#CYBEREXPLOITATION

Cyber Exploitation—Law Enforcement FAQs

1. What is cyber exploitation?

Cyber Exploitation is defined as the non-consensual distribution and publication of intimate photos or videos. These materials are usually stolen by ex-lovers, ex-spouses, associates, or even complete strangers through hacking, theft of a cell phone or computer, during a computer repair, a false personal ad, or other means. These photos or videos are then posted on websites or sold for profit to humiliate, degrade, harass, physically endanger, or extort the victim. In addition to intimate images, perpetrators often post other identifying information to accompany the image or video, including the victim's name, links to social media accounts, email addresses, physical addresses of their place of employment and residence, phone numbers, and even social security information.

2. What is the harm?

Cyber exploitation is a serious crime that often results in significant harm to a victim's personal and professional life and physical safety. Many victims of cyber exploitation face serious barriers to employment opportunities and academic success. In addition, victims suffer economic harm as a result of addressing the abuse and often suffer additional harm such as threats of physical violence, stalking, and criminal threats.[1]

While cyber exploitation affects both men and women, the Cyber Civil Rights Initiative's study[2] found that 90 percent of victims are women. The same study found that 93 percent of victims (of all sexes) suffered significant emotional distress as a result of their victimization, 51 percent had suicidal thoughts, and 49 percent stated they had been stalked or harassed online by users who saw their material. Further, decades of peer-reviewed research establishes that women often face more serious consequences as a result of sexual victimization. Cyber exploitation – like domestic violence, rape, and sexual harassment – disproportionately harms women and girls, leads to ongoing criminal threats and harassment, and undermines basic civil rights and public safety.

3. What California laws make cyber exploitation unlawful?

Two state laws expressly prohibit cyber exploitation—California Penal Code sections 647(j)(4)(A) and 647(j)(4)(B). In California, it is illegal for any person to intentionally distribute an image of an 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, when the persons agree or understand that the image shall remain private. The person distributing the image is

[1] Danielle Keats Citron, Hate Crimes in Cyberspace (Harvard University Press 2014).
[2] Cyber Civil Rights Initiative, End Revenge Porn Survey (2014). Survey results were obtained from an online survey, hosted on endrevengeporn.com from August 2012-December 2013 whereby participants self-selected into the study. Results depicted are reflective of a female-heavy sample, correlated with the gender demographics of visitors to the website.

criminally responsible when he/she knows or should know that the distribution of the image will cause serious emotional distress, and the person depicted suffers that distress. In addition, other California Penal Code sections, such as identity theft or extortion, may be triggered in a cyber exploitation case when a perpetrator steals images and uses them for any unlawful purpose or demands money to remove the unlawfully posted images.

Table of Computer Crimes in Califorina: *http://oag.dev.doj.ca.gov/sites/all/files/agweb/pdfs/ce/cyber-exploitation-penal-codes.pdf?*

4. List of Additional Penal Code Sections Used to Investigate and Prosecute Cyber Exploitation Crimes:

Penal Code section 422 Criminal Threats (Misdemeanor/Felony)[3]

- Willfully threatening to commit a crime which will result in death or great bodily injury to another person, with the specific intent that the statement, made verbally, in writing, or by means of an electronic communication device, is to be taken as a threat, even if there is no intent of actually carrying it out
- Penality: Up to one year in county jail or four years in state prison

Penal Code section 502 Unauthorized Access to Computers, Computer Systems, and Computer Data (Most are Felonies)[4]

- Gaining unauthorized access to computers, computer systems and computer data
- Penality: Fine not exceeding $10,000, imprisonment, or by both fine and imprisonment depending on the crime. In addition to any other civil remedy available, the person who suffers damage or loss to their property may bring a civil action against the violator for compensatory damages and injunctive relief, or other equitable relief

Penal Code section 520 Extortion (Felony)[5]

- Any person who extorts any money or other property from another, not amounting to robbery or carjacking, by means of force, or any threat (including exposing a secret)
- Penality: Imprisonment for two, three, or four years

Penal Code section 524 Attempted Extortion (Felony)[6]

- Any person who attempts to extort
- Penality: Imprisonment in the county jail not longer than one year or in the state prison or by fine not exceeding $10,000, or by both fine and imprisonment

Penal Code sections 182, 520, Conspiracy to Commit Extortion (Felony)[7]

- Two or more persons conspiring to extort money or property from another under circumstances not amounting to robbery
- Penality: Imprisonment for five, seven, or nine years

[3] Cal. Penal Code § 422.
[4] Cal. Penal Code § 502.
[5] Cal. Penal Code § 520.
[6] Cal. Penal Code § 524.
[7] Cal. Penal Code § 182; Cal. Penal Code § 520.

Penal Code section 530.5 Identity Theft (Felony)[8]

- Any person who willfully obtains someone's personal identifying information and uses that information for any unlawful purpose (not just theft)
- Penalty: Fine, by imprisonment in a county jail, or by both

Penal Code section 632 Recording Confidential Communications (Felony)[9]

- Any person who, intentionally and without the consent of all parties to a confidential communication, by means of any electronic amplifying or recording device, eavesdrops upon or records the confidential communication
- Penalty: Fine not exceeding $2,500, or imprisonment in the county jail or state prison, or by both fine and imprisonment

Penal Code section 646.9 Stalking (Felony/Misdemeanor)[10]

- Any person who willfully, maliciously, and repeatedly follows or willfully and maliciously harasses another person and who makes a credible threat with the intent to place that person in reasonable fear for his or her safety, or the safety of his or her immediate family
- Penalty: Imprisonment in the county jail or by a fine of not more than $1,000, or by both fine and imprisonment

Penal Code section 647(j) Invasion of Privacy under Disorderly Conduct (Misdemeanor)[11]

- Any person who looks into, views, or records areas an area where a person has a legal expectation of privacy, with the intent to invade the privacy of a person
- Penalty: Imprisonment in a county jail, a fine, or both

Penal Code section 653m Annoying or Threatening Communication (Misdemeanor)[12]

- Any person who, with the intent to annoy, harass, or threaten telephones or makes contact by means of an electronic communication devices with another is guilty of a misdemeanor
- Penalty: Six months in county jail, a fine up to one thousand dollars, or both

Penal Code section 653.2 Prohibited Distribution or Publication (Misdemeanor)[13]

- Any person who, by means of electronic or online publication of personal identifying information, intends to cause fear or unwanted contact with another
- Penalty: Up to one year in county jail, a fine of no more than one thousand dollars, or both

Penal Code section 1524(a) Search Warrant (*effective January 1, 2016)*[14]

---

[8] Cal. Penal Code § 530.5.
[9] Cal. Penal Code § 632.
[10] Cal. Penal Code § 646.9.
[11] Cal. Penal Code § 647(j).
[12] Cal. Penal Code § 653m.
[13] Cal. Penal Code § 653.2.
[14] Cal. Penal Code § 1524(a).

- Allows law enforcement to obtain a search warrant for cyber exploitation involving an adult or minor

Penal Code sections 502.01 and 647.8 Forfeiture (*effective January 1, 2016)*[15]

- Establishes forfeiture criminal proceedings for cyber exploitation images and the equipment used in committing the offense

List of Criminal and Related Cyber Exploitation Crimes under Federal Law:

18 U.S.C. section 875(c) Threat Through Interstate Communications[16]

- A perpetrator must: (1) knowingly make a communication containing a true threat to injure in interstate commerce or foreign commerce, and (2) intends the communication to be a true threat to injure another or knows that the recipient of the threat would understand it to be a threat
- Penalty: A fine, imprisonment for not more than two years, or both

18 U.S.C. section 1030 Unauthorized Access to a Computer[17]

- Unauthorized access to a protected computer to obtain information
- Penalty: A fine, imprisonment, or both

18 U.S.C. section 2261(A)(1)(A)/2261(A)(2)(A) Stalking Under Interstate Domestic Violence[18]

- A course of conduct that places a person in reasonable fear of death or serious bodily injury to that person, an immediate family member, or a spouse or intimate partner of that person
- Penalty: A fine, imprisonment, or both

5.What actions has the Attorney General taken to combat cyber exploitation and hold perpetrators accountable?

Attorney General Harris is committed to seeking justice for every victim of cyber exploitation in California and accountability for the perpetrators of these crimes.

- In 2011, the Attorney General created the eCrime Unit to identify and prosecute cyber crimes and other crimes involving the use of technology, including cyber exploitation. Drawing on the expertise of California law enforcement, the Department of Justice continues to play a critical role in the investigations and prosecutions of cyber exploitation website operators and other perpetrators. DOJ is leading the nation in prosecuting these crimes, having garnered the first successful prosecution of a cyber exploitation operator in the U.S. View Press Release: https://oag.ca.gov/news/press-releases/attorney-general-kamala-d-harris-announces-creation-ecrime-unit-targeting
- In 2015, Kevin Bollaert was sentenced to eight years imprisonment followed by ten years of supervised release for his operation of a cyber exploitation website that allowed the anonymous, public posting of intimate photos accompanied by personal identifying

[15] Cal. Penal Code §§ 502.01, 647.8.
[16] 18 U.S.C.A. § 875(c)
[17] 18 U.S.C.A § 1030.
[18] 18 U.S.C.A. § 2261.

information of individuals without their. *People of the State of Cal. v. Kevin C. Bollaert.* [19] View Press Release: *https://oag.ca.gov/news/press-releases/attorney-general-kamala-d-harris-issues-statement-cyber-exploitation-verdict*

- In June 2015, Casey E. Meyering pled no contest to extortion and conspiracy for his operation of a cyber exploitation website that posted stolen personal images of individuals without their consent and exploited those photos for financial gain. Meyering was sentenced to three years imprisonment. *People of the State of Cal. v. Casey E. Meyering.* View Press Release: *https://oag.ca.gov/news/press-releases/attorney-general-kamala-d-harris-announces-three-year-sentence-cyber*
- Charles Evens, who orchestrated a cyber exploitation hacking scheme where he stole private images from victims' accounts and sold them to another website, pled guilty to computer intrusion in June 2015. Evens was sentenced to three years imprisonment, concurrent with a Federal prison term for the same conduct a year earlier. View Press Release: *https://oag.ca.gov/news/press-releases/attorney-general-kamala-d-harris-announces-guilty-plea-hacker-involved-cyber*

6. What role do LEAs play in combatting Cyber Exploitation?

As first responders to this crime, law enforcement agencies have a legal responsibility to respond to reports of cyber exploitation and can play a significant role in mitigating the effects of this crime. Cyber exploitation victims should be encouraged to file a police report with law enforcement. Law enforcement are uniquely positioned to appropriately respond to incidents of crime and have the technical expertise to investigate and prosecute those who engage in these criminal acts.

7. What are effective components of a local law enforcement cyber exploitation policy?

To ensure the most effective law enforcement responses to cyber exploitation, the Department of Justice recommends law enforcement agencies develop special policies and protocols tailored to cyber exploitation. At a minimum, the Department of Justice recommends that any voluntary cyber exploitation law enforcement policy include:

- Report Writing and Evidence Collection: Guidelines covering report writing specific to cyber exploitation cases and the importance of collecting and preserving evidence (e.g. retrieving the complete URLs of all internet websites, digital copies of social media posts, IP addresses, archived content, and geo-location data). Officers should be encouraged to capture as much internet data as possible, documenting all methods of preservation. Printouts and screenshots, while helpful, do not include the valuable metadata that will assist in the prosecution of defendants.
- Encourage Victims fo File Report: Ensuring that all types of incidents are reported, including threats. Victims should not be turned away because a particular incident does not look serious enough. For instance, law enforcement should not disregard the criminal significance of the posting of a single nude photo without consent. Due to the nature of the internet, a single image can spread quickly throughout the online community; prevention and a rapid response is critical to curbing the damage caused by these crimes. A police report about an incident, including but

[19] On April 3, 2015, Superior Court Judge David Gill sentenced Bollaert to eighteen years in prison. On September 23, 2015, Judge Gill modified his ruling, ordering Bollaert to serve an eighteen year "split sentence" under California's realignment policy, as mandated by Assembly Bill 109 (2011).

not limited to a threat, is recognized by leading technology companies as sufficient validation for them to process a victim's take-down request; effectively eliminating an image from a particular company's website or social media platform.

- Educate Victims of Rights: Clear and easy language for officers to convey to victims that advises them of their right to privacy, anonymity, and confidentiality. In addition, victims should also be advised about the steps required to obtain a restraining order against any known perpetrator.
- Victim Referrals: Where applicable, including information about available community and mental health resources.

8. What additional resources does the Attorney General have to support our efforts?

The California Department of Justice can provide technical assistance to:

- improve investigatory and prosecutorial practices;
- better coordinate victims services with community-based organizations and technology companies;
- increase the efficiency and effectiveness of reports of cyber exploitation to technology companies hosting the unlawful images;
- and better understand privacy and confidentiality requirements in responding to reports of criminal behavior.

In addition, the Attorney General has released a law enforcement information bulletin to summarize new and existing laws governing cyber exploitation, available here:*http://oag.ca.gov/sites/all/files/agweb/pdfs/ce/cyber-exploitation-law-enforcement-bulletin.pdf?* Finally, you are encouraged to share your cyber exploitation strategies with California law enforcement by sharing best practices and participating in the Attorney General's Task Force on cyber exploitation to continue to improve our state's response to this important issue.

9. Where can I find the privacy statements and user rules from various technology companies, like Twitter, Facebook, and Google on Cyber Exploitation?

The Attorney General's Take Force has consolidated the hyperlinks of major technology companies' privacy and user guidelines. This is not a comprehensive list, but does provide substantial information regarding a victim's privacy rights. Visit Removing Images on the Attorney General's Cyber Exploitation website: ***http://oag.ca.gov/cyberexploitation***

Technology companies in the Attorney General's Task Force also authored a technology industry best practices guide that is useful to understanding how the private sector addresses these crimes. **Visit Technology Industry Best Practices on the Attorney General's Cyber Exploitation website: *http://oag.ca.gov/cyberexploitation***

10. What external resources exist for victims?

The following websites provide additional information:

CA Attorney General's Cyber Exploitation Website
Online resource hub with a range of tools for victims, the technology industry, and law enforcement to combat cyber exploitation.
http://oag.ca.gov/cyberexploitation

California Coalition Against Sexual Assault (CalCASA)

California says NO MORE is a California-specific campaign to raise public awareness and engage bystanders in the movement to end domestic violence and sexual assault. California Says NO MORE is supported by the California Coalition Against Sexual Assault (CALCASA) and the national NO MORE campaign. Victims can quickly locate domestic violence crisis centers using a zip code
https://www.casaysnomore.com/

Cyber Civil Rights Initiative
A non-profit organization that combats online harassment and abuse. Provides support, referrals and technical advice through a 24-hour Crisis Helpline: 844-879-CCRI (2274).
http://www.cybercivilrights.org/

End Revenge Porn
Website that provides advocacy and support for female and male victims of cyber exploitation.
http://www.endrevengeporn.org/

K&L Gates Cyber Civil Rights Legal Project
Founded by K&L Gates, the Cyber Civil Rights Legal Project offers legal assistance to victims of cyber exploitation on a pro bono basis. Spanish-speaking staff is available.
https://www.cyberrightsproject.com/

National Network to End Domestic Violence / Safety New Project
Overview of options for victims of cyber exploitation and legal recourses.
http://nnedv.org/downloads/NNEDV_ImagesAbuse_2014.pdf

The Victims of Crime Resource Center at McGeorge School of Law
Assists victims of cyber exploitation by providing free and confidential information about their legal rights, remedies, and community-based assistance. Contact: 1-800-VICTIMS (842-8467) or chat live at *http://www.1800victims.org/*

Without My Consent
Website that offers resources for both cyber exploitation victims and the attorneys that represent them.
http://www.withoutmyconsent.org/

Women Against Revenge Porn
Website that offers practical tips for removal of images and a directory of attorneys.
http://www.womenagainstrevengeporn.com/

Visit Victim Resources on the Attorney General's Cyber Exploitation website:
http://oag.ca.gov/cyberexploitation