


<p>California Department of Justice Division of Law Enforcement</p> <p>Larry J. Wallace, Director</p>		<h1>INFORMATION BULLETIN</h1>	
<p><i>Subject:</i> Assistance to Local Law Enforcement Agencies in Combatting Cyber Exploitation under New and Existing California Laws</p>	<p>No. DLE-2015-03</p>	<p><i>Contact for information:</i></p>	
	<p><i>Date:</i> October 13, 2015</p>	<p>Venus D. Johnson 916-324-5435</p>	

TO: All California State and Local Law Enforcement Agencies

This information bulletin provides a summary of new and existing state and federal laws that prohibit cyber exploitation and highlights the abilities of state and local law enforcement agencies to combat these crimes. Cyber exploitation is defined as the nonconsensual distribution and publication of intimate photos and videos.

Recent successful criminal prosecutions underscore the seriousness of cyber exploitation crimes under state law. These prosecutions also reflect the continued commitment of California law enforcement to preventing the commission of new crimes through coordinated responses to incident reports and victims' services. California law enforcement has an important role to play in combatting cyber exploitation and providing victim-centered services to the general public.

California Law Enforcement's Leadership in Combatting Cyber Exploitation

Attorney General Kamala D. Harris is committed to seeking justice for every victim of cyber exploitation in California and holding accountable 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. In February 2015, the Attorney General convened the leaders of major technology companies, victim advocacy groups, law enforcement, and elected officials to discuss the issue of cyber exploitation and commit to cross-sector strategies to combat these crimes. To create a space for the promulgation of effective remedies, the Attorney General established a Cyber Exploitation Take Force. The Task Force is charged with the development of a cyber exploitation best practice guide for the technology industry, training and materials to equip California law enforcement with the tools necessary to respond to these crimes, and education and prevention strategies that generate continued public awareness and improve public safety. The Commission on Peace Officer Standards and Training (POST) co-chairs the Take Force's law enforcement training and education subcommittee and has developed new materials to educate law enforcement statewide. **The California Department of Justice (DOJ) has created a robust cyber exploitation online toolkit with tailored resources for: victims, technology companies, and law enforcement. Please visit oag.ca.gov/cyberexploitation to access these resources.**

Drawing on the expertise of California law enforcement, the DOJ is committed to investigating and prosecuting cyber exploitation website operators and other perpetrators. The DOJ is a leader in prosecuting these crimes, having garnered the first successful prosecution of a cyber exploitation

operator in the U.S. 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.¹ In June 2015, Casey E. Meyering pleaded 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 was sentenced to three years imprisonment. Charles Evens, who orchestrated a cyber exploitation hacking scheme where he stole private images from victims' accounts and sold them to another website, pleaded guilty to computer intrusion in June 2015 and was sentenced to three years imprisonment, concurrent with a Federal prison term for the same conduct a year earlier.

These successful prosecutions underscore the seriousness of cyber exploitation crimes under state law and reflect the expertise and continued commitment of California law enforcement to prevent the commission of new crimes through coordinated responses to incident reports and victims' services.

New State Laws Regulating Cyber Exploitation—Effective January 1, 2016²

Assembly Bill 1310 (Gatto)— Disorderly Conduct: Unlawful Distribution of Image, Penal Code §§ 786, 1524.3

This law amends Penal Code § 1524 to allow search warrants to be issued for cyber exploitation crimes. It also expands and clarifies jurisdiction for the prosecution of cyber exploitation crimes to where: (1) the offense occurred, (2) the victim resided when the offense was committed, and (3) the intimate image was used for an illegal purpose. Since perpetrators often reside outside of the victim's jurisdiction, and the internet enables worldwide victimization, this change in the law allows state and local law enforcement to investigate and prosecute those who exploit their victims across multiple jurisdictions.

Senate Bill 676 (Cannella)— Disorderly Conduct: Invasion of Privacy, Penal Code §§ 502.01, 647.8

This law extends the forfeiture provision for possession of child pornography to cyber exploitation images, allowing law enforcement to remove these images from unauthorized possession. The forfeiture provisions apply to: illegal telecommunications equipment, or a computer, computer system, or computer network, and any software or data, when used in committing a violation of disorderly conduct related to invasion of privacy, as specified. The bill also establishes forfeiture proceedings for matter obtained through disorderly conduct by invasion of privacy.

Civil Remedies for Victims of Cyber Exploitation, Cal. Civil Code § 1708.85

As of July 2015, victims of cyber exploitation have a private right of action against their perpetrators. Assembly Bill 2643 (Wieckowski) codified a private right of action against any person who

¹ 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).

² Cal. Const. art. IV, § 8(c) (requiring that a statute enacted during regular session must go into effect on January 1 of the next year).

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 suffers general or special damages as described in Cal. Civil Code § 48(a).³ Cal. Civil Code § 1708.85. In addition to any other relief available at law, 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 distribution of material.⁴ *Id.* at § 1708.85(d). A court may also grant reasonable attorney's fees and costs to the prevailing plaintiff. *Id.* at § 1708.85(e).

Law enforcement should be aware of this civil remedy in order to advise victims that any court order, civil or otherwise, directed to the website that distributes or redistributes their stolen image is an effective method of getting the images removed from the internet. Website hosting companies are not allowed to act as a registrar to a website that violates the law, so it is critical to inform victims of this method of self-help.

Existing California Laws Regulating Cyber Exploitation

Cyber Exploitation: Disorderly Conduct, Penal Code §§ 647(4)(A)-(B)

It is illegal 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, when the persons agree or understand that the image shall remain private. The person distributing the image is liable when he/she knows or should know that distribution of the image will cause serious emotional distress, and the person depicted suffers that distress.

Under § 647, if a person is convicted of cyber exploitation, the court may require counseling as a condition of probation. Every person who, having been convicted of violating § 647, commits a second or subsequent violation of § 647, shall be punished by imprisonment in a county jail not exceeding one year, by a fine not exceeding \$1,000, or by both that fine and imprisonment.

Extortion, Penal Code §§ 519, 519(3)-(4), 520; Attempted Extortion, Penal Code §§ 524; 182; Conspiracy to Commit Extortion, Penal Code § 520

A person who publishes or threatens to publish private images of another with the intention of forcing the victim into prescribed conduct the victim would not have otherwise engaged in may be charged with extortion. Sites that encourage cyber exploitation and charge for the removal of images are engaging in extortion.

Under § 520, every person who extorts any money or other property from another, shall be punished by imprisonment for two, three, or four years. Under § 524, every person who attempts to

³ § 1708.85 enumerates six exceptions to liability in subsection (c), (1)-(6).

⁴ 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.

extort is punishable by 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 such fine and imprisonment.⁵

Unauthorized Access to Computers, Computer Systems, and Computer Data, Penal Code § 502

Pursuant to § 502, it is a crime for a person to access another's computer or computer network and copy, take, or delete data without permission. If a perpetrator takes private material from a victim's computer or uses a victim's email account, without permission, to send the images, then he/she may be prosecuted for computer intrusion. Under § 502, stringent penalties vary depending on the type of violation and the amount of damage inflicted.

Identity Theft, Penal Code § 530.5

Pursuant to § 530.5, it is a crime to willfully obtains someone's personal identifying information and uses that information for any unlawful purpose (not just theft). Under § 530.5, a person can be punished by a fine, by imprisonment in county jail, or by both.

Existing Federal Laws Regulating Cyber Exploitation

In addition to state statutes criminalizing cyber exploitation, federal statutes provide an additional tool for local law enforcement to better assist victims and combat perpetrators of cyber exploitation in California.

Extortion, 18 U.S.C. § 875(c)

Under 18 U.S.C. § 875(c), a person found guilty of extortion is liable for a fine and imprisonment of upwards of 20 years.

Unauthorized Access to a Computer, 18 U.S.C. § 1030(a)(2)(C)

Under 18 U.S.C. § 1030(a)(2)(c), a person found guilty of unauthorized access to a computer can be both fined upwards to \$10,000 and imprisoned for not more than 20 years.

Stalking, 18 U.S.C. § 2261A(2)

Under 18 U.S.C. § 2261A(2), a person found guilty of stalking can be both fined and imprisoned, with penalties dependent on whether any serious bodily injury to the victim results.

Best Practices for Law Enforcement in Combatting Cyber Exploitation Under California and Federal Law

To ensure the most effective law enforcement responses to cyber exploitation, the DOJ recommends law enforcement agencies develop policies and protocols specifically addressing cyber exploitation and other online harassment crimes. At a minimum, the DOJ recommends that the policies and protocols law enforcement agencies adopt include:

⁵ Please note that violators of § 524 must complete their sentence in state prison, while violators of § 520 must complete their sentence under the supervision of local custody under California's determinate sentencing. Cal. Penal Code § 1170(h).

- Guidelines covering report writing specific to cyber exploitation cases and the importance of collecting and preserving evidence (i.e. 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 volatile 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.
- Protocols to ensure that all types of incidents are reported, including threats. Victims should not be turned away because a particular incident does not look serious enough. 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 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.
- 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-centered responses, where applicable, including information about available community and mental health resources.

Additional Resources for Law Enforcement

The DOJ has created a robust cyber exploitation online toolkit with tailored resources for: victims, technology companies, and law enforcement. Please visit oag.ca.gov/cyberexploitation to access any of the resources listed below:

Computer Crimes List

Frequently Asked Questions for Victims

Frequently Asked Questions for Law Enforcement Agencies

Major Technology Company Privacy Policies Regarding Cyber Exploitation

We look forward to working with you to improve the reporting, investigation, and prosecution of cyber exploitation crimes across California.

Sincerely,



LANNY J. WALLACE, DIRECTOR
Division of Law Enforcement

For KAMALA D. HARRIS
Attorney General