Frequently Asked Questions *(side 2)*

How do victims file a crime report of cyber exploitation with law enforcement?

A report of cyber exploitation may be filed online or in person by the victim. All records of the exploitation saved through screenshots, printing, flash drive or hard drive should be documented. The crime description section of the complaint form/crime report should indicate a cyber exploitation crime is being reported.

If the images were uploaded in another state, can a victim file a report in California?

Cyber Exploitation cases may be prosecuted in the same jurisdiction where the offense occurred, where the victim resided when the offense was committed, or where the intimate image was used for an illegal purpose.

If I have a restraining order, does it also cover cyber exploitation?

If a victim believes that the subject of a restraining order is also the person posting the images, they may be able to go to the court or report it to law enforcement as a violation of that restraining order.

If someone wishes to report inappropriate images of a minor child, whom should they call?

Reports about cyber exploitation as it relates to children may be made to law enforcement or through the Cybertipline:
http://www.missingkids.com/cybertipline

Investigating Cyber Exploitation

Remember the Basics

- Document all elements of the crime
- Do your best to include who, what, when, where, how, and why
- Be respectful at all times
- When needed, seek help from a more experienced investigator

It is important for law enforcement officers to recognize that those who have been victimized are entitled to dignity whenever reporting crimes of cyber exploitation. Keep in mind that cyber exploitation is a sensitive subject for those affected by it, and respect a victim's request for confidentiality. Refrain from inquiries that are inappropriate or that pass moral judgment when documenting the crime.

Age does not determine the status of a victim of cyber exploitation. If a person believes he or she is a victim of cyber exploitation, that person (or his or her parent or guardian) is encouraged to report it to local law enforcement regardless of age or gender.

Evidence Collection and Preservation

Document the victim's report with enough detail to allow follow-up investigation. List the complete URLs of all internet websites involved and consider redacting sensitive information or images. Note the victim's emotional state, and any thoughts the victim may have about the circumstances surrounding the exploitation (e.g. were they the victim of an online intrusion).

Resources

Below are resources where victims may obtain additional information.

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

Cyber Civil Rights Initiative
A non-profit organization that combats online harassment and abuse. Provides support, referrals and technical advice through 24-hour Crisis Helpline. 844-878-CCRI(2274): *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
Offers legal assistance to cyber exploitation victims on a *pro bono* basis. Spanish speaking staff is available. *www.cyberrightsproject.com*

National Center for Missing & Exploited Children (NCMEC)
http://www.missingkids.com/home
Reports about cyber exploitation involving children may be made through the Cybertipline. *http://www.missingkids.com/cybertipline*

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

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. 1-800-VICTIMS (842-8467): Chat live at *www.1800victims.org*

Without My Consent
Offers resources for cyber exploitation victims and attorneys who represent them. *http://withoutmyconsent.org*

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

Cyber Exploitation

Quick Reference
for
Law Enforcement

Commission on Peace Officer Standards and Training

860 Stillwater Road
Suite 100
West Sacramento, CA 95605-1630

For a printable copy of this guide and additional information, visit
post.ca.gov/cyber-exploitation

ENFORCEMENT STATUTES

California Penal Code

The following abbreviated descriptions of these Penal Code sections are meant to be used as a guide to assist officers in finding the appropriate enforcement section(s). Please read the complete statute for details.

Note: ***(F)*** indicates felony; ***(M)*** indicates misdemeanor.

PC 182/520 – Conspiracy to commit extortion
Two or more persons conspiring to extort money or property from another under circumstances not amounting to robbery (***F***)

PC 422 – Criminal threats ***(F)***

PC 502 – Unauthorized access to computers systems, computers, and computer data
(Most are felonies)

PC 520 – Extortion
Every person who extorts any money or other property from another, under circumstances not amounting to robbery or carjacking, by means of force, or any threat (including exposing a secret) ***(F)*** [*2, 3, or 4 years*]

PC 524 – Attempted extortion
(This is a stand-alone "attempt" section. Do not use the 664 as an attempt section) ***(F)***

PC 530.5(a) – Identity theft
The use of someone's personal identifying information for any unlawful purpose (not just theft) ***(F)***

PC 632 – Recording confidential communications ***(F)***

PC 646.9 Stalking ***(F) or (M)***

PC 647(j) – Invasion of privacy
Looking into, viewing, or recording an area where a person has a legal expectation of privacy ***(M)***

PC 647(j)(4)(A) and (j)(4)(B) – Cyber exploitation
Any person who intentionally distributes the image of the intimate body part of another identifiable person ***(M)***

PC 653m – Annoying or threatening communication
Phone calls or contact by electronic device(s) with the intent to annoy, harass, or threaten ***(M)***

PC 653.2 – Prohibited distribution or publication
Electronic or online publication of personal identifying information with intent to cause fear or unwanted contact ***(M)***

PC 1524(a) – Search warrant
Cyber exploitation involving an adult or minor

United States Code, Title 18, Sections

875(c) – Extortion (*Federal*)
When defendant (1) knowingly makes a communication containing a true threat to injure in interstate commerce or foreign commerce, and (2) defendant intends the communication to be a true threat to injure another or knew that the recipient of the threat would understand it to be a threat

1030(a)(2)(C) - Unauthorized computer access
Unauthorized access to a protected computer to obtain information

2261A – Stalking (*Federal*)
Whoever-
(1) travels in interstate or foreign commerce or is present within the special maritime and territorial jurisdiction of the United States, or enters or leaves Indian country, with the intent to kill, injure, harass, intimidate, or place under surveillance with intent to kill, injure, harass, or intimidate another person, and in the course of, or as a result of, such travel or presence engages in conduct that-
(A) places that person in reasonable fear of the death of, or serious bodily injury to-
(i) that person;
(ii) an immediate family member (as defined in section 115) of that person; or
(iii) a spouse or intimate partner of that person; or
(B) causes, attempts to cause, or would be reasonably expected to cause substantial emotional distress to a person described in clause (i), (ii), or (iii) of subparagraph (A); or
(2) with the intent to kill, injure, harass, intimidate, or place under surveillance with intent to kill, injure, harass, or intimidate another person, uses the mail, any interactive computer service or electronic communication service or electronic communication system of interstate commerce, or any other facility of interstate or foreign commerce to engage in a course of conduct that-
(A) places that person in reasonable fear of the death of or serious bodily injury to a person described in clause (i), (ii), or (iii) of paragraph (1)(A); or
(B) causes, attempts to cause, or would be reasonably expected to cause substantial emotional distress to a person described in clause (i), (ii), or (iii) of paragraph (1)(A),

shall be punished as provided in section 2261(b) of this title.

http://uscode.house.gov/view.xhtml?req=(title:18 section:2261A edition:prelim) OR (granuleid:USC-prelim-title18-section2261A)&f=treesort&edition=prelim&num=0&jumpTo=true

Frequently Asked Questions

General questions/responses are provided below to assist you in addressing questions you may have as a law enforcement officer.

What is Cyber Exploitation?

Cyber Exploitation is defined as the non-consensual distribution of intimate photos and/or videos. The private material may have been stolen by ex-lovers, by ex-spouses, or by complete strangers through hacking, theft of a cell phone, during a computer repair, a false personal ad, or "photoshopping." These photos or videos may be posted to humiliate and degrade the victim, or used to extort them.

What California laws govern Cyber Exploitation?

It is illegal in California for any person who intentionally distributes 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, 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. The related statutes are included in the brochure.