



NATIONAL
CENTER ON
SEXUAL
EXPLOITATION

Established 1962

KINDSEY PENTECOST CHADWICK | Interim President

DAWN HAWKINS | CEO

BENJAMIN A. BULL, ESQ. | SVP & General Counsel

BOARD MEMBERS

RON DEHAAS | Chairman
Founder & CEO, Covenant Eyes

DAN O'BRYANT, ESQ. | Vice Chairman
Former Fellow, Weatherhead Center for International
Affairs, Harvard University

RHONDA GRAFF | Secretary
Former Aerospace Program Manager/Industrial Engineer

BETH COONS | Treasurer
Chairman, Farnsworth Companies

NATHAN ANDERSEN, ESQ.
General Counsel, LeSeuer Investments

KINDSEY PENTECOST CHADWICK | Interim President
President Emeritus, ItWorks! International

JOHN FOUBERT, PH.D.
Dean, College of Education, Union University

ROBERT GEORGE, PH.D.
McCormick Professor of Jurisprudence,
Princeton University

HON. TANYA GOULD
Director, Virginia Attorney General's Office on
Human Trafficking

DONALD L. HILTON, M.D.
Neurosurgeon, University of Texas - San Antonio

DONNA M. HUGHES, PH.D.
Retired Professor, Carlson Endowed Chair,
University of Rhode Island

AMBASSADOR SWANEE HUNT
Chair and Founder, Swanee Hunt Alternatives;
Eleanor Roosevelt Lecturer of Public Policy,
Harvard Kennedy School of Government

MARY ANNE LAYDEN, PH.D.
Director, Sexual Trauma and Psychopathy Program,
University of Pennsylvania

MOST REVEREND PAUL S. LOVERDE
Bishop, Dioceses of Arlington, VA, Retired

SHERRY NILLES
National Regent, Catholic Daughters of the Americas

PATRICK A. TRUMAN
President & CEO Emeritus of NCOSE

LINNEA W. SMITH, M.D.
Retired, Psychiatrist

MELEA STEPHENS, L.P.C., M.M.E.T.
Marriage and Family Therapist

JASON SYVERSON
Chair & Chief investment officer, S8
Impact Foundation

CAROLYN WEST, PH.D.
Professor, Clinical Psychology,
University of Washington

April 3, 2024

Mr. Thomas Dohmke
CEO, GitHub
88 Colin P Kelly Jr St
San Francisco, CA 94107

Mr. Satya Nadella
CEO, Microsoft Corporation
One Microsoft Way
Redmond, WA 98052

Re: GitHub on 2024 Dirty Dozen List for Proliferating and Normalizing AI-Generated Sexual Abuse and Exploitation

Dear Mr. Dohmke and Mr. Nadella:

We are writing to advise you that GitHub has been named to the annual Dirty Dozen List for the second consecutive year. NCOSE is deeply disappointed that since being named to the [2023 Dirty Dozen List](#),¹ GitHub has failed to make any substantial changes to stem the growing tide of AI-generated sexual abuse content and exploitation facilitated by the projects on your platform. As such, GitHub remains the world's *hub* for creating sexually exploitative technology. The List will be publicly released on Wednesday, April 10, 2024.

With GitHub being one of the world's leading code-hosting communities and the most prominent code-hosting platform for version control¹ and collaboration – [particularly generative AI](#) – GitHub has incredible power, reach, and influence.² However, this powerful position comes with immense responsibility—a responsibility that, regrettably, has been sorely neglected.

GitHub's current “developer-first” approach to content moderation and lax policy enforcement has allowed for the proliferation of projects focused on the creation of non-consensual sexually explicit deepfake imagery. For example, NCOSE researchers **identified a 20% increase** in “nudification” repositories on GitHub between May 2023 and

¹ [Version control](#) is the process of managing changes to source code (codes hosted on GitHub). Think of tracked changes, version history and number, and showing markup in Word or Google Docs.

February 2024. The lack of oversight on GitHub also contributes to the alarming increase in [AI-generated child sexual abuse material \(CSAM\)](#).³ GitHub currently hosts open-source models that are trained using CSAM and that create AI-generated CSAM.

GitHub's Role in the Egregious Expansion of AI-Generated Child Sexual Abuse Material (CSAM)

GitHub's failure to act against deepfake pornography and ban projects like DeepFaceLab is contributing to the rising prevalence of AI-generated child sexual abuse material. **Through your permissive attitude and lack of proactive moderation of sexually exploitative technology, you have lowered barriers to entry into open-sourced sexual exploitation and abuse.**

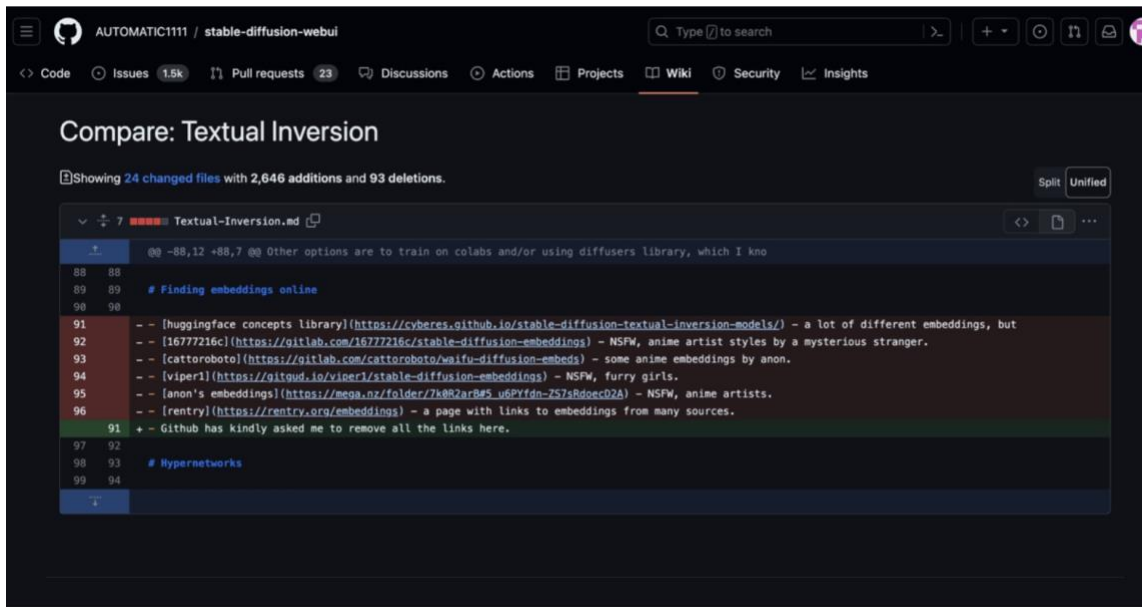
This year alone, hundreds of thousands of images of AI-generated CSAM have been reported across the globe: NCMEC, IWF, President Biden and VP Harris, the FBI, attorneys general from 54 US states and territories, the EU, Thorn, NCOSE, and many others have highlighted AI-generated CSAM as an imminent and rapidly developing threat to children globally.⁴ The disturbing consequences of GitHub's reluctance to act on sexually exploitative technology for the last five years has resulted in the use of such technology to exploit and abuse minors in unimaginable ways. According to the Ireland-based reporting hotline, [Hotline.ie](#), in 2022, they found 5,105 cases of classified CSAM containing computer-generated imagery (37% of all CSAM reports), compared to 1,329 cases (9%) in 2021.⁵ **Over nine out of ten cases of AI-generated CSAM contained preteens, and two-thirds were found to "display adults subjecting children to penetrative sexual activity, and bestiality or sadistic elements."**⁶

In December 2023, the Stanford Internet Observatory identified [more than 3,200 images of suspected CSAM](#)⁷ in the [LAION-5B](#)⁸ (on GitHub) training set, the data behind popular generative AI platform Stable Diffusion.

GitHub hosts source codes, collaborations, and communities fostering the growth and normalization of technology used to create AI-generated CSAM. In particular, the popular repository [AUTOMATIC1111/stable-diffusion-webui](#) has garnered significant attention. Despite its creation of sexually explicit and illicit content, according to GitHub, this project **was the [second most popular repository](#) tagged with 'artificial intelligence' in 2023.**⁹ The lack of defaulted content filters allows bad actors to use this code for exploitative and illicit purposes.

For example, this repository was temporarily suspended in late 2022 due to provision of textual embeddings that facilitated the creation of [sexually explicit images of individuals who appeared to be minors](#).¹⁰ It was reinstated in early 2023 after the removal of the allegedly offensive links.

Unfortunately, evidence shows that these banned links are still accessible through GitHub.



In June 2023, only a few months after being reinstated on GitHub, a [BBC investigation](#) found that the same project, AUTOMATIC1111/stable-diffusion-webui, was used to create AI-generated CSAM that was being bought and sold on Patreon.¹¹

While GitHub implements automated detection tools such as PhotoDNA to [proactively scan for child sexual abuse material](#) (CSAM),¹² you fail to implement comprehensive moderation practices by permitting technology [found to have generated CSAM](#),¹³ instead only moderating for CSAM itself.

Even when GitHub does use PhotoDNA to identify and report to the National Center for Missing and Exploited Children (NCMEC), these reports have failed to be sufficient enough for NCMEC to take any action. In 2022, [GitHub was one of 36 ESPs](#) with more than 90% of reports lacking actionable information.¹⁴ This meant GitHub's reports were so vague that NCMEC couldn't determine where the crime happened, or which law enforcement agency should receive the report.

NCOSE cannot stress enough the outright damaging impact your decisions—or rather, lack thereof—have incurred. Lives are being ruined, reputations destroyed, and the innocence of children stolen. Yet, GitHub remains silent, **prioritizing developers over the victims impacted by the technology being developed.**

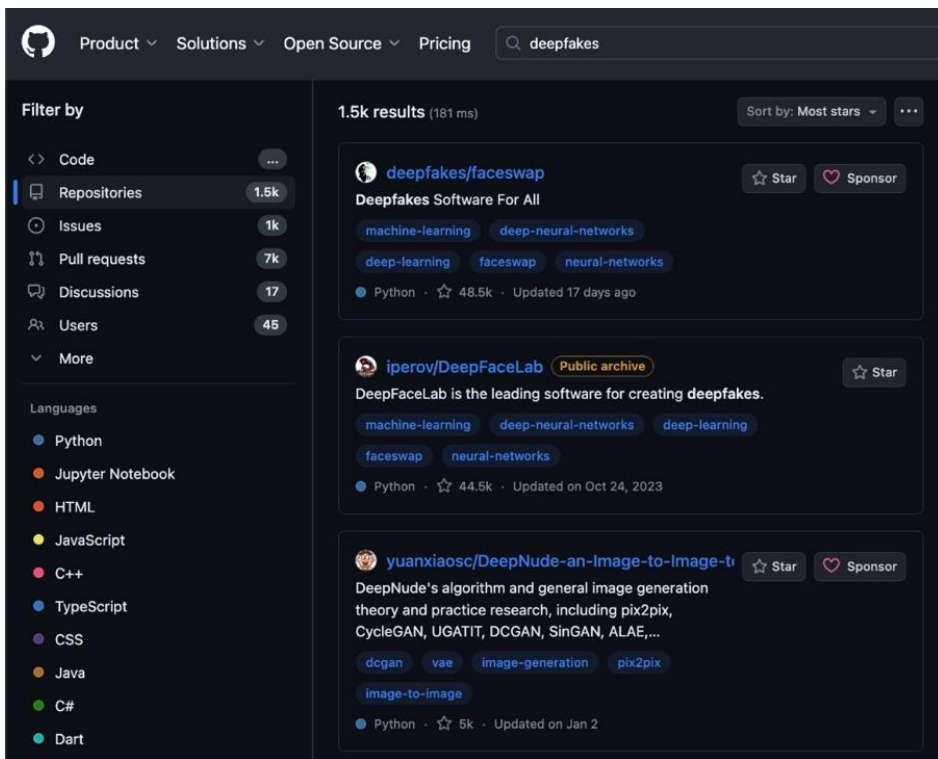
Image-Based Sexual Abuse (IBSA) is Facilitated on and Through GitHub

GitHub's platform, while claiming to foster innovation and collaboration within the software development community, has shamefully become a major facilitator of image-based sexual abuse (IBSA). Despite being named to the 2023 Dirty Dozen List, GitHub still allows the hosting and distribution of repositories that are directly involved in creating and circulating synthetic sexually explicit material (SSEM). This is an alarming and condemnable situation that demands immediate action.

Because of GitHub’s failure to effectively remove the original DeepNude source code, ban replications, and moderate GitHub for DeepNude-like replicas, “copycat” nudifying apps and bots continue to proliferate. A November 2023 study by Graphika found the number of links advertising ‘undressing apps’ **increased more than 2,400% from 2022 to 2023 on social media, including on X and Reddit.** ¹⁵

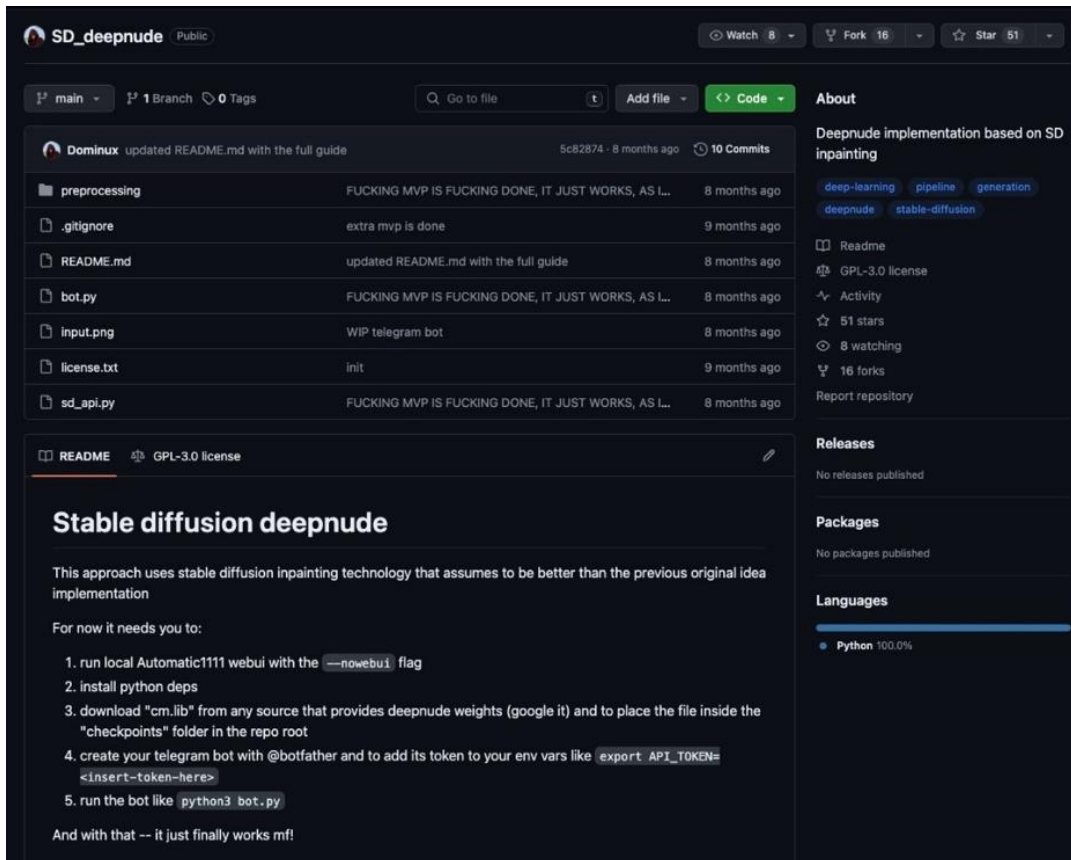
NCOSE researchers found a troubling **20% increase** in nudification repositories over the last nine months, increasing from 54 repositories in May 2023 to 68 repositories in February 2024, with the [original source code for DeepNude](#) still active on GitHub’s site. GitHub remains a major **hub** for sexually exploitative tools. ¹⁶

It is alarming to note that the three most popular repositories tagged with “deepfakes” on GitHub, namely deepfakes/faceswap, iperov/DeepFaceLab, and yuanxiaosc/DeepNude-an-Image-to-Image-technology, depicted in the image below, are utilized for creating non-consensual sexually explicit deepfake imagery. Despite GitHub banning or suspending these repositories in the past, they remain highly popular in terms of favorites (stars) and forks (replications), highlighting significant flaws in GitHub's developer-first content moderation practices. While research shows that [one in every three deepfake models is pornographic](#), ¹⁷ the three most popular repositories tagged with “deepfakes” are used for the creation of synthetic sexually explicit material (SSEM) on GitHub – somehow beating the statistical odds.



Captured February 14, 2024

Further, some repositories even guide users on how to use sexually exploitative codes on GitHub to develop bots on other platforms to “strip” women of their clothing.



Considering the fact that developer interest in deepfake technology is the [most common reason men watch deepfake pornography \(57%\)](#), followed by celebrity interest (48%), and fulfilling personalized sexual fantasies (33%),¹⁸ it is not surprising that the initial deepfake and nudification technologies were created by “[interested programmers](#),” rather than experienced developers.¹⁹

This network of “interested programmers” extends beyond GitHub’s site and encompasses platforms like Reddit, Discord, and Telegram, drawing from software that is rooted in GitHub's vast network of sexually exploitative repositories. Consequently, the circulation of deepfake content for sexual exploitation is a widespread and growing problem. According to a December 2023 research study by [Home Security Heroes](#), the availability of deepfake pornography online has witnessed a staggering [increase of 550%](#) between 2019 and 2023.²⁰

GitHub is also directly connected to dedicated deepfake pornography websites allowing links and scrapers for sites like [CelebJihad](#),²¹ one of the [origin sites](#)²² of Taylor Swift's deepfake abuse distribution, and Mr.DeepFakes, the most prolific deepfake pornography website in the United States. GitHub still hosts the source code for Mr.DeepFakes and [DeepFaceLab](#)²³ and remains one of the [top 10 referral sites](#)²⁴ to Mr.DeepFakes as of February 2024. This places GitHub at the center of a social pandemonium, promoting the sexual violation of women through non-consensual deepfake imagery.

Two things have remained the same with deepfakes since 2019: [their purpose – pornography, and their target – women](#).²⁵ Similar to Sensity AI’s findings in 2019 and 2021,²⁶ the same study by [Home Security](#)

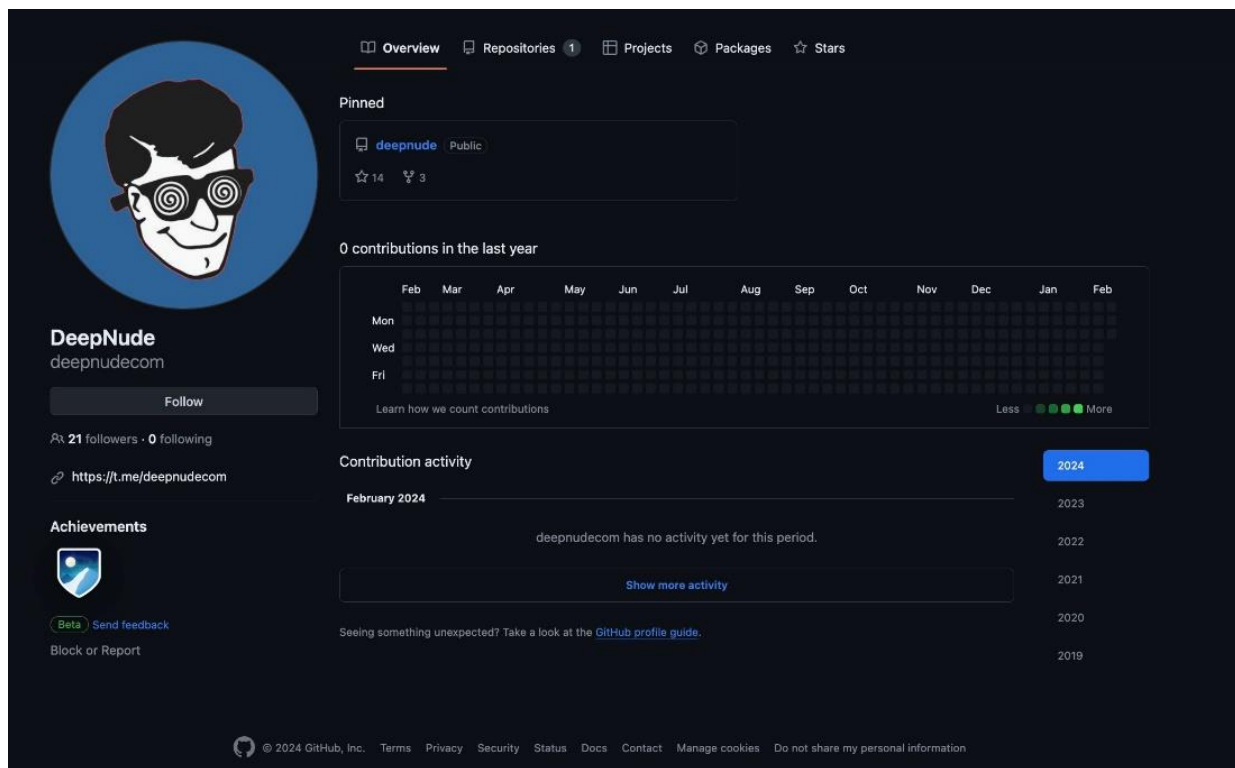
[Hereos](#)²⁷ found that 98% of all deepfake videos available online were of pornography and 99% of all forged (deepfake) pornography features women.

Insufficient Content Moderation Practices and Negligible Policy Enforcement

The overwhelming proliferation of open-source projects on GitHub that enable sexually exploitative content amplifies the accessibility of technology designed to perpetrate image-based sexual abuse (IBSA), AI-generated CSAM, and expose minors to sexually exploitative content and projects.


GitHub allows developers to remain anonymous, which aids them in distancing themselves from controversy while contributing to objectionable codes or forming covert networks to collaborate on sexually exploitative technologies.

GitHub's track record in dealing with problematic projects related to sexual exploitation is more than concerning. As of February 2024, the original DeepNude repository and its Telegram link (now defunct), along with other repositories hosting the [original source code for DeepNude](#),²⁸ exist on GitHub. This highlights a discrepancy between GitHub's [2019 public stance and promises](#)²⁹ to ban DeepNude and all DeepNude-like projects and your actual practices.



README Code of conduct GPL-3.0 license

Official DeepNude Algorithm



The original [DeepNude Software](#) and all its safety measures have been violated and exposed by hackers. Two days after the launch, the [reverse engineering](#) of the app was already on github. It is complete and runnable. So it no longer makes sense to hide the source code. The purpose of this repo is only to add technical information about the algorithm and is aimed at specialists and programmers, who have asked us to share the technical aspects of this creative tool.

DeepNude uses an interesting method to solve a typical AI problem, so it could be useful for researchers and developers working in other fields such as *fashion*, *cinema* and *visual effects*.

We are sure that github's community can take the best from this controversial algorithm, and inspire other and better creative tools.

This repo contains only the core algorithm, not the user interface.

How DeepNude works?

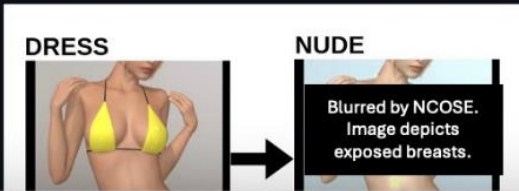
DeepNude uses a slightly modified version of the [pix2pixHD](#) GAN architecture. If you are interested in the details of the network you can study this amazing project provided by NVIDIA.

A GAN network can be trained using both **paired** and **unpaired** dataset. Paired datasets get better results and are the only choice if you want to get photorealistic results, but there are cases in which these datasets do not exist and they are impossible to create. DeepNude is a case like this. A database in which a person appears both naked and dressed, in the same position, is extremely difficult to achieve, if not impossible.

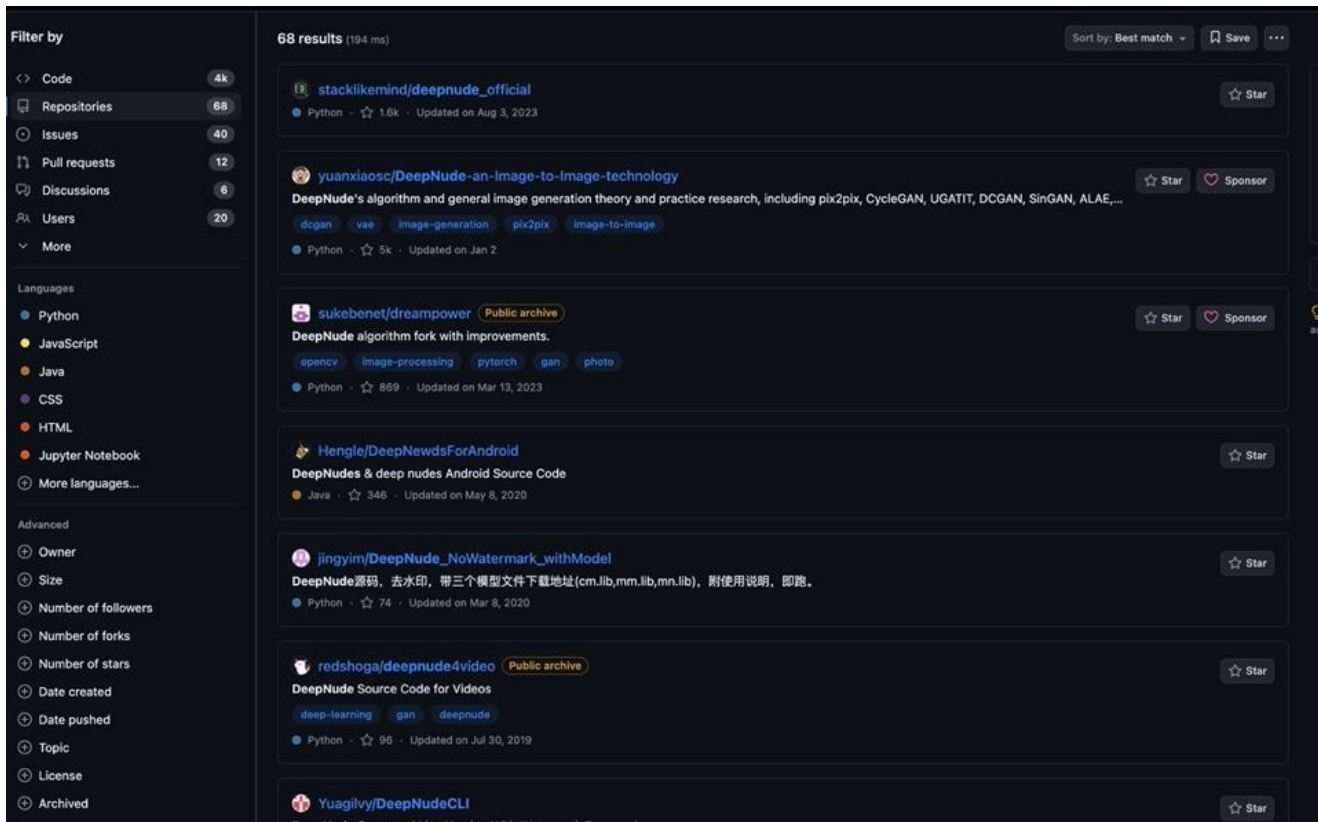
We overcome the problem using a *divide-et-Impera* approach. Instead of relying on a single network, we divided the problem into 3 simpler sub-problems:

- i. Generation of a mask that selects clothes
- ii. Generation of an abstract representation of anatomical attributes
- iii. Generation of the fake nude photo

Original problem:



Further, the ease of access to projects using similar or the original source code to DeepNude, amassing 4K+ forks (replications) on GitHub, illustrates a severe gap in the content moderation policies that must be addressed.



Captured February 14, 2024

NCOSE is deeply concerned about the extent of features on GitHub that may increase risk of harm to minors, such as [limited content moderation policies](#) and a lack of caregiver and teacher/administrative controls.³⁰

For example, a 15-year-old boy who had been creating and sharing deepfake and nudity-related codes on GitHub recently left the platform due to psychological and legal repercussions. In a second farewell message, he expressed a commitment to the “nudify” community, embedding HTML text with the source code and instructions, and upon downloading it, explicit deepfake pornography featuring celebrities was displayed.

Hey anons,

For a while now I've felt unsatisfied with my life, wasting my spare time doing shit like this rather than doing anything productive.

That's why hence forth [REDACTED] is dead, I am never visiting 4chan again, I am never logging back into this account. I'm going to delete my deepfake bot and my nudify guide.

Nobody should be drawn down the same path that I followed a year ago, wasting their time on illegal, degenerate shit that only brings depression and loneliness. I was 15 when I discovered nudifying, think what that discovery could do to yourself at 15. That one mistake was all that it took to for me to throw my life into the gutter. I've already been question by police months ago for something relating to this, I really can't do that again.

Sorry that this has to happen, sorry I lied to people, I need to do this for my own sake.

Hello again anons,

I know I said I was done with this

But contrary to what I said I've still been skimming through the nudify threads over the past couple of days every now and then

I see people who still want this guide and I've thought over my decision

Though I refuse to bring back my deepfake bot I still want to leave some small mark on this community that I wasted so much time on

Let this be a warning for all future 'wizards'

Don't parade what you do, don't save the images you make, don't get too attached.

Nudify is temporary, it is an illusion.

Live by this quote from my favourite book, Ready Player One:

"I realized, as terrifying and painful as reality can be, it's also the only place where you can find true happiness. Because reality is real."

██████████ signing off

For real this time

For real this time



The teenage boy then suggested that interested developers use the DeepFaceLab guide for more 'realistic' generations, which is only accessible by accessing the most prolific deepfake pornography website, Mr.DeepFakes.

Better Deepfake Software

While Roop Unleashed can produce passable deepfakes the often low quality of the fakes is an inherent issue with on-click deepfakes

To obtain a higher quality deepfake you should use [DeepFaceLab](#)

This tool takes much longer than Roop as it involves training a model on the source face and requires some input from the user

I cannot provide a guide on DeepFaceLab as I am not nearly experienced enough to be offering advice

[This guide](#) is the best way to learn to use the deepfake program

It goes into detail on the process of deepfaking and the settings involved

Made by ██████████

Contact me at ██████████@putlook.com

<https://mrdeepfakes.com/forums/threads/guide-deepfacelab-2-0-guide.3886/>

Link displayed in bottom left corner is the hyperlink attached to the words "This guide" referring to the DeepFaceLab guide on Mr.DeepFakes website.

This single narrative experience raises several concerns related to a minor creating and accessing harmful and potentially illegal content on GitHub.

Even when clearly harmful and exploitative repositories, like one described above, are brought to your attention, no action is taken. Despite being named to the 2023 Dirty Dozen List, NCOSE alerting a Microsoft contact we met at INHOPE 2023, and submitting numerous reports through your official reporting form back in November 2023 about the sexually exploitative repositories on your platform, with a follow-up email for each report in December 2023, **NCOSE has yet to receive anything more than an automated email stating**, “Hi, Our team is currently investigating the account in question to determine if their content or conduct violates GitHub's [Terms of Service](#).”³¹

[GitHub Support] - Report Content: iperov (content)

2 messages

GitHub Developer Support <developer@githubsupport.com>
Reply-To: GitHub Developer Support <developer@githubsupport.com>

Fri, Nov 17, 2023 at 3:42 A

Please do not write below this line

Your request has been updated.

You can add a comment by replying to this email.



GitHub (GitHub Support)

Nov 17, 2023, 9:42AM UTC

Hi,

Our team is currently investigating the account in question to determine if their content or conduct violates GitHub's Terms of Service.

Regards,

GitHub Trust & Safety



Nov 17, 2023, 3:42PM UTC

Report Content: iperov (content)

<https://github.com/iperov> <https://github.com/iperov/DeepFaceLab>

Reason

I want to report another type of malicious code.

Comments

This code pertains to creating deepfake pornography of women under the guise of a "normal and popular" deepfake repo. This repo, DeepFaceLab, and DeepFaceLive contain LIVE LINKS to the most prolific deepfake pornography website in the world, Mr.DeepFakes. Before its archive on November 9, 2023, this repo had amassed more stars and forks than the Stable Diffusion repo on GitHub, with 43.3k stars and 9.7k forks. Further, it is allegedly the deepfake software used to create 95% of all deepfakes. As research shows, roughly 90% of all deepfakes are of women and pornographic. GitHub's permissiveness of this repo has undoubtedly lowered the barrier of entry in open source coding for users to participate in AI-facilitated sexual abuse from creation to dissemination and monetization of non-consensual imagery. Your permissiveness of this repo has also helped close gaps in the representation of abusive tech more broadly by sending users to a non-consensual pornography website to learn how to use DeepFaceLab where they are offered "datasets" of non-consensual imagery, both clothed and exposed. As such, it is no accident nor coincidence that GitHub is one of the top ten referral sites for Mr.DeepFakes. You have (presumably) knowingly allowed thousands of Hubbers to be exposed to the most prolific deepfake pornography website, and despite prohibiting non-consensual content, you do not seem to find an issue with hosting codes, repos, or links to the very content you deem "intolerable." To GitHub, this may be just "another" code, but to those impacted by image-based sexual abuse, these codes and the exploitation they facilitate are weapons of abuse. By maintaining codes such as these, GitHub is complicit in the promotion, democratization, normalization, and, at times - the monetization of AI-facilitated sexual abuse / image-based sexual abuse.

Here are a few of the titles and corresponding links hosted by DeepFaceLab:

- mrdeepfakes, "the biggest NSFW English community": <https://mrdeepfakes.com/forums/>
- DeepFace Lab Guide: <https://mrdeepfakes.com/forums/thread-guide-deepfacelab-2-0-guide>
- Face Creation Guide: <https://mrdeepfakes.com/forums/thread-guide-deepfacelab-2-0-guide?pid=1845&pid18450>
- Google Colab Guide: <https://mrdeepfakes.com/forums/thread-guide-deepfacelab-google-colab-tutorial>
- Compositing: <https://mrdeepfakes.com/forums/thread-deepfacelab-2-0-compositing-in-davinci-resolve-vegas-pro-and-after-effects>
- Discussion and Suggestions: <https://mrdeepfakes.com/forums/thread-deepfacelab-2-0-discussion-tips-suggestions>
- Celebrity Facesets: <https://mrdeepfakes.com/forums/forum-celebrity-facesets>
- Pretrained Models: <https://mrdeepfakes.com/forums/forum-trained-models>

This is unacceptable, especially considering Danielle Leong's work to advocate for and build GitHub as a place grounded in consensual software. Why does GitHub prohibit non-consensual imagery but allow the codes/repos for CREATING non-consensual imagery to THRIVE on your platform? It is not enough to flaunt your commitment to a more humanitarian and equitable community if you do not think of the community in which these codes/repos will most certainly impact. "Access to SAFE AND HARMLESS technology is a fundamental human right. Everyone deserves to have the opportunity to create, innovate, and collaborate while contributing to our digital future. SIMILARLY, ACCESS TO TECHNOLOGY AND RELATED OPPORTUNITIES MUST NOT IMPEDE THE FUNDAMENTAL HUMAN RIGHT TO LIFE, LIBERTY, AND SECURITY OF PERSON BY THOSE IMPACTED BY TECHNOLOGICAL DEVELOPMENTS."

This email is a service from GitHub Support.

To: GitHub Developer Support <developer@githubsupport.com>

Tue, Dec 5, 2023 at 10:00 A

just checking in on this report - any updates?
(quoted text hidden)

Your current stance – that the [removal of a single project](#)³² is believed to cause significant downstream effects for countless software projects – fails to acknowledge the profound impact a project may have on those who have endured and continue to suffer from sexual abuse and exploitation. The removal of a single project could undoubtedly have **significant upstream effects for countless victim-survivors of IBSA, SSEM, and AI-generated CSAM.**

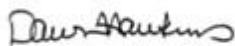
Despite the evident violations and abuses, GitHub remains focused on putting the needs of developers over those of victims of sexual abuse and exploitation. The proliferation of deepfake technologies and the ease with which they can be shared and distributed is a severe concern. GitHub must remove and block tools used for image-based sexual abuse and AI-generated CSAM on the platform. The well-being and safety of individuals, particularly women and children who are disproportionately affected by deepfake abuse, must be prioritized.

NCOSE requests GitHub make the following improvements:

1. **Ban private and public repositories dedicated to sexual deepfake, ‘nudifying,’ and AI-generated pornography software development from GitHub.** This includes removing current repositories and preventing the replication of related repositories for sexually exploitative technology software development.
2. **Ban private and public pornography and sexually explicit imagery scraping repositories from GitHub.** This includes removing current repositories and preventing the replication of related repositories for purposes of pornography and sexually explicit imagery scraping software development.
3. **Proactively moderate content and community forums** on GitHub.
4. **Default middle and high-school student repositories to ‘private’** to prevent minors’ exposure to the abundance of harmful content on GitHub.
5. Implement **basic, industry-wide safety standards:** parental controls, teacher/administrative controls, and age-gate repositories inappropriate for minor-aged users.

We have attached the 2023 notification letter we sent to GitHub last year for reference.

Thank you for your attention,



Dawn Hawkins

CEO



Kindsey P. Chadwick

Interim President

Cc:

Mike Hanley, Chief Security Officer and Senior Vice President of Engineering

Inbal Shani, Chief Product Officer

Shelley McKinley, Chief Legal Officer

Margaret Tucker, Public Policy Manager

Scott Guthrie, Executive Vice President, Cloud + AI Group, Microsoft

Ranjani Mani, Director of GenAI, Microsoft

Attached: 2023 Dirty Dozen List Notification Letter to GitHub

¹ NCOSE, “GitHub Notification Letter Dirty Dozen List 2023,” April 28, 2023, https://endsexualexploitation.org/wp-content/uploads/Microsoft-GitHub-Notification-Letter_DDL-2023_FINAL.pdf.

² Kyle Daigle, “Octoverse: The State of Open Source and Rise of AI in 2023,” *GitHub Blog*, November 8, 2023, <https://github.blog/2023-11-08-the-state-of-open-source-and-ai>.

³ David Thiel, Melissa Stroebel, and Rebecca Portnoff, *Generative ML and CSAM: Implications and Mitigations* (Thorn and Stanford Internet Observatory, June 24, 2023), <https://stacks.stanford.edu/file/druid:jv206yg3793/20230624-sio-cg-csam-report.pdf>.

⁴ Thiel, Stroebel, and Portnoff, *ibid*; Haley McNamara (NCOSE), “Your Daughter’s Face Could Be Hijacked For ‘Deepfake’ Porn,” *The Federalist*, December 4, 2023, <https://thefederalist.com/2023/12/04/your-daughters-face-could-be-hijacked-for-deepfake-porn>; David Thiel, “Investigation Finds AI Image Generation Models Trained on Child Abuse,” *Stanford Cyber Policy Center Blog*, December 20, 2023, <https://cyber.fsi.stanford.edu/news/investigation-finds-ai-image-generation-models-trained-child-abuse>; IWF, *How AI is Being Abused to Create Child Sexual Abuse Imagery* (Internet Watch Foundation, October 2023), https://www.iwf.org.uk/media/q4zll2ya/iwf-ai-csam-report_public-oct23v1.pdf; National Association of Attorneys General (NAAG), “54 Attorneys General Call on Congress to Study AI and Its Harmful Effects on Children,” news release, September 5, 2023, <https://www.naag.org/press-releases/54-attorneys-general-call-on-congress-to-study-ai-and-its-harmful-effects-on-children>; David Thiel, *Identifying and Eliminating CSAM in Generative ML Training Data and Models* (Stanford Internet Observatory, December 21, 2023), https://stacks.stanford.edu/file/druid:kh752sm9123/ml_training_data_csam_report-2023-12-21.pdf;

The White House, “Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence,” Presidential Actions, October 30, 2023, <https://www.whitehouse.gov/briefing-room/presidential-actions/2023/10/30/executive-order-on-the-safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence>; Hotline.ie, *Hotline.ie Annual Report 2022* (Dublin, Ireland: Hotline.ie, 2023), <https://www.hotline.ie/library/annual-reports/2023/Hotline-ie-Annual-Report-2022.pdf>.

⁵ Cormac O’Keeffe, “AI Driving Child Sex Abuse Imagery,” *Irish Examiner*, January 19, 2024, <https://www.irishexaminer.com/news/arid-41312179.html>.

⁶ Hotline.ie, *ibid*.

⁷ David Thiel, *Identifying and Eliminating CSAM in Generative ML Training Data and Models* (Stanford Internet Observatory, December 21, 2023), https://stacks.stanford.edu/file/druid:kh752sm9123/ml_training_data_csam_report-2023-12-21.pdf.

⁸ “LAION-AI,” GitHub, accessed March 4, 2024, <https://github.com/LAION-AI>.

⁹ AUTOMATIC1111/stable-diffusion-webui, “Compare: Textual Inversion,” GitHub, accessed March 4, 2024, https://github.com/AUTOMATIC1111/stable-diffusion-webui/wiki/Textual-Inversion/_compare/9d7346f7f3faa275305cc4a388a3335a0f53961b...bc9a09829dbc90760c8626c83824e05cfab5cb98.

¹⁰ *Ibid*.

¹¹ Angus Crawford and Tony Smith, “Illegal Trade in AI Child Sex Abuse Images Exposed,” *BBC*, June 28, 2023, <https://www.bbc.com/news/uk-65932372>.

¹² Kevin Xu, “2022 Transparency Report,” *GitHub Blog*, February 15, 2023, <https://github.blog/2023-02-15-2022-transparency-report>.

¹³ Emanuel Maiberg, “It Takes 2 Clicks to Get From ‘Deep Tom Cruise’ to Vile Deepfake Porn,” *Vice*, May 17, 2022, <https://www.vice.com/en/article/qjb7b7/ethical-deepfakes-deep-tom-cruise-ai-generated-porn>.

¹⁴ National Center for Missing & Exploited Children, “Cyber Tipline 2022 Report,” accessed March 5, 2024, <https://www.missingkids.org/cybertiplinedata>.

-
- ¹⁵ Margi Murphy, “‘Nudify’ Apps That Use AI to ‘Undress’ Women in Photos Are Soaring in Popularity,” *Time*, December 8, 2023, <https://time.com/6344068/nudify-apps-undress-photos-women-artificial-intelligence>.
- ¹⁶ OrgTestCodacy11KRepos110MB, “repo-2245-DeepNude-an-Image-to-Image-technology,” GitHub, accessed March 4, 2024, <https://github.com/OrgTestCodacy11KRepos110MB/repo-2245-DeepNude-an-Image-to-Image-technology>.
- ¹⁷ Home Security Heroes, “2023 State of Deepfakes: Realities, Threats, and Impact,” accessed March 5, 2024, <https://www.homesecurityheroes.com/state-of-deepfakes>.
- ¹⁸ Home Security Heroes, “2023 State of Deepfakes,” Infographic, accessed March 5, 2024, <https://www.homesecurityheroes.com/state-of-deepfakes/assets/pdf/state-of-deepfake-infographic-2023.pdf>.
- ¹⁹ Victoria Rousay, “Sexual Deepfakes and Image-Based Sexual Abuse: Victim-Survivor Experiences and Embodied Harms” (Master’s thesis, Harvard University, 2023), <https://dash.harvard.edu/handle/1/37374909>.
- ²⁰ Home Security Heroes, “2023 State of Deepfakes,” Infographic, *ibid*.
- ²¹ Takagotch, “CelebJihad,” GitHub, accessed March 4, 2024, <https://github.com/takagotch/CelebJihad>.
- ²² Lewis Pennock, “Celeb Jihad – The Website that Posted Deepfake AI Porn of Taylor Swift – Has Been Sharing Explicit Images of Celebrities for YEARS Without Punishment – And was Threatened by the Pop Star’s Lawyers in 2011 Over Fake Topless Photo,” *Daily Mail*, January 25, 2024, <https://www.dailymail.co.uk/news/article-13006441/celeb-jihad-deepfake-taylor-swift.html>.
- ²³ Iperov, “DeepFaceLab,” GitHub, archived November 9, 2023, accessed March 5, 2024, <https://github.com/iperov/DeepFaceLab>.
- ²⁴ Similar Web, “Mrdeepfakes.com,” accessed March 5, 2024, <https://www.similarweb.com/website/mrdeepfakes.com/#referrals>.
- ²⁵ Home Security Heroes, “2023 State of Deepfakes,” Infographic, *ibid*.
- ²⁶ Henry Ajder et al., *The State of Deepfakes: Landscape, Threats, and Impact* (Deeptrace, 2019), https://regmedia.co.uk/2019/10/08/deepfake_report.pdf; Giorgio Patrini, *The State Of Deepfakes 2020: Updates on Statistics and Trends* (Sensity, 2021), https://books.google.com/books/about/The_State_of_Deepfakes_2020.html?id=--SBzgEACAAJ.
- ²⁷ Home Security Heroes, “2023 State of Deepfakes,” Infographic, *ibid*.
- ²⁸ OrgTestCodacy11KRepos110MB, *ibid*.
- ²⁹ Maiberg, *ibid*.
- ³⁰ Daphne Leprince-Ringuet, “GitHub: We Won’t Take Down Any of Your Content Unless We Really Have to,” *ZDNET*, February 21, 2020, <https://www.zdnet.com/article/github-we-wont-take-down-any-of-your-content-unless-we-really-have-to>.
- ³¹ “GitHub Terms of Service,” GitHub Docs, accessed March 4, 2024, <https://docs.github.com/site-policy/github-terms/github-terms-of-service>.
- ³² Shelley McKinley, “Don’t Leave Developers Behind in the Section 230 Debate,” *GitHub Blog*, March 10, 2023, <https://github.blog/2023-03-10-dont-leave-developers-behind-in-the-section-230-debate>.



Established 1962

PATRICK A. TRUEMAN, J.D. | *Board Member*
President

DAWN E. HAWKINS
Chief Executive Officer

BENJAMIN W. BULL, J.D.
Sr. Vice President & General Counsel

BOARD MEMBERS

RON DEHAAS | *Chairman*
Founder & CEO, Covenant Eyes

DAN O'BRYANT, J.D. | *Vice Chairman*
Former Fellow, Weatherhead Center for International Affairs, Harvard University

RHONDA GRAFF | *Secretary*
Former Aerospace Program Manager/Industrial Engineer

KEN SUKHIA, J.D. | *Treasurer*
Trial and Appellate Lawyer, Sukhia Law Group, PLC

HADLEY ARKES, PH.D.
Ney Professor of Jurisprudence, Emeritus,
Amherst College

BETH COONS
Chairman, Farnsworth Companies

JOHN FOUBERT, PH.D.
Dean, College of Education, Union University

ROBERT GEORGE, PH.D.
McCormick Professor of Jurisprudence,
Princeton University

DONALD L. HILTON, M.D.
Neurosurgeon, University of Texas - San Antonio

DONNA M. HUGHES, PH.D.
Professor, Carlson Endowed Chair, University of
Rhode Island

AMBASSADOR SWANEE HUNT
Chair and Founder, Hunt Alternatives;
Eleanor Roosevelt Lecturer of Public Policy,
Harvard Kennedy School of Government

MARY ANNE LAYDEN, PH.D.
Director, Sexual Trauma and Psychopathology Program,
University of Pennsylvania

MOST REVEREND PAUL S. LOVERDE
Bishop, Dioceses of Arlington, VA, Retired

SHERRY NILLES
National Regent, Catholic Daughters of the Americas

KINDSEY PENTECOST
President, ItWorks! International

MARGARET RUCKS
Managing Director, Rucks Family Foundation

ALAN SEARS, ESQ.
Former President and CEO, Alliance Defending Freedom

LINNEA W. SMITH, M.D.
Retired, Psychiatrist

MELEA STEPHENS, L.P.C., M.M.F.T.
Marriage and Family Therapist

CAROLYN WEST, PH.D.
Professor of Clinical Psychology
University of Washington

JUSTICE MICHAEL J. WILKINS
Former Associate Chief Justice, Utah Supreme Court

April 28, 2023

Thomas Dohmke
CEO, GitHub
88 Colin P Kelly Jr St
San Francisco, CA 94107

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

Dear Mr. Dohmke,

We are writing to inform you that the National Center on Sexual Exploitation—a non-partisan nonprofit organization in Washington, DC dedicated to addressing the full spectrum of sexual exploitation—is placing GitHub on the annual Dirty Dozen List featuring 12 major contributors to sexual exploitation and abuse. The list will be revealed to the public on May 2.

As the [largest code-hosting community](#)¹ globally and the [most prominent code-hosting platform](#)² for version control and collaboration, comprised of over [100 million active developers](#),³ GitHub has incredible power and reach. Due to your platform's open-sourced design, reporting 413 million open-sourced code contributions in 2022 alone, GitHub has served as a primary leader in the democratization of the most recent software developments – such as with [generative AI](#) – and is arguably the most critical space in which AI tech develops.⁴

However, despite moving the tech industry forward in the last decade and establishing itself as a leader in the democratization of generative AI, **GitHub has also earned itself a title as a significant contributor to the creation of sexually exploitative technology⁵ and has been noted for facilitating the growing crime of image-based sexual abuse** – the capture, creation, and/or sharing of sexually explicit images without the subject's knowledge or consent. GitHub hosts guides, codes, and hyperlinks to sexual deepfake community forums dedicated to the creation, collaboration, and commodification of synthetic media technologies, and AI-leveraged 'nudifying' websites and applications that take women's images and "strip them" of clothing.⁶ Open-sourced repositories dedicated to

IBSA thrive on GitHub, allowing users to replicate, favorite (star), and collaborate on sexually exploitative technology without repercussions.

In 2019, the source code for a ‘nudging’ bot at the center of a deepfake ecosystem on Telegram that “stripped” images of more than 104,000 women was found on GitHub. Despite this technology violating GitHub’s policies and the company reportedly banning the source code and all replications (forks) – **the source code and hundreds of replications remain active on GitHub four years later, continuing to victimize and traumatize the women depicted in the abusive content.**

GitHub has also come under fire from reputable academic researchers. A study by [Winter and Salter](#) found that GitHub allowed sexual deepfakes to “intentionally spread to spaces with limited moderation, which has allowed the continued creation of non-consensual pornography.”⁷

[DeepFaceLab](#),⁸ **the most popular technology for creating sexual deepfakes (estimated to be used in the creation of 95% of all sexual deepfakes), is active on GitHub** and has been starred over [38 thousand times and replicated over 8.7 thousand times](#).⁹ Further, DeepFaceLab’s GitHub repository contains direct links to the most prolific sexual deepfake abuse website in the United States: Mr.DeepFakes.

In addition to the ones cited above, many more repositories dedicated to developing pornography and image-scraping technology/bots, as well as “save bots” that are frequently used to save sexually explicit and pornographic images from social media sites, remain rampant on GitHub. Image-based sexual abuse (IBSA) is occurring at unprecedented rates, and is facilitated by Internet and Communication Technologies – such as those being developed on GitHub. The online nature of IBSA limits the victim’s ability to escape abuse, as evidence remains online forever. Once an image is shared, there is no guarantee that it can be removed, especially with technology further restricting a victim’s ability to remove content, such as save bots. The technology being developed on GitHub is also part of a new wave of sexual violence. Sexual deepfakes allow anyone to be targeted and harassed online for something they never did or said.

We know GitHub prides itself on being an educational innovator – providing opportunities for teenagers (13+) and college students to learn coding and software development. These services are designed to be connected to learning management systems (LMS) such as [Google Classroom](#).¹⁰ Considering GitHub’s lack of content moderation and meaningful age verification measures, the significant number of sexually exploitative and obscene repositories publicly accessible to minors on GitHub is alarming. GitHub does not age-gate software developments that may be inappropriate for underage users – despite having a population of 1.9 million students using GitHub Classroom. Further, GitHub [defaults all student repositories to public](#).¹¹ Teachers/administrators must pay an extra fee to access features to privatize their repositories.

NCOSE recognizes the importance of and supports technological innovation and progress. **However, technological advances must not supersede or come at the cost of people’s safety and well-being.** Technology should be built and developed to fight, rather than facilitate, sexual exploitation and abuse. GitHub’s emphasis on developer happiness and free speech safety and well-being cannot mean allowing developers to commit crimes and harm others. By providing a space not only to create, but also to collaborate on and amplify abuse, GitHub is not only condoning criminal conduct – it is directly contributing to it.

The exponential growth in innovation and creative solutions offered by artificial intelligence are to be celebrated. Yet the dizzying advancements bear several intuitive risks to its users and begs the question: Who bears the brunt? An injustice occurs when the purported benefits of artificial intelligence employed by

GitHub are annulled by acute risks and/or demonstrable harms. Humanity may not be close to an ethical consensus, but at least [five ethical principles](#)¹² from the global corpus of principles and guidelines on ethical AI are clear. These include transparency, justice and fairness, non-maleficence, responsibility, and privacy. Moreover, artificial intelligence systems learn and make decisions that can have a profound impact on human dignity and individual autonomy. GitHub’s business model also breaches the ‘legacy’¹³ principle intrinsic to conversations concerning ethics. Rather than being compatible “with scenarios that most humans today would view as happy,” GitHub ostensibly opts in for scenarios that most humans today “would view as terrible.”

In recalibrating this imbalance, NCOSE urges GitHub to implement the following changes:

1. **Ban private and public repositories dedicated to sexual deepfake, ‘nudifying,’ and AI-generated pornography software development from GitHub;** this includes removing current repositories and preventing the replication of related repositories for sexually exploitative technology software development
2. **Ban private and public pornography and sexually explicit imagery scraping repositories from GitHub;** this includes removing current repositories and preventing the replication of related repositories for purposes of pornography and sexually explicit imagery scraping software development
3. **Proactively moderate content and community forums on GitHub**
4. **Default student repositories to private**
5. **Implement basic industrywide safety standards: parental controls, teacher/administrative controls, and age-gate repositories inappropriate for minor-aged users**

Image-Based Sexual Abuse (IBSA) is Facilitated on and through GitHub

[Image-based sexual abuse](#) (IBSA) is a broad term that includes a multitude of harmful experiences, such as non-consensual sharing of sexual images (sometimes called “revenge porn”), pornography created using someone’s face without their knowledge (or sexual deepfakes), non-consensual recording or capture of intimate nude images (including so-called “upskirting” or surreptitious recordings in places such as restrooms and locker rooms via “spycams”), recording of sexual assault, the use of sexually explicit or sexualized materials to groom or extort a person (also known as “sextortion”) or to advertise commercial sexual abuse, and more.¹⁴

Importantly, sexually explicit or sexualized material depicting children ages 0-17 constitutes a distinct class of material known as child sexual abuse material (CSAM – the more appropriate term for “child pornography”), which is illegal to knowingly possess, access, reproduce, and distribute under US federal law. CSAM [should not be conflated with IBSA](#),¹⁵ though the two crimes are closely related.

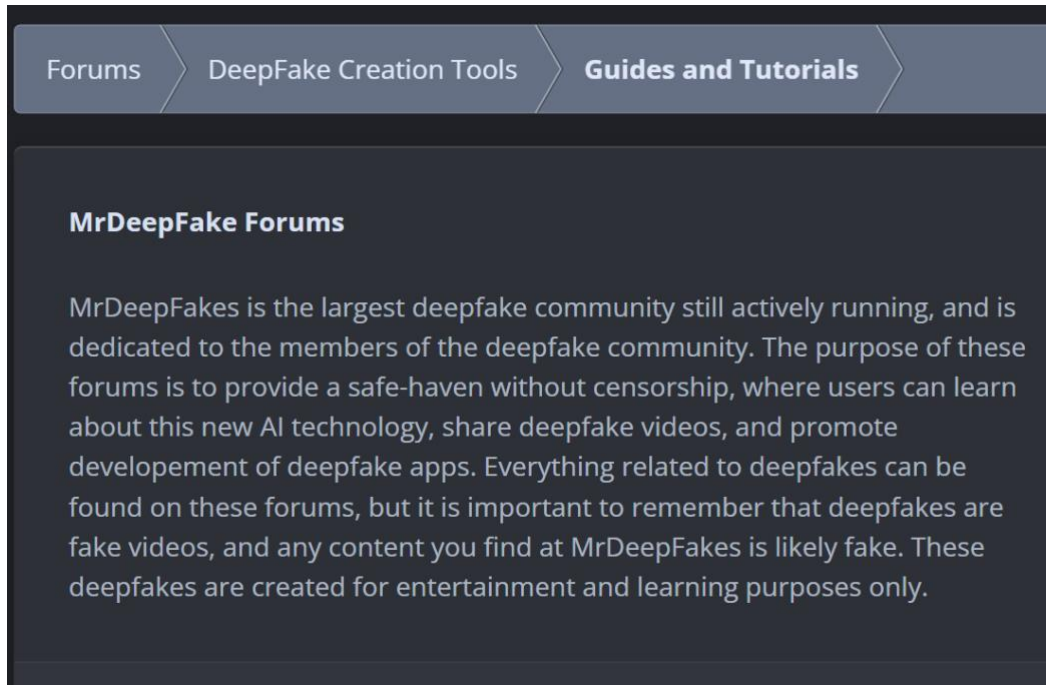
Although GitHub prohibits sexually explicit content, and [has a specific policy](#) banning non-consensual intimate imagery, “particularly where that content is amplified by its placement in profiles or other social contexts,”¹⁶ the lack of effective content moderation practices allows sexually exploitative technology and IBSA to thrive. Although GitHub implements automated detection tools such as PhotoDNA to [proactively scan for child sexual abuse material](#) (CSAM),¹⁷ GitHub fails to implement comprehensive moderation practices by permitting technology [found to have generated CSAM](#) and only moderating for CSAM itself.¹⁸ **GitHub hosts three of the most notorious technologies used for synthetic sexually explicit material (SSEM) abuse: DeepFaceLab, DeepNude, and Unstable Diffusion.**

Unstable Diffusion.

Unstable Diffusion, [an AI-generating “NSFW Community”](#)¹⁹ that began on Reddit and now operates a Discord server of over 254,000 members, has reportedly collected over [15 million “user donated”](#) pornographic and sexually explicit images to create their training database.²⁰ They openly refer users to the GitHub source code for [Stable Diffusion](#), a text-to-image generator for photorealistic image generation, and provide detailed instructions for necessary checkpoints to implement their own ‘NSFW’ additions.²¹ Further, they attribute Stable Diffusion’s source code to building the entirely ‘NSFW’ text-2-image generating website, [Unstability AI](#).²² Considering the method in which sexually explicit images were obtained via user “donations,” there is no way meaningful age or consent verification could have occurred. However, AI-generated pornography is not the only sexually exploitative source code GitHub hosts. GitHub also allows sexual deepfake source codes, collaboration, and communities to operate on the platform.

DeepFaceLab.

DeepFaceLab’s GitHub repository contains direct links to the most prolific sexual deepfake abuse website in the United States – Mr.DeepFakes. Not coincidentally, the creator of DeepFaceLab is also a founder of Mr.DeepFakes and advertises this connection openly on GitHub. DeepFaceLab is the leading deepfake software used in about [95% of all deepfake videos](#).²³ As of 2023, Mr.Deepfakes contains [over 20,000 videos of sexual deepfakes](#) (a rapidly expanding form of image-based sexual abuse), 13 million monthly visitors, and a community of over 250,000 members.²⁴ These communities further contribute to the sexual exploitation of women and the expansion of IBSA.



The DeepFaceLab repository on [GitHub directly sends users to the Mr.DeepFakes website](#) – a website dedicated to creating, requesting, and selling sexual deepfakes of celebrities and ‘other’ women.²⁵ Links to the software’s primary source material – guides and tutorials, supplementary material, and communication groups – are provided on the repository’s profile. The only way to learn how to use DeepFaceLab is by accessing the guide located on Mr.DeepFakes. While [these guides are marked “SFW.”](#) they directly refer

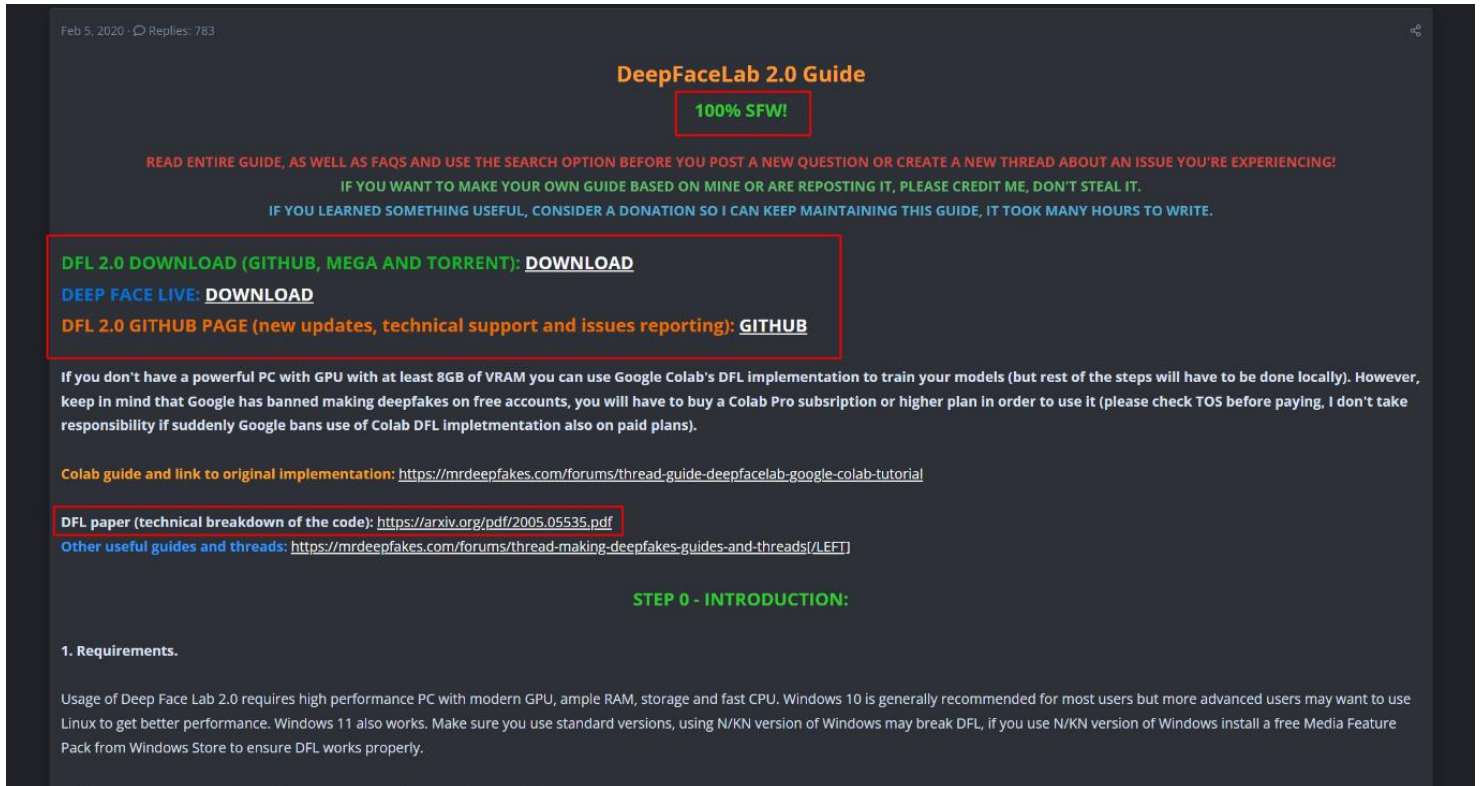
interested users to the Mr.DeepFakes website, in which misogyny, sexual objectification, and violence against women are seemingly commonplace.²⁶ As a [2022 Vice article](#) pointed out, “[i]t is impossible to support the DeepFaceLab project without actively supporting non-consensual porn.”²⁷

The image below depicts the ‘communication groups’ section on DeepFaceLab’s GitHub repository profile, containing direct links to dedicated sexual deepfake websites and social media groups.

Communication groups	
Discord	Official discord channel. English / Russian.
Telegram group	Official telegram group. English / Russian. For anonymous communication. Don't forget to hide your phone number
Русский форум	
mrdeepfakes	the biggest NSFW English community
reddit r/DeepFakesSFW/	Post your deepfakes there !
reddit r/RUdeepfakes/	Постим русские дипфейки сюда !
QQ群124500433	中文交流QQ群, 商务合作找群主
dfldata.xyz	中文交流论坛, 免费软件教程、模型、人脸数据
deepfaker.xyz	中文学习站 (非官方)

Search was conducted in April 2023

Once users click on the ‘mrdeepfakes’ link in the communication groups section on GitHub, they are directly sent to the Mr.DeepFakes Forum page in which the Official DeepFaceLab 2.0 Guide is available.










The screenshot shows a forum post titled "DeepFaceLab 2.0 Guide" with a "100% SFW!" badge. The post includes instructions to read the entire guide and use the search option. It provides links for downloading the DFL 2.0, Deep Face Live, and the DFL 2.0 GitHub page. A note mentions that users without a powerful PC can use Google Colab's DFL implementation. Links are provided for a Colab guide, a DFL paper, and other useful guides. The post is structured into sections, starting with "STEP 0 - INTRODUCTION:" and "1. Requirements." The requirements section states that Deep Face Lab 2.0 requires a high-performance PC with a modern GPU, ample RAM, storage, and a fast CPU. Windows 10 is recommended, but Linux is also supported for better performance. Windows 11 is also mentioned, with a note to use standard versions and avoid N/KN versions to prevent issues with DFL.

Search was conducted in April 2023

In a [BBC Documentary](#), Mr.Deepfakes expressed no concern or remorse for abusing women by creating sexual deepfakes of them, stating, “I think that as long as you’re not trying to pass it off as a real thing, that shouldn’t really matter because it’s basically fake. I don’t really feel that consent is required – it’s a fantasy, it’s not real.”²⁸ **By allowing repositories such as DeepFaceLab, GitHub is not only facilitating image-based sexual abuse, sexual exploitation, and the expansion of the deepfake marketplace, but it is also normalizing the use of generative-AI for these purposes.**

Research by NISOS and Sensity AI have established GitHub’s role as a primary actor in the commoditization of sexual deepfakes and the development of the sexual deepfake marketplace, which is currently the only marketplace identified for deepfake content.²⁹ More recently, academic research found that **GitHub was cited as one of the top ten referral sites to Mr.DeepFakes from January – February 2023.**³⁰ GitHub has undeniably been a significant contributor in the democratization of sexually exploitative technology and the development of the sexual deepfake marketplace.











	Domain (193)	Industry	Global Rank	Traffic Share ↓
1	 theporndude.com	Adult	#809	5.4M 51.69%
2	 urporn.com	Adult	#2,150	1.1M 10.44%
3	 simpcity.su	Adult	#560	646.1K 6.16%
4	xxx shufflesex.com	Adult	#5,244	488.9K 4.66%
5	 yandex.com	Search Engines	#113	468.1K 4.46%
6	xxx xxxporn123.com	Adult	#6,547	457.3K 4.36%
7	 forums.socialmediagirls.com	Adult	-	322.1K 3.07%
8	xxx vervesex.com	Adult	#13,414	152.3K 1.45%
9	 pornhub.com	Adult	#11	149.7K 1.43%
10	 github.com	Programming and Developer Software	#70	118.2K 1.13%

DeepNude.

Additionally, despite [GitHub’s public statement](#) against sexually exploitative source codes on the platform in 2019, which cited codes such as DeepNude as violating their policies and said similar codes or replications would be banned and removed from GitHub if they appeared,³¹ as of April 2023, similar codes remain active.³² NCOSE researchers searched “deepnude” on GitHub and received 54 results for similar repositories, some of which contained the [original source code for DeepNude](#).³³

54 repository results

Sort: Best match ▾

-
-  [stacklikemind/deepnude_official](#)
☆ 1.3k ● Python GPL-3.0 license Updated on Jul 5, 2020
-
-  [yuanxiaosc/DeepNude-an-Image-to-Image-technology](#)  Sponsor
DeepNude's algorithm and general image generation theory and practice research, including pix2pix, CycleGAN, UGATIT, ...
dcgan vae image-generation pix2pix image-to-image nerual-style cycle-gan deepface deepfakes
tensorflow2 style-gan deepnude zao sin-gan
☆ 4.6k ● Python Updated on Oct 2, 2021
-
-  [zhengyima/DeepNude_NoWatermark_withModel](#)
DeepNude source code, without watermark, with demo and model download link, one command to run offline, GAN/Pytorch/pix2p...
pytorch opencv python3 gan pix2pix image-to-image deepnude
☆ 1.4k ● Python MIT license Updated on Feb 10, 2021
-
-  [opendreamnet/dreampower](#)   Sponsor
DeepNude algorithm fork with improvements.
image-processing opencv pytorch gan photo deepnude dreampower dreamnet fake-nudes
☆ 710 ● Python GPL-3.0 license Updated on Mar 13
-
-  [Hengle/DeepNewsForAndroid](#)
DeepNudes & deep nudes Android Source Code
☆ 292 ● Java Updated on May 8, 2020
-
-  [redshoga/deepnude4video](#)
DeepNude Source Code for Videos
deep-learning gan deepnude
☆ 63 ● Python Updated on Jul 30, 2019
-
-  [Yuagilvy/DeepNudeCLI](#)
DeepNude Command Line Version With Watermark Removed
python torrent torch gan pix2pix deepnude
☆ 183 ● Python Updated on Dec 6, 2022
-

Pornography and sexually explicit imagery scrapers.

Pornography and sexually explicit imagery scrapers also thrive on GitHub. These have been used to scrape images from pornography and social media websites. Considering the growing body of evidence, survivor testimony, and lawsuits against the most visited pornography sites (Pornhub, XVideos, and XHamster) for hosting actual depictions of sex trafficking, child sexual abuse material (CSAM), rape, and various forms of image-based abuse (“revenge porn,” “upskirting/downblousing,” and “spycam shower footage”), GitHub’s allowance of these scrapers further contributes to the dissemination of criminal and/or nonconsensually captured content.

GitHub actively contributed to the creation of a dataset circling deepfake and AI communities that contained content depicting *actual instances* of sex trafficking, physical abuse, drugging, and rape of women from both Girls Do Porn and Czech Casting. [Videos from Girls Do Porn and Czech Casting](#) were

found to have been used to create a dataset for AI and deepfake communities to generate sexual deepfake and AI-generated pornography.³⁴

“Hubbers,” as GitHub refers to its users, utilized pornography scrapers on GitHub to scrape these images from mainstream pornography sites such as Pornhub.³⁵ One Czech Casting video that was identified in the database [was of a woman crying during filming](#) and asking the man to stop – and once he does, the camera zooms in on the woman and shows she is bleeding.³⁶ Disturbingly, the man in the video throws the woman a towel and directs her to clean her blood up.

When NCOSE researchers searched ‘porn’ in GitHub, over 3,000 results appeared. Based on the repositories on the first page of results, ‘porn’ frequently refers to pornography scrapers on GitHub – directly violating GitHub’s policies.

The screenshot shows a GitHub search interface with the following elements:

- Left sidebar:** A navigation menu with categories like Repositories (3K), Code (?), Commits (76K), Issues (11K), Discussions (284), Packages (24), Marketplace (0), Topics (77), Wikis (861), and Users (2K). Below this is a 'Languages' section listing Python (479), HTML (335), JavaScript (291), Java (91), PHP (82), CSS (65), Shell (65), and TypeScript (55).
- Search results header:** A red box highlights '3,314 repository results'. A 'Sort: Best match' dropdown is visible on the right.
- Repository list:**
 - ceres993434/PornHubBot:** A red box highlights the repository name. Description: '全球最大成人网站PornHub爬虫 (Scrapy, MongoDB)'. 376 stars, Python, MIT license, updated May 1, 2021.
 - imfht/fanhaodaquan:** Description: '番号大全.' 3.3k stars, Python, MIT license, updated Jun 15, 2022.
 - zhaoxianjin/91porn:** Description: '91Porn Android 客户端, 突破游客每天观看10次视频的限制, 还可以下载视频'. 967 stars, Java, updated Jul 15, 2018.
 - techGay/v9porn:** Description: '9*Porn Android 客户端, 突破游客每天观看10次视频的限制, 还可以下载视频'. 4.6k stars, Java, MIT license, updated Jun 11, 2022. Tags: dagger2, rxjava2, mvp-architecture, retrofit2, rxcache.
 - mariosemes/PornHub-downloader-python:** A red box highlights the repository name. Description: 'Download stuff from PH the easy way.' 652 stars, Python, GPL-3.0 license, updated Jul 6, 2022. Tags: python, python3, downloader, youtube-dl, easy-to-use, youtube-dl-wrapper, prettytable, pornhub, orginizer, pornhub-downloader, beautifulsoup4.

pornhub-scrapers ☆ Star

Here are 6 public repositories matching this topic...

Language: All ▾

Joel2B / XVideos-PornHub-RedTube-API ☆ Star 72 ▾

<> Code Issues Pull requests

This script scrapes the HTML from different web pages to get the information from the video (XVideos, PornHub, RedTube) and you can use it in your own video player.

php crawler video scrapper xvideos pornhub redtube pornhub-downloader pornhub-api
scrapping-php pornhub-scrapers

Updated on Dec 5, 2022 ● PHP

scoooooott / tinyPornManager ☆ Star 60 ▾

<> Code Issues Pull requests

Made for pornhub. Fork from tinyMediaManager v3


metadata scraper jsoup okhttp3 pornhub tinymediamanager pornhub-metadata pornhub-scrapers


Updated on Aug 10, 2022 ● Java


Unfortunately, pornography is the perfect content to generate photorealistic images because it demonstrates the most explicit and detailed portions of the human body, providing a unique sense of realism lacking in other types of AI-generated content. However, because AI-generated pornography requires large quantities of data, how this ‘data’ is acquired is not always consensual ... enter GitHub.


The pornography and sexually explicit imagery scrapers hosted on GitHub [‘scrape’ popular pornography tube sites](#) to collect content for deepfake and generative AI pornography datasets.³⁷ These scrapers identify and download free content from mainstream sites such as Pornhub and XVideos, essentially creating an infinite personal pornographic database. GitHub facilitates the creation of personal pornographic databases created without the consent or knowledge of the individuals in the stolen content. This forgoes meaningful age and consent verification, particularly because pornography sites fail to implement their own age and consent verification methods. **Hosting such repositories further demonstrates GitHub’s pivotal role in contributing to IBSA and sexual exploitation.**


Similar repositories host codes for “save image” bots. These are deployed on social media sites [such as Reddit](#) and are often used to save pornographic and non-consensual sexually explicit imagery.³⁸

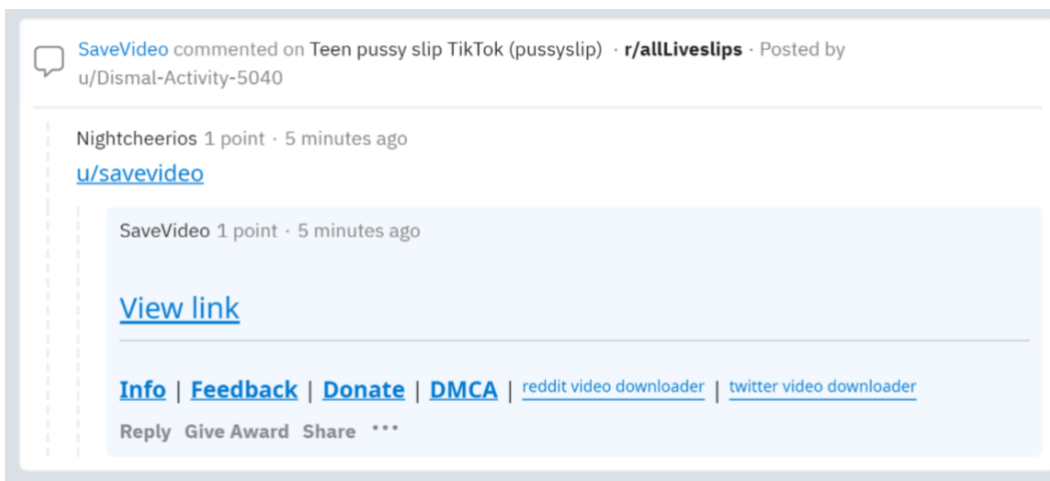
- 
[arsscriptum/PowerShell.SaveRedditVideo](#)
 ☆ 1 ● PowerShell Updated on Nov 10, 2022

- 
[amuwal/Reddit-Saved-Video-Downloader](#)
 ● Python Updated on Jul 19, 2022

- 
[yomoe/reddit_save_video](#)
 ● Python Updated on Mar 8

- 
[TrSaka/Reddit-Video-Saver](#)
 ● C++ Updated on Jul 3, 2022

- 
[mikemykhaylov/redditSaveBot](#)
 Telegram bot for saving **Reddit videos** built on Cloud Functions 🤖
 python reddit telegram-bot google-cloud-platform ytdl cloud-functions
 ● Python MIT license Updated 5 days ago



These are only a *few* of the examples of IBSA and sexual exploitation occurring as a result of GitHub’s lack of moderation practices. NCOSE urges GitHub to ban repositories dedicated to the creation of sexual deepfakes, ‘nudifying’ apps/bots/sites, AI-generated pornography, pornographic and sexually explicit image-scraping, and “save bots” on social media sites.

GitHub is a primary actor in the democratization of developing software, especially generative-AI. NCOSE welcomes technological innovation and development. However, the trauma and embodied harms from SSEM are unequivocal. Without GitHub’s proactive moderation of sexually exploitative technology and obscene content, IBSA will continue to proliferate.

Minors’ Accessibility and Exposure to Pornography and Sexually Explicit Content

NCOSE is deeply concerned about the extent of features on GitHub that may increase risk of harm to minors, such as [limited content moderation policies](#) and a lack of caregiver and teacher/administrative controls.³⁹

GitHub rates itself as 13+, and actively promotes numerous educational opportunities for students from middle school to college to learn software development and coding. Over [1.5 million students](#)⁴⁰ signed up for the [Student Developer Pack](#),⁴¹ geared toward minor-aged users and student-teacher collaboration and development on GitHub, by 2019. GitHub allows teachers and administrators to connect GitHub accounts to learning management systems such as Google Classroom, Canvas, and Moodle. The use of Google Classroom in primary education exponentially rose during the pandemic and [surpassed 150 million student users](#) by 2021.⁴² **GitHub requires a valid email to create an account, but fails to implement other basic safety features for students, such as age verification and meaningful content moderation.**

NCOSE researchers did not find evidence of teacher/administrative safety controls for underage student users. While teachers can restrict public access to joining classroom repositories, “[by default visibility to student repositories is public](#).”⁴³ GitHub places the responsibility on administrators to upgrade their accounts to access private student repository capabilities – *for a fee*. Every child should be safe online, especially in an environment promoted for his or her education and learning services. **GitHub is asking parents and teachers to put a price on their child’s safety. This feature should be free and on by default.**

Further, NCOSE researchers also did not find evidence of parental controls for underage users. Considering the open-sourced format of the platform and the amount of sexually exploitative source coding available, parental controls are urgently necessary to further protect GitHub’s youngest users.

GitHub is already a complex and daunting platform for even knowledgeable users, and is not widely known among the general public (including parents and guardians). These factors, combined with its open-sourced format, and the lack of proactive content moderation, gives minors near unmitigated access to GitHub’s slew of sexually exploitative technology source codes.

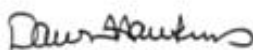
Open-sourced repositories are crucial to the exchange and access of information and technology, but they must not come at the price of abuse and exploitation of others. As sexual deepfakes and AI-generated pornography continue to grow at unprecedented rates, GitHub must hold itself accountable for providing sexually exploitative technologies. GitHub has the chance to slow IBSA from the beginning, as limited access to sexually exploitative technology would significantly reduce its presence and victim pool.

GitHub is in a unique position to implement meaningful change and lead the industry in ethical AI technology innovation. We are optimistic that your corporation will rise to the challenge.

Respectfully,



Patrick Trueman, Esq.
President



Dawn Hawkins
CEO

Cc:

Mike Hanley, Chief Security Officer & SVP of Engineering

Inbal Shani, Chief Product Officer

Shelley McKinley, Chief Legal Officer

¹ Ishan Gaba, “What is GitHub And How To Use It?” Lesson 8, SimpliLearn, last modified February 3, 2023, <https://www.simplilearn.com/tutorials/git-tutorial/what-is-github>.

² “Octoverse 2022: The State of Open Source Software,” GitHub, accessed April 24, 2023, <https://octoverse.github.com>.

³ “Let’s Build from Here,” GitHub, accessed April 24, 2023, <https://github.com>.

⁴ Damian Brady, “What Developers Need to Know about Generative AI,” *GitHub Blog*, April 7, 2023, <https://github.blog/2023-04-07-what-developers-need-to-know-about-generative-ai>.

⁵ Henry Ajder et al., *The State of Deepfakes: Landscape, Threats, and Impact* (Deeptrace, 2019), https://regmedia.co.uk/2019/10/08/deepfake_report.pdf; Henry Ajder, Giorgio Patrini, and Francesco Cavalli, *Automating Image Abuse: Deepfake bots on Telegram* (Sensity, 2020), <https://www.medianama.com/wp-content/uploads/Sensity-AutomatingImageAbuse.pdf>; Rob Volkert, *Deep Fakes: Understanding the Illicit Economy for Synthetic Media* (Alexandria, VA: NISOS, 2020), <https://cdn2.hubspot.net/hubfs/6068438/Resources/NISOS%20-%20Deep%20Fakes%20White%20Paper.pdf>; Emanuel Maiberg, “It Takes 2 Clicks to Get From ‘Deep Tom Cruise’ to Vile Deepfake Porn,” *Vice*, May 17, 2022, <https://www.vice.com/en/article/qjb7b7/ethical-deepfakes-deep-tom-cruise-ai-generated-porn>; Rachel Winter and Anastasia Salter, “DeepFakes: Uncovering Hardcore Open Source on GitHub,” *Porn Studies* 7, no. 4 (2020): 382-397, [doi:10.1080/23268743.2019.1642794](https://doi.org/10.1080/23268743.2019.1642794).

⁶ Ajder et al., *ibid*; Ajder, Patrini, and Cavalli, *ibid*; Giorgio Patrini, *The State Of Deepfakes 2020: Updates on Statistics and Trends* (Sensity, 2021), https://books.google.com/books/about/The_State_of_Deepfakes_2020.html?id=--SBzgeEACAAJ; Volkert, *ibid*; Hany Farid, “Creating, Using, Misusing, and Detecting Deep Fakes,” *Journal of Online Trust & Safety* 1, no. 4 (2022), [doi:10.54501/jots.v1i4.56](https://doi.org/10.54501/jots.v1i4.56).

⁷ Winter and Salter, *ibid*.

⁸ iperov, “DeepFaceLab,” GitHub, accessed April 26, 2023, <https://github.com/iperov/DeepFaceLab>.

⁹ Ivan Perov et al., “DeepFaceLab: Integrated, Flexible and Extensible Face-Swapping Framework,” *arXiv* (2021), [doi:10.48550/arXiv.2005.05535](https://doi.org/10.48550/arXiv.2005.05535). iperov, *ibid*.

¹⁰ “Importing a Roster from Google Classroom,” GitHub Docs, accessed April 26, 2023, <https://docs.github.com/en/education/manage-coursework-with-github-classroom/teach-with-github-classroom/connect-a-learning-management-system-course-to-a-classroom#importing-a-roster-from-google-classroom>.

¹¹ Arelia Jones, “Set Up Your Digital Classroom with GitHub Classroom,” *GitHub Blog*, March 18, 2020, <https://github.blog/2020-03-18-set-up-your-digital-classroom-with-github-classroom>.

¹² Anna Jobin, Marcello Ienca, and Effy Vayena, “The Global Landscape of AI Ethics Guidelines,” *Nature Machine Intelligence* 1, (2019): 389-399, doi.org/10.1038/s42256-019-0088-2.

¹³ Max Tegmark, *Life 3.0: Being Human in the Age of Artificial Intelligence* (Alfred A. Knopf, 2017), https://books.google.com/books/about/Life_3_0.html?id=Am9MnQAACAAJ.

¹⁴ NCOSE, “Image Based Sexual Abuse,” National Center on Sexual Exploitation, accessed April 21, 2023, <https://endsexualexploitation.org/issues/image-based-sexual-abuse>.

¹⁵ NCOSE, “5 Types of Image-Based Sexual Abuse You Should Know About,” *National Center on Sexual Exploitation*, April 11, 2023, <https://endsexualexploitation.org/articles/5-types-of-image-based-sexual-abuse-you-should-know-about>.

¹⁶ “GitHub Sexually Obscene Content,” Acceptable Use Policies, GitHub Docs, accessed April 26, 2023, <https://docs.github.com/en/site-policy/acceptable-use-policies/github-sexually-obscene-content>.

¹⁷ Kevin Xu, “2022 Transparency Report,” *GitHub Blog*, February 15, 2023, <https://github.blog/2023-02-15-2022-transparency-report>.

¹⁸ Maiberg, *ibid*.

¹⁹ Mohit Pandey, “Meet the Hot Cousin of Stable Diffusion, ‘Unstable Diffusion,’” *AIM*, November 18, 2022, <https://analyticsindiamag.com/meet-the-hot-cousin-of-stable-diffusion-unstable-diffusion>.

²⁰ “r/unstable_diffusion,” Reddit, accessed April 24, 2023, https://www.reddit.com/r/unstable_diffusion/comments/1loxtix/official_march_update_for_unstable_diffusion.

²¹ “Stable Diffusion Online,” Stable Diffusion, accessed April 26, 2023, <https://stablediffusionweb.com>.

²² “Welcome to Unstable Diffusion's Image Generation AI,” Unstability.ai, accessed April 24, 2023, <https://www.unstability.ai/>.

²³ Perov et al., *ibid*; iperov, *ibid*.

-
- ²⁴ Sophie Cockerham, “Deepfake Porn Wrecks Lives – but, as One Woman Discovered, it Takes just 8 Seconds to Make an Image,” *Metro*, October 21, 2022, <https://metro.co.uk/2022/10/21/deepfake-porn-takes-seconds-to-make-but-can-wreck-lives-17605029>.
- ²⁵ Maiberg, *ibid*.
- ²⁶ TMBDF, “DeepFaceLab 2.0 Guide,” *MrDeepFakesForums*, February 5, 2020, <https://mrdeepfakes.com/forums/threads/guide-deepfacelab-2-0-guide.3886>.
- ²⁷ Maiberg, *ibid*.
- ²⁸ Cockerham, *ibid*.
- ²⁹ Ajder et al., *ibid*; Volkert, *ibid*.
- ³⁰ Victoria Rousay, “Sexual Deepfakes and Image-Based Sexual Abuse: Victim-Survivor Experiences and Embodied Harms” (Master’s thesis, Harvard University Division of Continuing Education, April 20, 2023), <https://dash.harvard.edu/handle/1/37374909>; SimilarWeb, “Top 10 Incoming Sites to Mr.DeepFakes.com, January 2023-February 2023,” *SimilarWeb + Mr.DeepFakes*, January 2023, https://pro.similarweb.com/#/digitalsuite/websiteanalysis/referrals/incoming-traffic/*/999/2m?webSource=Total&key=mrdeepfakes.com.
- ³¹ Joseph Cox, “GitHub Removed Open Source Versions of DeepNude,” *Vice*, July 9, 2019, <https://www.vice.com/en/article/8xzjpk/github-removed-open-source-versions-of-deepnude-app-deepfakes>; James Vincent, “Copies of AI Deepfake App DeepNude are Easily Accessible Online — and Always Will Be,” *The Verge*, July 3, 2019, <https://www.theverge.com/2019/7/3/20680708/deepnude-ai-deepfake-app-copies-easily-accessible-available-online>; Samantha Cole, “AI-Generated Fake Porn Makers Have Been Kicked Off Their Favorite Host,” *Vice*, January 31, 2018, https://www.vice.com/en/article/vby5jx/deepfakes-ai-porn-removed-from-gfycat?utm_source=mbtwitter.
- ³² Opendreamnet, “The Leading Platform for Photo Nudification Join 7,000+ Satisfied Users! Our User-Friendly Platform Offers Seamless Photo Nudification across Multiple Devices, with Secure Storage for up to 12 Months!”; Opendreamnet, “DreamTime and DreamPower: DeepNude Algorithm Fork with Improvements”; DeepNudecom, “DeepNudecom”; iperov, “DeepFaceLab”; Wiggers and Silberling, “Meet Unstable Diffusion, the Group Trying to Monetize AI Porn Generators,” November 17, 2022; Vincent, “Copies of Ai Deepfake App DeepNude Are Easily Accessible Online - and Always Will Be.”
- ³³ orgTestCodacy11KRepos110MB, “repo-2245-DeepNude-an-Image-to-Image-technology,” GitHub, accessed April 26, 2023, <https://github.com/orgTestCodacy11KRepos110MB/repo-2245-DeepNude-an-Image-to-Image-technology>.
- ³⁴ Samantha Cole, Emanuel Maiberg, and Anna Koslerova, “‘Frankenstein’s Monster’: Images of Sexual Abuse Are Fueling Algorithmic Porn,” *Vice*, November 10, 2020, <https://www.vice.com/en/article/akdgnp/sexual-abuse-fueling-ai-porn-deepfake-czech-casting-girls-do-porn>.
- ³⁵ Dawn Beatty, “Diversity, Inclusion, and Belonging at GitHub in 2022,” *GitHub Blog*, October 27, 2022, <https://github.blog/2022-10-27-diversity-inclusion-and-belonging-at-github-in-2022>.
- ³⁶ Cole, Maiberg, and Koslerova, *ibid*.
- ³⁷ *Ibid*.
- ³⁸ u/Kryptonh, “SaveVideo,” Reddit, accessed April 26, 2023, <https://www.reddit.com/user/savevideo>.
- ³⁹ Daphne Leprince-Ringuet, “GitHub: We Won’t Take Down Any of Your Content Unless We Really Have To,” *ZDNET*, February 21, 2020, <https://www.zdnet.com/article/github-we-wont-take-down-any-of-your-content-unless-we-really-have-to>.
- ⁴⁰ Frederic Lardinois, “GitHub Adds 21 New Partners to its Free Student Developer Pack,” *Tech Crunch*, August 20, 2019, <https://techcrunch.com/2019/08/20/github-adds-21-new-partners-to-its-free-student-developer-pack>.
- ⁴¹ “Where Future Developers Meet,” GitHub Education, accessed April 26, 2023, <https://education.github.com>.
- ⁴² Melanie Lazare, “A Peek at What’s Next for Google Classroom,” *Google Blog*, February 17, 2021, <https://blog.google/outreach-initiatives/education/classroom-roadmap>.
- ⁴³ Jones, *ibid*.