

States are starting to crack down on cyberflashing, but it might not be enough

October 6 2022, by Cody Mello-Klein



Credit: Alyssa Stone/Northeastern University

In September, California took steps to crack down on "cyberflashing," following Texas and Virginia to become the third state to pass a law aimed at curbing this form of digital harassment.

California's Forbid Lewd Activity and Sexual Harassment, or FLASH, Act gives people who have electronically received unsolicited, explicit material the ability to pursue up to \$30,000 in civil damages. Ari Waldman, a Northeastern professor of law and computer science, says the FLASH Act is another move in the right direction, but he argues more needs to be done at the state and federal level to get [online platforms](#) actively involved.

"Legal institutions are not used to getting involved in understanding algorithms and understanding how defaults work and understanding design," says Waldman, who also serves as faculty director of the Center for Law, Information and Creativity. "What they're used to doing is telling platforms that they have to give people notice and that's not enough here, so [laws like this] are a convenient way to get involved in something."

From [dating apps](#) to wireless file sharing, cyberflashing has become a serious concern for both users and platform holders. A survey done by Bumble, which describes itself as a "women-first" dating app, found that one of out of every two women said they had received an unsolicited nude while using the app. Bumble threw its support behind the bills passed in all three states and is working on getting similar legislation passed in New York, Washington, D.C., and Pennsylvania.

When it comes to getting involved in the often-tricky world of regulating online activity, civil laws like the ones passed in California and Virginia are "a convenient approach that doesn't involve the complex nitty gritty of actually doing something about it on a systemic level," Waldman says. Civil laws like the FLASH Act are designed to deter negative behavior by giving people who have suffered harm a legal mechanism to get compensation. Texas opted to take a different approach by criminalizing cyberflashing altogether.

The debate over whether civil or [criminal law](#) is better equipped to deter behavior like this is not new to cyberflashing, Waldman says.

"Some people feel that making it a criminal law has more of an effect because with criminal laws, you can go to jail, you have higher fines," Waldman says. "Other people feel that criminal law is not really the best tool at regulating stuff related to sex and sexual expression."

Waldman says in taking a criminal law approach in any situation can also have "complicating factors."

"What happens when a cyberflasher happens to be under 18, and then the person who receives it without their consent also is now in possession of child pornography?" Waldman says. "Passing one law—criminal or civil—is not the end of these stories."

Criminal law can play a role, Waldman says, but it has to be deployed deliberately and purposefully.

However, Waldman argues more of a difference can be made by working to encourage, and even require, platforms and [technology companies](#) to make changes on their end. In some cases, it means changing the design philosophy and "defaults" associated with the technology, including Air Drop. The Bluetooth and Wi-Fi enabled feature on iPhones allows file-sharing between iPhone users from up to 30 feet away, even if they're not on each other's contact lists. It has also been used to send unsolicited obscene photos to total strangers.

"When Air Drop is defaulted to 'anyone can send you anything,' that is a design choice that is creating a particular vision of how this company feels people should connect," Waldman says. "That vision is open connection. We need to encourage platforms to be more protective of privacy and safety than open connection."

Platforms also tend to approach cases of harassment as one-off incidents instead of viewing them as part of a larger pattern of harassment.

Waldman says if a user wants to report an incident of cyberflashing or get a harassing comment taken down, they can flag it but platforms rarely "look beyond the four walls of the one picture you flagged."

"If you are more able to provide context—and platforms don't really like that—and show how all of these tools are being used against you as part of a larger pattern, then there might be more options for redress," Waldman says.

Unfortunately, there are some concrete barriers to regulating online platforms. One is that lawmakers typically don't understand what platforms do or how they work, Waldman says. But more concerning is a major legal and constitutional hurdle: Section 230.

"The main obstacle for states telling platforms what they can and cannot allow is that, for better or for worse, the First Amendment doctrine and Section 230 of the Communications Decency Act pretty much immunizes these platforms from regulation and from lawsuits and a lot of other things that could provide outside limits on what they do," Waldman says.

Section 230 is a federal law that was passed in 1996 as part of the CDA and provides near blanket immunity for online platforms when it comes to third-party content.

Recent developments in online law could also make it even more difficult for states or the federal government to get companies to remove or regulate content on their platforms. Texas' House Bill 20 prohibits social media companies from removing posts or users based on a political "viewpoint."

The Texas law is part of a broader conservative movement that claims there is an anti-conservative bias among major tech companies and social media platforms. Although these claims have been disputed, social media companies do have policies—effective or ineffective—that prohibit graphic content, hate speech and bullying.

"Any conversation about the law's role here has to be told with a context that there is one major political party that's trying to use law to manipulate platforms to do what it wants to, to advance its causes," Waldman says. "You can't talk about these laws without talking about the disingenuous activities that one side is engaged in because they color how we approach law generally."

The days of changing how platforms regulate cyberflashing are still a ways off, Waldman says. But the FLASH Act and the recent rush of new legislation that's making its way through state legislatures is at least a place to start.

"Obviously, there are limitations for how this is going to work, but it's a convenient approach that doesn't involve the complex nitty gritty of actually doing something about it on a systemic level," Waldman says.

Provided by Northeastern University

Citation: States are starting to crack down on cyberflashing, but it might not be enough (2022, October 6) retrieved 19 April 2024 from <https://techxplore.com/news/2022-10-states-cyberflashing.html>

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.