Cyber Exploitation and Perpetration of Digital Abuse

by Christina M. Gagnier*

Editor's Note: This article discusses the phenomenon of cyber abuse, which has become, unfortunately, an increasingly common method used by modern day stalkers to subjugate and terrify their victims, who often are current or past intimate partners. Digital abuse takes on a variety of forms, including online harassment, cyberstalking, identity theft, unlawful surveillance, and other types of invasion. In this article, author Christina Gagnier discusses a range of legal remedies that have been put adopted by various jurisdictions—most notably, the state of California, which has taken on a leadership role in devising responses aimed to combat this devasting manifestation of intimate partner violence.

There is a common misconception that if something happens in the "online world," it stays online. With the proliferation of digital abuse, it is far too simple to view these forms of harassment in a silo: even if the harassment occurs online, it is still happening IRL (in real life), having permanent and public implications for victims. A single explicit photograph or video capture can go viral within minutes, resulting in serious long-term emotional and financial distress to the victim. Cyber exploitation is simply an extension of tactics that stalkers have been using in their victimization of individuals offline. Technology has enabled stalkers to engage in such abuse in a more pervasive and rapid fashion.

Various approaches have been taken to combat cyber exploitation and digital abuse. California's model for employing a multipronged approach to combatting cyber exploitation and digital abuse, tying together criminal penalties, civil remedies, statewide office activism and law enforcement training, may serve as a model that can be adopted in other states.

---

*Christina M. Gagnier is on the clinical faculty, Intellectual Property, Arts & Technology Clinic, University of California at Irvine School of Law. She leads the Internet, Intellectual Property and Technology Practice at Gagnier Margossian LLP, and sits on the Board of Directors of Without My Consent. Contact: withoutmyconsent.org.

As California's approach is not without its faults, this piece explores approaches to strengthening existing and future laws in order to enhance protections for victims and access to justice. Federal efforts to criminalize nonconsensual pornography, the Intimate Privacy Protection Act, are examined as an effort to standardize the approach to crimes, such as nonconsensual pornography, on the national stage.[1]

I. DEFINING DIGITAL ABUSE

Many descriptors are applied to what may constitute digital abuse and online harassment. There is not a "one size fits all" term or definition that can be applied to every instance of abuse that a victim may encounter online. Digital abuse, in its unfortunate growth as a tactic of perpetrating domestic violence, cannot be simply defined, which often means it is not easily regulated. The means of abuse employed can include intimidation, anonymous harassment, defamation of character, voyeurism, cyber stalking, impersonation through electronic means (identity theft), extortion, unlawful surveillance, sexual harassment, and other invasions of privacy, including nonconsensual pornography. Often, these means of abuse are employed concurrently to render the victim into a state where he or she feels completely helpless as the use of technology allows a forum to make this abuse public on the Internet.

In California, the Office of the Attorney General utilizes the term "cyber exploitation" and defines it as "the non-consensual distribution or publication of intimate photos or videos online."[2] This was adopted through a process facilitated by a subcommittee of the Attorney General's Cyber Exploitation Task Force and has been applied by other agencies in California.

While the law is attempting to keep pace, with state legislatures actively trying to legislate practices such as nonconsensual pornography, many states have not enacted either civil or criminal laws that address all of the behaviors that may constitute digital abuse. It is often confusing for victims to understand their rights and what course to justice they may have because the abuse perpetrated upon their person may not squarely fit within the elements of one criminal or civil statute.

II. AS CALIFORNIA GOES, SO SHOULD THE NATION?

California stands to serve as an example for employing a multipronged approach to combatting cyber stalking, nonconsensual pornography, and other forms of digital abuse, tying together criminal redress, civil remedies, statewide office activism and law enforcement training. This approach is not without its faults: victims still find themselves unaware of how to approach law enforcement and the judicial system in order to curb abusive behaviors. Further, some of the laws crafted to combat digital abuse contain deficiencies

[1] Intimate Privacy Protection Act of 2016, H.R. 5986, 114th Cong (2016).
[2] State of California, Office of the Attorney General, #*CyberExploitation.* Available at *https://www.oag.ca.gov/cyberexploitation.* Last accessed February 10, 2017.

that place a burden on victims to prove harm has been caused to their person, and some of these laws do not cover certain forms of digital abuse.

A. CRIMINAL PENALTIES AND CIVIL REDRESS

Protections under California law incorporate the codification of the various tactics used by perpetrators to abuse victims. For example, California Penal Code § 528.5 addresses impersonation, also known as identity theft, and California Penal Code § 647(j)(1-3) addresses voyeurism.

In 2013, the California State Legislature passed Senate Bill 152, introduced by Senator Anthony Cannella, which was subsequently enacted and codified as California Penal Code § 647 (j)(4), the unlawful distribution of an image, commonly known as nonconsensual pornography.[3] This amended provision of the California Penal Code makes it a misdemeanor to intentionally distribute "the image of the intimate body part or parts of another identifiable person, or an image of the person depicted engaged in an act of sexual intercourse, sodomy, oral copulation, sexual penetration, or an image of masturbation by the person depicted or in which the person depicted participates, under circumstances in which the persons agree or understand that the image shall remain private."[4] The statute contains an intent requirement, that is, that the person "distributing the image knows or should know that distribution of the image will cause serious emotional distress, and the person depicted suffers that distress."[5]

Like many of California's criminal statutes, there is a civil corollary. California Civil Code § 1708.85, introduced as Assembly Bill 2643 by Senator Bob Wiechowski in 2014, created a private right of action for victims of nonconsensual pornography.[6] The private right of action is against any person who intentionally distributes nonconsensual content without the other person's consent, and is based on the reasonable expectation of privacy that the victim had that "the material would remain private."[7]

Other privacy-related criminal and civil offenses such as extortion, defamation, and other invasions of privacy are addressed through other California Civil Code provisions or the common law.

B. STATEWIDE OFFICE ACTIVISM

As a response to the proliferation of cyber exploitation as a tool of abuse and the emergence of business models predicated on the distribution of nonconsensual images, former California State Attorney General and now United States Senator Kamala Harris led the charge on issues relating to cyber exploitation by launching an initiative to combat these forms of abuse in all forms.

---

[3] 2013 Cal. Legis. Serv. ch. 466, § 1, at 4035 (amending Cal. Penal Code § 647).
[4] *Id.*
[5] *Id.*
[6] Cal. Civ. Code § 1708.85 (2014).
[7] *Id.*

In 2015, the Office of the Attorney General launched the Cyber Exploitation Task Force, bringing academics, lawyers, technologists, policy makers, and victim advocates into the same room to discuss the main points and gaps in the system that make it hard for each stakeholder to effectively combat cyber exploitation, online harassment, and digital abuse.[8]

Cross-sectoral collaboration led to the adoption of new digital abuse reporting portals on sites like Twitter to specifically report instances of abuse versus being directed into the general "Help" queue of the platform.[9] Educational resources were created for victims and other stakeholders to facilitate the takedown process of nonconsensual content.[10]

In October 2016, then-Attorney General Harris announced the creation of the California Cyber Crime Center (C4), an initiative now located within the California Department of Justice that brings together digital forensic capabilities and cybersecurity expertise to law enforcement agencies across the state of California.[11] This enables agencies across California to work collaboratively in investigations related to cyber crime and digital abuse.

C. EQUIPPING LAW ENFORCEMENT

Another instrumental part of an effective approach to combatting digital abuse is equipping law enforcement to work with victims to facilitate the reporting, investigation, and prosecution of crimes related to digital abuse.

Following the adoption of Senate Bill 676 and Assembly Bill 1310 in 2015, the California Commission on Peace Officer Standards Training (POST) created materials and trainings providing guidance to law enforcement agencies and officers as to the new laws that were passed in California regarding cyber exploitation, the criminal penalties for various forms of online harassment and how to work with victims who report these crimes. Evidence collection can prove to be critical in these cases, which can include ensuring that victims take screenshots of the relevant criminal conduct, that law enforcement obtains identifying information related to potential suspects, the types of devices being used (a desktop computer, laptop computer or mobile device), and other digital information that can be used to build a case and stop the abuse. To that end, officers in California are being trained on identifying these crimes and knowing how to capture the right information to enable investigation and prosecution.

---

[8] State of California, Office of the Attorney General, *#CyberExploitation*. Available at *https://www.oag.ca.gov/cyberexploitation.* Last accessed February 10, 2017.

[9] Twitter.com, Help Center, *Someone on Twitter is Engaging in Abusive or Harassing Behavior.* Available at *https://support.twitter.com/forms/abusiveuser.* Last accessed February 10, 2017.

[10] State of California, Office of the Attorney General, *#CyberExploitation.* Available at *https://www.oag.ca.gov/cyberexploitation.* Last accessed February 10, 2017.

[11] State of California Department of Justice, Attorney General Announces California Cyber Crime Initiative in Fresno, *Forensic Magazine*, October 11, 2016. Available at *https://www.forensicmag.com/news/2016/10/attorney-general-announces-california-cyber-crime-center-initiative-fresno.*

D. WITH PROGRESS STILL COMES NEED FOR REFORM

While many of the laws passed in the last decade aim to protect victims of cyber exploitation and other forms of digital abuse, the effect of some of these laws results in shifting the burden on victims to prove they, indeed, have been victims of abuse. Even though the common law in many states when it comes to privacy has traditionally protected individuals who share private information with another individual where it is reasonable to believe that the information will remain private, many of the laws drafted to protect victims of digital abuse do not necessarily apply this principle, resulting in a construct that places too large a burden on victims to prove they have suffered harm.

Even California's perceptibly robust and forward approach to tackling issues like nonconsensual pornography is not without its faults. California Penal Code § 647 (j)(4) does not protect victims who may have themselves taken a photo, a "selfie," and shared it with a third party in what they believed to be a trusted confidential exchange. In some instances, victims are forcibly made to take and share these images with partners, or risk further emotional or physical abuse. The law may be effectively surrendering the rights of victims of domestic violence who were forced to create such content and share it.

Some state nonconsensual pornography laws, such as the California law, contain an intent requirement, namely, that the perpetrator must have possessed the intent to cause the victim severe emotional distress.[12] This can be hard for victims to prove. Critics of this approach believe that any distribution, regardless of intent, should be penalized. The sharing of nonconsensual pornography on its face should be enough to carry criminal penalties.

Another issue with California Penal Code § 647(j)(4) is that the law is not applicable to individuals who may have had their devices or cloud storage hacked into, which, again, is problematic for victims who perhaps had no intent of sharing the intimate content in the first place.

Perhaps most problematic is the failure of this law to apply to redistributions of nonconsensual pornography. Much of the emotional and financial toll associated with nonconsensual pornography is the lengths to which a victim has to go to get the image or images removed from the Internet. Redistribution exacerbates this problem, and conceivably should be penalized in a fashion similar to the initial publication. While existing privacy laws that may provide a framework focusing on the initial publication of content, the intent of those laws is not to subject someone or some entity to civil penalties based on every single publication of defamatory content.

In the instance of nonconsensual pornography, it is hard to believe this content is being shared for any expressive means. One of the obstacles that emerges in the legislative drafting of these laws are concerns regarding potential First Amendment challenges. If the law is not going to survive a First

[12] Cal. Pen. Code § 647(j)(4) (2013).

Amendment challenge, the law will not be of much use for victims as it will not survive judicial scrutiny. Yet, if the laws crafted lack teeth to adequately punish perpetrators and do not support the public policy goal of deterring this behavior in other would-be perpetrators, they may be rendered ineffective.

III. FEDERAL APPROACH TO CYBER EXPLOITATION AND DIGITAL ABUSE

While legislating at the state level has been a victory for victims of digital abuse, with laws in 34 states and counting tackling the distribution of nonconsensual pornography, the lack of a cohesive, national framework to address these types of tactics leaves victims having to navigate a patchwork of laws. Cases become exceedingly difficult when the perpetrator and the victim live in different states. California Assembly Bill 1310, introduced by Assemblymember Mike Gatto, expanded jurisdiction in California so that victims could walk into any law enforcement agency in California to report cyber exploitation.[13] While this aids victims in California, there is still an issue with interstate crime. Although California supplemented the 2013 adoption of its nonconsensual pornography law, other states have failed to follow course.

At the federal level, there are a handful of existing laws that may be employed to address cyber exploitation and digital abuse. Federal law currently criminalizes tactics including identity theft,[14] voyeurism,[15] and cyberstalking.[16] Nonconsensual pornography may also become a federal crime. H.R. 5896, the Intimate Privacy Protection Act, authored and introduced by Representative Jackie Speier (D-CA), would amend Title 18 of the United States Code to make the distribution of nonconsensual pornography a crime.[17] The law would provide, in part, that "it is unlawful to knowingly distribute a private, visual depiction of a person's intimate parts or of a person engaging in sexually explicit conduct, with reckless disregard for the person's lack of consent to the distribution."[18] The law explicitly targets the behavior of individuals and contains a "safe harbor" for third party intermediaries, platforms like Google, Facebook and other social networking services, rendering them not liable for content posted by third parties, known as user generated content. Like many of the laws that have been enacted at the state level, a careful balance must be arrived so as to avoid running afoul of Section 230 of the 1996 Communications Decency Act, which, generally, provides immunity for platforms from content posted by their users.

---

[13] A.B. 1310 (CA. 2015).
[14] *See* 18 U.S.C. § 1028 (2012).
[15] *See* 18 U.S.C. § 1801 (2012).
[16] *See* 18 U.S.C. § 2261A(2) (2012).
[17] Intimate Privacy Protection Act of 2016, H.R. 5986, 114th Cong (2016).
[18] *Id.*

IV. OUTLOOK

The momentum in legislating digital abuse is a positive trend, with a diversity of states, including Arizona,[19] Colorado,[20] Delaware,[21] Georgia,[22] Hawaii,[23] New York,[24] Utah,[25] and Wisconsin having criminalized nonconsensual pornography.[26] Legislative action has been largely non-partisan and a number of other states, like Missouri, are currently considering laws to combat nonconsensual pornography among other forms of digital abuse as part of their civil and criminal codes.

The creation and application of model laws that could apply to cyber exploitation and other forms of digital abuse could be instrumental in rectifying some of the current deficiencies in some state laws. For example, the requirement that a victim prove that he or she has suffered "emotional distress" or "severe emotional distress," or that some other form of "special damages," is problematic. These types of elements in a criminal statute, along with others, place the onus on the victim to prove that he or she has suffered harm rather than taking the commission of the crime, such as nonconsensual pornography, as harmful on its face by virtue of having been committed in the first instance. Some states have amended these provisions from previous versions of their statutes, but there remains work to be done. Model laws, taking into consideration these issues for both civil and criminal statutes, could lead to standardization of how states tackle the panoply of tactics that perpetrators use to abuse victims online.

Even with states legislating in the hope of preventing crimes related to digital abuse and providing victims with the means of civil redress, digital abuse continues to grow as a tool used by perpetrators of harassment. While the availability of avenues to justice is pivotal, victims can face monumental challenges, which include lack of initial access to navigate the legal system. Reforms to the actual access points to the justice system for digital abuse crimes may be necessary. In California, a key step to beginning many of these cases is to obtain a temporary restraining order. This process is overseen by the family law division of the Superior Court of California, which may not be the appropriate forum for the management of cases related to cyber crimes. Creating consistency in the processes, types of venues, and forms for victims to file their claims would go a long way in making the process of image removal, often through court order, more efficient and efficacious. Additionally,

[19] Ariz. Rev. Stat. Ann. § 13-1425 (Supp. 2014).
[20] Colo. Rev. Stat. Ann. § 18-7-107 (Supp. 2014).
[21] Del. Code Ann. tit. 11, § 1335 (West, Westlaw through 79 Laws 2014, ch. 443).
[22] Ga. Code. Ann. § 16-11-90 (West Supp. 2014).
[23] Haw. Rev. Stat. § 711-1110.9 (LexisNexis Supp. 2014).
[24] N.Y. Penal Law § 250.45 (West, Westlaw through L.2014, chapters 1 to 550).
[25] Utah Code Ann. § 76-5b-203 (West, Westlaw through 2014 Gen. Sess.).
[26] Wis. Stat. § 942.09 (2013–2014).

the non-profit sector finds itself having to provide resources for victims for digital abuse as the state has yet to provide these resources.[27]

Further, there are difficulties inherent in trying to remove the remnants of harassing content, including nonconsensual pornography, defamatory content, and other forms of abuse. While the perpetrators may find themselves subject to criminal and civil penalties, victims are still faced with the burden, including the emotional toll, financial burden, and time drain, of attempting to remove content. The way that search engines cache images and the inability to stop redistribution leaves individuals finding themselves continually "re-victimized" every time another instance of this content emerges.

California has taken an approach within its Office of the Attorney General and with law enforcement training that has yet to be emulated in other states. This type of activism, leadership, and equipment of law enforcement is critical to prosecution of these crimes at all levels and, hopefully, deterrence of the commission of digital abuse overall.

Nationwide, momentum continues to build through both legislative and advocacy channels. Non-profit organizations and leaders in the effort to bring awareness to cyber exploitation and digital abuse, such as the Cyber Civil Rights Initiative and Without My Consent, actively work with victims and victim support organizations to enable their pursuit of justice. The steady drumbeat created by these organizations and other advocates will lead to more states taking a multifaceted approach to abuse and, most importantly, enable more victims to seek the justice they deserve.

[27] Without My Consent, *Something Can Be Done! Resource Guide*. Available at *http://withoutmyconsent.org/resources#boxes-box-scbd_welcome_block.* Last accessed February 10, 2017.