

Penny P. Profit
BUAD 307
October 15, 2011

APPLICATIONS PAPER
OPTION #1

**THE IDENTITY WIPER:
SECONDARY MARKET RESEARCH**

Note: Managerial implications of the information and analysis have been featured in red in this sample. **This is intended only to identify passages of this type so that you may get a feeling for what such discussion may look like.** You are NOT expected to put managerial implications in red in your actual paper. The instructions for this assignment call for you to “highlight” managerial implications. This is NOT meant to be taken literally—the idea is that these should be emphasized and discussed in sufficient detail rather than as a cursory afterthought.

PROPOSAL: The Identity Wiper would consist of software that would change personal information—such as the names of a child and family member, birthdays, city of residence, phone numbers, and e-mail addresses—to bogus values in order to prevent children from giving out information that might be abused by online predators or others who might abuse this information.

Online Use By Children and Teenagers

Children and teenagers continue to use and interact through the Internet at increasing rates and frequency. This trend has been facilitated by such factors as the growth—both in sophistication and size—of social networking sites and other online communities, increasing access to high speed Internet, and greater skills in Internet use. Based on non-attributed research, the *Financial Times* (Taylor, 2006) reports that 54% of teenagers confirm having communicated with a stranger online, some one in seven having actually met a stranger in person who was first encountered online, and 47% having received “pornographic e-mail.” With the proliferation of social networking sites since then, these numbers may well have increased.

In her 2010 *Berkeley Technology Journal* article, Charlotte Chang statistics on Internet usage by both U.S. adults and children. A 2009 Pew Research Associates study found that 93% of individuals between twelve and seventeen use the Internet regularly. A 2009 Nielsen study was found that children from ages two through four are often exposed to Internet content while sitting on their parents' laps.

Cheng concludes that one of the attractions of the Internet is that it allows children and teenagers to create and experiment with fictional identities in their interactions with others whom they will not see in person. Although this may be attractive activity that can help these children and teenagers, it is also a potentially dangerous one. As Cheng puts it: "Just as teenagers can create personas that are different from their real world identity, so too can sexual predators' and cyberbullies" (p. 502). In many cases, teenagers may be likely understand that giving away certain types of information away may be dangerous. For younger children, however, this type of understanding may be lacking. They may not truly understand that there are people on the Internet who are dangerous and should not be trusted with personal information. Even if such a child experiments with an "alternate" identity, this is likely to be intermixed with actual reality. Even to the extent that such younger children may have some understanding of the dangers of giving away "critical" information, they may lack a pragmatic understanding of what constitutes such critical information. Thus, mere education on "safe" online behavior may not be sufficient to protect children. Other remedies—such as the Identity Wiper and alternative offerings—may be needed.

Online Predators and Cyber Bullies

Accurately estimating the actual number of online predators in the U.S. and

the rest of the world is difficult (Collier 2009; Ramirez, 2006). Only a small number are caught and prosecuted. These predators can come in various forms. Some may confine inappropriate activity to online interactions while others may attempt to initiate physical contact. Much of the research conducted suggests that as a matter of pragmatics, the chances of experiencing “cyber bullying” are much higher than coming into contact with an online predator (*U.S. News & World Report* 2011; Collier 2009; Chang 2010; Spink et al 2010). Nevertheless, because child predators are very dangerous, it is important for families to take strong precautions even if chances of encountering one are statistically very low. **The rise of cyber bullying, however, is a problem that may not be addressed effectively in the current vision of the Identity Wiper. Online bullies may know—and be known to—the child and may already have much of the “objective” information about the child—e.g., name, place of residence, and approximate age—that the Identity Wiper is intended to keep from predators. Cyber bullies may be more likely to exploit more subjective and personal information—e.g., fears, current life stressors, relationships with others, school problems, and embarrassing “secrets”—that may be shared inadvertently or in a moment of weakness. Prior to this research, the Identity Wiper was envisioned mostly as simple text search mechanism that would replace strings of easily recognized words, names, and numbers. Identifying information that would be exploited by cyber bullies would be much more difficult and would probably require some fairly elaborate computer algorithms. Therefore, the scope of the Identity Wiper should be reexamined.**

Parenting Activity and Existing Solutions

Some parents try to “manually” limit the amount of time their children spend

online. This is not in and of itself a method for preventing contact with predators and bullies, although less time spent on the Internet will probably reduce the opportunity to interact with these individuals. Although clearly worried about the dangers of online predators that they have seen in the media, they are often more concerned about the impact of “excessive” Internet usage on the amount of time spent “in person” with friends and family (“Many Parents Frown... 2010).

The software and online tools currently available seem to fall into several overlapping types (Yao 2009; Mosberg 2010, “McAfee Safe Eyes...” 2011; “Parents Should Screen...” 2011; Taylor 2006):

- Programs which limit the amount of time that can be spent online.
- Programs which limit the types of activities that can be done. It is possible, for example, with some software to set up different accounts for each child so that different permissions can be set for each. One may be permitted to surf web sites but may not be authorized to use e-mail or send text messages. An older sibling may be given these privileges.
- “Filtering” programs which limit the specific web sites that can be visited. Such software may either “block” specifically selected “banned” sites, allowing everything else, or may allow the child only to visit approved sites. In either case, parents do not necessarily have to identify themselves which specific sites should be permitted or banned since the software publishers make available frequently updated lists of sites of either type.
- In combination with the above filtering software, web sites which are specifically designed to be “child friendly” and feature appropriate content. KidZui is one such site. This approach will, of course, greatly limit the options for the child online.
- “Monitoring” programs which may not block any activity or communication by itself, but will instead notify the parents—usually by e-mail—of inappropriate disclosures and activities after the fact.

Software to control Internet usage is not unique to children. In the industrial setting, many firms now report using filtering programs to prevent their employees from accessing inappropriate sites during the workday. Some of the more advanced programs used by network administrators appear to offer considerable flexibility. One application, for example, allowed a firm to limit the bandwidth allowed for use at any one time by sites such as YouTube, preserving computer resources while not

necessarily imposing an outright ban on the use of a specific site. It is also possible to grant access to certain shopping and predominantly personal use sites only during lunch hours or other permitted time intervals. Other applications—which often raise greater concerns about invasion of privacy—can be used to track the online activities of users of company computers. Blocking software may also be used to block “inappropriate” sites on which employees might be tempted to spend excessive time on non-work related activities (e.g., Facebook). Such software is rather controversial since it can also be used by some governments that seek to censor Internet content (Chou et al 2010; Sonne and Stecklow 2011).

Table 1 summarizes the main programs and services currently available by category:

Table 1 SOME EXISTING INTERNET MONITORING/USAGE RESTRICTION PROGRAMS*	
Program and Price (if available)	Capabilities
Monitoring Programs/Services	
SafeEyes (\$49.95)	Reports of instant messaging chats, e-mails, and web use through e-mail reports
eBlaster (\$99.95)	Copies of Chats and e-mails sent with e-mail; e-mail alerts provided
ContentProtect (\$39.99)	Reports of instant message, tracking of web activity; e-mail or pager alerts
IM Einstein (\$40)	Recording of instant messages and chats; e-mail, phone, or pager reports
CyberSieve (\$39.99)	Logs of web use available online; notice of “forbidden” activities.
Zephyr (N/A)—component of MySpace	Only allows parents to check log-on status and profile changes from remote computers
Filtering Software/Services	
Internet Explorer	Content blocking based on Content Rating

<p style="text-align: center;">Table 1 SOME EXISTING INTERNET MONITORING/USAGE RESTRICTION PROGRAMS*</p>	
	Association guidelines.
CyberPatrol	Blocking of specific or all chat and instant messaging sites and activity; blocking of undesirable search engines and other sites; protection against revelation of personal sensitive information
CYBERSitter	Unspecified filtering and other capabilities
SafeKeeper Plus	“Suite” programs to control Internet activity; ability to monitor activity; tracking of suspected predators
WebWatcherKids (\$99.00)	“Real time” filtering content; access to monitoring of key strokes by child from everywhere
BeNetSafe	Automatic monitoring of child Internet activity with reporting of “reckless” activity

*Adapted from Chou et. al. 2010; Mosberg 2009; “McAfee Safe Eyes 2011; Taylor 2006

From the above, it is clear that most of programs and services offered different from the Identity Wiper in their approach. CyberPatrol offers a feature that is somewhat similar to the proposed idea. This software program is reportedly able to “prevent” the browser from revealing certain “sensitive” information such as credit card information, addresses, and phone numbers (Chou et al 2010). No articles were found that evaluate this feature and its effectiveness. Overall, however, it should be noted that the Identify Wiper is likely to be a complement to, rather than a substitute for, many of the other offerings.

Predators are not necessarily the only source of concern among parents and public policy makers. Many individuals strongly value their privacy and may find the disclosure of personal information objectionable more on the basis of principle than on the basis of any risk of substantive harm information about a minor child should be

collected into a lasting database. The *Do Not Track Kids Act of 2011* was introduced into the House of Representatives in April of 2011, aiming to limit the collection of data on children. Thus, the Identity Wiper—in addition to its protection against online predators—offers as a bonus that commercial firms be prevented from collecting accurate personal data.

Additional Technological Issues

A great deal of Internet communication today is done through portable devices such as cellular phones. Several software programs similar to the types discussed above are now available for selected cell phones and operating systems (Cheng, 2010). With Windows and the Macintosh operating systems dominating the desktop and laptop computer markets, making two versions would be a reasonable task. However, making versions that would work on cellular phones could be more difficult. Although the Windows 7 mobile, Apple iPhone, and Android cell phone operating systems dominate, a number of additional ones are available. Further, because cellular phone operating systems are in a less mature stage than personal computer systems, there may be a greater danger that operating system software updates will cause compatibility problems. To the extent that cell phone “apps” may be less well integrated, safeguards may not function consistently across each one, especially as new apps are introduced. If the Identity Wiper cannot be used consistently across platforms, its value is likely greatly diminished.

Ethical Concerns

Even when intended to protect the safety of children, attempts by parents and other authorities to interfere with—or actively distort—communication may conjure

up images of censorship and the type of society portrayed in George Orwell's legendary book *1984*. Although it may be justified to use such methods with young children who cannot understand when they are putting themselves into danger, encouraging the use of this type of technology to regulate teenagers may be inappropriate. Since parents would not be bound by any recommendations made by the publisher, and since it would not be possible to impose controls limiting the use of the controls to younger children, making this type of tool readily available raises serious ethical questions. In principle, such software could even be used by one spouse to limit communication. An adult could likely access computers outside the home, but doing so would be cumbersome.

General Discussion

This research suggests that a large number of products currently exist to help protect children against inappropriate Internet contacts and disclosure of personal information. Many of these product features are complimentary, and some products contain more than one—e.g., a filter restricting site access and a tool for parental notification of behaviors of concern. One existing product offers a feature that is specifically intended to prevent the disclosure of sensitive information, while the others seem focused on either a limitation on the targets with which communication be made or reporting once critical incidents have already occurred.

Although the current research uncovered concerns—among children, teenagers, as well as parents—about the intrusive nature of some of the measures offered, the articles did not give a clear indication of the level of satisfaction with current systems. This issue, then, will need to be assessed through primary research. Prices

of services offered, where reported, seemed to be in the same \$30-\$100 range that has been anticipated for a product of the type proposed. The price did not come up as an issue in the articles read, and thus willingness to pay must be examined in primary research.

General concerns about the intrusiveness of online “snooping” came up in many articles. The articles did not offer any insight into how these might be balanced against protection from online threats. It was also evident from articles that many measures may be readily circumvented, especially by tech-savvy teenagers. This suggests that there may be a strong need for cooperation and mutual support among parents and children for the objectives of the program. These are issues that should be addressed through primary research.

The concerns discussed in previous sections on potential for misuse of this application and the serious problems that are raised by usage of the Internet across platforms—on computers, computer tablets such as the iPad, cellular phones, and other portable devices—suggest that, at the very least, extensive additional analysis is needed before a decision to proceed with this product can be made. These problems may ultimately prove insurmountable, but it is difficult to make definitively conclude this with the current analysis.

REFERENCES

“BizRocket.Com, Inc Delivers Cutting-Edge Cyberbullying, Online Predator Defense Software; Enhances Pre-Teen Social Networking Site in the Midst of Social Media Acquisition Boom” (2010), *Marketing Weekly News*, Aug 13, 246.

Chang, Charlotte (2010), "Internet Safety Survey: Who Will Protect the Children?" *Berkeley Technology Law Journal*, 25(1), 501.

Cheng, Roger (2010), "Protecting Kids on Phones: Companies Develop Software to Scan Mobile Messages, Send Alerts to Parents," *Wall Street Journal* (Eastern edition), Aug 11, B.5.

Chou, Chen-Huei, Atish P Sinha, and Huimin Zhao (2010), "Commercial Internet Filters: Perils and Opportunities," *Decision Support Systems*, March, 48(4), 521.

Collier, Anne (2009), "A Better Safety Net," *School Library Journal*, 55(11), 36.

Cooper, Will (2011) "NMA Research Uncovers Kids' Digital Habits," *New Media Age*, Feb 24, 1.

"Five Defendants Sentenced for Child Pornography Crimes Uncovered as a Result of International Investigation" (2010), *Marketing Weekly News*, Jul 24, 189.

Goldman Getzler, Wendy (2010), "The new wave of surfing," *KidScreen*, Jul/Aug, 28.

"Many Parents Frown on Kids' Internet Use, Survey Says: They worry about diminished time spent with friends, family," (2011), *U.S News & World Report*, December 28.

"McAfee Safe Eyes Wins the National Parenting Center's 2011 Seal of Approval" (2011), *Marketing Weekly News*, May 21, 1036.

Mossberg, Walter S. (2008), "KidZui's Parent Plan Lets Children Explore In Safe Corner of Web," *Wall Street Journal*, Mar 20, B.1.

Pachner, Joanna and Alicia Androich (2011), "Kids in Play," *Marketing*, Mar 14, 116(3), 27-31.

"Parents Should Screen Kids' Summer Web Surfing: Expert Racism, Violence, Cyberbullying Online Among Things to Monitor" (2011), *U.S. News & World Report*, May 31.

Ramirez, Rosa (2006), "Targeting Online Predators: 200 Law Officers, Educators Sharpen Skills at Seminar," *Rocky Mountain News*, October 3, 20A.

Sonne, Paul and Steve Stecklow (2011), "U.S. Products Help Block Mideast Web," *Wall Street Journal* (Eastern edition), Mar 28, A.1.

Spink, Amanda, Susan Danby, Kerry Mallan, and Carly Butler (2010), "Exploring Young Children's Web Searching and Technoliteracy," *Marketing*, 66(2), 191.

Stecklow, Steve and Julia Angwin (2011), "House Releases 'Do Not Track' Bill," *Wall Street Journal* (Eastern edition). May 7, B.3.

Taylor, Paul (2006), "Need a Cybernanny? Software For Parents Who Are Looking to Protect Their Children from Online Hazards," *Financial Times*, Nov 11, 10.

Ward, Greg (2010), "Digital is just a small part of the media mix for today's children," *New Media Age*, Nov 4, 9.

Yao, Deborah (2009), "Web-Monitoring Software Gathers Data on Kids' Chats," *Marketing News*, Oct 15, 22.