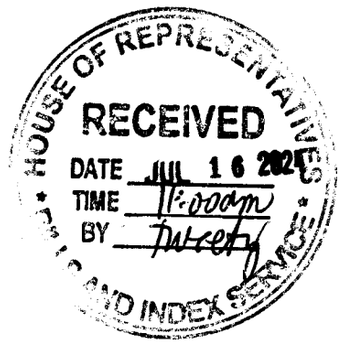
Republic of the Philippines
HOUSE OF REPRESENTATIVES
Quezon City

NINETEENTH CONGRESS
Second Regular Session

HOUSE BILL NO. 10608



Introduced by: Hon. Keith Micah "Atty. Mike" D.L. Tan

AN ACT
PROVIDING PROTECTION FOR CHILDREN USING THE INTERNET

EXPLANATORY NOTE

This bill seeks to promote the safety of children while using the Internet in consonance with Section 3(2), Article XV, of the 1987 Constitution, which provides that, "The State shall defend the right of children to assistance, including proper care and nutrition, and **special protection from all forms of neglect, abuse, cruelty, exploitation, and other conditions prejudicial to their development**" (*emphasis supplied*).

It is in line with Section 13, Article II, which mandates the State to promote and protect the physical, moral, spiritual, psychological, and social well-being of children and in pursuit of the principles of the United Nations Convention on the Rights of the Child (UNCRC), which recognizes that "In all actions concerning children, whether undertaken by public or private social welfare institutions, courts of law, administrative authorities or legislative bodies, the best interests of the child shall be a primary consideration."

The UNCRC also establishes that all children have a right to education; to leisure, play and culture; to obtain appropriate information; to freedom of thought and expression; to privacy and to express their views on matters that affect them in accordance with their evolving capacities. It also protects children from all forms of violence, exploitation and abuse and discrimination of any kind and ensures that the child's best interest should be the primary consideration in any matters affecting them.

The measure is in response to the exponential growth and impact of new technologies that are now thoroughly integrated into the lives of countless children and young people.

According to the UNICEF, "The proliferation of Internet access points, mobile technology and the growing array of Internet-enabled devices – combined with the immense resources to be found in cyberspace – provide unprecedented opportunities to learn, share and communicate."[1]

With these developments, however, are the risks of using the Internet. These include children being exposed to inappropriate content for their age or to inappropriate contact, including from potential perpetrators of sexual abuse. They can suffer reputational damage associated with publishing sensitive personal information either

[1] Guidelines for the Industry on Child Online Protection, UNICEF, 2015 Edition

online or through 'sexting', having failed to fully comprehend the implications for themselves and others of their long-term 'digital footprints'.[2]

Privacy, illegal content, harassment, cyberbullying, misuse of personal data or grooming for sexual purposes and abuse are issues that accompany the use of Internet by children that must be acted upon with urgency and firmness.

The 2020 Child Online Safety Index (COSI), the world's first-real-time analytic platform to help nations see the status of their children's online safety by the DQ Institute, an international think-tank that is dedicated to setting global standards for digital intelligence, gave the Philippines a below average score of 28.3 among thirty (30) countries that have the best online safety for children.

Accordingly, the report shows that children the world over are facing "cyber-pandemic", specifically 8 – 12 years old children where 17% of them experienced risky contact or offline meeting with strangers or sexual contact; 39% experienced reputational risks; 29% are exposed to risky content (violent or sexual); 45% are affected by cyber-bullying; 13% are at risk for gaming disorder; 7% are at risk for social media disorder; 28% experienced cyber threats; and 60% are exposed to cyber risks.

A study by cybersecurity company Surfshark, on the other hand, found that Filipino children's exposure to online risks such as cyberbullying, phishing and hacking was the second-highest in the world.[3]

Thus, the imperativeness of creating a clear and predictable "legal and regulatory environment which supports businesses and other thirds parties to meet their responsibilities to safeguard children's rights throughout their operations..."[4]

In this light, the proposed legislation gears towards the adoption of a regulatory policy where an effective mechanism for the development of protection or safeguarding policy to identify, prevent, and mitigate the adverse impacts of information communication technology on children may be established.

It primarily engages the participation of relevant stakeholders with an interest in online child protection such as industry players and educators insofar as they are among the key stakeholders in the child online protection ecosystem.

Industry players, in particular, have enormous responsibility to help promote awareness of the online safety of children by building robust checks and balances to identify the user and provide children with a conducive online environment. A regulatory framework such as those that provide certain obligations for companies to detect, block and/or remove harm against children from platform services, as well as to

---

[2] Ibid.

[3] Filipino kids are the second most vulnerable to online threats globally — study, Ramon Royandoyan, Philstar.com, April 26, 2022 (https://www.philstar.com/business/2022/04/26/2176906/filipino-kids-are-second-most-vulnerable-online-threats-globally-study#:~:text=MANILA%2C%20Philippines%20—%20Filipino%20kids%20are,second%2Dhighest%20in%20the%20world.) Accessed on 20 June 2024

[4] Guidelines for policy-makers on Child Online Protection, International telecommunication union, 2020

provide clear reporting routes and access to support is certainly imperative if children are to be protected online.[5]

According to DQ Institute, "Social media, gaming, telecom, and device companies must include **child online safety as a core business principle** (*Emphasis supplied*)."

This proposal builds on the UN Guiding Principles on Business and Human Rights, which call on businesses to meet their responsibility to respect children's rights by avoiding any adverse impacts linked to their operations, products or services.

The bill mandates mobile service providers, internet service providers, content providers, online retailers, app developers, and user-generated content, interactive and social media providers to create a safe and age-appropriate digital environment for children of diverse ages; identify, prevent and mitigate the adverse impacts of information and communications technologies on children's rights; and create a safer, more enjoyable digital environment for children.

It requires online users to submit a valid proof of identification prior to registration for social media services and provides protection of children's online privacy.

Following the recent enactment of a law in Florida, USA that restricts social media use for children, the measure also provides for a ban on children under 14 years of age from having social media accounts.

This bill draws from the broad recommendations of the Child Online Protection (COP) Initiative, a multi-stakeholder network launched by the International Telecommunication Union (ITU), a UN specialized agency for information and communication technologies.

In view thereof, approval of this bill is earnestly sought.

Keith Micah "Atty. Mike" D.L. Tan
4th District, Quezon

[5] Ibid.

Republic of the Philippines
HOUSE OF REPRESENTATIVES
Quezon City

NINETEENTH CONGRESS
Second Regular Session

HOUSE BILL NO. 10608

Introduced by: Hon. Keith Micah "Atty. Mike" D.L. Tan

AN ACT
PROVIDING PROTECTION FOR CHILDREN USING THE INTERNET

Be it enacted by the Senate and the House of Representatives of the Philippines in Congress assembled:

SECTION 1. *Title.* – This Act shall be known as the "Child Online Protection Act."

SEC. 2. *Declaration of Policy.* – Consistent with Section 13, Article II of the Philippine Constitution, the State recognizes the vital role of the youth in nation-building and promotes and protects their physical, moral, spiritual, intellectual, and social well-being. It is also the policy of the State to provide special protection to children from all forms of abuse, neglect, cruelty, exploitation and discrimination and other conditions, prejudicial to their development.

The best interests of children shall be the paramount consideration in all actions concerning them, whether undertaken by public or private institutions. Every effort shall be exerted to promote the welfare of children and enhance their opportunities for a useful and happy life.

Towards this end, the State shall vigorously promote online protection for children by securing their interactions and transactions in the Internet.

SEC. 3. – *Definition of Terms:*

(a) "Application developer" or "app developer" refers to a professional responsible for designing and coding functional software programs and applications;
(b) "Child" refers to person below eighteen (18) years of age or those over but are unable to fully take care of themselves or protect themselves from abuse, neglect, cruelty, exploitation or discrimination because of a physical or mental disability or condition;
(c) "Content provider" refers to an entity that supplies material such as text, music, or images for use on websites;
(d) "Internet service provider" refers to a public telecommunication entity (PTE) or value-added service (VAS) provider duly authorized by or registered with the National Telecommunications Commission (NTC) that provides users or other entities with data connection allowing access to the internet through physical transport infrastructure, and such access is necessary for internet users to access content and services on the internet, and for content providers to publish or distribute materials online;

(e) "Mobile service provider" refers to a public telecommunications entity or virtual network operator, or an entity that provides mobile telecommunications service to subscribers;
(f) "Notice and takedown" refers to a procedure or process for the swift removal of illegal content;
(g) "Online retailer" refers to a business that sells goods over the internet and transports goods by mail or parcel delivery;
(h) "Social media" refers to a digital technology that allows the sharing of ideas and information, including text and visuals, through virtual networks and communities;
(i) "Social media platform" refers to an online forum, website, or application that satisfies each of the following criteria:

(a) Allows users to upload content or view the content or activity of other users;
(b) Ten percent or more of the daily active users who are younger than 16 years of age spend on average 2 hours per day or longer on the online forum, website, or application on the days when using the online forum, website, or application during the previous 12 months or, if the online forum, website, or application did not exist during the previous 12 months, during the previous month;
(c) Employs algorithms that analyze user data or information on users to select content for users; and
(d) Has any of the following addictive features:

(1) Infinite scrolling, which means either:

(i) Continuously loading content, or content that loads as the user scrolls down the page without the need to open a separate page; or
(ii) Seamless content, or the use of pages with no visible or apparent end or page breaks.

(2) Push notifications or alerts sent by the online forum, website, or application to inform a user about specific activities or events related to the user's account.
(3) Displays personal interactive metrics that indicate the number of times other users have clicked a button to indicate their reaction to content or have shared or reposted the content.
(4) Auto-play video or video that begins to play without the user first clicking on the video or on a play button for that video.
(5) Live-streaming or a function that allows a user or advertiser to broadcast live video content in real-time.

(e) "User-generated content" refers to any form of visual media that is created by users of an online system, and made accessible via social media;

SEC. 4. *Creating a Safe and Age-Appropriate Online Environment for Children.* – In pursuit of creating a safe and age-appropriate digital environment for children of diverse ages, mobile service providers, internet service providers, content providers, online retailers, app developers, and user-generated content, interactive and social media providers shall:

(a) Develop a child protection or safeguarding policy to identify, prevent, and mitigate the adverse impacts of information communication technology on children;
(b) Integrate due diligence on child online protection issues into risk assessment frameworks at the organizational and product or technology levels to identify adverse impacts on children that are directly linked to their operations, products or services;
(c) Establish operational-level grievance and reporting mechanism for any child's rights violations such as inappropriate content or contact and breach of privacy;
(d) Use customer terms and conditions and/or acceptable use policies to explicitly state the company's position on the misuse of its services and the consequences of any abuse;
(e) Develop notice and take down (NTD) and reporting processes that allow users to report inappropriate content or contact on the specific profile/location where it was observed;
(f) Employ appropriate technical measures to prevent underage access and exposure to inappropriate content or services such as parental control tools, age-differentiated experiences with password-protected content, block/allow lists, purchase/time controls, opt-out functions, filtering and moderating;
(g) Ensure that content and services that are not age-appropriate for all users are marked with prominent display options to control access or offered together with age verification, if possible.
(h) Adapt and implement heightened default privacy settings for collection, processing, storage, sale and publishing of personal data, including location-related information and browsing habits gathered from children;
(i) Offer clear reporting tools and develop processes to act on reports of inappropriate content, contact and misuse and provide detailed feedback to service users on the reporting process; and
(j) Monitor where, when, and how children may encounter potentially harmful advertising messages intended for another market segment.

SEC. 5. *Identification, Prevention and Mitigation of the Adverse Impacts of ICT.* – Internet service providers shall identify, prevent and mitigate the adverse impacts of information and communications technologies on children's rights and identify opportunities to support the advancement of children's rights.

Towards this end, ISPs shall:

(1) Identify customers' age where appropriate and implement a suitable solution to individual services;
(2) Provide mechanisms such as parental control software and tools that enable parents to manage their children's access to Internet resources in the form of white lists, content filters, usage monitoring, contact management, or time/program limits;
(3) Within the service itself, at the point of uploading content, include reminders about such topics as the type of content that is considered to be inappropriate; and
(4) Provide children with information on safer Internet use on the landing page.

SEC. 6. *Promoting Enjoyable Digital Environment for Children.* – User-generated-content, interactive and social media service providers shall create a safer, more enjoyable digital environment for children of diverse ages by taking the following actions:

(1) Communicate in customer-friendly language within the terms of service and user guidelines a clear set of house rules that define (a) the nature of the service and what is expected of its users, (b) what is and is not acceptable in terms of harmful content, behaviors, (c) language as well as prohibiting illegal usage; and (d) consequences of any breach;
(2) Enforce minimum age requirements and take steps to identify and remove underage users who have misrepresented their age to gain access; and
(3) Protect younger users from uninvited communication and ensure that privacy and information-collection guidelines are in place;
(4) Review hosted images and videos and delete the inappropriate ones when found; and
(5) Ensure that secure passwords are used as a step towards protecting children in gaming and other social media settings and develop tools that actively seek to remove content that is illegal or in breach of the terms of condition and service as well as tools to prevent uploading of known illegal content to the site.

SEC. 7. *Electronic Identification Requirement.* – Social media providers and other similar online platforms shall require online users to submit a valid proof of identification prior to registration for their services.

For Philippine-based users, government-issued identification cards, including barangay certification of identity shall be sufficient proof of identification for purposes of this Act.

Existing members shall be required to submit a valid identification card as a condition for continuing membership on their platform.

SEC. 8. *Prohibiting Social Media Accounts for Children Below Fourteen (14) Years of Age.* – A social media platform shall prohibit a child who is younger than fourteen (14) years of age from entering into a contract with a social media platform to become an account holder.

In furtherance of this prohibition, a social media platform shall terminate any account held by an account holder younger than 14 years of age, including accounts that the social media platform treats or categorizes as belonging to an account holder who is likely younger than 14 years of age for purposes of targeting content or advertising, and provide ninety (90) days for an account holder to dispute such termination. Termination shall be effective upon the expiration of the 90 days if the account holder fails to effectively dispute the termination.

A social media platform shall prohibit a child who is 14 or fifteen (15) years of age from entering into a contract with a social media platform to become an account holder, unless the child's parent or guardian provides consent for such child to become an account holder.

SEC. 9. *Protection of Children's Privacy.* – Mobile network operators are hereby prohibited from collecting, using or disclosing personal information from children in a manner that violates the provisions of this Act. An operator of such website or online service or the operator's agent shall not be held liable for any disclosure made in good faith and following reasonable procedures in responding to a request for disclosure of personal information to the parent of a child as provided under this Act.

SEC. 10. *Collection of Personal Information from Children.* – The collection of personal data from children by any website or online service directed to children may be allowed provided that the following requirements are complied with:

(a) The operator provides notice on the website or online service of what information is collected from children, how the operator uses such information, and the operator's disclosure practices for such information; and
(b) The operator obtains verifiable parental consent for the collection, use or disclosure of personal information from children.

SEC. 11. *When Consent is Not Required.* – Verifiable parental consent shall not be required under the following circumstances:

(a) Online contact information collected from a child that is used only to respond directly on a one-time basis to a specific request from the child and is not used to recontact the child and is not maintained in retrievable form from the operator;
(b) A request for the name or online contact information of a parent or child that is used for the sole purpose of obtaining parental consent or providing notice under this Section and where such information is not maintained in retrievable form by the operator if parental consent is not obtained after a reasonable time;
(c) Online contact information collected from a child that is used only to respond more than once directly to a specific request from the child and is not used to recontact the child beyond the scope of that request:

    (i) If, before any additional response after the initial response to the child, the operator uses reasonable efforts to provide a parent notice of the online contact information collected from the child, the purposes for which it is to be used, and an opportunity for the parent to request that the operator make no further use of the information and that it is not be maintained in retrievable form; or
    (ii) without notice to the parent in such circumstance as the Department of Information and Communication and Technology (DICT) may determine are appropriate, taking into consideration the benefits to the child of access to information and services, and risks to the security and privacy of the child, in rules and regulations promulgated for the effective implementation of this Act.

(d) The name of the child and online contact information, to the extent reasonably necessary to protect the safety of a child participant on the site, is:

    (i) Used only for the purpose of protecting such safety;
    (ii) not used to recontact the child or for any other purpose; and
    (iii) not disclosed on the site;

If the operator uses reasonable efforts to provide a parent notice of the name and online contact information collected from the child, the purposes for which it is to be used, and an opportunity for the parent to request that the operator make no further use of the information and that it not be maintained in retrievable form; or

(e) The collection, use or dissemination of such information by the operator of such website or online service is necessary:

(i) to protect the security or integrity of its website;
(ii) to take precaution against liability;
(iii) to respond to judicial process; or
(iv) to provide information to law enforcement agencies or for an investigation on a matter related to public safety.

SEC. 12. *Role of the Department of Information and Communications Technology*. - The DICT shall be the primary agency tasked with the protection of children using the Internet and the implementation of this Act.

SEC. 13. *Public Awareness Programs* - The DICT shall, in consultation with the Philippine Information Agency and other relevant agencies of government, private sector, and civil society organizations, develop, lead, undertake and coordinate a nationwide program to heighten public awareness and involvement in furtherance of the purposes of this Act. The program shall utilize existing resources and efforts of the national government, local governments, private organizations, and non-government organizations and shall include:

(a) Identifying, promoting, and encouraging best practices for Internet safety;
(b) Establishing and carrying out a national outreach and Internet Safety Education campaign regarding Internet safety utilizing various media and Internet-based resources;
(c) Facilitating access to, and the exchange of, information regarding Internet safety to promote up-to-date knowledge regarding Internet safety; and
(d) Facilitating access to Internet safety education and public awareness efforts of the government, nonprofit organizations, and other appropriate entities.

SEC. 14. *Digital Citizenship Literacy Program*. – The promotion of digital citizenship literacy program shall be inculcated in all levels of education nationwide. Consistent with Section 5 of Republic Act No. 10533, or the "Enhanced Basic Education Act of 2013", the Department of Education (DepEd) shall ensure that the K to 12 curriculum shall be supported by programs on digital literacy.

The Commission on Higher Education (CHED) and the Technical Education and Skills Development Authority (TESDA) shall ensure the promotion of programs on digital citizenship literacy.

SEC. 15. *Online Safety Coordinators*. – There shall be appointed an Online Safety Coordinator (OSC) in all primary and secondary schools. They shall ensure the protection of all students from potential harms that may occur through the Internet and electronic media and serve as the main contact persons on all online-related issues. OSCs shall act as auditor of online safety measures, including the collection and recording of online safety incidents.

SEC. 16. *Penalties*. – Violations of this Act shall be penalized by imprisonment ranging from one (1) year to three (3) years or a fine of not less than Five hundred thousand pesos (Php500,000.00) but not more than Two million pesos (Php2,000,000.00) or both, at the discretion of the court.

SEC. 17. *Appropriations*. – The amount necessary to carry out the provisions of this Act is hereby authorized to be appropriated in the General Appropriations Act of the year following its enactment into law and thereafter.

SEC. 18. *Separability Clause.* – If for any reason, a provision or part thereof is declared invalid, other provisions not affected thereby shall remain in full force and effect.

SEC. 19. *Repealing Clause*. – All Acts, decrees, executive orders, rules and regulations contrary or inconsistent with the provisions of this Act are hereby repealed or modified accordingly.

SEC. 20. *Effectivity Clause*. – This Act shall take effect fifteen (15) days following its publication in two (2) national newspapers of general circulation.

Approved,