hugging Face, and GitHub have become primary repositories for AI models designed for nudification and deepfake creation, enabling both at commercial scale.[22] One study found a huge rise in easily accessible deepfake models on model-hosting platforms, particularly on Civitai.[23] Over 34,000 deepfake model variants, many of which indicate an intention or capability to generate NSII, have been downloaded almost 15 million times since 2022 and were available on popular repositories.[24] Models hosted by these platforms allow users to generate pornographic videos of anyone they have an image of.[25] In some cases, models hosted on these platforms power some of the most prolific NSII creation websites and services.[26]

Simultaneously, app stores such as Google Play Store and Apple App Store serve as critical hosts for mobile applications that specialize in nonconsensual "undressing" of women. These apps often utilize the underlying models hosted on the platforms, creating an interconnected ecosystem where model repositories provide the technical foundation and app stores provide user-friendly access points. While the exact number of nudify apps remains unclear, research from July 2025 examined 85 model-hosting platforms and found they collectively attracted an average of 18.5 million visitors over six months, with the potential to generate up to $36 million annually.[27]

Even when models violate terms of service, model-hosting platforms have found it difficult to prevent abuse of these tools.[28] After Civitai banned 50,000 models that were being used to generate NSII, users migrated thousands of these models to another popular model-hosting platform as part of a concerted community effort to preserve the models.[29] Even when they attempt to remove bad actors, these platforms struggle with enforcement and face diverse technical challenges. For example, for text-to-image generators, platforms can develop safeguards that refuse to generate images based on an inappropriate written prompt—but it is more challenging to build such protections into tools that generate videos based on images.[30]

Distribution Networks

Social Media Platforms: Online platforms play a pivotal role in allowing users to create NSII through bots, directing users to nudify sites via advertisements, or enabling the circulation of NSII. In the context of NSII targeting public officials, perpetrators often leverage mainstream social media platforms to give the explicit content a broader audience. The harms of NSII are magnified when such content spreads widely.[31] Though most mainstream social media platforms actively prohibit NSII, enforcement is often insufficient, as demonstrated by a recent case involving Taylor Swift, where such content was viewed 27 million times in 19 hours.[32]

The role of social media platforms as a marketing tool for NSII services is growing. NSII providers leverage mainstream platforms to advertise their capabilities or direct users to their own websites via referral link spam. A 2023 report estimated the volume of referral link spam for nudify services increased by more than 2,000 percent on platforms, including Reddit and X, from January to December 2023.[33] In June 2025, Meta sued one such company that had advertised on Facebook and Instagram.[34]

Deepfake Platforms: Following their widespread deplatforming on mainstream social media platforms, portions of the deepfake community migrated to dedicated platforms to continue discussing deepfake technology and share their creations. These platforms are home to forums explicitly devoted to technical assistance, dataset sharing, and the deepfake market.[35] A 2024 estimate has 94 percent of NSII material hosted on sites dedicated to the practice.[36] One of the most prominent of these platforms received 17 million visitors a month before it was shut down by its internet service provider.

Bots: Some online communities are centered on sharing and trading images of nonconsensual intimate images. One Telegram channel with over 45,000 unique members hosted bots that allow users to submit a photo and receive a nude back within minutes.[37] A 2024 investigation found 50 nudify bots on Telegram that had reached over 4 million monthly users combined.[38] Even after the bots are removed, the software that powers the programs can be found on open source repositories and torrenting websites.[39] These communities all share tips and tricks for other methods for generating the same type of videos without the bot.[40]

Supporting Infrastructure

Search Engines and App Stores: Platforms that support discovery of deepfake platforms or apps through search play an important role in the visibility of NSII. In 2023, Google was the single largest driver of traffic to deepfake porn websites.[41] In recent years, intimate deepfake videos of women could be found at the top of Google search results.[42]

Internet Service Providers: Internet service providers (ISPs) offer the infrastructure on which nudify apps or deepfake platforms rely. In some cases, ISPs do act to remove websites when they violate their terms of service. A service provider withdrew its support for one of the most prominent and mainstream marketplaces for intimate deepfakes after facing mounting scrutiny.[43] As an internet governance mechanism, however, ISP removals are a particularly blunt instrument that can be abused to wipe entire websites alleged of hosting obscene content off the internet.[44]

Online Payment Providers: Payment providers play a pivotal role in the NSII ecosystem, as most nudification applications or platforms operate as commercial enterprises. Many of these applications rely on third-party payment processors or cryptocurrency transactions.[45] One study found cryptocurrency to be the most popular avenue for payment for nudify apps. Nevertheless, many platforms still attempt to use mainstream payment providers like PayPal, despite policies that typically ban processing payments for NSII services.[46] The potential power of payment processors to influence platform behavior became evident when they threatened to stop processing payments from Civitai unless the platform updated its rules to prevent hosting models that could be abused to create NSII.[47]

The Targeting of Female Public Officials

Internet-based platforms can allow female politicians to communicate directly with their constituents, overcoming the marginalization and bias they might face in traditional media outlets. These platforms also expose them to alarming levels of sexism, harassment, and threats, which can have damaging effects on young women's political ambitions.[48]

University of Virginia law professor Danielle Citron argues that women are often "canaries in the coal mine" when it comes to early uses of digital technologies, offering early warning indicators of how new digital tools will be misused.[49] In 2007, online harassers targeted a software developer and prominent blogger with rape and death threats, doctored images, and doxxing, posting her Social Security number and home address online. Although her blog, "Creating Passionate Users," was building her reputation in the tech community, she suspended it and canceled public appearances.[50]

Highly visible women, including media personas, human rights defenders, and public officials, often become early targets of technology-facilitated abuse, serving as harbingers of broader patterns to come. As one female parliamentarian observed about nonconsensual synthetic intimate imagery (NSII): "Whatever new things come up, it's always used against the women first. They are the victim in every case. AI is not an exception in any way."[51] #MyImageMyChoice, a nonprofit that researches NSII prevalence, notes that one of the groups of women disproportionately targeted is those connected to politics.[52]

Women politicians report being extremely concerned about the pervasiveness of gender-based abuse in the digital space as a real barrier and a serious disincentive for young women to consider a political career.[53] In a recent global survey of 14,000 girls and young women, half of the respondents experienced harassment for voicing political opinions. Of those that experienced harassment, 20 percent self-censored online as a result.[54] One study found strong evidence that in Kenya and Colombia, online harassment and threats decreased politically active women's willingness to voice political opinions online.[55] Generally, experts are concerned that NSII will have a higher cost for female politicians, who already face higher levels of harassment and defamation than men in the field.[56]

Case Studies and Key Insights

The following analysis focuses specifically on the targeting of public officials with nonconsensual synthetic intimate imagery (NSII), investigating the patterns and tactics used in 100 incidents weaponizing NSII against public officials across 14 countries. To identify documented cases, this research employed keyword searches to identify English-language reports of NSII targeting politicians or public officials. This research drew from media reporting, artificial intelligence (AI) incident databases, academic papers, and think tank reports.[57]

The data collection took place over a four-month period between February and June 2025. The research surfaced reports of NSII targeting public officials between 2017 and 2025. The vast majority of examples (92 of 100) took place between 2022 and 2025. This may be a result of the widespread availability of AI tools, increased media awareness of the issue of NSII, or other factors. This research did not have a specific geographic focus but was intended to surface any English-language report of NSII targeting a public official.

There are several limitations to the methodology. As sourcing involved English-language AI incident databases and keyword searches, predominantly English-language sources surfaced.[58] This likely leaves crucial data gaps from non-English language sources. In addition, the analysis relied on the reporting of third parties or self-reporting, which naturally yielded data gaps, in particular on which platforms NSII surfaced, how much user engagement it received, and how quickly platforms acted to limit its spread. Given the reliance on third parties, it was not possible to independently verify the accuracy of reports.

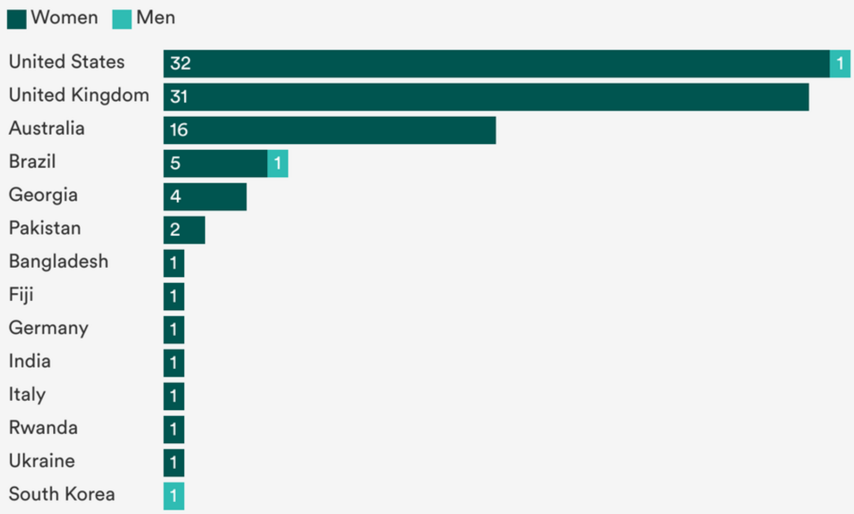
The observations presented here emerge from a limited set of case studies and constitute a qualitative analysis of available data. Given the limitations of this analysis, it is impossible to broadly generalize about the prevalence of NSII globally, the tactics employed, or the types of officials most frequently targeted. Another important caveat is that similar to other forms of image-based sexual abuse, NSII is likely a significantly underreported phenomenon. The limited number of documented cases should not be interpreted as evidence of low prevalence, but rather as a reflection of the challenges in documenting and reporting these attacks. When researchers do investigate, they find ample examples. In the United States, one report found tens of thousands of sexualized deepfakes depicting 26 members of Congress (25 women and one man).[59]

Demographics

NSII attacks disproportionately target female officials, with women comprising the vast majority of victims in documented cases. Out of 100 examples, only three involved male public officials: the governor of São Paulo, a former South Korean president, and one member of the U.S. Congress (see Figure 1). Female targets span the entire spectrum of public officials, from high-profile presidential candidates to local city commissioners, ambassadors, and civil servants.

Figure 1 | Women Public Officials Are Disproportionately Impacted by Nonconsensual Synthetic Intimate Image Attacks

Documented number of public officials subject to NSII attacks, by country



Source: New America analysis of publicly available data.

NEW AMERICA

Electoral Timing

In at least 42 of the documented cases, women were targeted during critical political moments, including during campaign periods and the weeks immediately prior to an election. The strategic timing of these attacks points toward NSII as a tool of political interference. By targeting women during high-visibility campaign periods and elections, perpetrators can maximize both the psychological impact on victims and the potential to influence voter perceptions at crucial moments. This timing pattern demonstrates that NSII can undermine women's political representation precisely when their voices and leadership are most visible and consequential.

→ **CASE STUDY**

Cara Hunter, a politician in Northern Ireland, was weeks away from the 2022 national legislative elections when her face was superimposed onto the face of another person in a deepfake video.[60] According to the politician, the video was shared thousands of times across WhatsApp and social media.[61] The timing created particularly difficult choices: She had to weigh whether to issue a public rebuttal immediately or wait until after voting concluded. As she reflected, "Years of building trust in my community and in one fell swoop, it meant [nothing]."[62]

Targeting Political Opposition

In five documented cases, perpetrators weaponized NSII against challengers to political incumbents and opposition figures across different regions. By targeting women who challenge existing power structures, these attacks serve to delegitimize political opposition and maintain the status quo. NSII targeting opposition figures aligns with broader trends showing that opposition politicians are targeted with abuse at higher rates than ruling party politicians.[63]

→ **CASE STUDY**

In the Republic of Georgia, Salomé Zourabichvili, the country's first elected female president, faced backlash after she pardoned the founder and former director of an opposition television channel. Following the official pardon, manipulated images spread on Facebook falsely depicting her as a prostitute and demanding her removal from office.[64] Although initially backed by the ruling party, the president lost its support. This conflict continued to escalate, culminating in the ruling party initiating an impeachment proceeding against her three months after she issued the pardon.[65]

State-Backed Influence Operations

The integration of NSII into broader state-backed influence campaigns represents an escalation that combines traditional information operations with gendered attacks designed to exploit misogyny. The weaponization of NSII against female political figures includes a pattern in which Russian influence actors disproportionately target female candidates with gender-specific disinformation.[66]

In one case, NSII targeting Ukrainian parliamentarian Svitlana Zalishchuk had suspected Russian origins.[67] In another targeting the Georgian president, NSII content was shared by pro-Kremlin sources.[68] Though these cases could not be confirmed to originate from Russian state actors, five cases involved targeting women leaders in countries that Russia had previously invaded, including the Republic of Georgia and Ukraine. Modern conflicts increasingly involve information campaigns, where sexual deepfakes can serve as powerful propaganda tools to undermine women leaders' authority and distract from substantive political issues. Zalishchuk became the target of NSII on social media immediately after delivering a high-profile speech at the United Nations on how the conflict with Russia was impacting Ukrainian women. Tweets that included crudely manipulated nude images of her began to circulate during the early months of Russia's 2014 invasion of Crimea.[69]

→ CASE STUDY

A pornographic video falsely depicting U.S. presidential candidate Hillary Clinton in a sex act was traced to a Reddit account with suspected links to the Russian government-affiliated Internet Research Agency (IRA). This account, later confirmed by Reddit as the IRA's most popular Reddit account, had almost 100,000 upvotes before it was removed by the site. The account posted the video on several platforms before the 2016 election. The same video was subsequently posted to an American pornography website where it was viewed 250,000 times.[70]

Cultural Sensitivities

NSII attacks can be particularly devastating for women politicians and public officials in conservative societies and traditional communities where cultural shame carries severe consequences.[71] In four documented instances, perpetrators exploited local cultural sensitivities by portraying female public officials as violating moral codes. In some countries, women can be murdered for violating cultural expectations of modesty.[72] NSII perpetrators exploit cultural taboos, transforming digital harassment into potentially physical danger.

→ **CASE STUDY**

Azma Bukhari, the information minister of Pakistan's most populous province, had her face digitally superimposed onto the sexualized body of an actor in a fabricated video. The minister, one of the few women leaders in the country, became aware of the video when it quickly spread on social media.[73] The politician described being "shattered" when the deepfake came to her attention and did not appear publicly for days after the video appeared online. After initially hesitating, she ultimately brought her case to Lahore's High Court.

Tactics

The use of face-swapping technology was the most frequently cited NSII creation method, with perpetrators superimposing women's faces onto existing, often pornographic content in the majority of documented cases. The technical sophistication ranged dramatically from crude photo manipulation to advanced AI-generated deepfakes, potentially created through "nudify" applications. Traditional, pre-AI editing techniques such as Photoshop remain prevalent (in at least 21 cases) alongside newer AI tools (72 cases referenced "deepfakes" or "AI" creation tools), making it challenging to distinguish between fully AI-generated content, AI-assisted alterations, and content created using legacy manipulation methods. Though not included in this analysis, the research revealed several instances in which perpetrators used real images of women that they misattributed as portraying public officials. In one example, images of an American actress in a bikini went viral after they were inaccurately described as depicting Croatia's first post-independence female head of state.[74]

Several of the documented cases involved crudely manipulated images or videos that were easily identifiable as fabricated. The obvious artificiality of the content, however, did not diminish its capacity to delegitimize or humiliate female politicians. Rather than aiming for deceptive, realistic images or videos, perpetrators prioritized creating content to delegitimize or demean female officials, a goal achieved regardless of the content's believability.

The persistence of harm from clearly fake content demonstrates that the damage stems less from the potential deception of viewers than from the act of sexualization itself. When women officials are depicted in explicit scenarios, even obviously fabricated ones, the content reduces them from serious political actors to sexual objects in the public consciousness. The threat landscape also includes several sophisticated examples, such as seamlessly integrated deepfake videos of Italy's prime minister that were uploaded to American adult websites, showing the technology's evolution toward increasingly convincing forgeries.[75]

Perpetrators drew from diverse image sources, ranging from official government photographs to personal social media content. In one notable case, Sabrina Javellana, a local city commissioner in Florida, was targeted using photographs sourced from her personal Instagram account three years before she assumed office, demonstrating how perpetrators mine targets' digital histories for usable material.

In the limited number of cases in which data was available on the specific accounts circulating NSII on social media, perpetrators often distributed the images or videos through fake accounts designed to obscure the true source. These "sock puppet" accounts impersonated credible figures, such as a journalist, to lend legitimacy to the malicious content. In most instances, the offending posts were eventually removed by the platforms. But in general, NSII rarely remained confined to a single platform. Instead, media reporting suggests NSII content circulated across multiple mainstream social media sites, maximizing potential reach and making content removal for victims more difficult due to platform fragmentation.

Impact Analysis

NSII inflicts both individual and systemic harms that extend far beyond personal violations. Individual public officials targeted by sexualized deepfakes experience direct psychological trauma, reputational damage, and the added burden of mounting legal and administrative responses to these attacks. The broader implications, however, pose an even greater threat to democratic participation. NSII functions as a weapon designed to undermine women's political engagement at every level. It weakens the standing of current female candidates and officials, discourages women from entering politics, and pressures those already in office to withdraw from public service entirely. By weaponizing sexuality against women in politics, NSII threatens to reshape political participation.

Individual-Level Impacts

NSII inflicts both psychological and professional damage on targeted women, undermining both their mental health and their credibility as public figures. The psychological toll can be significant. Azma Bukhari noted being "depressed" after being targeted, while Cara Hunter called the experience "the most horrific and stressful time of my entire life," trauma that still impacted her life three years after the initial abuse.[76]

Beyond personal suffering, NSII undermines women's policy positions and expertise. As Hunter explained, "It was a campaign to undermine me politically. It has left a tarnished perception of me that I can't control. I'll have to pay for the repercussions of this for the rest of my life."[77] Svitlana Zalishchuk noted, "It was all intended to discredit me as a personality, to devalue me and what I'm saying." Months after the social media campaign, a journalist asked the Ukrainian politician if it was true that she ran naked through the streets of Kyiv.[78]

Being targeted by NSII forced female public officials to shoulder legal and administrative burdens, often while juggling campaign responsibilities or official duties. Several filed formal complaints with police or electoral courts, while others felt compelled to publicly debunk the content on social media platforms. Two Brazilian candidates, Letícia Arsenio and Loreny Caetano, posted rebuttal videos to their social media pages to debunk and condemn the content.[79]

The legal responses varied by jurisdiction but consistently demanded time and resources from victims. In Brazil, multiple candidates filed police reports during election season, including a city council candidate and two mayoral candidates, while another mayoral candidate pursued a criminal complaint through the electoral court.[80] Italy's prime minister, Giorgia Meloni, filed a civil defamation suit against two men who circulated explicit deepfake videos of her and ultimately had to take time away from her official responsibilities to testify during the trial.[81]

Collective Harms

NSII targeting of female public officials can threaten fundamental democratic principles by deliberately attempting to influence voting behavior and undermine support for women candidates. This manipulation of electoral processes through sexualized attacks represents a direct assault on democratic participation and fair representation. In addition, the knowledge that one's likeness could be artificially injected into pornographic content may discourage women from engaging with online platforms or pursuing public roles altogether.

Perhaps most concerning is the resulting behavioral change among women in politics. Some may be deterred from seeking office in the first place, while others already in positions of power may choose to self-censor their views or limit their public visibility to avoid becoming targets. Evidence from individuals targeted by NSII reveals both behavioral changes and devastating psychological consequences, including depression and post-traumatic stress disorder.[82] These effects can be extensive: While in office as one of the youngest elected officials in Florida's history, Sabrina Javellana made her social media accounts private, changed how she dressed for public appearances, and stopped walking alone at night.[83]

The psychological, legal, and administrative burdens can prove so overwhelming that some women abandon their political careers entirely. Javellana left her career as a politician after being targeted by NSII, overwhelmed by the volume of material created about her and the prohibitive cost of hiring a lawyer to pursue each perpetrator. She decided not to seek reelection, despite being confident she could win, feeling safer outside the public eye.[84]

The Florida case highlights critical vulnerabilities for local and younger politicians who lack the resources available to high-profile national figures when combating NSII. With limited budgets and staff, they may simply decide that the personal and financial costs of public service have become too high. The result is a chilling effect that could drive women away from local politics, where they may begin their political careers and where women are still underrepresented.[85]

This systematic intimidation has the potential to reduce women's full participation in democratic governance and limit the diversity of voices in political discourse. This is not merely a hypothetical concern: Several female

British lawmakers quit ahead of the United Kingdom's 2019 general election, with some explicitly citing vicious abuse and intimidation as reasons for stepping down.[86]

Limitations of Legal and Technical Frameworks

As of August 2025, there are no international conventions specifically designed to protect victims of sexualized deepfakes.[87] The United Nations Cybercrime Convention addresses the dissemination of nonconsensual intimate images but does not refer directly to AI-generated content.[88] Only a handful of countries explicitly criminalize nonconsensual synthetic intimate imagery (NSII). This legal gap exists despite growing public concern about sexually explicit deepfakes, particularly those targeting young women and girls. When surveyed, individuals in Western Europe, the United States, Mexico, and Australia support legal intervention against the nonconsensual creation and distribution of "pornographic" deepfakes.[89]

Almost all Western legal systems criminalize intimate image abuse, as do numerous Asian countries.[90] However, many jurisdictions have excluded deepfakes from the criminal law, including Canada, Japan, and New Zealand, among others.[91] This is, in part, due to concerns over criminalizing protected speech, such as artistic expression. Scholars argue existing laws regulating intimate image abuse, defamation, copyright, privacy, and data violations could be applied to instances of NSII. These arguments remain unproven, as the legal theory is unclear until tested in courts.[92]

Scholars continue to be divided on legislative interventions.[93] Several countries with strong free speech protections, including the United States, United Kingdom, and Australia, among others, are now enacting legislation to combat the creation and distribution of NSII. Free speech advocates worry that well-intentioned laws could become vehicles for broader censorship, potentially restricting legally protected content if it is labeled as "obscene" or "indecent." In the United States, these concerns specifically focus on the notice and takedown provision of the TAKE IT DOWN Act, which goes a step further in mandating the removal of NSII within 48 hours of a victim's verified request.[94] According to free speech advocates, attempts to comply with the law incentivize the use of unreliable and overly broad automated detection techniques to remove content at scale.[95] Legal interventions can often be blunt instruments that may be overinclusive, leading to the removal of legitimate expression, while also underinclusive of extremely harmful content.

Among the countries examined in the documented cases, only the United States, United Kingdom, Australia, and South Korea have laws explicitly addressing NSII (see Table 1). Even in nations with such legislation, many women officials reported feeling they had no meaningful legal recourse available to them.[96] Current legal frameworks face several limitations that hinder female public officials from seeking effective remedies when targeted by NSII. While the following analysis is not exhaustive, it highlights key legal gaps revealed through the documented cases.

Table 1 | Nonconsensual Synthetic Intimate Imagery (NSII) Legislation Around the Globe

Country	Law	Technical Term Used	Prohibits Creation of NSII	Prohibits Distribution of NSII	Victims Required to Prove Intent
Australia	Criminal Code Amendment (Deepfake Sexual Material) Bill (2024)	“Digital technology”	No	Yes	No
France	Criminal Code Article 226-8-1 (2024)	“Algorithmic processing”	No	Yes	No
South Korea	Act on Special Cases Concerning the Punishment of Sexual Crimes (2024)	None**	Yes	Yes	No
United Kingdom	Data (Use and Access) Act (2025)	None*	Yes	Yes	No
United States	TAKE IT DOWN Act (2025)	“Digital forgery”	No	Yes	Yes

* Article 138 refers to “purported intimate images” to include an image which “appears to be, or to include, a photograph or film of the person (but is not, or is not only, a photograph or film of the person.”
** Article 14-2 refers to "false video products," including editing, synthesizing, or processing photographs, videos, or audio targeting the face, body, or voice of a person.

Source: New America analysis of publicly available data.

NEW AMERICA

Jurisdictional Issues

As with all efforts to prevent cybercrime, NSII enforcement is hampered by jurisdictional constraints. Sexually explicit deepfakes can be created and published online from anywhere in the world, leading to inconsistent responses and making enforcement particularly challenging. Differing legal systems, privacy laws, and definitions of what constitutes a crime complicate investigations and evidence collection. In particular, bad-faith actors, such as nudify apps, intentionally host websites in countries that allow NSII or do nothing to stop it. This jurisdictional maze creates impunity for perpetrators who exploit gaps between national legal systems, often leaving victims with fewer hopes of meaningful legal recourse.

Proving Intent to Cause Harm

Laws that include a "malicious intent" or "intent to deceive" requirement aim to protect free speech by targeting only the most harmful, and intentional, violations, rather than restricting speech more broadly.[97] Victim advocates argue that these clauses create loopholes, leaving room for perpetrators to claim they merely shared NSII out of "admiration" for their target with no intention to harass or harm the subject.[98] Research suggests that the majority of perpetrators have other motives, including voyeurism, profit, and social status.[99] Requiring evidence of a perpetrator's intent to cause harm or to deceive also places the burden of proof on survivors and police. Furthermore, many of the documented cases discussed above involved obvious forgeries rather than convincing depictions of the subject. Despite the implausible nature of these images and apparent lack of deceptive intent, targeted public officials still faced significant harassment. The harm remained regardless of the content's believability or the perpetrator's motivations.

Recognition of these loopholes has driven legal reforms in several countries. The United Kingdom initially included intent requirements in its Online Safety Act but later removed them, eliminating the need for victims to prove that perpetrators intended to cause harm, distress, or humiliation.[100] South Korea took a similar approach, crafting laws that do not require proof of malice or harmful intent. Following a surge in sexually explicit deepfakes targeting teenage students, South Korea passed some of the strictest laws governing NSII, even criminalizing the viewing of sexually explicit deepfakes.[101]

Failing to Ban Creation

Even in jurisdictions where laws criminalizing NSII exist, most focus only on the distribution or sharing of content rather than the creation. Only the United

Kingdom and South Korea specifically ban the creation of NSII. Narrowing the scope of the law to distribution of NSII can limit victims' legal options for seeking justice. For example, Australia amended its Criminal Code in 2024 to criminalize knowingly sharing NSII. However, the amendment offered little recourse to at least 16 Australian civil servants who were the targets of sexualized deepfakes created by a colleague. Because the fake nude images remained on the perpetrator's phone, police informed the civil servants that charges could not be laid because there was "no evidence to suggest the images had been distributed."[102]

Defining Technical Terms in the Law

Regulating technically complex phenomena like AI poses definitional challenges for lawmakers.[103] Before federal legislation criminalizing the distribution of NSII, U.S. states struggled to consistently define technical terms such as "deepfakes," "artificial intelligence," and "synthetic media."[104] A Texas law defines a deepfake as a "video, created with the intent to deceive, that appears to depict a real person performing an action that did not occur in reality," while a Minnesota law more broadly defines deepfakes as "any video recording, motion-picture film, sound recording, electronic image, or photography, or any technological representation of speech or conduct" that is substantially derivative. Definitions of technical terms can quickly become obsolete, and they impact what recourse victims can seek. As NSII researcher Kaylee Williams notes, the Texas law reflects earlier conceptions of deepfakes and would complicate efforts by women targeted by sexually explicit deepfake images from seeking recourse, since the definition only includes videos.[105]

Recognizing these limitations, most countries with laws criminalizing NSII favor broader, technology-neutral approaches over specifically targeting "deepfakes." The U.S. TAKE IT DOWN Act refers to "digital forgeries," covering visual depictions created using "software, machine learning, artificial intelligence, or any other computer-generated technological means," including altering authentic depictions.[106] The United Kingdom specifically opted for a "technology-neutral" approach to AI regulation.[107]

Other countries follow similar patterns. Though Australia's criminal code mentions "deepfakes," the law more broadly criminalizes content created "using digital technology (including artificial intelligence)."[108] France's NSII provisions target content generated by "algorithmic processing," encompassing not just AI-generated material but also images or videos altered by traditional software that does not rely on AI.[109]

Detection Tools

Longstanding technical responses to deepfakes and synthetic media are ill-equipped to effectively address NSII targeting public officials. In the United States, the Department of Homeland Security and Federal Bureau of Investigation advise caution when posting personal photos or videos online, but for women in public life, this guidance is unrealistic.[110]

The most common response to stopping the dissemination of deepfakes is through deepfake detection (tools designed to identify AI-generated or manipulated media).[111] While platforms may leverage detection tools to assist with enforcement efforts, they provide insufficient remedies for victims of NSII and suffer from accuracy issues, particularly in detecting deepfakes of people of color.[112] These tools can be useful for tracking which websites generate the most reported abuse material, especially since many AI nudification platforms watermark the content they produce.[113] However, detection technology does little to address the core harm of delegitimizing and demeaning content that has already circulated and caused damage: Correctly identifying a deepfake does not automatically stop it from spreading or offer restitution for the visibility it already had.

AI Labeling and Content Provenance

Content provenance systems, which aim to establish the origins and edits of digital content, similarly fail to address the fundamental problem of demeaning or delegitimizing material. While these systems may prove helpful in specific dangerous situations where women face life-threatening repercussions from NSII, they offer limited protection against the broader reputational and psychological harms that constitute the primary impact of these attacks.

Image provenance can help with understanding which base models are being used for the creation of illegal and objectionable NSII content. Many AI nudification platforms watermark the content they produce. With the help of detection tools, it is possible to track which websites are generating the most reported abuse material, though watermarking offers limited utility if users remove watermarks once a model is downloaded.[114]

Platform Policies and Enforcement

Internet intermediaries (service providers that enable people to use the internet) take inconsistent approaches to NSII, creating uneven protection for victims. Many mainstream social media platforms, model-hosting platforms, search engines, and payment providers do ban NSII content or ban their services from enabling the creation of NSII, but enforcement remains inconsistent. One 2024 study found that 100 percent of NSII reported to X under its “copyright infringement” mechanism was removed within 25 hours, compared with 0 percent of content reported under the platform’s “nonconsensual nudity” reporting mechanism.[115] In spite of policies banning deepfake models without an individual’s consent, popular model-hosting platforms struggle to enforce violations.[116] Companies may be more proactive with the TAKE IT DOWN Act now criminalizing NSII, but how effectively the legislation will address enforcement inconsistencies is yet to be determined.

Many platforms have traditionally relied on victim self-reporting, placing the burden on those who have been harmed to identify and report abusive content —a process that can be both traumatic and inadequate given the speed at which content can spread across multiple platforms.

Recommendations

For Civil Society, Media, and Academia

- **Conduct research on the prevalence and impact of NSII targeting women in politics to establish the full scope of this threat to democratic participation.** There are significant research gaps on how NSII affects women across levels of political engagement, with a particular lack of attention to local politicians who may face attacks without the protective resources available to higher-profile politicians. Greater public awareness can challenge the normalization of gender-based attacks against women in politics and support developing resources for victims.

- **Increase investigative reporting that publicly identifies platforms facilitating NSII, including platforms that fail to enforce their own terms of service.** Naming and shaming platforms that enable NSII creation and distribution can drive meaningful policy change and enforcement improvements. According to one NSII investigative journalist interviewed for this report, Telegram removed channels facilitating NSII creation after a *Wired* article was published on the topic.[117]

For Governments

- **Enhance collaboration between governments to develop coordinated responses to cross-border NSII cases through the International Criminal Police Organization (Interpol).** As the world's largest international police organization, Interpol facilitates international police cooperation and is well-positioned to provide investigative support, training, and cooperation on preventing NSII creation and distribution. The Korean National Police Agency called for increased collaboration on deepfake sex crimes through Interpol during a February 2025 Interpol convening.[118]

- **Issue public advisories clarifying how existing laws apply to NSII.** Legal clarity educates victims about their legal options and deters potential perpetrators who may believe NSII exists in a legal gray area. For example, the U.S. Federal Bureau of Investigation released a public service announcement in March 2024 clarifying that AI-generated child sexual abuse material is illegal.[119]

- **Pursue legal action against prominent NSII platforms that advertise their services as creating fake nonconsensual nude or sexually explicit images of women.** High-profile lawsuits create powerful deterrent effects across the entire ecosystem of NSII platforms. A lawsuit brought by the San Francisco City Attorney's office against prominent deepfake nude websites resulted in 10 of the 16 named platforms being shut down.[120]

- **Establish clear institutional arrangements within government bodies for receiving complaints and conducting investigations, and ensure that reporting mechanisms for public officials are well-known, accessible, and perceived as fair and effective.** Clear, accessible reporting mechanisms will increase documentation of attacks, enabling better resource allocation and support for victims. Survey data shows many parliamentarians remain unaware of existing measures to combat gender-based violence in political workplaces and do not report attacks through existing channels.[121] Directing public officials to available resources, such as the National Image Abuse Helpline in the United States, could reduce barriers to reporting.[122]

For Technology Companies

- **AI developers should implement safety-by-design features to prevent NSII creation.** Robust filtering of sexually explicit content during pre-training of an AI model can dramatically reduce its capacity to produce NSII, while investment in image provenance technologies can enable identification of AI-generated content.

- **AI model-hosting platforms should require watermarking for all uploaded models.** Watermarking would help identify which models are generating NSII and enable more effective enforcement actions against those models.

- **Social media platforms should share aggregated data on NSII prevalence and distribution patterns.** Data collection on NSII is ethically challenging, making it difficult for academics to study the prevalence of NSII on social media. Sharing aggregated, anonymized data (such as trends over time, removal statistics, and demographic patterns) that protects victim identities with vetted researchers can support academic research and evidence-based policy development.

- **Social media platforms should establish specialized incident reporting programs for women in politics.** Women politicians face unique vulnerabilities, and most women parliamentarians do not report attacks to online platforms.[123] By establishing clear policies on AI-generated intimate images and optimizing reporting processes for users' needs, platforms can improve response times and provide greater protection for women in politics.[124]

- **Social media platforms should participate in StopNCII.org's cross-platform hash-sharing mechanism while implementing robust verification processes before removal.**[125] StopNCII.org allows users to generate a hash (digital fingerprint) of intimate images or videos and share the hash with participating companies. The unique hash value of the image allows companies to detect and remove images from being shared online at scale. Proper verification is needed to avoid this mechanism being abused to remove legitimate content that does not constitute NSII.

- **Technology companies should commit to industry-wide pledges that increase friction for NSII creation and distribution across the entire technology ecosystem.** The Secure by Design Pledge, in which companies agree to make security a fundamental aspect of product design and development, offers a useful model for developing voluntary commitments.[126] An industry-wide pledge would encourage companies to prioritize preventing NSII creation and distribution as a core principle of product design and deployment.

- **Payment providers should devote resources to proactively enforcing policies that prohibit their services from supporting NSII platforms.** Payment providers play a critical role as enablers of the commercial NSII ecosystem. Aggressive enforcement of existing policies will remove financial incentives that drive much of NSII creation and force platforms to shut down when they cannot monetize their services.

Conclusion

In shining a light on the targeting of public officials with nonconsensual synthetic intimate imagery (NSII), this report aims to discourage the normalization of NSII in political life that both threatens individual well-being and weakens democratic institutions and processes. The evidence demonstrates that NSII functions as a deliberate weapon designed to manipulate electoral processes and undermine women's political engagement. These attacks inflict severe psychological trauma, professional damage, and substantial legal burdens that can overwhelm officials' capacity to serve effectively, with some abandoning their careers in electoral politics entirely.

The systemic implications extend far beyond individual harm. NSII creates a chilling effect that deters women from seeking office, pressures current officials to self-censor or limit their public visibility, and ultimately reduces the diversity of voices in political discourse. When women are driven from politics through sexualized attacks, society loses their perspectives, expertise, and leadership. Addressing NSII targeting of public officials is therefore essential not only to protect individual victims but to preserve the integrity and inclusiveness of democratic governance.

Notes

1 Inter-Parliamentary Union (IPU), *Sexism, Harassment, and Violence Against Women Parliamentarians* (IPU, 2016), https://www.ipu.org/resources/publications/issue-briefs/2016-10/sexism-harassment-and-violence-against-women-parliamentarians.

2 Inter-Parliamentary Union, *Sexism, Harassment, and Violence Against Women Parliamentarians*, https://www.ipu.org/resources/publications/issue-briefs/2016-10/sexism-harassment-and-violence-against-women-parliamentarians.

3 Pavlina Pavlova, "The Digital War on Women: Sexualized Deepfakes, Weaponized Data, and Stalkerware That Monitors Victims Online," *Ms. Magazine*, November 21, 2024, https://msmagazine.com/2024/11/21/women-online-harrassment-abuse-deepfake-violence-revenge-porn/.

4 Rebecca Umbach et al., "Non-Consensual Synthetic Intimate Imagery: Prevalence, Attitudes, and Knowledge in 10 Countries," *CHI '24: Proceedings of the 2024 CHI Conference on Human Factors in Computing Systems* (May 11, 2024), https://doi.org/10.1145/3613904.3642382.

5 Suzie Dunn, "Legal Definitions of Intimate Images in the Age of Sexual Deepfakes and Generative AI," *McGill Law Journal* 69, no. 4 (October 2024), https://lawjournal.mcgill.ca/article/legal-definitions-of-intimate-images-in-the-age-of-sexual-deepfakes-and-generative-ai/.

6 Nicola Henry et al., *Image-Based Sexual Abuse: A Study on the Causes and Consequences of Nonconsensual Nude or Sexual Imagery* (Routledge, 2020), 4–5.

7 Dunn, "Legal Definitions of Intimate Images in the Age of Sexual Deepfakes and Generative AI," https://lawjournal.mcgill.ca/article/legal-definitions-of-intimate-images-in-the-age-of-sexual-deepfakes-and-generative-ai.

8 Jillian Rubman, "Supporting Learning with AI-Generated Images: A Research-Backed Guide," MIT Sloan Teaching & Learning Technologies, March 6, 2024, https://mitsloanedtech.mit.edu/2024/03/06/supporting-learning-with-ai-generated-images-a-research-backed-guide/.

9 Samantha Cole, "AI-Assisted Fake Porn Is Here and We're All Fucked," *Vice,* December 11, 2017, https://www.vice.com/en/article/gal-gadot-fake-ai-porn/.

10 Asher Flynn et al., "Deepfakes and Digitally Altered Imagery Abuse: A Cross-Country Exploration of an Emerging Form of Image-Based Sexual Abuse," *British Journal of Criminology* 62, no. 6 (2022): 1341–58, https://academic.oup.com/bjc/article-abstract/62/6/1341/6448791.

11 Security Hero, *2023 State of Deepfakes: Realities, Threats, and Impact* (Security Hero, 2023), https://www.securityhero.io/state-of-deepfakes/.

12 Alexios Mantzarlis and Santiago Lakatos, "AI Nudifiers Continue to Reach Millions and Make Millions," *INDiCATOR*, July 13, 2025, https://indicator.media/p/ai-nudifiers-continue-to-reach-millions-and-make-millions.

13 Danielle Keats Citron, *Hate Crimes in Cyberspace* (Harvard University Press, 2016); Tarleton Gillespie, *Custodians of the Internet: Platforms, Content Moderation, and the Hidden Decisions That Shape Social Media* (Yale University Press, 2018); Asher Flynn, Jonathan Clough, and Talani Cooke, "Disrupting and Preventing Deepfake Abuse: Exploring Criminal Law Responses to AI-Facilitated Abuse," in *The Palgrave Handbook of Gendered Violence and Technology*, ed. Anastasia Powell, Asher Flynn, and Lisa Sugiura (Palgrave Macmillan, 2021), 583–603.

14 “Nonconsensual Content Policy,” Pornhub, September 2024, https://help.pornhub.com/hc/en-us/articles/4419871787027-Non-Consensual-Content-Policy; “New Decision Addresses Meta’s Rules on Nonconsensual Deepfake Intimate Images,” Oversight Board, July 25, 2024, https://www.oversightboard.com/news/new-decision-addresses-metas-rules-on-non-consensual-deepfake-intimate-images/; “Never Post Intimate or Sexually Explicit Media of Someone Without Their Consent,” Reddit, July 5, 2023, https://support.reddithelp.com/hc/en-us/articles/360043513411-Never-Post-Intimate-or-Sexually-Explicit-Media-of-Someone-Without-Their-Consent; Noelle Martin, “Image-Based Sexual Abuse and Deepfakes: A Survivor Turned Activist’s Perspective,” in *The Palgrave Handbook of Gendered Violence and Technology*; Asher Flynn et al., “Deepfakes and Digitally Altered Imagery Abuse: A Cross-Country Exploration of an Emerging Form of Image-Based Sexual Abuse,” *British Journal of Criminology* 62, no. 6 (November 2022): 1341–58, https://academic.oup.com/bjc/article-abstract/62/6/1341/6448791.

15 S. 146 - TAKE IT DOWN Act (2025), https://www.congress.gov/bill/119th-congress/senate-bill/146; “CCRI Statement on the Passage of the TAKE IT DOWN Act (S. 146),” Cyber Civil Rights Initiative, April 28, 2025, https://cybercivilrights.org/ccri-statement-on-the-passage-of-the-take-it-down-act-s-146/.

16 Cassidy Gibson et al., “Analyzing the AI Nudification Application Ecosystem,” *arXiv.org*, November 14, 2024, https://arxiv.org/abs/2411.09751.

17 Santiago Lakatos, *A Revealing Picture* (Graphika, December 8, 2023), https://graphika.com/reports/a-revealing-picture.

18 Gibson et al., “Analyzing the AI Nudification Application Ecosystem,” https://arxiv.org/abs/2411.09751.

19 Ashley Belanger, “Nudify App’s Plan to Dominate Deepfake Porn Hinges on Reddit, 4chan, and Telegram, Docs Show,” *Ars Technica*, July 1, 2025, https://arstechnica.com/tech-policy/2025/07/nudify-apps-plan-to-dominate-deepfake-porn-hinges-on-reddit-docs-show/.

20 Emmet Lyons and Leigh Kiniry, “Meta’s Platforms Showed Hundreds of ‘Nudify’ Deepfake Ads, CBS News Investigation Finds,” CBS News, June 6, 2025, https://www.cbsnews.com/news/meta-instagram-facebook-ads-nudify-deepfake-ai-tools-cbs-news-investigation/; Belanger, “Nudify App’s Plan to Dominate Deepfake Porn,” https://arstechnica.com/tech-policy/2025/07/nudify-apps-plan-to-dominate-deepfake-porn-hinges-on-reddit-docs-show/.

21 Gibson et al., “Analyzing the AI Nudification Application Ecosystem,” https://arxiv.org/abs/2411.09751.

22 Gibson et al., “Analyzing the AI Nudification Application Ecosystem,” https://arxiv.org/abs/2411.09751; Rachel Winter and Anastasia Salter, “DeepFakes: Uncovering Hardcore Open Source on GitHub,” *Porn Studies* 7, no. 4 (2020): 382–97, https://www.tandfonline.com/doi/abs/10.1080/23268743.2019.1642794.

23 Will Hawkins, Brent Mittelstadt, and Chris Russell, “Deepfakes on Demand: The Rise of Accessible Nonconsensual Deepfake Image Generators,” *FAccT ’25: Proceedings of the 2025 ACM Conference on Fairness, Accountability, and Transparency* (June 23, 2025), https://dl.acm.org/doi/10.1145/3715275.3732107.

24 Hawkins, Mittelstadt, and Russell, “Deepfakes on Demand,” https://dl.acm.org/doi/10.1145/3715275.3732107.

25 Emanuel Maiberg, “‘Configuration Issue’ Allows Civitai Users to AI Generate Nonconsensual Porn Videos,” *404 Media*, May 20, 2025, https://www.404media.co/configuration-issue-allows-civitai-users-to-ai-generate-nonconsensual-porn-videos/.

26 “Re: GitHub Hosting Source Code for Sexually Exploitative Technology, Facilitating Image-Based

Sexual Abuse (IBSA), Sexual Exploitation, and Promoting the Dangerous Use of Generative-AI," National Center on Sexual Exploitation, April 28, 2023, https://endsexualexploitation.org/wp-content/uploads/Microsoft-GitHub-Notification-Letter_DDL-2023_FINAL.pdf.

27 Mantzarlis and Lakatos, "AI Nudifiers Continue to Reach Millions and Make Millions," https://indicator.media/p/ai-nudifiers-continue-to-reach-millions-and-make-millions.

28 Maiberg, "'Configuration Issue' Allows Civitai Users to AI Generate Nonconsensual Porn Videos," https://www.404media.co/configuration-issue-allows-civitai-users-to-ai-generate-nonconsensual-porn-videos/; Hawkins, Mittelstadt, and Russell, "Deepfakes on Demand," https://dl.acm.org/doi/10.1145/3715275.3732107.

29 Emanuel Maiberg, "Hugging Face Is Hosting 5,000 Nonconsensual AI Models of Real People," *404 Media*, July 15, 2025, https://www.404media.co/hugging-face-is-hosting-5-000-nonconsensual-ai-models-of-real-people/.

30 Maiberg, "'Configuration Issue' Allows Civitai Users to AI Generate Nonconsensual Porn Videos," https://www.404media.co/configuration-issue-allows-civitai-users-to-ai-generate-nonconsensual-porn-videos/.

31 Beatriz Kira, "When Non-Consensual Intimate Deepfakes Go Viral: The Insufficiency of the U.K. Online Safety Act," *Computer Law & Security Review* 54 (September 2024), https://www.sciencedirect.com/science/article/pii/S0267364924000906.

32 Kat Tenbarge, "Nude Deepfakes Images of Taylor Swift Went Viral on X, Evading Moderation and Sparking Outrage," NBC News, January 25, 2024, https://www.nbcnews.com/tech/misinformation/taylor-swift-nude-deepfake-goes-viral-x-platform-rules-rcna135669.

33 Lakatos, *A Revealing Picture*, https://graphika.com/reports/a-revealing-picture.

34 "Taking Action Against 'Nudify' Apps," Meta, June 12, 2025, https://about.fb.com/news/2025/06/taking-action-against-nudify-apps/; Kolina Koltai and Melissa Zhu, "Meta's Suit Against Hong Kong Firm Was Just the Beginning–More Companies Linked to CrushAI 'Nudify' Apps," *Bellingcat*, June 18, 2025, https://www.bellingcat.com/news/americas/2025/06/18/meta-crushai-crushmate-deepfake-nudify-apps/.

35 Brian Timmerman et al., "Studying the Online Deepfake Community," *Online Trust and Safety* 2, no. 1 (2023), https://tsjournal.org/index.php/jots/article/view/126.

36 "Deepfake Abuse: Landscape Analysis (The Exponential Rise of Deepfake Abuse in 2023–2024)," #MyImageMyChoice, 2024, https://myimagemychoice.org/.

37 Karen Hao, "A Deepfake Bot Is Being Used to 'Undress' Underage Girls," *MIT Technology Review*, October 20, 2020, http://www.technologyreview.com/2020/10/20/1010789/ai-deepfake-bot-undresses-women-and-underage-girls/.

38 Sammi Carmela, "'Nudify' Deepfake Bots on Telegram Are up to 4 Million Monthly Users," *Vice*, October 16, 2024, https://www.vice.com/en/article/nudify-deepfake-bots-telegram/.

39 James Vincent, "Deepfake Bots on Telegram Make the Work of Creating Fake Nudes Dangerously Easy," *The Verge*, October 20, 2020, https://www.theverge.com/2020/10/20/21519322/deepfake-fake-nudes-telegram-bot-deepnude-sensity-report.

40 Maiberg, "'Configuration Issue' Allows Civitai Users to AI Generate Nonconsensual Porn Videos," https://www.404media.co/configuration-issue-allows-civitai-users-to-ai-generate-nonconsensual-porn-videos/.

41 Cecilia D'Anastasio and Davey Alba, "Google and Microsoft Are Supercharging AI Deepfake Porn," Bloomberg News, August 24, 2023, https://www.bloomberg.com/news/articles/2023-08-24/google-microsoft-tools-behind-surge-in-deepfake-ai-porn.

42 "Deepfake Abuse: Landscape Analysis," https://myimagemychoice.org/.

43 Layla Ferris, "AI-Generated Porn Site Mr. Deepfakes Shuts Down After Service Provider Pulls Support," CBS News, May 5, 2025, https://www.cbsnews.com/news/ai-generated-porn-site-mr-deepfakes-shuts-down/.

44 Emily B. Laidlaw, "Mechanisms of Information Control: ISPs," in *Regulating Speech in Cyberspace: Gatekeepers, Human Rights, and Corporate Responsibility* (Cambridge University Press, 2015).

45 Kolina Koltai, "AnyDream: Secretive AI Platform Broke Stripe Rules to Rake in Money from Nonconsensual Pornographic Deepfakes," *Bellingcat*, November 27, 2023, https://www.bellingcat.com/news/2023/11/27/anydream-secretive-ai-platform-broke-stripe-rules-to-rake-in-money-from-nonconsensual-pornographic-deepfakes/; Kolina Koltai, "Behind a Secretive Global Network of Non-Consensual Deepfake Pornography," *Bellingcat*, February 23, 2024, https://www.bellingcat.com/news/2024/02/23/behind-a-secretive-global-network-of-non-consensual-deepfake-pornography/.

46 Gibson et al., "Analyzing the AI Nudification Application Ecosystem," https://arxiv.org/abs/2411.09751.

47 Maiberg, "'Configuration Issue' Allows Civitai Users to AI Generate Nonconsensual Porn Videos," https://www.404media.co/configuration-issue-allows-civitai-users-to-ai-generate-nonconsensual-porn-videos/.

48 Lucina Di Meco, "Online Threats to Women's Political Participation and the Need for a Multi-Stakeholder, Cohesive Approach to Address Them," paper presented at the 65th session of the Commission on the Status of Women (CSW 65), UN Women Expert Group Meeting, New York, October 5–8, 2020, https://www.unwomen.org/sites/default/files/Headquarters/Attachments/Sections/CSW/65/EGM/Di%20Meco_Online%20Threats_EP8_EGMCSW65.pdf; Maarja Lühiste et al., "When Does Fame Not Matter? Examining Gender Differences in Politicians' Social Media Experiences," *Politics & Gender* (July 30, 2025), https://www.cambridge.org/core/journals/politics-and-gender/article/when-does-fame-not-matter-examining-gender-differences-in-politicians-social-media-experiences/78BB8D1D35DD19124167E06BF47951F3.

49 Robert Chesney, Danielle Citron, and Hany Farid, "All's Clear for Deepfakes: Think Again," *Lawfare*, May 11, 2020, https://www.lawfaremedia.org/article/alls-clear-deepfakes-think-again; Danielle Citron, "Cyber Civil Rights," *Boston University Law Review* 89, no. 1 (2009): 61, https://www.bu.edu/law/journals-archive/bulr/volume89n1/documents/CITRON.pdf.

50 Citron, "Cyber Civil Rights," 61, 64–65, https://www.bu.edu/law/journals-archive/bulr/volume89n1/documents/CITRON.pdf.

51 Pranshu Verma and Cat Zakrzewski, "AI Deepfakes Threaten to Upend Global Elections. No One Can Stop Them," *Washington Post*, April 23, 2024, https://www.washingtonpost.com/technology/2024/04/23/ai-deepfake-election-2024-us-india/.

52 "Deepfake Abuse: Landscape Analysis," https://myimagemychoice.org/.

53 Di Meco, "Online Threats to Women's Political Participation," https://www.unwomen.org/sites/default/files/Headquarters/Attachments/Sections/CSW/65/EGM/Di%20Meco_Online%20Threats_EP8_EGMCSW65.pdf.

54 Plan International, *State of the World's Girls 2020: Free to Be Online?* (Plan International, 2020), https://plan-international.org/publications/free-to-be-online/.

55 National Democratic Institute (NDI), *Tweets That Chill: Analyzing Online Violence Against Women in Politics* (NDI, 2019), https://www.ndi.org/sites/default/files/NDI%20Tweets%20That%20Chill%20Report.pdf.

56 Vandinika Shukla, "Deepfakes and Elections: The Risk to Women's Political Participation," *Tech Policy Press*, February 29, 2024, https://www.techpolicy.press/deepfakes-and-elections-the-risk-to-womens-political-participation/.

57 The author used the Partnership on AI AI Incident Database, the OECD AI Incident Database, the Rest of World 2024 AI Elections Tracker, the Resemble.AI Deepfake Incident Database, and the Political Deepfakes Incidents Database.

58 The author used the following Boolean operation: ("artificial intelligence-generated image" OR "artificial intelligence-generated video" OR "deepfake" OR "deepfake porn" OR "nonconsensual intimate image" OR "synthetic media") AND ("public official" OR "politician" OR "candidate").

59 American Sunlight Project (ASP), *Deepfake Pornography Goes to Washington: Measuring the Prevalence of AI-Generated Non-Consensual Intimate Imagery Targeting Congress* (ASP, December 11, 2024), https://static1.squarespace.com/static/6612cbdfd9a9ce56ef931004/t/67586997eaec5c6ae3bb5e24/1733847451191/ASP+DFP+Report.pdf.

60 "Creator of Deepfake Images of MLA Yet to Be Found," BBC News, January 23, 2025, https://www.bbc.com/news/articles/cz6p390ygnzo.

61 Rebecca Black, "Stormont MLA Targeted by Deepfake Video Urges Legal Clampdown," *The Standard*, January 14, 2025, https://www.standard.co.uk/news/tech/stormont-northern-ireland-democracy-b1204769.html.

62 Mark Scott, "Deepfake Porn Is Political Violence," *Politico*, February 8, 2024, https://www.politico.eu/newsletter/digital-bridge/deepfake-porn-is-political-violence/.

63 Amnesty International India, *Troll Patrol India: Exposing Online Abuse Faced by Women Politicians in India* (Amnesty International India, 2020), https://decoders.blob.core.windows.net/troll-patrol-india-findings/Amnesty_International_India_Troll_Patrol_India_Findings_2020.pdf.

64 "Manipulated Photos Depicting Salome Zourabichvili Have Been Circulating On Facebook," Myth Detectors, June 27, 2023, https://mythdetector.ge/en/manipulated-photos-depicting-salome-zourabichvili-have-been-circulating-on-facebook/.

65 "Georgian Dream Launches Impeachment Proceedings Against President," *Civil Georgia*, September 1, 2023, https://civil.ge/archives/557470.

66 Julia Smirnova et al., *Digitale Gewalt Und Desinformation Gegen Spitzenkandidat: Innen Vor Der Bundestagswahl 2021* (Institute for Strategic Dialogue, September 2021), https://www.isdglobal.org/isd-publications/digitale-gewalt-und-desinformation-gegen-spitzenkandidatinnen-vor-der-bundestagswahl-2021/; Samantha Bradshaw and Amélie Henle, "The Gender Dimensions of Foreign Influence Operations," *International Journal of Communication* 15 (2021), https://ijoc.org/index.php/ijoc/article/view/16332.

67 Nina Jankowicz, "How Disinformation Became a New Threat to Women," *Coda*, December 11, 2017, https://www.codastory.com/polarization/how-disinformation-became-a-new-threat-to-women/.

68 Natia Kekenadze, Tina Gogoladze, and Salome Giunashvili, *Sexist Language and Gendered*

Disinformation 2023 (Media Development Foundation, 2023), https://mdfgeorgia.ge/uploads//Genderl1%20Report-ENG.pdf.

69 Jankowicz, "How Disinformation Became a New Threat to Women," https://www.codastory.com/polarization/how-disinformation-became-a-new-threat-to-women/; "Manipulated Photos Depicting Salome Zourabichvili Have Been Circulating On Facebook," Myth Detectors, June 27, 2023, https://mythdetector.ge/en/manipulated-photos-depicting-salome-zourabichvili-have-been-circulating-on-facebook/; "A Photo of Vera Kobalia Is Being Circulated on Social Media," Myth Detectors, January 11, 2023, https://mythdetector.ge/ka/sotsialur-qselshi-vera-qobalias-programulad-damushavebuli-photo-vrtseldeba/; Kekenadze, Gogoladze, and Giunashvili, *Sexist Language and Gendered Disinformation 2023*, https://mdfgeorgia.ge/uploads//Genderl1%20Report-ENG.pdf.

70 Ben Collins, "Russia-Linked Account Pushed Fake Hillary Clinton Sex Video," NBC News, April 10, 2018, https://www.nbcnews.com/tech/security/russia-linked-account-pushed-fake-hillary-clinton-sex-video-n864871.

71 Inter-Parliamentary Union (IPU), *Sexism, Harassment, and Violence Against Women in Parliaments in the Asia-Pacific Region* (IPU, March 2025), https://www.ipu.org/resources/publications/issue-briefs/2025-03/sexism-harassment-and-violence-against-women-in-parliaments-in-asia-pacific-region.

72 Kelly Ng, "Pakistan: U.S. Teen Shot Dead by Father over TikTok Videos," BBC News, January 30, 2025, https://www.bbc.com/news/articles/cy8pvw3xxxeo.

73 AFP, "Deepfakes Weaponised to Target Pakistan's Women Leaders," France 24, December 3, 2024, https://www.france24.com/en/live-news/20241203-deepfakes-weaponised-to-target-pakistan-s-women-leaders.

74 Louis Baudoin-Laarman, Jean-Gabriel Fernandez, and Pedro Noel, "Images of the Croatian President in a Bikini: Beware the Fakes," AFP, July 14, 2018, https://factcheck.afp.com/images-croatian-president-bikini-beware-fakes.

75 Seb Starcevic, "Italy's Giorgia Meloni Called to Testify in Deepfake Porn Case," *Politico*, March 21, 2024, https://www.politico.eu/article/italian-pm-giorgia-meloni-called-to-testify-in-deepfake-porn-case/.

76 AFP, "Deepfakes Weaponised to Target Pakistan's Women Leaders," https://www.france24.com/en/live-news/20241203-deepfakes-weaponised-to-target-pakistan-s-women-leaders; "Creator of Deepfake Images of MLA Yet to Be Found," https://www.bbc.com/news/articles/cz6p390ygnzo.

77 Scott, "Deepfake Porn Is Political Violence," https://www.politico.eu/newsletter/digital-bridge/deepfake-porn-is-political-violence/.

78 Jankowicz, "How Disinformation Became a New Threat to Women," https://www.codastory.com/polarization/how-disinformation-became-a-new-threat-to-women/.

79 Marcelo Macedo Soares, "Candidata Aciona PF Após ter Fotos e Video Manipulados por Inteligência Artificial," *Agenda do Poder*, September 7, 2024, https://agendadopoder.com.br/candidata-aciona-pf-apos-ter-fotos-e-video-manipulados-por-inteligencia-artificial/; Juliana Causin, "'Nudes' Falsos, Deepfake e Jingles Sintéticos Marcam uso da IA no Primeiro Turno e Apontam Desafios para 2026," *O Globo*, October 15, 2024, https://oglobo.globo.com/politica/noticia/2024/10/15/nudes-falsos-deepfake-e-jingles-sinteticos-marcam-uso-da-ia-no-primeiro-turno-e-apontam-desafios-para-2026.ghtml.

80 Soares, "Candidata Aciona PF Após ter Fotos e Video Manipulados por Inteligência Artificial," https://agendadopoder.com.br/candidata-aciona-pf-apos-ter-fotos-e-video-manipulados-por-inteligencia-artificial/; Beatriz Farrugia, "Brazil's

Electoral Deepfake Law Tested as AI-Generated Content Targeted Local Elections," DFRLab, November 26, 2024, https://dfrlab.org/2024/11/26/brazil-election-ai-deepfakes/;Leticia Dauer, "É #FAKE Foto de Tabata Amaral em Pose Sensual; Trata-se de Deepfake," *g1*, September 15, 2024, https://g1.globo.com/fato-ou-fake/sao-paulo/noticia/2024/09/15/e-fake-foto-de-tabata-amaral-em-pose-sensual-trata-se-de-deepfake.ghtml; Causin, "'Nudes' Falsos, Deepfake e Jingles Sintéticos Marcam uso da IA no Primeiro Turno e Apontam Desafios para 2026," https://oglobo.globo.com/politica/noticia/2024/10/15/nudes-falsos-deepfake-e-jingles-sinteticos-marcam-uso-da-ia-no-primeiro-turno-e-apontam-desafios-para-2026.ghtml; Paulo Piassi, "Prefeita de Bauru Registra Boletim de Ocorrência Contra Veiculação de Deepfake com seu Rosto Sobre Corpo Nu," *g1*, September 19, 2024, https://g1.globo.com/sp/bauru-marilia/eleicoes/2024/noticia/2024/09/19/prefeita-de-bauru-registra-boletim-de-ocorrencia-contra-veiculacao-de-deep-fakes-com-seu-rosto-sobre-corpo-nu.ghtml.

81 Starcevic, "Italy's Giorgia Meloni Called to Testify in Deepfake Porn Case," https://www.politico.eu/article/italian-pm-giorgia-meloni-called-to-testify-in-deepfake-porn-case/.

82 Nicole Krättli, "Fake Porn—Real Victims," video, *Neue Zürcher Zeitung*, September 1, 2023, https://www.nzz.ch/english/video-fake-porn-real-victims-how-women-become-targets-of-artificial-intelligence-ld.1754001; Danielle Keats Citron, *The Fight for Privacy: Protecting Dignity, Identity, and Love in the Digital Age* (W. W. Norton & Company, 2022); Asia A. Eaton and Clare McGlynn, "The Psychology of Nonconsensual Porn: Understanding and Addressing a Growing Form of Sexual Violence," *Policy Insights from the Behavioral and Brain Sciences* 7, no. 2 (2020), https://journals.sagepub.com/doi/10.1177/2372732220941534.

83 Coralie Kraft, "Trolls Used Her Face to Make Fake Porn. There Was Nothing She Could Do," *New York Times Magazine*, July 31, 2024, https://www.nytimes.com/2024/07/31/magazine/sabrina-javellana-florida-politics-ai-porn.html.

84 Kraft, "Trolls Used Her Face to Make Fake Porn," https://www.nytimes.com/2024/07/31/magazine/sabrina-javellana-florida-politics-ai-porn.html.

85 Justin de Benedictis-Kessner, "Women Are Still Underrepresented in Local Government, Despite a Woman Running for President," Ash Center for Democratic Governance and Innovation, September 20, 2024, https://ash.harvard.edu/articles/women-are-still-underrepresented-in-local-government-despite-a-woman-running-for-president/.

86 Bianca Britton, "There Were Never More Women in U.K. Parliament. Now There's an Exodus," CNN, October 31, 2019, https://www.cnn.com/2019/10/31/uk/female-mps-standing-down-uk-election-intl-gbr.

87 Equality Now, *Deepfake Image-Based Sexual Abuse, Tech-Facilitated Sexual Exploitation, and the Law* (Equality Now, January 17, 2024), https://equalitynow.org/resource/briefs/briefing-paper-deepfake-image-based-sexual-abuse-tech-facilitated-sexual-exploitation-and-the-law/.

88 Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes, *Draft United Nations Convention Against Cybercrime* (United Nations, August 7, 2024), https://docs.un.org/en/A/AC.291/L.15.

89 Umbach et al., "Nonconsensual Synthetic Intimate Imagery: Prevalence, Attitudes, and Knowledge in 10 Countries," https://doi.org/10.1145/3613904.3642382; Matthew B. Kugler and Carly Pace, "Deepfake Privacy: Attitudes and Regulation," *Northwestern University Law Review* 116, no. 3 (2021), https://scholarlycommons.law.northwestern.edu/nulr/vol116/iss3/1/.

90 Gian Marco Caletti and Kolis Summerer, "Criminalizing Intimate Image Abuse: An Introduction," in *Criminalizing Intimate Image Abuse: A Comparative Perspective*, ed. Gian Marco Caletti and Kolis Summerer (Oxford University Press, 2024), 3.

91 Henry et al., *Image-Based Sexual Abuse: A Study on the Causes and Consequences of Non-Consensual Nude or Sexual Imagery*, 137.

92 *Deepfake Image-Based Sexual Abuse, Tech-Facilitated Sexual Exploitation, and the Law*, https://equalitynow.org/resource/briefs/briefing-paper-deepfake-image-based-sexual-abuse-tech-facilitated-sexual-exploitation-and-the-law/.

93 Bobby Chesney and Danielle Citron, "Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security," *California Law Review 107* (December 2019), 1753–820, https://www.californialawreview.org/print/deep-fakes-a-looming-challenge-for-privacy-democracy-and-national-security; Rebecca A. Delfino, "Pornographic Deepfakes: The Case for Federal Criminalization of Revenge Porn's Next Tragic Act," *Fordham Law Review* 88, no. 3 (2019), https://shorturl.at/sg7Nu; Anne Pechenik Gieseke, "The New Weapon of Choice: Law's Current Inability to Properly Address Deepfake Pornography," *Vanderbilt Law Review* 73, no. 5 (2020), https://scholarship.law.vanderbilt.edu/vlr/vol73/iss5/4/; Karolina Mania, "The Legal Implications and Remedies Concerning Revenge Porn and Fake Porn: A Common Law Perspective," *Sexuality & Culture* 24, no. 6 (2020), https://link.springer.com/article/10.1007/s12119-020-09738-0; Matthew Feeney, *Deepfake Laws Risk Creating More Problems Than They Solve* (Regulatory Transparency Project, March 2021), https://rtp.fedsoc.org/paper/deepfake-laws-risk-creating-more-problems-than-they-solve/; Tyrone Kirchengast, "Deepfakes and Image Manipulation: Criminalisation and Control," *Information & Communications Technology Law* 29, no. 3 (2020), https://www.tandfonline.com/doi/abs/10.1080/13600834.2020.1794615.

94 Kaylee Williams, "Free Speech Advocates Express Concerns as TAKE IT DOWN Act Passes U.S. Senate," *Tech Policy Press*, February 21, 2025, https://www.techpolicy.press/free-speech-advocates-express-concerns-as-take-it-down-act-passes-us-senate/.

95 "Re: Concerns Regarding the TAKE IT DOWN Act," Center for Democracy and Technology, February 12, 2025, https://cdt.org/wp-content/uploads/2025/02/TAKE-IT-DOWN-Sign-On-Letter_21225.pdf.

96 David Braue, "Public Servant Creates Sexual Deepfakes of Colleagues," *Information Age*, April 29, 2025, https://ia.acs.org.au/article/2025/public-servant-creates-sexual-deepfakes-of-colleagues.html.

97 Kaylee Williams, "U.S. States Struggle to Define 'Deepfakes' and Related Terms as Technically Complex Legislation Proliferates," *Tech Policy Press*, September 12, 2024, https://www.techpolicy.press/us-states-struggle-to-define-deepfakes-and-related-terms-as-technically-complex-legislation-proliferates/.

98 Kaylee Williams, "Exploring Legal Approaches to Regulating Nonconsensual Deepfake Pornography," *Tech Policy Press*, May 15, 2023, https://www.techpolicy.press/exploring-legal-approaches-to-regulating-nonconsensual-deepfake-pornography/.

99 Mary Anne Franks, "The Criminalization of Nonconsensual Pornography in the United States," in *Criminalizing Intimate Image Abuse: A Comparative Perspective*, ed. Gian Marco Caletti and Kolis Summerer (Oxford University Press, 2024), 170.

100 Shiona McCallum, "Revenge and Deepfake Porn Laws to Be Toughened," BBC News, June 27, 2023, https://www.bbc.com/news/technology-66021643.

101 Williams, "Exploring Legal Approaches to Regulating Nonconsensual Deepfake Pornography,"

https://www.techpolicy.press/exploring-legal-approaches-to-regulating-nonconsensual-deepfake-pornography/; Seungmin (Helen) Lee, “South Korea’s Evolving AI Regulations,” Stimson Center, June 12, 2025, https://www.stimson.org/2025/south-koreas-evolving-ai-regulations/.

102 Braue, “Public Servant Creates Sexual Deepfakes of Colleagues,” https://ia.acs.org.au/article/2025/public-servant-creates-sexual-deepfakes-of-colleagues.html.

103 Matt O’Shaughnessy, “One of the Biggest Problems in Regulating AI Is Agreeing on a Definition,” Carnegie Endowment for International Peace, October 6, 2022, https://carnegieendowment.org/posts/2022/10/one-of-the-biggest-problems-in-regulating-ai-is-agreeing-on-a-definition.

104 Williams, “U.S. States Struggle to Define ‘Deepfakes’ and Related Terms as Technically Complex Legislation Proliferates,” https://www.techpolicy.press/us-states-struggle-to-define-deepfakes-and-related-terms-as-technically-complex-legislation-proliferates/.

105 Williams, “U.S. States Struggle to Define ‘Deepfakes’ and Related Terms as Technically Complex Legislation Proliferates,” https://www.techpolicy.press/us-states-struggle-to-define-deepfakes-and-related-terms-as-technically-complex-legislation-proliferates/.

106 S. 146 - TAKE IT DOWN Act (2025), https://www.congress.gov/bill/119th-congress/senate-bill/146.

107 Sunak Government, *A Pro-Innovation Approach to AI Regulation* (U.K. Department for Science, Innovation & Technology, 2023), https://www.gov.uk/government/publications/ai-regulation-a-pro-innovation-approach/white-paper.

108 Criminal Code Amendment (Deepfake Sexual Material) Bill 2024 No., 2024, Criminal Code Act 1995, https://www.aph.gov.au/Parliamentary_Business/Bills_LEGislation/Bills_Search_Results/Result?bId=r7205.

109 Christelle Coslin, Christine Gateau, and Alexis de Kouchkovsky, “France Prohibits Non-Consensual Deep Fakes,” Hogan Lovells, July 15, 2024, https://www.hoganlovells.com/en/publications/france-prohibits-non-consensual-deep-fakes.

110 *2023 State of Deepfakes: Realities, Threats, and Impact*, https://www.securityhero.io/state-of-deepfakes/.

111 Gibson et al., “Analyzing the AI Nudification Application Ecosystem,” https://arxiv.org/abs/2411.09751.

112 Loc Trinh and Yan Liu, “An Examination of Fairness of AI Models for Deepfake Detection,” *arXiv.org*, May 2, 2021, https://arxiv.org/abs/2105.00558; Kyle Wiggers, “Deepfake Detectors and Datasets Exhibit Racial and Gender Bias, USC Study Shows,” *VentureBeat*, May 6, 2021, https://venturebeat.com/ai/deepfake-detectors-and-datasets-exhibit-racial-and-gender-bias-usc-study-shows; Patrick Hall and Andrew Burt, “Do Deepfakes Discriminate? Auditing a Deepfake Detection System for Systemic Bias (presentation, Fourth Workshop on Payments, Lending, and Innovations in Consumer Finance, Philadelphia Federal Reserve, Philadelphia, October 26–27, 2022), https://www.philadelphiafed.org/-/media/frbp/assets/events/2022/consumer-finance/hall-deep-fakes-presentation-102722.pdf.

113 Gibson et al., “Analyzing the AI Nudification Application Ecosystem,” https://arxiv.org/abs/2411.09751.

114 Hawkins, Mittelstadt, and Russell, “Deepfakes on Demand,” https://dl.acm.org/doi/10.1145/3715275.3732107.

115 Li Qiwei et al., “Reporting Non-Consensual Intimate Media: An Audit Study of Deepfakes,” *arXiv.org*, September 18, 2024, https://arxiv.org/abs/2409.12138.

116 Hawkins, Mittelstadt, and Russell, “Deepfakes on Demand,” https://dl.acm.org/doi/10.1145/3715275.3732107.

117 Matt Burgess, “Millions of People Are Using Abusive AI ‘Nudify’ Bots on Telegram,” *Wired,* October 15, 2024, https://www.wired.com/story/ai-deepfake-nudify-bots-telegram/.

118 Lee Ji-hye, “South Korea: Police Announce 682 Arrests for Deepfake Sex Crimes, Urge Interpol Cooperation,” *Hankyoreh*, February 13, 2025, https://www.business-humanrights.org/ko/latest-news/s-korea-police-announce-682-arrests-in-deepfake-sex-crime-busts-call-for-interpol-collaboration/.

119 Federal Bureau of Investigation, “Child Sexual Abuse Material Created by Generative AI and Similar Online Tools Is Illegal,” Alert No. I-032924-PSA, March 29, 2024, https://www.ic3.gov/PSA/2024/PSA240329; Shelby Grossman, Riana Pfefferkorn, and Sunny Liu, “AI-Generated Child Sexual Abuse Material: Insights from Educators, Platforms, Law Enforcement, Legislators, and Victims,” Stanford Digital Repository, May 29, 2025, https://purl.stanford.edu/mn692xc5736.

120 “City Attorney Shuts Down 10 Websites That Create Nonconsensual Deepfake Pornography,” City Attorney of San Francisco, June 2, 2025, https://sfcityattorney.org/2025/06/02/city-attorney-shuts-down-10-websites-that-create-nonconsensual-deepfake-pornography/.

121 *Sexism, Harassment, and Violence Against Women in Parliaments in Europe*, 12, https://www.ipu.org/resources/publications/issue-briefs/2018-10/sexism-harassment-and-violence-against-women-in-parliaments-in-europe.

122 “National Image Abuse Helpline,” Cyber Civil Rights Initiative, https://cybercivilrights.org/contact-us/.

123 *Sexism, Harassment, and Violence Against Women in Parliaments in the Asia-Pacific Region*, https://www.ipu.org/resources/publications/issue-briefs/2025-03/sexism-harassment-and-violence-against-women-in-parliaments-in-asia-pacific-region.

124 Becca Branum and Mi Yeon Kim, *Rapid Response: Building Victim-Centered Reporting Processes for Non-Consensual Intimate Imagery* (Center for Democracy & Technology, July 2025), https://cdt.org/insights/rapid-response-building-victim-centered-reporting-processes-for-non-consensual-intimate-imagery/.

125 “How Does StopNCII Work?,” video, https://stopncii.org/.

126 “Secure by Design Pledge,” Cybersecurity and Infrastructure Security Agency, https://www.cisa.gov/securebydesign/pledge.