Identity Theft and Exposure to Harmful Content—Internet Risks for Teenagers

Limor Ezioni

Children and teenagers are part of a weak and vulnerable population group. Their internet activity exposes them to two substantial risks: exposure to harmful content and identity theft and its use for slander and bullying. This article examines the characteristics and scope of the problem. It proposes ways of minimizing the damage that these risks pose to children and teenagers, while dealing with the existing privacy restrictions.

Keywords: Internet, internet bullying, identity theft, pornography, children, teenagers

Introduction

Technological development has many advantages but also more than a few disadvantages, ranging from society's absolute dependence on technology, which causes exposure to the shutdown of services and information leaks due to cyberattacks, to the possibility of financial fraud, and physical damage to critical processes. Despite the severity of these disadvantages, children and teenagers continue to be exposed to them, particularly to two dangerous phenomena: identity theft through the internet and exposure to harmful content.

Identity theft through the internet has become one of the main concerns in cyberspace, with teenagers being one of the most vulnerable risk groups.

Adv. Dr. Limor Ezioni, dean of law at the Academic College for Law and Science (Sha'arei Mishpat), is currently writing a book about cyber law and regulation. She provides professional legal counsel and representation in both criminal and civil law for teenagers and adults.

Identity theft and the use of false identities are, in many cases, aimed at slander and shaming campaigns, which are liable to have severe consequences for the teenagers whose identities were stolen, by affecting their future and their development. In addition to identity theft, children and teenagers are exposed to harmful content. Prolonged exposure to such content affects their social development, augments their violent inclinations, and is also liable to lead to the formation of distorted models of interpersonal relationships.

The information revolution, particularly digital communications on the internet, is based on leveling the differences between societies and cultures for the lofty purposes of educational, economic, and social development. The freedom to use the internet was a phenomenon that presumably promised social and economic development even in the most inaccessible places. Globalization ensued, in which information, knowledge, intellectual property, and capital were transferred quickly and easily between different countries. At the same time, the information revolution caused people to be dependent on the ability to transmit large volumes of various types of information at high speeds on diverse platforms.[1] The focus on—and some would say the addiction to—the ability to share information has repressed the need for controls over the content of the information. Under the banner of "net neutrality," the need and ability to exercise any control of content whatsoever has been suppressed. In theory, justice was on the side of the advocates of freedom who claimed and understood that this approach was likely to have desirable social effects even beyond the immediate benefits, such as those based on the desired externalities of net neutrality. In practice, however, the conditions justifying fair use of the internet do not exist in a place where the net neutrality model is in effect.[2] As a result, an unconstrained space has been created that allows the transmission of harmful content of any type whatsoever to any user.

In the absence of any control mechanisms by both the party distributing the information and the party receiving it, the internet has become a theater of lawlessness that victimizes mainly the weak. Teenagers and children are exposed to extremely harmful content, even against their will. The situation

1 M. F. Mahmood and N. Hussin, "Information in Conversion Era: Impact and Influence from 4th Industrial Revolution," *International Journal of Academic Research in Business and Social Sciences* 8, no. 9 (October 13, 2018): 320–328.

2 Keith N. Hylton, "Law, Social Welfare, and Net Neutrality," *Review of Industrial Organization* 50, no. 4 (June 2017): 417–429.

has become intolerable; in many cases, even an internet search for innocent content leads to pop-up windows with pornographic content inviting the user to enter a pornographic website. The inconceivable availability of this content makes it difficult for parents to cope with the phenomenon. Thus, without having any system of control, children and teenagers have become unwilling consumers of pornography.

As a weak and vulnerable population group, children and teenagers are subject to rapid manipulation and influence, creating a broad platform for another harmful use of the internet. The development of social networks has brought many benefits: Use of the internet can help create a widespread network of connections and colleagues with shared interests; the ability to distribute information on a large scale in a short period of time; and also the ability to market business services and products equally to everyone on a scale once only available to corporations with abundant resources. At the same time, the extensive use of the social networks has also caused problems: Identity theft, especially of teenagers, has become an affliction. The methods used to steal identities are highly developed and sophisticated, including penetrating an existing account, taking it over, and using it, or creating a fabricated account in the victim's name and connecting with his or her network of acquaintances. When teenagers are involved, the purpose is the same in most cases: posting and distributing malicious content in order to hurt the account's owner.

The key question arising in this context is whether ways can be found to minimize the two main risks for teenagers on the internet: the exposure to harmful content and identity theft, while also maintaining a balance between the need for freedom of information and privacy— the core of liberal democracy—and the need for better protection of children and teenagers.

Blocking Children and Teenagers from Harmful Content on the Internet

The idea that children have the right to protection when they are surfing the internet is a basic principle in a world that has an assortment of laws aimed at preventing abuse and exploitation on the internet. Nonetheless, the behavior of the content providers and the difficulty in instilling normative

surfing habits for children stretch the boundaries of protection and confront legislators around the world with new dilemmas.[3]

According to an article on the Global Kids Online blog,[4] the efforts to make the internet a safer place for children require creating a balance between developing digital skills among youth and devising a general policy for safeguarding the rights of children. The article showed that children begin using the internet at a young age and spend a great deal of time online. As a result, the likelihood of their being exposed to harmful content at an extremely young age has increased. The prevalence of smartphones exacerbates the problem and makes exposure possible at all hours of the day and night, including in situations where no parent or responsible adult is present. Moderate and judicious use of the internet can benefit children, but extensive and unrestrained use of it is liable to generate long-term negative effects on them. As children who lack skills in using the internet are apt to encounter educational and social difficulties, parents' attempts to restrict their use of the internet are liable to provide a doubled-edge sword and result in a destructive response. According to a survey conducted by the blog, 14 to 36 percent of youth between the ages of nine and seventeen have had a harmful experience on the internet.[5]

The United Kingdom has attempted to deal with this problem by a decision to create a mechanism for verifying the age to prevent youth from surfing on pornography websites. The British Board of Film Classification is responsible for implementing this mechanism. This approach is based on forcing broadband internet providers and cellular networks operators to block websites and applications that do not include means of identification for verifying the surfer's age. It is unclear, however, how an age verification system will be operated and what can be done to prevent it from being

3 Monica Bulger, Patrick Burton, Brian O'Neill, and Elisabeth Staksrud, "Where Policy and Practice Collide: Comparing United States, South African, and European Union Approaches to Protecting Children Online," *New Media and Society* 19, no. 5 (January 16, 2017): 750–764.

4 "Making the Internet Safer for Children: The Global Evidence," *Global Kids Online*, February 6, 2018.

5 Ibid.

bypassed without infringing on the surfers' privacy and without sharing personal particulars with providers of pornographic and harmful content.[6]

One of the operators of major pornographic websites, such as YouPorn, PornHub, and RedTube, proposed using a combination of a credit card, an SMS message, and passport or driver's license to verify the user's date of birth.[7] It appears that this method generates especially difficult privacy problems. In any case, as this essay was written, implementation of this mechanism had been postponed until a future date.[8]

Israel has also been dealing with this matter, including an attempt to enact a law blocking harmful content. A discussion has taken place for several months about ways of blocking teenagers' access to harmful content on the internet. A joint subcommittee of the Knesset Science and Technology Committee and the Knesset House Committee approved a bill along these lines in December 2018. The wording of the law allows internet subscribers to choose whether they wish to block their access to harmful content. Discussion of the bill, referred to as the "Pornography bill," focused mainly on two aspects. The first was the need to define the harmful content to be blocked, or more generally, the difficulty in regulating content on the internet, an area in which the state usually does not intervene. The second concerned infringement of privacy. The bill has been changed several times, but in general, it asks internet providers to send notices to subscribers, who will have to inform the providers whether they wish to activate a service that blocks harmful content.

In the discussion of the legislation, several points were raised, including the necessity of not treating all children in the 6–18 age range the same way, because it can be assumed that the damage caused by exposure to harmful content is not the same in every age group. The need to impose responsibility on providers of pornographic content, as well as on internet providers, also was discussed, including the suggestion that they place a warning panel with an age restriction across their website. At the same time, maintaining an open internet infrastructure free from censorship in order to protect the public's freedom was considered. It was also proposed to allow users who

6 Mark Jackson, "Age Verification and UK ISP Internet Porn Ban Quietly Delayed," *ISP News*, March 12, 2018.

7 Tom Allen, "PornHub's Age ID System Will Require Punters to Hand Over Their Date of Birth," *Inquirer*, February 1, 2018.

8 Jackson, "Age Verification and UK ISP Internet Porn Ban Quietly Delayed."

do not respond to the service provider's request that they agree to a content filter to continue receiving service without the filter being forced on them without their consent.[9]

The legislation, which requires companies providing internet services to respond to questions about blocking, will, in practice, create records making it possible to know which subscribers requested blocking and which said they did not want it. While the bill forbids the internet providers from using this information, the very existence of the record is liable to constitute a severe invasion of a person's privacy, especially when unauthorized parties could obtain the content of the records as a result of a malfunction or theft.

It is difficult to set clear and precise criteria for filtering material on the internet. As early as 1964, in a trial concerning freedom of speech, US Supreme Court Justice Potter Stewart said that he could not define pornography but was able to identify it by sight ("I know it when I see it"). Despite the difficulty, the large internet companies, such as Facebook, YouTube, and other internet platforms already filter content. It can be assumed that a public committee that will be formed will propose guidelines for facilitating the filtering of harmful content. These guidelines can be improved over time.

The main problem with the pornography bill remains that of privacy. Here technology that was developed for targeted advertising can help. The internet has materially changed the advertising market by facilitating advertising that focuses on predefined target markets. The major internet companies gather a great deal of information about internet users, including variables such as age, gender, language, location, family status, number of children, and so forth. This information is collected without the user's knowledge and stored for the purpose of building a profile that facilitates targeted advertising. For example, advertising for expensive school bags is published now only for parents with children of a specific age group living in certain areas, and who meet a particular income criterion. This technology is also used to conduct political campaigns before an election. In this way, specific messages can be directed to targeted audiences in every cross-section and segment.

The use of such technology for filtering purposes can be positive for children and teenagers. Using this technology, children in every age bracket can be identified on the internet, making it possible to immediately block

9 Gideon Allon, "'Porno Bill' Approved by Ministerial Legislative Committee," *Israel Hayom*, December 12, 2018.

content according to the users' age. The same method can also be used to establish filtering levels according to age group. For example, one filter can be used for the 5–9 age bracket, another for the 9–12 age bracket, and so on, instead of applying a general filter for all youth. This method will also prevent infringing on the users' privacy, because the filter will identify the user's group by its defined criteria and not the actual user.

No technology, however, is free from error. It can be assumed that cases will occur in which children are exposed to harmful content after this technology is applied, or in which adults will be blocked from such content. Experience from the advertising industry shows, however, that these exceptions are confined to a small number of cases. The use of the proposed technology will, therefore, substantially reduce the scope of the problem and facilitate a balance between the breach of privacy and other freedoms and the need to protect children and teenagers and allow them healthy and proper development.

Theft of Teenagers' Identities on the Internet

"Hi, Noa, we don't know each other, but someone is using your picture and has created a profile on Facebook." This was a notice received by Noa Benosh.[10] That is how Noa realized that an imposter was using her photographs on a fictitious Facebook account. Yariv (a pseudonym), a tenth-grade student, woke up one morning to discover that posts, which he had not written and pictures he did not know, had been posted on his Instagram account; someone apparently had broken into his account and posted malicious and humiliating content on it. He found himself trying to tell his friends in order to minimize the damage but with little success. Some were quick to respond, and some took advantage of the event to magnify the damage. These kinds of incidents are occurring at an increasing pace.

Social networks have become very popular. According to a report by Global Social Media Research, as of 2018, the number of social networks users worldwide was 3.2 billion, and this figure is growing at a rate of 13 percent a year.[11] The vast majority of youth have accounts on social

10 Noa Benosh, "A Person Suddenly Discovers that His Identity on Tinder Has Been Stolen," *Ynet*, January 12, 2018.

11 Dave Chaffey, "Global Social Media Research Summary 2018," *Smart Insights*, November 23, 2018.

networks, and 45 percent of them are almost constantly connected.[12] These figures are stunning in themselves. In addition to their popularity among youth, social media is also fertile ground for bullying as well as illegal and criminal activity. The main crimes on the internet, which are very common, can be divided into a number of categories: bullying and harassment, online threats, and identity theft for similar purposes. Table 1 below illustrates the scope of internet bullying in various countries (not including Israel), some of which results from identity theft and shaming campaigns and refers (in percentages) to parents who reported that their children had been exposed to bullying on the internet.[13]

Table 1. Percentage of Parents Reporting that Their Children Have Been Exposed to Cyber Bullying

Country	2011	2016	2018
India	32	32	37
Brazil	20	19	29
United States	15	34	26
Belgium	12	13	25
South Africa	10	25	26
Malaysia	–	–	23
Sweden	14	20	23
Canada	18	17	20
Turkey	5	14	20
Saudi Arabia	18	17	19
Australia	13	20	19
Mexico	8	20	18
United Kingdom	11	15	18
China	11	20	17

An analysis of the table shows the horrifying dimensions of the problem. The problem in Israel is presumably similar in scope as in other western countries (such as the United States, Sweden, and the United Kingdom).

12 Monica Anderson and Jingjing Jiang, "Teens, Social Media, & Technology 2018," *Pew Research Center, Internet and Technology*, May 31, 2018.

13 Sam Cook, "Cyberbullying Facts and Statistics for 2016–2018," *Comparitech*, November 12, 2018.

Youth make extensive use of the internet, but unfortunately, their judgment in response to the content posted on websites is extremely poor. They share many personal details without any control, including their full names, pictures, names of family members, telephone numbers, important dates, residential addresses, and so forth. All this constitutes a good platform for identity theft, which thieves can utilize to ostensibly make plausible posts. The level of security awareness among youth is also extremely low as they use unsecured wireless internet connections and usually employ the same passwords for different accounts. Many also share passwords not only with family members but also with friends.[14] The general impression among the public that youth are more aware than adults of the security problems on the internet is erroneous. In most cases, young people do not exercise basic internet hygiene, such as updating security measures and refraining from the disclosure of sensitive particulars on the internet. These phenomena make them easy prey for identity theft, both for the purpose of penetrating the social networks and for stealing identities of family members in order to commit fraud. A study conducted in the United States among 500 parents of children whose identity was stolen showed that the group with the highest risk of identity theft is the 12–17 age group (44 percent).[15]

What can be done about this problem? Identity theft and impersonation on the internet are a criminal offense in Israel under a number of laws. The Computers Law (1995) imposes a three-to-five-year prison term for one who "disrupts the proper operation of a computer or interferes with its use . . . deletes computer material alters it . . . performs an action with respect to information so it would result in the production of false information or false output . . . penetrates computer material located in a computer." The clause that is almost certainly relevant to the discussion here concerns an action resulting in false information or false output. In addition to this law is the Protection of Privacy Law (1981). Although this law concerns protecting a person's private information in databases, it is worthy to consider whether social media providers can be included in this definition. This would extend the responsibility of the major internet companies to the user's information,

14 Leigh, "Teenagers Are Easy Victims of Identity Theft," *Homeschooling Teen Magazine*, 2018.

15 Matt Tatham, "Survey: 12 Years Old is the Average Age of a Child Identity Theft Victim," *Experian*, August 26, 2018.

its security, and prevention of its use for fraud. Finally, the Prohibition of Defamation Law (1965) can be applied. Under this law, defamation is defined as something whose publication is liable "(1) to degrade a person (an individual or a corporation) before others or to make him the object of hatred, contempt, or ridicule; (2) to cause a person to be regarded with contempt for acts, conduct, or characteristics attributed to him; (3) to injure a person in his position, whether a public position or any other position, or in his business, occupation or profession; (4) to cause a person to be regarded with contempt because of his race, origin, religion, place of residence, age, gender, sexual inclination, or handicap." Impersonation on the internet and leaving malicious and humiliating posts can be subject to criminal charges and can also be considered a civil wrong entitling the victims to compensation.

It is difficult to determine how to reduce the exposure of young people to social networks, which sometimes amounts to an addiction. For this reason, in addition to relying on the law, other action should be taken. It is essential to teach young people how to behave on the internet, both in securing accounts and in selecting the content that they access, while helping them to realize the significance and consequences of sharing personal information on the internet. As it is impossible to completely eliminate the problem, in addition to these actions, it is also important to devote attention and provide assistance to the victims. A number of volunteer organizations have already begun moving in this direction.

The internet, social networks, and instant messaging applications create many positive opportunities to even out differences and provide equal opportunities. At the same time, however, the risks facing young people as a very vulnerable group are immense. We would be wise to create better and more sophisticated defense mechanisms for preventing attacks and bullying by impersonation. We should also demand that the major internet companies take more determined action to address these problems.

Conclusion

Children and teenagers are exposed to many internet risks and lack suitable tools for coping with them. This article analyzed two main risks: exposure of youth to harmful content and identity theft for purposes of humiliation, shaming, and slander. Various countries, including the State of Israel, have already begun taking steps in providing tools to minimize exposure of young

people to harmful content. The initial attempts, however, have encountered resistance from two main directions. The first is the argument that it is necessary to preserve net neutrality and avoid any censorship of internet content. The second is the difficulty in finding a mechanism that will prevent invasion of privacy. The mechanism proposed in this article can help solve the problem by blocking harmful content according to criteria of the internet users, as is already being done by the major internet companies in providing advertising services that target specific audiences.

Youth are not sufficiently aware of the possibility that their identity could be stolen and used for bullying purposes. For most of them, the risk of becoming a victim is usually intangible, and therefore they are unaware of the grave consequences posed by these incidents. Unfortunately, identity theft can destroy young people's ability to develop or critically injure them. It is advisable to adopt a multi-faceted solution to the problem of identity theft, by raising awareness among youth at risk, instilling suitable behavior on the internet, strictly enforcing the existing laws, and above all, aiding those injured by this affliction. This is only a start, however, as the damage suffered by young people on the internet can be significant. It is important and correct to expand the research around how to minimize and address this problem.