MATRIX OF PHILIPPINE LAWS RELATED TO ONLINE SEXUAL EXPLOITATION OF CHILDREN (OSEC)

#ShutDownOSEC

This matrix has been drawn from an exhaustive mapping of existing laws related to protecting children from online sexual exploitation, with the aim of aiding a Congressional oversight of existing laws. Based on the results of this mapping, Child Rights Network urges our legislators to take into account the following points:

1. Clearly define and take into account the technological nuances of OSEC, and also provide legal definitions for essential terms including m"streaming" and "live streaming." This includes delineating OSEC as a transnational crime and an extraditable offense to ensure the investigation and prosecution of OSEC across borders.
2. Strengthen the powers of government authorities to implement OSEC-related laws and ensure that crimes are investigated and perpetrators are punished accordingly.
3. Widen the scope of existing laws to ensure that private entities, including Internet Content Hosts and Internet Service Providers are compelled to aid in prevention and investigation of OSEC cases. This includes clearly delineating the obligations of social media networks, hotel or mall owners/operators, Internet cafes/kiosks or lessors of business establishments, banks, money remittance centers and credit card companies in relation to shutting down OSEC.
4. Focus should be given to providing mandatory services and programs specifically designed for victims of OSEC to facilitate their rehabilitation and reintegration back to society. Clear provisions should also be written to holistically ensure that the government has appropriate measures to prevent, protect, and rehabilitate children from OSEC.

MAIN PHILIPPINE LAWS FOR CHILD PROTECTION ONLINE

LAW	FEATURES	GAPS	RECOMMENDATIONS
R.A. 9775 "Anti-Child Pornography Act of 2009"	The law punishes a whole spectrum of acts, which can include OSEC, related to child pornography from its production and distribution to its possession. It also imposes an obligation to Internet Service Providers ("ISPs"), internet content hosts, mall owners, lessors of business establishments, photo developers, information technology professionals, credit card companies, banks, and governmental branches to help eradicate OSEC and report cases of child pornography.	The law does not explicitly consider the often ephemeral quality of OSEC committed through the viewing or "live streaming" of online content that does not need the offender to do any act of downloading or retaining any form of child pornography. The law also does not fully contemplate the role of social media in OSEC.	In order to address the often ephemeral quality of the commission of OSEC, a definition of streaming and live streaming should be included in the law. Because the commission of OSEC is often perpetrated or initiated through social media networks, there should also be clear obligations imposed on them to not only report OSEC cases but also to prevent the commission of the same.
R.A. 9208 AS EXPANDED BY R.A. 10364 "Anti-Trafficking in Persons Act"	The original law punishes acts of trafficking as well as acts that promote the trafficking of persons. The amendment punishes persons who use trafficked persons for prostitution, and raises the penalty of an offense if the trafficked person is a child.	The law does not specifically address persons who view children online. The amended law also does not impose any obligation on ISPs, internet content hosts, or business establishments to prevent OSEC-related trafficking, or cooperate in the prosecution against the offenders. It is also insufficient in addressing the reality that children may be recruited online.	The law may be strengthened to provide the obligation to notify and cooperate with law enforcement when it finds reasonable suspicion of OSEC-related trafficking, ensure that there are technological or other practical safeguards in place to prevent or detect recruitment and trafficking, and train its employees to ensure that they may be able to detect the possibility of unlawful activity.
R.A. 10175 "Cybercrime Prevention Act of 2012"	The law punishes offenders who commit any of the acts defined and punishable under R.A. 9775 by imposing a penalty that is one degree higher than that provided under the latter law if the unlawful activity was committed through the use of a computer system.	While the law punishes any act which aids or abets the commission of a child pornography, or is an attempt to commit a cybercrime, the said provisions were struck down by the Supreme Court as unconstitutional for being vague.	The law should be amended to sufficiently address persons who may be considered "accomplices or accessories" to OSEC.
R.A. 9995 "Anti-Photo and Video Voyeurism Act of 2009"	The law punishes offenders who engage in photo or video coverage of persons who are engaged in sexual activities without their consent and taking into consideration their privacy expectations.	The law does not craft an exception for children wherein their consent should not even be a defense against liability under the law. It also does not focus on the attempt to capture photos or videos, but only on the consummated act.	The law should be amended to remove consent as a defense in cases involving children and also punish attempts to capture photos or videos of sexual activities.

LAW	FEATURES	GAPS	RECOMMENDATIONS
R.A. 9995 "Anti-Photo and Video Voyeurism Act of 2009"	The law explicitly defines and punishes child prostitution and other sexual abuse, and child trafficking. Under the amendment, the law now explicitly enumerates prohibited acts constituting the "worst forms of child labor," which include the sale and trafficking of children, child prostitution and child pornography, and exposure to sexual abuse.	The law has a narrow view when it punishes attempts to commit child prostitution. It also does not cover situations wherein the offender does not actually get to see videos or children despite trying to lure a child. There is also no clear punishment for an attempt to make a child engage in obscene or indecent shows.	The law should be amended to cover attempts to commit child prostitution, even if the attempt is not successful.

ANCILLARY LAWS THAT AFFECT CHILD PROTECTION PROCEDURES

R.A. 11313 "Safe Spaces Act"	The law defines gender-based online sexual harassment as "online conduct targeted at a particular person that causes or likely to cause another mental, emotional or psychological distress, and fear of personal safety. If the offended party is a minor, the law imposes a higher penalty on the offender.	The law does not fully consider OSEC as one of its punishable crimes.	The law must be amended for the elements of gender-based online sexual harassment to cover OSEC.
R.A. 10929 "Free Internet Access in Public Places Act	The law creates a "Free Public Internet Access Program" in public places. It tasks the Department of Information and Communications Technology (DICT), along with other concerned sectors and agencies, to develop standards and mechanisms for the protection of children online.	This is not a penal law. Hence, it will not be able to punish OSEC. By also giving more spaces free internet access, this may lead to more opportunities to perpetuate OSEC.	The law must be amended for the elements of gender-based online sexual harassment to cover OSEC.
R.A. 4200 "Anti Wire-Tapping Law"	The law prohibits "any person, not being authorized by all the parties to any private communication or spoken word, to tap any wire or cable, or by using any other device or arrangement, to secretly overhear, intercept, or record such communication or spoken word" by using recording devices.	The law does not punish OSEC as it primarily punishes unauthorized intercepting or recording of private communications. It does not contemplate acts constituting OSEC.	The definition of wire-tapping should be amended to include as punishable acts situations that facilitate OSEC or give access to OSEC materials.
R.A. 9160, as amended, "Anti-Money Laundering Act" (AMLA)	The law seeks "to protect and preserve the integrity and confidentiality of bank accounts and to ensure that the Philippines shall not be used as a money laundering site for the proceeds of any unlawful activity," which includes child trafficking and pornography.	As the law essentially punishes the act of using the banking system in order to make it appear that the proceeds of an unlawful activity originated from legitimate sources, an act constituting OSEC must first be considered a violation of another penal law before the law itself can be applied. The law also has a high threshold amount, which is P500,000 in one banking day.	The implementing rules of the law should have provisions that are specific enough or realistic enough to account for money transactions that are OSEC-related. The high threshold amount required before a suspicious account is flagged and reported to the AMLC should also be amended.
R.A. 1405, R.A. 6426 Banking laws	Philippine banking laws, in relation to OSEC, delve into how the proceeds which are deposited in banks may be inquired into, frozen, or garnished when such proceeds are related to the commission of crimes.	If an offender has a foreign currency deposit account and is convicted of a crime relating to OSEC, the law technically does not allow the account to be garnished for any monetary penalty imposed by the court.	To strengthen the punishment of OSEC, there should be explicit legislation that allows garnishment.
R.A. 10173 "Data Privacy Act"	The law punishes any unauthorized processing, accessing due to negligence, committing improper disposal, processing for unauthorized purposes, unauthorized access or intentional breach, malicious or unauthorized disclosure of personal or sensitive personal information or concealment of security breaches involving sensitive personal information	The law does not impose higher obligations or higher penalties for entities who handle children's personal or sensitive information.	There should be a higher standard of responsibility expected for entities that hold a child's information. This would mean that internet content hosts should be liable in case it allows OSEC material that identifies a child in their systems. There should be corresponding penalties for such entities who hold a child's information and do not take steps to protect it.