Republika ng Pilipinas
KAGAWARAN NG KATARUNGAN
Department of Justice
Manila

Office of Cybercrime
Advisory Opinion No. 01
02 March 2015

ADVISORY ON SEXTORTION

INTRODUCTION

This Advisory is issued to increase awareness on the growing problem of "sextortion" and to the public on how to avoid being victimized and what to do when the crime happens.

It is an emerging issue following the large number of complaints received and results of the enforcement operations conducted by the Philippine National Police-Anti-Cybercrime Group (PNP-ACG), and the Department of Justice-Office of Cybercrime (DOJ-OOC), in coordination with INTERPOL, against organized crime groups involved in sextortion.

The *modus operandi* of sextortion offenders is to assume fake identities before engaging a victim. Upon gaining the victim's trust, the offender lures the victim to perform a sexual act and secures a picture or a video of the sexual conduct. The offender then threatens to circulate the material unless the victim pays a certain amount of money.

"Sextortion" is a crime committed in cyberspace where the offender obtains nude pictures or videos from victims, and then blackmails them for money to avoid the publication of the nude material.[1]

The threat to publish the victim's nude picture or video on the internet if no payment is made is the crime of "grave threats."[2]

RELEVANT LAWS

1. Act No. 3815 or "The Revised Penal Code"

[1] INTERPOL; PNP-ACG
[2] Defined and penalized under paragraph 1 of Article 282 of Act No. 3815 or The Revised Penal Code, as amended

Sextortion is defined and penalized under paragraph 1 of Article 282 of Act No. 3815 or The Revised Penal Code, as amended (RPC). The provision defines "grave threats" as a crime having the following elements: *first*, that the offender threatens another with the infliction of a wrong upon his person, honor, or property; *second*, that such wrong amounted to a crime; and *third*, that the offender made the threat demanding money or imposing any other condition.

Should the offender succeed in extorting the victim and is actually paid with the amount demanded, the crime committed is "robbery", defined and penalized under Articles 293 and paragraph 5 of Article 294 of the RPC. The following are its elements: *first*, that there is personal property belonging to another; *second*, that there is unlawful taking of that property; *third*, that the taking is with intent to gain; and *lastly*, that there is violence against or intimidation of persons.[3]

Intent to gain is presumed from the overt act of taking the property of another, unless special circumstances reveal a different intent.[4] If the demand is satisfied by the payment of the victim, the crime is transformed from "Grave Threats" to "Robbery with Intimidation of Persons".

Intimidation is defined in Black's Law Dictionary as unlawful coercion; extortion; duress; putting in fear.[5] In "Robbery with Intimidation of Persons", the intimidation consists in causing or creating fear in the mind of a person or in bringing in a sense of mental distress in view of a risk or evil that may be impending, real or imagined.[6] Such fear of injury to person or property must continue to operate in the mind of the victim at the time of the delivery of the money.[7]

2. R.A. No. 10175 or the "Cybercrime Prevention Act of 2012"

The commission of sextortion in cyberspace is also punishable under Republic Act No. 10175 or the "Cybercrime Prevention Act". Section 6 of the law imposes a penalty one degree higher to that imposed by the Revised Penal Code if the crime is committed by, through and

---

[3] Consulta vs. People of the Philippines, G.R. No. 179462, February 12, 2009

[4] *Ibid.*

[5] People v. Alfeche, Jr., G.R. No. 102070, July 23, 1992, 211 SCRA 770, 779.

[6] People v. Marco, 12 C.A. Rep. 377.

[7] *Ibid.*

with the use of information and communications technologies.[8] As the offender in sextortion consummates the crime of "grave threats" (or "robbery", if the victim actually paid the extorter) through the use of a computer system, he can be prosecuted for violation of the Cybercrime Law. This is without prejudice to the offender's liability under the Revised Penal Code or other special laws.[9]

Sextortion offenders may also be held liable for content-related offenses. For example, if the commission of the unlawful or prohibited acts under the Anti-Child Pornography Act are done through a computer system, the penalty to be imposed is one degree higher.[10] Higher penalties for cybercrime offenses such as sextortion are justified because the offender can easily evade identification and is able to reach far more victims or cause greater harm.[11]

3. R.A. No. 9995 or "the Anti-Photo and Video Voyeurism Act of 2009"

Sextortion also falls under the crime of "Photo or Video Voyeurism". Under the law, the mere taking of a photo or a video coverage of a person or group of persons performing a sexual act or any similar activity, or the capturing of an image of a person's private area without the consent of the person involved and under circumstances in which the person/s has/have a reasonable expectation of privacy is punishable.[12] Consent is irrelevant and the offender is liable if the photo or video coverage or recording is published through the internet.[13]

4. R.A. No. 9775 or the "Anti-Child Pornography Act of 2009"

If the victim involves a minor, the offender may also be held liable for "Child Pornography". The law punishes the inducement of a child to perform in the creation or production of any form of child pornography.[14] "Child pornography", as defined, refers to any representation, whether visual, audio, or written combination thereof, by

---

[8] Section 6 of Republic Act No. 10175 or the "Cybercrime Prevention Act of 2012"

[9] Section 7, *Id.*

[10] Section 4 (c) (2), *Id.*

[11] G.R. No. 203335, Disini vs. Secretary of Justice, February 11, 2014.

[12] Section 4 (a) of Republic Act No. 9995 or the "Anti-Photo and Video Voyeurism Act of 2009"

[13] Section 4 (d), *Id.*

[14] Section 4 (a) of Republic Act No. 9775 or the "Anti-Child Pornography Act of 2009".

electronic, mechanical, digital, optical, magnetic or any other means, of a child engaged or involved in real or simulated explicit sexual activities.[15]

Mere possession of any form of child pornography is punishable.[16] If the crime is carried out by a group of three (3) or more persons conspiring or confederating with one another, the crime is syndicated child pornography and the penalty imposed by law is higher.[17]

ADVISORY

In view of the foregoing, the following points are stated:

1. **THE PUBLIC SHOULD BE CAUTIOUS IN SHARING PRIVATE INFORMATION ONLINE AND SHOULD WATCH OUT FOR SUSPICIOUS SOCIAL MEDIA ACCOUNTS.**

The cyberspace is pervasive and complex. The public should be reminded that any kind of data or information voluntarily entered or uploaded online, can be viewed, read, or used by any person who may or may not be allowed access to such. It is important to exercise due diligence in online dealings and activities and to be proactive in protecting one's own privacy.

Although one of the purpose of social media sites is to connect and socialize with people, internet users are encouraged to avoid online connections with people they do not know. Growing trust and comfort with online connections can place a person in a compromising situation. Legitimate intentions are rare in cyberspace where fake identities are easily manufactured.

Given the nature of the internet and online social media, the public should keep personal information confidential, or limit its disclosure. Unregulated internet presence poses serious danger as it provides insight into the victim, his family, and his friends, which can be used by the offender in committing sextortion.

Self-regulation is the best way to avoid becoming a victim of sextortion. In using social networking sites, internet users should learn to properly utilize privacy settings and use of these security measures to prevent the commission of sextortion.

[15] Section 3 (b), *Id.*
[16] Section 4 (l), *Id.*
[17] Section 5, *Id.*

There are signs that reveal a suspicious internet user. Extorters typically use attractive profiles and are persistent in showing interest in the victim to lure him into adding the extorter to his network. They can have random people in their network and public interactions with strangers to fake authenticity. They use multiple social media platforms (Facebook, Twitter, Skype, Instagram, etc.) to gather information from their targeted victims. Further, they initiate lewd conversation to entice their victim into sexual conduct. Never trust these anonymous individuals.

Adding strangers to one's network permits access to user-generated content and other information that can be used against the potential victim. Anyone is a potential target. It is good practice to decline friendly requests of unknown identities to prevent becoming a sextortion victim.

2. SCHOOL AUTHORITIES AND PARENTS SHOULD GUARD MINORS FROM THE DANGERS OF THE INTERNET AND EDUCATE THEM OF INTERNET ETIQUETTES.

In *Vivares et. al. vs. St. Theresa's College*[18], the Supreme Court recognized the need for monitoring the cyber activities of minors, to wit:

> "Responsible social networking or observance of the 'netiquettes' on the part of teenagers has been the concern of many due to the widespread notion that teenagers can sometimes go too far since they generally lack the people skills or general wisdom to conduct themselves sensibly in a public forum."

Minors are the ones most vulnerable to become victims of sextortion because of their general trait of curiosity and gullibility. In view of the risks that minors are exposed to in their online activities, school authorities and parents having custody or control over them carry a burden to exercise proper supervision over them and to educate them on proper net etiquette.

Minors should be made aware of the nature of online social networks. Any information uploaded on these websites are left permanently in the provider's databases and are beyond the

[18] G.R. No. 202666, September 29, 2014.

control of its users. This digital footprint left online impacts on their future reputations. Privacy tools is also not an assurance of safety because it is easy for other users to share content of another uploader.

Given the above, schools should incorporate lessons on proper online conduct in their curriculum. They should make sure that minors are aware of the dangers of the internet and the repercussions of improper online activities. They should also have very strict rules that is properly implemented and they should know how to deal with cybercrimes should it occur.

Parents and guardians should also involve themselves in the interpersonal relations of minors. They should discuss internet usage freely with their child/ward, without making it appear that they are monitoring them, and suggest to them safety measures to prevent becoming a victim of cybercrimes.

Minors are generally incapable to pay extorters as they have no source of income. They are also in the age when they feel pressured to be accepted by society. When minors become victims of sextortion, they are at risk of doing the extreme to prevent the distribution of their lewd picture or video, and would go as far as taking their own lives to avoid its social stigma. Parents and guardians thus have the responsibility of giving support to minors who have been victims of sextortion, and assist them in reporting the crime to law enforcement authorities.

3. ANY PERSON WITH KNOWLEDGE OF SEXTORTION VIOLATIONS SHOULD IMMEDIATELY REPORT AND ASK FOR THE ASSISTANCE OF LAW ENFORCEMENT AUTHORITIES.

A victim of sextortion starts to become aware that he/she has been victimized when after exposure or the performance of a sexual activity, communications with the extorter is suddenly cut-off. In the event that this happens, it is recommended that the victim preserve all computer data he/she can, and ask for help from his/her family, friends, and/or law enforcement authorities.

Sextortion violators are usually part of an organized group who can victimize more if their criminal activities are not addressed. Victims of sextortion should refuse to pay extorters and instead report the commission of the crime to law enforcement authorities. There is no assurance that the extorter will delete the compromising photo/video if the victim pays the amount demanded. Hence, prompt report is important so that the crime will be quickly investigated and data that may serve as evidence may be preserved.

Sextortion can have a strong emotional impact upon victims. There are victims who go as far committing suicide. The public is advised to take the effects of sextortion seriously and create a culture of acceptance to victims who ask for their support.

The public is urged to contact appropriate government agencies, such as the PNP-Anti-Cybercrime Group at (02) 723-0401 local 5313, NBI-Cybercrime Division at (02) 523-8231 local 3455, or DOJ-Office of Cybercrime at (02) 523-8481 local 222, to report any cybercrime violations such as sextortion.

4. INTERNET SERVICE PROVIDERS AND TELECOMMUNICATIONS COMPANIES SHOULD COMMIT TO PRESERVE COMPUTER DATA AND COOPERATE WITH LAW ENFORCEMENT AUTHORITIES IN THE PROSECUTION OF SEXTORTION OFFENDERS.

Internet Service Providers (ISPs) and telecommunications companies (telcos) should take note of their responsibilities under the law to preserve and retain computer data. It is essential that they cooperate with concerned government agencies and provide the necessary assistance in the investigation and prosecution of offenders.

The following are the basic steps in the complaint process of sextortion, which is the same procedure as to other cybercrimes:

1. The commission of the crime is reported by the victim or the informant to law enforcement authorities (DOJ-OOC/PNP/NBI).
2. The law enforcement authorities will contact the complainant and gather evidence.
3. If the information provided and evidence gathered are sufficient, preservation order will be sent to the concerned ISP, copy of which is furnished to the DOJ-OOC.

4. Once data are preserved by the ISP, law enforcement authorities should then apply for a court warrant for its disclosure.
5. Law enforcement authorities will verify the information obtained from the ISP, and gather additional evidence for the application of search warrant.
6. Once a search warrant is issued, law enforcement authorities will submit pre-operation report to the Office of Cybercrime prior to the conduct of search and seizure operations.
7. If digital evidence is seized/found, proper incident response procedure will be followed and post-operation report will be submitted to the Office of Cybercrime.
8. The law enforcement authorities will then conduct forensic analysis on the digital evidence, and proceed with the filing of cases against the offenders.

The vast reach and effects of the internet makes it necessary to cooperate and collaborate with all stakeholders to combat cybercrimes, which has transnational dimension. Violators are finding new and more elaborate ways to commit the crime. Thus, a holistic response and mutual assistance is necessary, not just between local counterparts but also with the international community.

"Sextortion" is only one form of cybercrime. There are multiple crimes embodied in the "Cybercrime Prevention Act" that can be committed using a computer system. Each sector of the community should be watchful and vigilant of violators, in fulfillment of the goal to eradicate cybercrimes and protect persons from online abuse.

This Advisory is issued by the DOJ-OOC in line with its mandate to provide legal advice and information on cybercrimes. All are enjoined to disseminate and faithfully observe this Advisory.

LEILA M. DE LIMA
Secretary