Children's Legal Rights Journal

Volume 37 | Issue 1 Article 7

2017

Statistically Speaking: The Numbers Behind Cybercrimes

Nana Otutua-Amoah

Statistically Speaking: The Numbers Behind Cybercrimes

By: Nana Otutua-Amoah

I. INTRODUCTION

Imagine trying to apply for a loan and being told, at the age of eighteen before even getting your first credit card, that you will not be able to secure a loan because of your bad credit. Imagine being a child, threatened and bullied online when you expect to feel safe. What would be your next steps and to whom would you go to for assistance? How would your parents or caretakers deal with these issues involving your online identity? Parents and caretakers continue to struggle with answering these questions as children continue to have an increased access to the Internet.

This article will briefly highlight the data and statistics behind cybercrimes committed against children and the information accessible to caretakers to ensure that their children's privacy is protected. Earlier this year, The Wall Street Journal confirmed that there has been an increase in the number of child victims of identity theft. The article narrated the experiences of a woman by the name of Ms. Betz-Hamilton, whose identity was stolen at the age of 11. She did not find out until she was 19 and in college, and the steps to repair her credit were numerous. According to the author, "data breaches exposing children's personal information online are becoming more common." As children's access to the Internet continues to grow, there are rising concerns about the potential for the victimization of children. To combat the rise in child identity theft, parents and caretakers should use protective measures to monitor their children's online activities.

II. DATA ABOUT INCREASED USAGE OF THE INTERNET

In 2015, the United Nation's Office on Drugs and Crime published an open source research and study on information and communications technologies and the abuse and exploitation of children. The report on this study focused on "child sexual abuse material, commercial sexual exploitation of children, cyberenticement, solicitation and grooming; cyberbullying, cyberharassment and cyberstalking; and exposure to harmful content." According to the Child Exploitation and Online Protection Centre (CEOP), "78[%] of households in developed countries had access to the [I]nternet" by the end of 2013. Across the world, global data shows that children's routine use of the Internet is expanding in regards to the number of hours children spend online and the number of children going online. For example, "25[%] of children in the United States under the age of six are online regularly and nearly 60[%] of children between the ages of six and nine years use the Internet every day." While this United State's statistic is significant, the global trend shows that children from all over the world are increasingly having access to the Internet and using the Internet on a daily basis.

III. ROLE OF PARENTS, CHILDREN, AND PERPETRATORS

As children's access to the Internet continues to increase, they become more vulnerable in the digital space. Some children may not fully understand the repercussions and dangers of sharing their personal information online. After all, this is the first generation to be born into the "digital world," according to Sociology scholar, Eszter Hargittai. Hargittai notes that children born after the onset of the Internet are more likely to incorporate various aspects of the digital sphere into their childhood. To make the problem worse, it is a challenge for parents and

caretakers to protect their children's online presence. Today, children use the Internet in schools and sometimes on their phones, away from parental supervision. Parents usually do not have the advanced technological understanding to protect their children from harming themselves online.

Advancement in technology has eased criminal collaboration and communication "with regard to the commission of acts of child abuse and exploitation." Thieves and sexual predators are using the Internet and online services to further the commission of typical abuse and exploitation acts that are committed against children. In addition, the advancement in technology has also made it easier for identity thieves and sexual predators to take advantage of children who are not careful about divulging their personal information or interacting with strangers.

On the other hand, technology has also brought about new forms of child abuse and exploitation. For example, the Comprehensive Study on Cybercrime divides cybercrime into three different categories: "acts against the confidentiality, integrity and availability of computer data or systems, computer related acts for personal or financial gain, or harm and computer content-related acts." The study indicated that children were exposed to pornographic content when they browsed the Internet. According to reported data, more than half of the pornographic images that children viewed, they did so accidently. Specifically, a 2006 survey found that out of 42% of children between the ages of ten and seventeen, more than half indicated that the exposure was unwanted. The results of the survey also indicated that children who have been harassed for sexual encounters online were more likely to experience unwanted exposure to harmful content. Although it is difficult for parents to provide supervision at all time, parents must take the necessary steps to ensure that their children are safe and secure online.

IV. GENDER AND AGE IN CHILD SEXUAL ABUSE

The National Juvenile Online Victimization Study showed that 83% of child sexual abuse materials contained images of prepubescent children. Statistics show that girls are more likely to be victims of online abuse and exploitation. According to the United Nations Office on Drugs and Crime, there was an estimated 70% increase of child sexual abuse material focused on girls under the age of 10. However, this is starting to change, as demonstrated by a recent sample of collected sexual abuse images wherein 76% of the pictures were of girls, 10% boys and 10% both genders. All the same, girls have a higher likelihood of being victims of cyberbullying than boys, according to a survey conducted by Microsoft. Girls are also exposed to a higher proportion of harmful content in relation to child sexual abuse material and explicit material sent by perpetrators. Lesbian, gay, bisexual, and transgender youth tend to experience cyberbullying at a higher degree than other youth. According to a recent United States research, over 50 percent of youth who identified as LGTBQ reported being victim of cyberbullying. In general, girls and LGTBQ children are at a higher risk of being victims of online child sexual abuse.

V. CYBERTHEFT DATA

Cyber thieves target children because it is easy to use their identities to the thieves' benefit. Children are often targeted for bank account, credit card and government benefit fraud. In order to commit fraud, a criminal only needs the child's social security number so the perpetrator is often someone close to the child. For instance, the Industry Trade Advisory Center (ITAC) survey found that 27% of identity thefts in the U.S. committed against children, are committed

by people that the children know outside of their parents, and the other percentage of identity theft is from information from forms that a parent filled out about their child.

Other information needed to commit identity theft can come from schools and hospitals that store children's personal information. According to the National Cyber Security Alliance, 1 in 5 households have been notified by their child's school about a data breach which exposed their child's private information. This shows that not only is it dangerous for children to use the Internet because of the heightened risk of exposure to identity theft, but institutions that collect children's information can also possibly breach that data. In an effort to combat this problem, the government initially stepped in and passed the Children's Online Privacy Protection Act (COPPA) rule in April 2000. The rule sets out certain requirements for website operators in an effort to allow parents to control information shared about their children. According to the Federal Trade Commission, one requirement is that each website operator will need parental consent before collecting any personal information from children. Parents are also given the right to have any information found about their children deleted. While the COPPA rule was a first move towards protecting children's privacy, many people felt it was inadequate and ineffective. In 2012, the COPPA rule was amended as a response to children's increased usage of the Internet. The amended rule restricts more website operators from collecting personal information about children's online identity. In March 2015, the Protect Children from Identity Theft Act was introduced in Congress to allow parents to freeze their children's credit files. If this bill is passed, parents in any state will be able to protect their children's identity by having the ability to protect their child's personal information.

VI. PROPOSAL

In regards to child online sexual abuse, parents should use parental controls to filter and block any aspect of unwanted online content. Parents are able to record all contents entered into the home computer or laptop with a keystroke recoding software, which provides parents with the ability to monitor their child's online activities. Also, parents should pay attention to the websites their children use and should flag any inappropriate website for a follow up by an evaluator or law enforcement agency. Parents can also use hotlines – specifically the Online Child Sexual Abuse (OCSARP) – to report any suspected activities. Ultimately, it is the parents' responsibility to educate their child first about the various risks associated with using information and communication technology.

In reference to child identity theft, parents have been warned to be vigilant and to look through any mail that their children receive. Also, parents have been informed to take action whenever they are informed of a data breach. Parents should initiate a free credit monitoring for their child and contact credit-reporting companies to see if there is a credit report in their child's name. In addition, if the parent lives in one of the 22 states that allow parents and legal guardians to freeze a minor's credit, the parent should do so to prohibit cyber thieves from misusing their child's credit. The Internet is a digital platform with a plethora of educational, recreational, and social advantages for children. While parents have the ultimate responsibility, the Government needs to step in with laws protecting children. A child should not have to endure the dangers of being a victim of cybercrimes and it's the responsibility of federal laws, state laws and regulations, as well as caretakers, to ensure that children will never have to imagine themselves in such a scenario.

Sources

Brent Singer, *What is Child Identity Theft,* PARENTS (2013), http://www.parents.com/kids/safety/tips/what-is-child-identity-theft.

ENOUGH IS ENOUGH INTERNET SAFETY STATISTICS, http://enough.org/stats_internet_safety (last visited Nov. 11, 2016).

Eszter Hargittai, *Digital Na(t)ives? Variation in Internet Skills and Uses among Members of the "Net Generation,"* 80 SOC. INQUIRY 92 (2010), http://www.webuse.org/pdf/Hargittai-DigitalNativesSI2010.pdf.

FTC Seeks Public Comment on Riyo Proposal for Parental Verification Method Under COPPA l Rule, FEDERAL TRADE COMMISSION (2015), https://www.ftc.gov/news-events/press-releases/2015/07/ftc-seeks-public-comment-riyo-proposal-parental-verification.

Heather Morton, *Identity thieves are targeting children who may not even discover they've had their personal information stolen for several years, 40* STATE LEGISLATURES MAGAZINE NO. 6 (June 2014), http://www.ncsl.org/research/civil-and-criminal-justice/identity-theft-strikes-young.aspx.

Heather Morton, *Consumer Report Security Freeze State Laws,* NATIONAL CONFERENCE OF STATE LEGISLATURES (March 2016), http://www.ncsl.org/research/financial-services-and-commerce/consumer-report-security-freeze-state-statutes.aspx.

ITRC FACT SHEET 120: IDENTITY THEFT AND CHILDREN, http://www.idtheftcenter.org/Fact-Sheets/fs-120.html (last visited Nov. 11, 2016).

Joshua Warmund, *Can COPPA work? An Analysis of the Parental Consent Measures in the Children's Online Privacy Protection Act,* 11 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 189, (2000).

Priya Anand, *Cyberthieves Have a New Target Children,* THE WALLSTREET JOURNAL, Jan. 24, 2016, http://www.wsj.com/articles/cyberthieves-have-a-new-target-children-1454295685?mg=id-wsj#livefyre-comment.

Protect Children from Theft Act of 2015, H.R. 1703, 114th Cong. §605(c) (2015).

UNITED NATIONS OFFICE ON DRUGS AND CRIME, STUDY ON THE EFFECTS OF NEW INFORMATION TECHNOLGOIES ON THE ABUSE AND EXPLOITATION OF CHILDREN (2015), http://www.unodc.org/documents/organized-crime/cybercrime/Study_on_the_Effects.pdf (last visited Nov. 11, 2016).