ORGANIZATION FOR
SOCIAL MEDIA SAFETY

(855) 446-3767
contact@ofsms.org
6520 Platt Avenue, Suite 914
West Hills, CA 91307

March 8, 2023

Chair and Distinguished Members of the Public Safety Committee:

As a consumer protection organization focused on social media and its related dangers, the Organization for Social Media Safety is very concerned about the threat posed by deepfake technology. "Deepfakes" are forged videos created via artificial intelligence where a person's likeness, including their face and voice, is realistically swapped with someone else's. One of the many dangers posed by this new technology is the ability to create malicious pornographic deepfakes, pornographic videos that misappropriate an individual's likeness. That is why the Organization for Social Media Safety supports HF 1370, which will protect individuals from severe emotional harm and reputational damage by criminalizing the creation and distribution of malicious pornographic deepfakes.

We agree with the current, prevailing philosophy in many states of creating criminal liability only with great hesitancy. Importantly, this caution is not a total bar to new criminal provisions but rather calls for a careful analysis of each proposal. In supporting HF 1370, we have asked ourselves the following questions:

- Does the proposal respond to a new danger?
- Is that danger severe?
- Are there no viable alternatives to the proposal?
- Will the proposal accomplish its objective in deterring the danger and protecting Minnesotans?
- Is the proposal constitutional?

Criminal legislation drafted in response to new, technology-driven dangers and approved in Minnesota in recent years has satisfied these criteria. For example, Minnesota has passed legislation prohibiting revenge porn, the nonconsensual distribution of consensually obtained, sexually graphic images or videos, a new danger created by the popularization of smartphones that can capture quality video and then mass distribute such video through social media. Like Minnesota's revenge porn legislation, HF 1370 is also the only effective, targeted response to a similar, emerging, and severe threat.

Malicious Pornographic Deepfakes Are A New Threat

While the ability to swap a person's likeness into a video has for several years been available only to movie and television studios, it has now suddenly and rapidly become accessible to the general masses. Deepfake technology first appeared in late 2017 when an anonymous user on the online forum Reddit posted an algorithm that leveraged existing artificial intelligence algorithms to create hyper-realistic fake videos. Other users then shared the code on GitHub, a major code sharing service, where it became free software and publicly available. Applications, like FakeApp, soon appeared to simplify the programming process. And today, deepfake technology continues to improve and spread.

Malicious Pornographic Deepfakes Are A Severe Danger

The danger of deepfake technology lies in its ability to generate fake videos so realistic that one cannot distinguish the actual from the forged. Since its introduction, the technology has been used extensively to create fake pornographic videos of women without their consent. And, as the technology improves and becomes more accessible, this malicious deepfake pornography will include more of the most vulnerable of Minnesotans, such as survivors of abusive relationships and minors. It has already targeted women with the intent to cyberbully, take revenge, and extort spurring emotional trauma, lasting reputational damage, and severe mental anguish.

The extent of the potential harm of malicious pornographic deepfakes cannot be underestimated. Since deepfake technology enables a form of revenge porn, though one not requiring the need to capture actual footage, previous research on the dangers of revenge porn serves as a foundation for understanding the potential effects of deepfakes. In a 2015 study from the Cyber Civil Rights Initiative, 51 percent of victims of revenge porn indicated that they had considered committing suicide, and 39 percent said the crime affected their career and professional lives. And, since deepfakes do not have the limiting factor of requiring actual footage, their potential impact is far more widespread.

The statements of victims of malicious pornographic deepfakes further clarify their potential harms:

- "I was sent to the hospital with heart palpitations and anxiety, the doctor gave me medicine. But I was vomiting, my blood pressure shot up, my body had reacted so violently to the stress," said Rana Ayyub, an investigative journalist.

- "I just cannot explain the level of violation and also shame that I felt," said Noelle Martin, an 18-year-old student.

HF 1370 Is the Only Policy Option

The unique dynamics of deepfake technology also render other traditional policy options ineffective. We appreciate that HF 1370 adds civil liability for the dissemination of malicious pornographic deepfakes. However, while using deepfake technology to produce pornographic videos with misappropriated identities may incur civil liability in certain cases, tort law will often be insufficient to deter this danger and inadequate as a remedy to the victims. The reasons include:

- To recover in a civil suit against an individual, the plaintiff ultimately needs to be able to identify the defendant, but creators of deepfake pornography can and almost always do distribute their product anonymously. Identifying the creator through the civil discovery process when the offending material has likely passed through thousands of computers, and thousands of different IP addresses, would be onerous, costly, and time consuming to the point of futility in an overwhelming majority of cases.

- Proving and recovering damages from deepfake pornography in the context of a civil lawsuit will be especially difficult. Severe emotional distress and reputational damage, particularly for younger victims, are harder to prove and calculate than physical or economic injuries. In addition, the prospect of even obtaining full compensation from individual deepfake creators is often slim. These challenges will create a high degree of uncertainty with regard to monetary recovery and, in conjunction with the high cost of both initiating civil lawsuits generally and pursuing deepfake lawsuits specifically, will prevent most victims from obtaining legal representation and/or initiating civil cases.

These obstacles are why even wealthy celebrities have not pursued civil litigation with existing, applicable causes of action like defamation or false light claims. And so, relying solely on civil law will leave victims of malicious deepfake pornographic videos without protection or remedy.

HF 1370 Is an Effective Solution

HF 1370 will prove an effective policy against the production of malicious pornographic deepfakes. Criminal liability is simply an effective deterrent. And, in many cases, particularly the most severe, law enforcement officials will be able to identify and prosecute malicious pornographic deepfake creators. That is because law enforcement officials, unlike civil litigants, have more powerful investigative tools at their disposal, including the ability to issue timely warrants and conduct interviews, and they can leverage the resources, skill and experience of existing cybercrime units.

Malicious pornographic deepfakes are already spreading across the internet and through social media causing untold harm. Sadly, soon they will invade our high schools and middle schools and will become commonly used for cyberbullying, revenge, and harassment. Waiting to act until the worst of the damage from malicious pornographic deepfakes unfolds should not be an option. HF 1370 will protect vulnerable women and girls throughout Minnesota, and the Organization for Social Media Safety stands in strong support.