

The Dark Side of the Web—A Risk for Children and Adolescents Challenged by Isolation during the Novel Coronavirus 2019 Pandemic

Pietro Ferrara, MD^{1,2}, Giulia Franceschini, MD², Giovanni Corsello, MD^{1,2}, Julije Mestrovic, MD^{1,3}, Ida Giardino, MD⁴, Mehmet Vural, MD^{1,5}, Tudor Lucian Pop, MD, PhD^{1,6}, Leyla Namazova-Baranova, MD, PhD^{1,7}, and Massimo Pettoello-Mantovani, MD, PhD^{1,8}

In response to the global novel coronavirus disease 2019 (COVID-19) pandemic, many countries around the world adopted social isolation measures to contain the spread of the virus.¹ For children and adolescents, limitations in face-to-face activities and interactions with their traditional peer groups has been a frustrating experience. After disease containment measures, which included school closures, social distancing, and home quarantine, children and adolescents faced a prolonged state of physical isolation from their peers, teachers, extended family, and community networks that affects their emotional and behavioral health.² Parents and pediatricians are reporting signs of mental distress in children of all ages within the context of the pandemic.³ In several cases, this unexpected social isolation has paradoxically improved the psychosocial state of fearful children, and the mental health of those who have been victims of bullying.⁴ School function improved with distance learning and socialization may have increased using virtual connections to create a larger social group.⁵

However, children and adolescents who experience a prolonged state of physical isolation may look for alternative, somehow attractive or unconventional forms of socialization, available on the internet. Children may be exposed to the risks of unsupervised cyberspace exploration beyond the open web, which may lead them to areas that are usually not available to visitors. They may pass the gates of the “open” and “deep web” sections and enter into the dangerous “dark web” zones, which predominantly host unethical and criminal activities. In those shadowy corners of the worldwide web, there exist dangers ranging from identity theft and the drug trade to suicide chat rooms and child pornography.⁶

This commentary, authored by European Paediatric Association/Union of National European Paediatric Societies and Associations members of the working group on social pediatrics, briefly discusses the features of the dark web and its implications for children and adolescents. Our aim is to raise awareness of pediatricians and families on the growing risk of child exploitation through the web at a time when vulnerable young people face home lockdowns with potential abusers intruding on their privacy.

Definition of Open, Deep, and Dark Web

The open or surface web is the portion of the world wide web (www.) that is readily accessible to the public and searchable with conventional web search engines that includes the network of indexed websites. The surface web is estimated to include between 1% and 5% of the entire web, and the standard search engines are able to reach approximately 0.03% of the information that is available; much of the rest remains submerged in areas of the web not openly accessible.^{7,8} These areas are identified as the deep web and the dark web, terms that are frequently abused and confused and usually associated with criminal activities. The term *deep web* describes the series of largely legitimate contents present on the web that are not indexed by common search engines and include pages on the internet that cannot be found by performing a search using the available internet platforms (eg, Google, Yahoo, Bing). Users need to know the exact address of the site to gain access. Another way to access a deep web site is to click on a link available after entering the deep web or by using an access code. This is true of private sections developed by public and private organizations, including banks, government, and academic institutions, which typically grant their members access to confidential databases, archives, or professional private chats.

The term *dark web* indicates the set of publicly accessible contents that are hosted on websites whose IP address is hidden, but can be accessed by using dedicated software, as long as they know the address (Table I; available at www.jpeds.com). Elements belonging to the dark web are private content exchanged between users within closed computer networks, which are internal structures defined as darknets. Although not all content in the dark web is illegal, more than 60% of the sites on the dark web host illicit material.⁹

From the ¹European Paediatric Association, Union of National European Paediatric Societies and Associations (EPA/UNEPSA), Berlin, Germany; ²Italian Society of Pediatrics, Rome, Italy; ³Medical School of Split, University Hospital of Split, Split, Croatia; ⁴Department of Biomedical Sciences, University of Foggia, Foggia, Italy; ⁵University of Istanbul, Istanbul University Cerrahpaşa, Medical Faculty, Istanbul, Turkey; ⁶University of Medicine and Pharmacy Iuliu Hațieganu, Cluj-Napoca, Romania; ⁷Russian Academy of Pediatrics, Moscow, Russia; and ⁸Department of Pediatrics, Scientific Institute “Casa Sollievo della Sofferenza”, Foggia, Italy

The authors declare no conflicts of interest.

0022-3476/\$ - see front matter. © 2020 Elsevier Inc. All rights reserved.
<https://doi.org/10.1016/j.jpeds.2020.10.008>

COVID-19 Novel coronavirus disease 2019

The Accessibility to the Dark Web and Its Risks for Children

The most popular way to access the dark web is via dedicated browsers, such as The Onion Router, which has more than 2.5 million users each day.¹⁰ Other browsers enabling access to the dark web exist, such as I2P and Tails.¹¹

The Onion Router, launched in 2002, uses the principle of onion routing, developed at the United States Naval Research Laboratory in the 1990s, in which the user data are first encrypted and then transferred through different relays present in the network.¹² Thus, it creates multilayered encryption (like layers of an onion) and keeps the identity of the user safe. A single encryption layer is decrypted at each successive Onion Router relay, and the remaining data are forwarded to any random relay until it reaches its destination server. Therefore, the last Onion Router node-exit relay appears to the destination server as the origin of the data, making it difficult to trace the identity of the user or the server by any surveillance system.

It is technically not illegal to access the dark web through the Onion Router browser. The US government and military use these types of shielded communication to share information and protect their agents and informants. It is also perceived as a right to privacy and encryption, as well as a safe space for journalists and whistleblowers. However, the danger of the dark web comes when users are technically naive and/or not careful with the contents. Children and adolescents in particular may be unprepared and easily fall victim to hackers, give away personal information without intention, or slip into illegal activity. There is also the potential for psychological damage because the large number of illegal activities available in the dark web includes a considerable amount of disturbing material.¹³

During the months of the COVID-19 pandemic, education and other important socializing activities for children and adolescents have been productively supported by the use of the web. However, at the same time, this has exposed them to clandestine groups, such as pedophile and other illegal networks, that have seen the increased use of the web as an opportunity to intensify their activities to approach unsupervised minors. Increased risks for children and adolescents reaching the dark web during the COVID-19 pandemic are multiple¹⁴ and include online grooming for various purposes, introduction to suicide, and child pornography.⁷ Child pornographic content is shared among offenders who redistribute them online through the dark web, causing life-long harm to the victims.⁷

Protecting Children from Dark Web Hazards during COVID-19

Staying confined as a family should be perceived as an important opportunity for parents to turn a negative occurrence into a positive experience.¹⁵ This situation offers an opportu-

nity for parents and families to interact constructively with their children, stay positive, manage stress, and support them in filling their time with meaningful and healthy activities. The majority of school activities, free time, and social interactions, as well as time with friends and family outside the typical “nuclear family” have moved online during the COVID-19 crisis. Parents and caregivers shift their expectations and plan around screen time to modulate what is necessary for schoolwork. They can expand the time schedules of children to include additional online time for educational leisure activities, like virtual tours of zoos or museums or connecting with classmates via online educational activities, including games and networks. Children could spend their time on the web with positive activities and learn about cooperation and kindness. A large number of educational resources, platforms, and technologies have been created that provide parents and educators with a considerable selection that must be supported by an increased competence and familiarity with the technology.^{16,17} In this new social context, pediatricians can play a central role in advising families on how to best manage the time of their children and protect them from the risks of an uncontrolled increased usage of web resources during the pandemic.^{18,19}

Conclusions

The current global health crisis has brought unprecedented changes in people’s interactions and routines owing to social distancing and confinement. In several countries, only essential businesses were functioning normally, and many adults in institutions and companies worked from home and children followed their school lessons online. Families, communities, businesses, and governments were forced to become familiar and progressively depend on the internet, digital technology, and social media to retain a semblance of normalcy, continue their daily activities, and expand their use for entertainment. This new social setting has created unique challenges and opportunities but has also exposed the most vulnerable part of the population—children and adolescents—to the unprecedented risks of the infosphere, which include uncontrolled access in dark areas of the web.²⁰ Governments are working to develop measures that aim at strengthening national prevention, response, and support services^{21,22} (Table II; available at www.jpeds.com). Pediatricians and educational institutions can and should play a central role in directly supervising and managing the social side effects of the COVID-19 pandemic in their communities.^{23,24} ■

Reprint requests: Massimo Pettoello-Mantovani, MD, PhD, Department of Pediatrics, Scientific Institute “Casa Sollievo della Sofferenza”, University of Foggia, Foggia, Italy. E-mail: mpm@unifg.it

References available at www.jpeds.com

References

1. Somekh I, Somech R, Pettoello-Mantovani M, Somekh E. Changes in routine pediatric practice in light of Coronavirus 2019 (COVID-19). *J Pediatr* 2020;224:190-3.
2. Blanchard L, Gurka MJ, Blackman JA. Emotional, developmental, and behavioral health of American children and their families: a report from the 2003 National Survey of Children's Health. *Pediatrics* 2006;117:e1202-12.
3. Jiao WY, Wang LN, Liu J, Fang SF, Jiao FY, Pettoello-Mantovani M, et al. Behavioral and emotional disorders in children during the COVID-19 epidemic. *J Pediatr* 2020;221:264-6.e1.
4. Loades ME, Chatburn E, Higson-Sweeney N, Reynolds S, Shafran R, Brigden A, et al. Rapid systematic review: the impact of social isolation and loneliness on the mental health of children and adolescents in the context of COVID-19. *J Am Acad Child Adolesc Psychiatry* 2020;59(11):1218-39.e3.
5. Bennett SD, Cuijpers P, Ebert DD, McKenzie Smith M, Coughtrey AE, Heyman I, et al. Practitioner review: unguided and guided self-help interventions for common mental health disorders in children and adolescents: a systematic review and meta-analysis. *J Child Psychol Psychiatry* 2019;60:828-47.
6. The United States Department of Justice. Criminal Division. Child Exploitation and Obscenity Section (CEOS). www.justice.gov/criminal-ceos/child-pornography. Accessed October 2, 2020.
7. da Cunha BR, MacCarron P, Passold JF, Dos Santos LW Jr, Oliveira KA, Gleeson JP. Assessing police topological efficiency in a major sting operation on the dark web. *Sci Rep* 2020;10:73.
8. The Royal Institute of International Affairs. Global Commission on Internet Governance. The impact of the dark web on internet governance and cyber security. Paper Series: No. 6. Ed. Centre for International Governance Innovation and Chatham House, London; 2015.
9. Spitters M, Verbruggen S, van Staalduinen M. Towards a comprehensive insight into the thematic organization of the Tor hidden services. In: Paper presented at 2014 IEEE Joint Intelligence and Security Informatics Conference. September 24-26; 2014. p. 220-3. The Hague, the Netherlands.
10. Moore D, Rid T. Cryptopolitik and the darknet. *Survival* 2016;58:7-38.
11. Tamsoweb Organization. Seven dark web browsers for deep web browsing in 2020. <https://tamsoweb.blogspot.com/2019/11/7-dark-web-browsers-for-deep-web.html>. Accessed October 3, 2020.
12. Reed MG, Syverson PF, Goldschlag DM. Anonymous connections and onion routing. *IEEE J Sel Areas Commun* 1998;16:482-94.
13. Ferrara P, Caporale O, Cutrona C, Sbordonone A, Amato M, Spina G, et al. Femicide and murdered women's children: which future for these children orphans of a living parent? *Ital J Pediatr* 2015;41:68.
14. UNICEF. 17 April Report, Children at increased risk of harm online during global COVID-19 pandemic. UNICEF warns. www.unicef.org/albania/press-releases/children-increased-risk-harm-online-during-global-covid-19-pandemic-unicef-warns. Accessed October 3, 2020.
15. Corsello G, Ferrara P, Chiamenti G, Nigri L, Campanozzi A, Pettoello-Mantovani M. The child health care system in Italy. *J Pediatr* 2016;177S:S116-26.
16. Pan European Game Control. Parental control tools. <https://pegi.info/parental-controls>. Accessed October 4, 2020.
17. Common Sense Media. Reviews for what your kids want to watch (before they watch it). www.commonsensemedia.org/. Accessed October 4, 2020.
18. Ehrich JH, Kerbl R, Pettoello-Mantovani M, Lenton S. Opening the debate on pediatric subspecialties and specialist centers: opportunities for better care or risks of care fragmentation? *J Pediatr* 2015;167:1177-8.e2.
19. Ferrara P, Corsello G, Ianniello F, Sbordonone A, Ehrich J, Giardino I, et al. Internet addiction: starting the debate on health and well-being of children overexposed to digital media. *J Pediatr* 2017;191:280-1.e1.
20. Floridi L. *The fourth revolution: How the infosphere is changing human reality*. Oxford: Oxford University Press; 2014.
21. Council of Europe. Protecting and empowering children during the Covid-19 pandemic. <https://www.coe.int/en/web/children/covid-19>. Accessed October 4, 2020.
22. USAGov. U.S. Government Services and Information. Government Response to Coronavirus, COVID-19. www.usa.gov/coronavirus. Accessed October 4, 2020.
23. McIntosh ED, Janda J, Ehrich JH, Pettoello-Mantovani M, Somekh E. Vaccine hesitancy and refusal. *J Pediatr* 2016;175:248-9.e1.
24. Pettoello-Mantovani M, Pop TL, Mestrovic J, Ferrara P, Giardino I, Carrasco-Sanz A, et al. Fostering resilience in children: the essential role of healthcare professionals and families. *J Pediatr* 2019;205:298-9.e1.

Table I. Different areas of the web

Areas	Description
Open web	The publicly visible part of the internet that can be accessed through standard search engines; includes indexed websites. Accessible by using conventional legal search engines: Google, Yahoo, Reddit, CNN.com , and others
Deep web	The internet that is generally hidden from public view. The deep web is not accessed via standard search engines. Much of its content is ordinary and legitimate. Organizations have websites that can only be read by authorized employees or clients, with their information password protected. One example is the medical history of an individual, which can be accessed by authorized persons. Type of contents accessible: Academic databases, medical records, financial records, legal documents, selected scientific reports, selected government reports, subscription only information, organizations-specific repositories.
Dark web	Generally accessible using dedicated software. This includes The Onion Router, I2P, and other software programs including Subgraph OS, Tails, Opera, Whonix, Firefox, and Waterfox. The Onion Router provides anonymizing software that can be accessed via a Google search and then downloaded free of charge. The Onion Router itself is not the dark web, but is a way to browse both the open and dark web, without being able to identify the user or track its activity. Type of contents accessible: Drug trafficking, pornography, sexual soliciting and abuse activities, assassination market, unlicensed guns traffic, fake IDs, terrorism, gambling, hacking tools, stolen credit cards, political protest and violence instigation and other illegal activities.

Table II. Prevention, response, and social support services needed during the COVID-19 pandemic

Monitor how restricted movement and lockdowns may exacerbate offline and online forms of violence and advise legislators based on latest data and existing models. Enforce existing regulations and strengthen law enforcement to help monitor activities and respond to increased online risks. Allot sufficient resources to bolster, train, and equip core child protection workers qualified to keep children safe throughout the pandemic. Activate center-based supports and home visits for those severely affected or adapt and deliver social services virtually.

Train health, education, and social service workers on the impact that COVID-19 may have on child well-being, including increased online risks. Providing front line mental health/psychosocial support with skills to talk to children about COVID-19 and address their anxiety and insecurity. Identify vulnerable children, including those separated, disabled, or in conflict settings, and those who may have lost parents or primary caregivers to the pandemic.

Raise awareness among government departments of the potential increased online risks to children during the pandemic. Develop a coordinated institutional approach. Ensure that social service providers, schools, parents, caregivers, and children are aware of local reporting mechanisms, including the support numbers of local helplines and hotlines. In the absence of these services, local helplines and hotlines should be developed to support children in distress. Nationally based Child Helpline should be also developed. Families and carers should be instructed to contact the police when imminent danger is perceived. (Major international reporting networks include INHOPE Hotlines and IWF portals).

Promote educational initiatives on child online safety, to complement efforts to connect children to resources for online learning, socialization, and play. This should include raising awareness about online risks and resources, using media and other communications channels to spread key messages.