

THE IDENTITY WIPER: FINAL PROJECT

EXECUTIVE SUMMARY

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. Currently existing child Internet protection offerings include “filtering” software programs and/or services that tend to either restrict access to questionable sites “monitoring” programs and services that report dangerous behavior by the child. The Identity Wiper program could be used to allow children access to a larger number of Internet sites that feature valuable material for education and/or personal growth and to serve as an added safeguard against disclosure of sensitive information to online predators.

The analysis completed in the course of this project suggests that cautious optimism may be warranted. Limited time and resources did not permit the completion of sufficient research and analysis to support a definitive decision on the merits of launching this venture. Additional research on consumer perception of this product in its own right and relative to competitors, the perceived value of the product, consumer willingness to pay, and willingness to expend the time and effort needed to set up and operate this software is needed before a meaningful decision on whether to proceed can be made.

Responses to substantive comments made on previous papers are also included.

REPLIES TO QUESTIONS RAISED ON THE PROPOSAL

Comment: Would this program cause compatibility problems with other programs that might need access to the Internet? How would access be controlled for each user?

Reply: Each software program that runs in a computer's memory will consume some of the computer's processing power. Therefore, the computer will be slowed down when the Identity Wiper is running. One way to minimize the disturbance of the program is to activate it only when a child's Windows user account is entered. The program would not have to run for the adults of the household who could enter into their own accounts on the computer with the appropriate password. It is unlikely that legitimate programs controlled by the child would need to use the "sensitive" information, so no compatibility programs are anticipated.

Comment: Of the other programs offered, which one(s) do you see as the greatest competitive threats? Why are these stronger potential competitors?

Reply: The filtering programs—CyberPatrol, CYBERSitter, SafeKeeper Plus, WebWatcherKids, and BeNetSafe—are more similar to the Identity Wiper in their approach and are thus closer substitutes. The monitoring programs do not emphasize as much an immediate threat, and thus, these tend to serve a complimentary purpose. The built-in features of Internet Explorer 7 and the America Online access program arguably offer a more closely integrated solution and are included in these programs without additional charge. Thus, these are probably more serious threats. As discussed in Assignment #5, many potential buyers may find the different programs and services complimentary, with each filling in certain gaps not completely served by others.

Comment: How serious is the problem of inconsistent information—e.g., weather information not being consistent with conditions in the area that is being substituted for

the child's actual residence area—likely to be?

Reply: It will clearly not be possible to create a system which will supply completely consistent information. Therefore, if a predator spends enough time, he or she will likely become aware that the information that is being supplied is not credible. There is a possibility that a clever predator might find ways to get the child to reveal information indirectly. Thus, the system is not completely secure. However, the system will make it more difficult to get at the confidential information. Delays that result will increase the likelihood that the child will reveal information about the communication to family members.

To increase the effectiveness of the system, it may be possible to create a database suggesting the most effective distortions based on similarity of characteristics. If, for example, if towns can be identified that are of similar size and have similar climates, these could be randomly substituted for each other.

TENTATIVE ASSESSMENT OF PROSPECTS

This project was completed as part of the requirements for one course. No special resources were made available, and I was the only individual available to work on the project along with other course work and work from three other courses. Thus, the secondary market research completed was limited, and no primary market research data was actually collected. It is, therefore, not possible to make a fully informed evaluation of the potential of this venture. The discussion below is tentative and subject to the collection of the additional information discussed in the previous section.

Overall, this project suggests a cautiously optimistic outlook. The Identity Wiper appears to have potential to serve both as a substitute for or compliment to

many other child protection programs and services that are currently available. Because the Identity Wiper is somewhat more difficult to use than are many other programs, this program will most likely appeal only to part of the market. Figure 1 illustrates this potential market within the context of the total number of families with computers and the subset of these families that use protection programs or services of any kind. The relative sizes of the circles are not the actual associated shares of the population.

A major problem that the Identity Wiper will likely face is gaining awareness among potential customers. In the “old days,” most software was sold in retail stores. If stores decided to carry a software program, it would be placed on the shelves next to other programs in the same category, allowing consumers to compare packages. Today, however, software is often downloaded directly by the consumer directly from the publisher’s site. This means that each site may mention only one program. Comparing programs side by side is thus more difficult for those who do not go through the effort to identify product reviews in forums such as *Consumer Reports*, *PC Magazine*, or *CNET.com*. Since several different software programs exist, there will likely be considerable competition for search engine rankings under the relevant key terms.

If the research described previously in this report suggests that there is likely to a large sales potential for this product, it may be possible to justify paying for right-side advertising on Google and other search engines under key terms such as “child Internet protection” or “Internet predator protection.” However, if the Identity Wiper turns out to have potential only as a niche program, such search engine advertising may not be cost effective. Within a reasonable time after its launch, the Identity Wiper would probably be included in the reviews of child Internet protection programs in forums such as *PC Magazine*

and CNET.com, but only a limited number of parents are likely to be dedicated

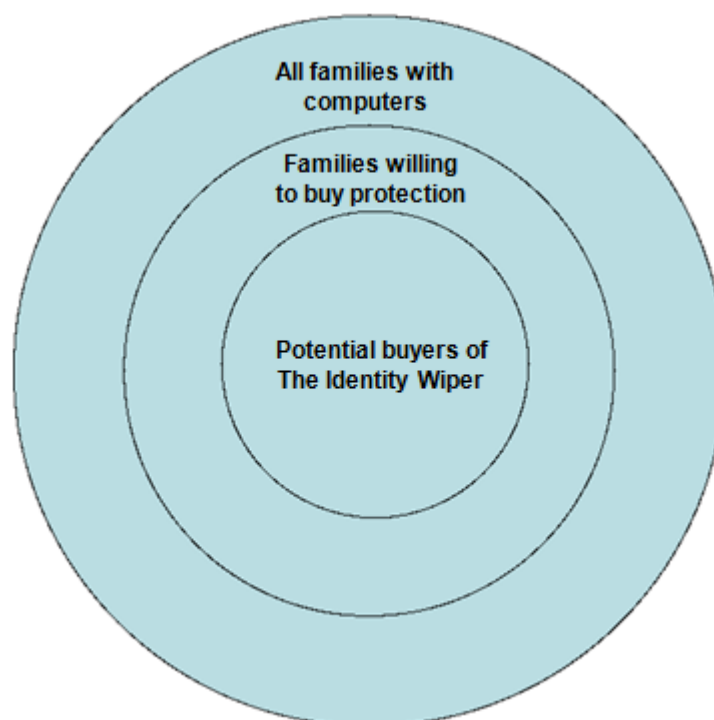


Figure 1: Potential Market for the Identity Wiper

and resourceful enough to seek out and read these reviews. There is also some potential for spread through word of mouth, this word of mouth involves a chicken-and-egg problem in the sense that people must be aware of and use the program before they can spread the word.

A technical problem discussed in the proposal is the possibility that the data substitution will become obvious because of inconsistency between substituted pieces of information and other information communicated—e.g., a discussion of weather that would not occur in the decoy city. This raises problems both in reducing the quality of communication with other “legitimate” parties such as same age peers or relatives and in motivating predator efforts to circumvent the protection. However, predators who detect this information distortion may decide to move on, avoiding this child who is “too much trouble” to be worthwhile. Effectively re -

directing the predator to another potential victim raises ethical concerns, but many parents may choose to go with this outcome. Additional research is needed on the extent to which the detection of information distortion becomes a problem and the extent to which the protection can be effectively circumvented.