#SAFERKIDSPH

## The Private Sector

The private sector plays a crucial role in both facilitating and mitigating OSAEC in the country. In the context of OSAEC, private sector players include telecommunication companies and Internet service providers (ISPs), Internet cafés, banks and remittance centers, non-government organizations (NGOs), international agencies, and private individuals. Most private sectors work collaboratively with the government, with the latter acting as a regulating body, e.g., the Department of Information and Communications Technology (DICT) and its attached agencies, the National Telecommunications Commission (NTC), and the National Privacy Commission (NPC); as well as an implementing body, e.g., the Department of Social Welfare and Development (DSWD), and local government units (LGUs).

## Role of the Private Sector in the Promotion of OSAEC

Private organizations in the technology sector may inadvertently be portrayed as facilitators of OSAEC when their services are used as medium for the transmission of child sexual abuse material. Their roles include (1) providers of Internet services; (2) operators of Internet cafés; (3) developers of software applications and communication tools that include social media platforms, messaging applications, video streaming tools, and chat rooms; and (4) providers of online payment channels and services.

**Internet service providers**. Telecommunication companies give free data access to certain social media platforms such as Facebook, messaging applications such as Messenger and Twitter, and video streaming sites such as YouTube in an effort to maintain customer loyalty as well as increase their subscriber base. Combining these with the enabling policy environment provided by RA 10929, children with their own mobile devices are thus given unsupervised access to the Internet anytime and anywhere, which increases their risk of exposure to OSAEC. In interviews with private sector respondents, it has been intimated that technology does help in the proliferation of child pornography.

**Use of Internet cafés and PisoNet**. Public access to the Internet from contact points such as PisoNet establishments and Internet cafes “caters to those who do not have space for personal computer at home, who do not own any device”, as stated by a key informant of this study. Managers of Internet cafés function as regulators and set rules on computer and software use, including software that will allow him or her to monitor the sites that a user is visiting, and limit access to certain sites upon his or her discretion. In this light, the informant says that “the manager’s values define what the shop may or may not allow the child to do.”

While Internet Cafes may have managers who can regulate through installation of technological safeguards, this is not assured nor standardized in absence of a local ordinance or a clear regulation from a national agency. This possibility of regulation is totally absent in online platforms such as the PisoNet where a user is left to navigate the facility without any form of guidance or regulation. Thus, the manager or owner of PisoNet computers may or may not impose any rules and restrictions on the sites that child patrons can access. The length of time that the child uses the computer is based on the amount of money the child has; this transfers control from the owner to the child. Typically, for those

with no personal computer or Internet access at home, PisoNet establishments and Internet cafés are the children's first encounter with the Internet.

**Social media platforms and messaging applications**. The additional online functionalities of social media and messaging apps led to the further sharing, distribution, and even live streaming of OSAEC videos and related materials. Chat rooms, especially those that are integrated in online games, allow players to anonymously meet one another and engage in various forms of interaction, from simple chatting to exchanging virtual artifacts and trading, and sharing private account information that allows gamers to become social media friends online and later on, offline. Some even use encryption and anonymization technologies and go to the Darknet to avoid detection. Children who have stopped going to school, who have run away from home, or who are left unsupervised by their parents and guardians, allowing them to access the Internet from morning until evening, are in grave danger of being involved in OSAEC.

The lack of sufficient computer literacy among private individuals is also a cause for alarm. A number of reported cases revealed that OSAEC usually takes place at home, with family members and neighbors as perpetrators. At home, a personal computer (either desktop or laptop) and a network router allow one to easily connect to the Internet and access online applications. The low- cost connectivity packages further make such a setup affordable even in poor communities. Even if family members are not the perpetrators, their general lack of knowledge about how computers work further compounds the problem. As one key informant elaborates, "Families (users) do not realize that once you upload something online, it's there forever." Even if photos and videos have been removed from one social media platform, most devices are set to automatically download a copy of these files onto the recipient's storage, which makes it possible that a copy of the picture or video is still somewhere on the World Wide Web because people shared it with others. The rampant posting and sharing of media files may also cause accidental exposure of adolescents and children to sexually explicit materials online.

**Online payment channels**. While frequent money transfers made through banks and remittance centers can be used as red flags for identifying possible OSAEC activities, online payment facilities offered by banks and electronic payment channels through mobile phone companies are surfacing as the new mode of monetary exchange for the conduct of OSAEC-related activities. This promotes the easier transfer of money among facilitators and perpetrators while reducing the ability of financial regulating bodies and law enforcement agencies to monitor and control such transactions. The added secrecy afforded by such online technologies, e.g., creation of fake identities or accounts with pseudonyms, increases their appeal to individuals involved in illicit trades such as OSAEC.

**Emerging threats**. As technologies to support online transactions continue to develop, they pose an emerging threat against efforts to combat OSAEC that has not yet surfaced from the key informant interviews. The Darknet—a portion of the Internet that is not publicly available— has an impending impact in how our law enforcement agencies, already depleted in manpower and technical knowledge, can cope with monitoring and preventing OSAEC. The "no censure" philosophy of this underground network renders useless the filtering and blocking of illegal sites, allowing the exchange of child sexual abuse and exploitation materials to freely take place under a blanket of anonymity.

New online payment platforms or networks such as PayPal and Bitcoin provide an alternative to traditional methods such as credit cards and money orders. They allow the electronic transfer of money between accounts held by online vendors, auction sites, and commercial users. Because the accounts are created online, no physical verification of the account owners take place, which permits account holders to hide behind pseudonyms. Similarly, digital anonymous currencies like Bitcoin enable underground networks to flourish behind a curtain of hidden names.

**Addressing these risks**. Technology companies and financial institutions can play a major role in the fight against OSAEC by helping the government prepare for these new technologies. These can be in the form of policy re-formulation that considers children as major users of technology, training of law enforcement personnel in using the technologies and in understanding possible ways by which the technology can be misused, and awareness campaigns to educate the public on the benefits as well as the potential dangers of such technologies.

## Role of the Private Sector in the Prevention of OSAEC

While the design of the technology itself can make it vulnerable for exploitation in facilitating OSAEC, some sectors acknowledge that the use of technology can also help mitigate the problem. These technology-based prevention measures include (1) raising awareness, (2) integrating in K-12 curriculum, and (3) monitoring content.

**Raising awareness**. Non-government organizations are using Facebook and Twitter (e.g., #StopChildPorn) to educate and to raise awareness about OSAEC, and to offer helplines for victims and their families. Communities and private citizens can also use these channels to report possible incidents of OSAEC. DSWD uses its social media pages to promote related programs. By sharing their advocacies online, the DSWD believes that others may develop a similar mindset relative to online protection and get the community to participate as well. A spokesperson from their office states that "…if negative material can be propagated online, why can't positive material be propagated online?"

Through its Digital Thumbprint Program, Globe, in cooperation with Optus and SingTel, conducts training workshops on cybersecurity, safety, online responsibility and leadership, and empowerment to educate Filipino youth about the impact of their online behavior.

**Curriculum integration**. Technology adoption has both positive and negative impacts on our lives and that of children. No amount of laws, policies, and guidelines can ever be enough to combat the OSAEC threat. As illustrated in Figure 1, constantly progressing technology and the equally changing manifestations of technology-enabled crimes warrant a more proactive approach to address this problem. Even people's cultural norms are changing as a result of technology adoption.

The more sustainable solution is in properly educating the youth on the benefits and risks in the World Wide Web. Cyberspace has become the extension of the children's physical and real world (Teunissen, 2012). Values education on proper social behavior in the physical world should acknowledge that a new form of social interaction is also occurring in the cyberworld. As children spend more time online for their education and entertainment, they should be properly taught how to be good individuals in the


online community. This education should begin from the homes where the family structure establishes the socio-cultural foundation that should be carried over to the larger community. Online rights and responsibilities such as respect for privacy, freedom of expression and universal access, and even the basic “do not talk to strangers” prescription, should continue to be taught even in the digital age.

**Monitoring content**. Telecommunication companies, while restricted by the Data Privacy Act to monitor content that passes through their network and share subscriber information, resort to other strategies in order to help in the fight against OSAEC. Globe Telecom, for example, partners with content providers like YouTube for Kids to give a thematic service centered on educating younger children, preventing them from just freely exploring all videos in the platform. PLDT, on the other hand, gives parents the ability to monitor and manage Internet access of their children at home.

Technology companies also subscribe to a set of guidelines to help address the challenges in mitigating OSAEC. Facebook has put in place a system of reviewing content that has been reported to them and takes action accordingly. International organizations such as UNESCO also mobilize governments, the private sector, civil society, and the technical community for “the complementary development and application of shared principles, norms, rules and decision-making procedures, and activities that shape the evolution and use of the Internet.”

Technology-based solutions are available to help safeguard children from accessing harmful web content. These mechanisms include a) content control software, b) content inspection using AI, and c) keyword trends analysis. Content control software can filter content and restrict materials that are delivered through the web, email, and other file sharing platforms. Meanwhile, regulating content can span across several levels: at the national level, where government agencies impose policies and laws on Internet censorship (especially through public Wi-Fi) to promote child online safety; at the ISP level where content delivered to clients is restricted; at the community level, where schools can limit content available to students through network-based filtering; and at the family level, where parents can impose restrictions through their browsers.

Content inspection can either be manual or automated. Manual inspection is not only subjective but is also time-consuming and taxing for someone examining the content. Software tools that utilize artificial intelligence are currently being developed to conduct automated inspection and does away with human intervention. However, depending on the materials being examined and the criteria set by the programmers or administrators, the accuracy of the inspection software raises credibility issues with the public. Another alternative involves using augmented intelligence, where the software makes an initial analysis and flags potential problems, while an individual verifies and decides on the content in question.

Content inspection is not limited to materials that are shared online through social media platforms. Other applications can integrate content inspection features, such as surveillance systems to monitor user behavior, image processing technologies to detect nudity in the materials that are uploaded to photo sharing and video streaming sites, and analysis of chat logs for potential grooming and exploitation in the message threads. However, data privacy and confidentiality considerations must be

put in place to address ethical issues posed by the use of such technologies on public sites and platforms.

**Potential risks in over-use of technology-based solutions**. While technology offers much promise in addressing the challenges in detecting OSAEC, one key informant expressed caution in this regard:

*"Kasi sometimes, there's a tendency to rely too much on technology to solve the problem, actually. Ako, from my perception, going to old-fashioned police work can do already a lot. Some people nagtataka kung ba't kumalat yung child sex dun sa Cordova sa Cebu. Isa sa mga malls dun sa Mactan Island, makikita mo mga puti kahawak kamay yung mga bata." (Sometimes, there a tendency to rely too much on technology to solve the problem, actually. From my perception, going to old-fashioned police work can do already a lot. Some people wonder why child sex spread in Cordova, Cebu. In one of the malls in Mactan Island, you will see white people (foreigners) holding the hands of (Filipino) children.)*