Deanna Kirby

George Mason University

IT 103-004

February 26, 2013

IT 103 Research Paper: Smartphone Internet Safety for Children

"By placing this statement on my webpage, I certify that I have read and understand the GMU Honor Code on http://oai.gmu.edu/honor-code/ . I am fully aware of the following sections of the Honor Code: Extent of the Honor Code, Responsibility of the Student and Penalty. In addition, I have received permission from the copyright holder for any copyrighted material that is displayed on my site. This includes quoting extensive amounts of text, any material copied directly from a web page and graphics/pictures that are copyrighted. This project or subject material has not been used in another class by me or any other student. Finally, I certify that this site is not for commercial purposes, which is a violation of the George Mason Responsible Use of Computing (RUC) Policy posted on http://universitypolicy.gmu.edu/1301gen.html web site."

Smartphone Internet Safety for Children

When talking about smartphone security, many people think about physical phone security – how to keep smartphones from getting lost, stolen or damaged. Since smartphones can be expensive, the physical condition of the phone may be first priority for owners rather than the risks associated with using the Internet on the smartphone. One purpose of this essay is to show some of the dangers that children under 18 can come across when connecting to the Internet using smartphones, including malware being downloaded to the phone, viewing of inappropriate websites, and personal information being passed onto third parties. The main concern for parents and guardians is the very nature of the smartphone: it is easy to hide, and difficult for parents to monitor. Another purpose of this essay is to explore ways that parents can monitor smartphone usage and alleviate their concerns regarding their child's safety.

New Technology: Smartphones

Smartphones are phones that have extended capabilities that go beyond making phone calls. Users can download "apps," short for "applications," which are installed to the smartphone and used for various purposes; some of the most popular apps are for games, weather, maps, and social networking (Nielsen Company, 2010). According to an FTC study, there are a large number of apps on the market – the Android and Apple markets combined have approximately 880,000 apps for purchase or download (Poss & Hasty, 2012, p. 1). Apps usually have access to information about the phone and user – "…the user's precise [geographical location], phone number, list of contacts, call logs, unique device identifiers…" – and this information can be passed on to third parties, although sometimes it may not be clear to a user that the app is even

collecting such information, if there is no disclosure or the user does not read the disclosure (Poss & Hasty, 2012, p.1).

There is evidence that children are learning how to use smartphones at young ages. A study from software company AVG found that children are better at using technology than they are at basic life skills; for example, "More children aged 2-5 can play with a smartphone application… than tie his or her shoelaces …" (2010). Another study by Nielsen suggests that the number of teens 13 – 17 years old with smartphones is growing at a rapid rate (2012). Smartphones typically have Internet access and files can be downloaded to the phone; therefore smartphones pose similar security concerns that personal computers would have. From studies such as the Nielsen and AVG studies, it seems that children own and use smartphones at a young age. This may lead to an increase in problems typically associated with Internet usage, such as malware, since smartphones mimic the Internet capabilities of personal computers.

Benefits of Smartphones for Children: Safety and Education

While there are dangers, there are also benefits to allowing children to use smartphones. There are safety apps such as Life360, which allows children to quickly "check-in" with parents, or apps that allow parents to remotely take control of the phone (Luckerson, 2012). An app called "SmartShepherd" was developed in the wake of a school shooting and has a panic button that when pressed will make sounds to ward off attackers and will send photos, text files, and GPS coordinates to the parents ("Life-saving Smartphone App," 2013). Such an app could prove life saving in a potentially fatal situation.

There are also educational benefits to smartphones. Smartphones have the potential to be educational tools by providing games and activities that increase intellectual stimulation. Some

educational settings have begun to see these benefits. For example, one museum developed a smartphone "spot the difference" game using paintings displayed in the museum, as a way of getting children to look at the artwork (Fabrikant, 2012). Educators have also developed ways to use smartphones in the classroom – for example some teachers have set up "classroom blogs," where they use smartphones to take videos and photographs of children's learning; parents can later visit the classroom blog, and educators can use the information on the blog to develop future teaching techniques (Parnell & Bartlett, 2012). Overall, parents and educators have begun to see the possible educational benefits of smartphone usage among children.

Security Issues: Malware on Phones

Like computers, smartphones can become infected with malware – programs such as spyware, which spies on your actions, or adware, which causes unwanted advertisements. An example of a harmful program is a program called DroidCleaner, disguised as a program used to clean up Google's OS (Operating System); however, the app spies on phone conversations, can download a user's pictures and other content, and can send, download, and delete SMS (text) messages (Thompson, 2013). The malware can even be transferred to a computer through a USB cord and tap into the microphone and record sounds, which are then sent back to the creator of the app (Thompson, 2013). In the hands of a child, an app like this could be dangerous because it opens up the child to risk of being spied on for devious purposes such as to stalk or kidnap the child. The child may not be aware of the risk that they have put themselves in and parents may not be aware the child's phone is infected.

Some children may not have the intellectual capabilities to distinguish apps that are potentially dangerous from apps that are "trusted," or they may not recognize the signs that their

phone security has been compromised. Some advice for parents to prevent malware from being downloaded is to only allow downloads from a trusted app store such as the app store associated with the device, or to download anti-virus app to the phone; however, some experts believe anti-virus software is limited in its capabilities because it may not detect new viruses (Endler, 2012). The best advice for concerned parents is to block apps from being downloaded to the phone, set limits on which apps may be installed, and/or tell children not to store sensitive data on the phone that could be stolen and used if the phone is compromised.

Social Issues: Inappropriate Websites

Just like it is difficult to monitor apps that children are downloading, it can be difficult to monitor what websites children visit on their smartphones. A personal computer can be located in a central area in the home where parents can monitor what the child is doing online. However, because smartphones are intended to be portable they can be used anywhere – such as in the child's room with the door shut. In a UK study, researchers found that of the 8 – 15 year olds surveyed, 1 in 5 admitted to looking at inappropriate websites on their smartphone (Silver, 2012). An unmonitored child could choose to view pornography or other age-inappropriate materials on a smartphone rather than a personal computer, since a smartphone can be kept out of parent's sight and is difficult for the parent to monitor every day. There a number of parental control apps that can block specific websites from being viewed on the children's smartphone, such Kaspersky Parental Control which allows parents to block websites by choosing a premade list ("Kaspersky Lab," 2012). The parent should talk to their children about what is considered inappropriate, and find a suitable parental control app if desired or needed.

Legal Issues and Ethical Issue: Sharing Children's Information

The issue of apps collecting children's personal data is both a legal and ethical issue – legal issue because it calls into question whether child safety laws are being violated, and an ethical issue because even if it is legal there is still debate about whether it is ethical to collect and pass on data about children. The main concern lies in the fact that when downloading apps, including apps meant for children, sometimes users are not given a disclosure as to whether information is passed on to third parties – an FTC study found that out of the tested apps meant for children, only 16 percent provided a privacy policy or disclosure (Sperry, 2012). Even on devices where there is a screen confirming what permissions the app will have once installed, the permissions and why they are needed for the app are often not well-explained (Poss & Hasty, 2012, p.10). Children could be using apps that are passing on personal information such as the child's location without parents being told when downloading the app, or because parents and children do not understand exactly what permissions they are giving to the app and for what it will be used.

The question of legality is directly related to the 1998 law COPPA, Children's Online Privacy Protection Act, which was created to protect children under 13 from having their personal information collected without parent's consent; among the stipulations of the act are what information must be included in a privacy policy and how consent for the use of the child's data can be obtained from parents ("COPPA FAQ's," 2008). In 2012, the FTC "close[d] the loophole" that allowed apps to collect personal information through plug-ins and pass it onto third parties without the child or parent's knowledge ("FTC Strengthens Kids' Privacy," 2012). Like the other issues mentioned in this essay, this is an issue that parents do not have full control

over; they may be forced to not allow their child to use any apps because even with new COPPA regulations, app developers could still find "loopholes" to collect information. Safely downloading apps for children often involves "reading the fine print" – something which consumers, particularly parents, need to be aware of.

Conclusion

One study states that 55 percent of surveyed parents feel they have the least control over their child's mobile phones, compared to other computing devices ("More Than Half of US Parents," 2012). However, this is not the case, as this essay shows – there are different techniques, including apps, to monitor children (Luckerson, 2012). One possible course of action for parents is to set clear boundaries for what is appropriate to do on the smartphone, and to use what is available to them to enforce these boundaries. For malware there are anti-virus apps or only downloading from trusted app stores; for inappropriate content there are parental control apps or other monitoring apps; and for the issue of apps collecting personal data, parents can block or prohibit apps from being downloaded altogether or they can read the disclosures before an app is downloaded. The child should know that the purpose of the monitoring is to keep the child safe from harm – electronic surveillance can sometimes "send the wrong message," the message being that the parents do not trust their children, and it is best to be clear with children about the purpose of the surveillance and monitoring (Luckerson, 2012). When used correctly, children will gain the educational and safety benefits of smartphones – however, it is up to guardians to make sure children are safe when using the Internet on smartphones.

References

AVG. (2010). Forget swimming and riding a bike – young children today more likely to have mastered computer games. Retrieved February 24, 2013, from http://www.avg.com/us-en/press-releases-news.ndi-672

This study by AVG shows that children are more skilled at using technology than they are at basic life skills like tying shoes. This illustrates that children are learning to use technology at younger ages.

COPPA FAQ's. (2008). *Federal Trade Commission*. Retrieved February 25, 2013, from http://www.ftc.gov/privacy/coppafaqs.shtm

This FAQ is published by the Federal Trade Commission and it is about COPPA. It summarizes the act's key points and clears up any confusion about the act.

Endler, M. (2012). Does mobile antivirus software really protect smartphones? *Information Week*. Retrieved February 25, 2013, from http://www.informationweek.com/security/antivirus/does-mobile-antivirus-software-really-pr/240008673

This article outlines some of the reasons why anti-virus apps may not be as powerful as they are believed to be. Though the article is aimed towards people who work in the IT field, it provides information about anti-virus apps' effectiveness.

Fabrikant, G. (2012). Engaging children with the siren call of the app. *New York Times*, p. 16. Retrieved February 25, 2013, from LexisNexis Academic at http://www.lexisnexis.com.mutex.gmu.edu/hottopics/lnacademic/?verb=sr&csi=6742&sr=

HLEAD(Engaging+children+with+the+siren+call+of+the+app.)+and+date+is+October+28%2C+2012

This article is about how some museums are trying to use smartphone technology in exhibits and activities in order to better engage children. It is an example of educational institutions using smartphones as an educational tool.

FTC strengthens kids' privacy, gives parents greater control over their information by amending children's online privacy protection rule. (2012). *Federal Trade Commission*. Retrieved February 25, 2013, from http://www.ftc.gov/opa/2012/12/coppa.shtm

This press release by the FTC outlines the changes made to COPPA in 2012, regarding the way that apps for smartphones collect children's personal data. The article clearly outlines the specific changes made.

Kaspersky Lab announces its first parental control apps for Android and Apple iOS smartphones. (2012). *Kaspersky Lab*. Retrieved February 25, 2013, from http://usa.kaspersky.com/about-us/press-center/press-releases/kaspersky-lab-announces-its-first-parental-control-apps-android

This press release summarizes the features of Kaspersky Lab's Parental Control app, an example of a parental control app that can limit children's access to potentially harmful material. There are many other parental control apps that have similar features so this provides a look at what parental control apps can do.

Life-saving smartphone app released early to public by Legacy Technology Group. (2013). *Business Wire*. Retrieved February 24, 2013, from http://www.businesswire.com/news/home/20130104005470/en/Life-Saving-Smartphone-App-Released-Early-Public-Legacy

This press release is about an app called SmartShepherd, developed after a string of school shootings. The app is an example of apps that can potentially save lives, and it shows how smartphones can be used as tools for safety.

Luckerson, V. (2012). Smart-phone apps help parents track children's movements, activities. *TIME*. Retrieved February 25, 2013, from http://business.time.com/2012/09/14/should-you-use-your-smartphone-to-track-your-kids/

This article lists some of the different apps that parents can use to keep children safe, and contains comments from parents themselves, a mobile analyst, and the creator of one of the apps. The article serves as an example of how smartphones can be used as safety and monitoring tools.

More than half of US parents think smartphones are beneficial for child development but worry about lack of safety and controls. (2012). *Business Wire*. Retrieved February 25, 2013, from ProQuest http://search.proquest.com/docview/1022295592?accountid=14541

This survey shows the lack of control that parents feel they have over their children's mobile devices. The study also reveals that although parents feel this way, very few of them actually utilize security programs.

Nielsen. (2012). Young adults and teens lead growth among smartphone owners. *Nielsen Wire*. Retrieved February 24, 2013, from http://blog.nielsen.com/nielsenwire/online_mobile/young-adults-and-teens-lead-growth-among-smartphone-owners/

This blog post summarizes a report published by Nielsen that illustrates how teenagers are the group that are getting smartphones at the quickest rate – the rate of smartphone

ownership among teenagers is up from previous years. The blog post includes the methodology used to obtain the survey results.

Nielsen Company. (2010). *The state of mobile apps*. Retrieved February 24, 2013, from http://blog.nielsen.com/nielsenwire/wp-content/uploads/2010/09/NielsenMobileAppsWhitepaper.pdf

This report published by the Nielsen Company focuses on many aspects of apps. Most relevant for this essay are the sections about what types of apps people use on their smartphones.

Parnell, W., & Bartlett, J. (2012). iDocument: How smartphones and tablets are changing documentation in preschool and primary classrooms. *Young Children*, *67*(3), 50–57. Retrieved February 24, 2013, from http://search.proquest.com.mutex.gmu.edu/docview/1019288810?accountid=14541

This journal article is about how some teachers are using smartphones as a method of documenting the learning process, so that parents and other educators can look at it. This article illustrates how smartphones can be used in an educational setting.

Poss, P., Hasty, A., Bristow, A., Letzler, R., & Shores, M. (2012). *Mobile apps for kids: current privacy disclosures are disappointing*. Retrieved February 24, 2013, from www.ftc.gov/os/2012/02/120216mobile_apps_kids.pdf

This report published by the FTC is critical in that it specifically outlines how apps are failing to notify parents that data may be collected and passed on. It is highly informative and was particularly useful for this essay. The report is part of the FTC's study of app privacy policies, and it was one of the reports that showed the need for COPPA to be amended.

Silver, K. (2012). Smartphones exposing children to pornography and violence as one-in-five admit to viewing inappropriate material. *Daily Mail UK*. Retrieved February 25, 2013, from http://www.dailymail.co.uk/news/article-2093772/Smartphones-exposing-children-pornography-violence-1-2m-youngsters-admit-logging-on.html

This article provides general statistics on how many children view pornography or other inappropriate material on their smartphones. Though it is specific to the United Kingdom, it shows that children can and do access pornography on their smartphones.

Sperry, T. (2012). Smartphone apps can compromise kids' data, FTC says. *CNN*. Retrieved February 25, 2013, from http://www.cnn.com/2012/12/10/tech/apps-children-data

This CNN article summarizes some of the FTC's main concerns about apps collecting data on children, and provides statistics on how many apps actually contained a privacy policy or disclosure before download.

Thompson, C. (2013). New malware attacks smartphone, computer to eavesdrop. *CNBC*. Retrieved February 24, 2013, from http://www.cnbc.com/id/100431624/New_Malware_Attacks_Smartphone_Computer_to_Eavesdrop

This article provides an example of dangerous malware that can unintentionally be loaded onto a smartphone, resulting in compromised data. Also, it shows how malware can be disguised as helpful programs – in this case, it was disguised as a cleaning tool.