#CYBEREXPLOITATION

Cyber Exploitation—Victims 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 California: *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

[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.

- Penality: Imprisonment for five, seven, or nine years.

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

[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.

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

- 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

[14] Cal. Penal Code § 1524(a).
[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.

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 information of individuals without their consent and charged for the take down of these photos. *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 vcitims 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. Does the Attorney General's office provide legal representation to victims of cyber exploitation?

No, our office cannot provide legal representation to individuals. If you are interested in speaking with an attorney about an instance of cyber exploitation, you can access a complete list of California Bar-certified lawyers organized by county or by calling: 1-866-44-CA-LAW or online at: *http://www.calbar.ca.gov/Public/LawyerReferralServicesLRS.aspx*. The Cyber Civil Rights Legal Project offers legal assistance on a pro bono basis for victims of cyber exploitation. Spanish-speaking staff is available. *www.cyberrightsproject.com*. You can also file a consumer complaint against the business with the California Attorney General's Public Inquiry Unit at: *https://oag.ca.gov/contact/consumer-complaint-against-business-or-company*. For more information on external resources, please read FAQ #20.

7. Do victims have a private right of action against their perpetrator(s)?

Yes, as of July 2, 2015 victims of cyber exploitation have a private right of action against their perpetrators under California law. Assembly Bill 2643 (Wieckowski) codified a private right of action against any person who intentionally distributed a photograph or recorded image of another without consent, if: (1) the person knew that the other person had a reasonable expectation that the material would remain private, (2) the distributed material exposes an intimate body part or shows an act of intercourse, oral copulation, sodomy, or other act of sexual penetration, and (3) the other person

[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).

suffers general or special damages as described in civil code section 48(a).[21] In addition, a California court may order equitable relief, including a temporary restraining order, or a preliminary injunction or a permanent injunction ordering the defendant to cease the distribution of the material.[22] *Id.* A court may also grant reasonable attorney's fees and costs to the prevailing plaintiff. *Id.*. Finally, a victim may be able to bring a tort claim for the public disclosure of private fact and/or the intentional infliction of emotional distress depending on the circumstances of the case.

8. Can I file a civil complaint or participate in a criminal investigation anonymously?

Yes, under state law, a plaintiff in a civil proceeding may proceed using a pseudonym, either John Doe, Jane Doe, or Doe, as a substitute for the true name of the plaintiff and may exclude or redact from the pleadings and documents filed in the action other identifying characteristics such as an address, age, marital status, and race or ethnic background.[23] You also have the right to engage with law enforcement and participate in a criminal investigation and prosecution anonymously, using a pseudonym (i.e. Jane or John Doe).

. What should I do if I have experienced cyber exploitation?

1. **Download and save copies** of the photos or videos through screenshots, printing, flash drive, hard drive along with the site information. It is important to save all records such as text messages, emails, and any other type of correspondence prior to attempting to take down the content.

2. **Set up Search Engine Alerts** to notify you when any photos or videos appear with your name on a new site online.

Use the images to set up a reverse image search to find related images from around the web. When you search using an image, your search results may include: similar images, websites that host the image, and other sizes of the images you searched for.

3. **Get Assistance**

- File a police report at your local police department so you will have documentation of your complaint.

- If your case involves hacking, fraud, or conduct that occurs online, report the conduct to your local branch of the FBI and the Internet Crime Complaint Center (*www.ic3.gov)*

[21] Cal. Civil Code § 1708.85(c)(1-6) enumerates six exceptions to liability; *but cf.* Cal. Civil Code. § 48(a) is amended by Actions And Proceedings—Libel And Slander—Classification, 2015 Cal. Legis. Serv. Ch. 343 (A.B. 998).

[22] A court may grant injunctive relief maintaining the confidentiality of a plaintiff using a pseudonym. A plaintiff in a civil proceeding pursuant to § 1708.85, may proceed using a pseudonym, either John Doe, Jane Doe, or Doe, for the true name of the plaintiff and may exclude or redact from all pleadings and documents filed in the action other identifying characteristics of the plaintiff.

[23] Cal. Civil Code § 1708.85(f)(1)-(4).

- File a consumer complaint against the business with the California Attorney General's office at: *https://oag.ca.gov/contact/consumer-complaint-against-business-or-company*

- If you have reason to fear that the person who has posted your images online poses a threat to your physical safety, then you can seek to obtain a criminal or civil harassment protection order. If the harasser is a current or former intimate partner or family member then you can file a domestic violence restraining order. Contact your local law enforcement agency or district attorneys office for further guidance.

Research whether you want to register the copyright with the U.S. Copyright Office. The Digital Millennium Copyright Act (DMCA) is a federal law that addresses copyright infringement. If you took the photo or video yourself, you still own the copyright.[24] In order to register your image, you must submit the image(s) directly to the U.S. Copyright Office. Your copyright does not change, even when you give the image to someone else.

4. **Start the Removal Process** by submitting a Digital Millennium Copyright (DMCA) take-down request to websites that have posted your images without consent. A DMCA notice informs the website owner that you own the copyright to your photo and that you want the photo removed. Even if you physically hand over, text, or email a picture of yourself to another person, or took the picture yourself, you still own the copyright if you took the image yourself. Many of the social media platforms have included notice and takedown provisions as necessary to comply with the DMCA. In filing a notice, follow the DMCA takedown process of the website exactly and if you have registered with the U.S. Copyright Office, mention it in your takedown request to each website operator or social media company.[25]

Visit Removing Images on the Attorney General's Cyber Exploitation website: *http://oag.ca.gov/cyberexploitation/*

10. How can I file a complaint with law enforcement about cyber exploitation?

Contact your local police or sheriff department to file a complaint. Several departments allow you to report a crime online. Make sure to save a copy of the police report to keep for your records.

You can also file a consumer complaint against the business with the California Attorney General's Public Inquiry Unit at: *https://oag.ca.gov/contact/consumer-complaint-against-business-or-company*

11. What happens when I report cyber exploitation to law enforcement?

The crime report is given to a (investigator/district attorney) who investigates the matter. You will receive an email confirmation once you submit a complaint online or a written copy if in-person. Upon review, if further investigation of your case is needed, you may be contacted. However, do not hesitate to contact the investigator or district attorney should you have any questions, concerns, or new evidence to report.

[24] Digital Millennium Copyright Act, PL 105–304, October 28, 1998, 112 Stat 2860.
[25] United States Copyright Office, available at: www.copyright.gov.

12. Do I have to choose between a criminal investigation and a civil adjudication against my perpetrator?

No. You have options, and you don't have to decide right away. You can choose to participate in both a civil adjudication and a criminal investigation. Criminal remedies involve the filing of a complaint with the police and then working with either a state or federal prosecutor to see whether the government might pursue criminal charges. Civil remedies involve the hiring of an attorney to pursue money damages and an injunction order to stop the unlawful conduct.

Remember, you also may have the right to engage and participate with law enforcement using a pseudonym (i.e. Jane or John Doe).

13. What is the time limit to report an incident of cyber exploitation?

All individuals, including a survivor or witness, are encouraged to report an instance of cyber exploitation regardless of when or where it occurred. You are encouraged to report an incident as soon as possible to maximize the ability to respond promptly and effectively (e.g. to preserve evidence and ensure public safety). Please remember that successful prosecution of these crimes in a court of law is dictated by each law's statute of limitations, which vary by statute. Please also read FAQ #4 for a list of state and Federal statutes regarding cyber exploitation.

14. What if I do not want to turn to law enforcement to address my cyber exploitation incident?

California law enforcement agencies have been at the forefront of protecting victims against cyber crimes. Law enforcement agencies are not only trained in evidence collection, but have technical expertise that can play a significant role in mitigating cyber exploitation. If you choose not to report to a law enforcement agency, you can still register your copyright with the U.S. Copyright Office to request removal of the unwanted content. Please also read FAQ #20 for more information on external resources.

15. Are there geographic limitations to cyber exploitation under California law?

Pending Legislation AB 1310 will allow cyber exploitation cases to be prosecuted in the same jurisdiction in which the offense occurred, where the victim resided when the offense was committed, or where the intimate image was used for an illegal purpose.

If you reside in the State of California, you can still proceed with a criminal case against an actor who lives outside of California. If you decide to bring forth a civil matter then you should consult with an attorney to determine whether a case against an actor outside of California is possible.

16. Who will have access to my report of cyber exploitation, and does confidentiality change depending on whether I report to a technology company/website owner or law enforcement agency?

The law enforcement agency will have access to your report of cyber exploitation. This includes the assigned officer or detective investigating the case, his or her supervisor, the district attorney, and

potentially an outside law enforcement agency participating in a related investigation. However, your confidentiality is important and you have the right to engage with law enforcement using a pseudonym.

For reports to companies and website owners, privacy options may differ depending on the company or website owner. You will want to read the privacy statements in order to determine whether your information will remain confidential. The Attorney General's Take Force on cyber exploitation has provided links to privacy statements of major companies. This is not a comprehensive list, but does provide substantial information regarding your privacy rights.

Visit Removing Images on the Attorney General's Cyber Explotiation Website:
http://oag.ca.gov/cyberexploitation

17. What are the implications of reporting an instance of cyber exploitation if I am an undocumented immigrant?

California law enforcement agencies are encouraged, though not required, to provide privacy protections to ensure that an individual's immigration status is protected, whether they are a bystander reporting a crime or a victim/survivor. With respect to the threat of deportation, please be advised that state law limits the discretion of state and local law enforcement agencies to detain an individual pursuant to a federal immigration detainer request unless certain conditions are met.[26] Further, federal law provides additional protections for victims of an enumerated crime that are currently assisting or has previously assisted law enforcement in the investigation or prosecution of a crime. [27] Here, the Victims of Trafficking and Violence Prevention Act of 2000 aims to strengthen the ability of law enforcement agencies to investigate and prosecute crimes while also protecting victims who have suffered substantial mental or physical abuse due to the crime and are willing to assist law enforcement authorities in the investigation or prosecution of the crime.[28]

18. What do I do if I know someone who is a survivor?

The first step in helping survivors heal is to believe them. Know the resources in your community and help your friend connect with those resources. Once a survivor confides in you, connect her or him with resources, like a counseling center, advocacy office, the police, or a public safety group. If they just want to talk to someone, listen. Please also read FAQ #20 for more information on external resources.

---

[26] Transparency and Responsibility Using State Tools Act (TRUST Act), Gov. Code §§ 7282, 7282.5; Stats. 2013, ch. 570; *see also* Attorney General Kamala D. Harris, California Department of Justice Information Bulletin No. 14-01, Responsibilities of Local Law Enforcement Agencies under Secure Communities and the TRUST Act (June 25, 2014), available at: http://oag.ca.gov/sites/all/files/agweb/pdfs/law_enforcement/14-01_le_info_bulletin.pdf.
[27] Victims Of Trafficking And Violence Protection Act Of 2000, PL 106–386, October 28, 2000, 114 Stat 1464.
[28] *See* United States Citizenship and Immigration Services, Victims of Criminal Activity: U Nonimmigrant Status, available at: http://www.uscis.gov/humanitarian/victims-human-trafficking-other-crimes/victims-criminal-activity-u-nonimmigrant-status/victims-criminal-activity-u-nonimmigrant-status.

19. What if I discover images of someone I know who may be a victim?

Contact the person and let them know, and then provide them with the information on this website. They should file a police report with their local police station or online with the California Attorney General's Public Inquiry Unit at: *https://oag.ca.gov/contact/consumer-complaint-against-business-or-company.*

20. 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 locator.
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