Students’ and Parents’ Attitudes towards Online Privacy:  
An International Study

Eric K. Clemons  
The Wharton School  
clemons@wharton.upenn.edu

Josh Wilson  
The Wharton School  
wilsonjs@wharton.upenn.edu

Abstract

Young internet users engage in risky or inappropriate behavior, including sending email and texts about their sexual activities and the sexual activities of others, and other activities that could either be embarrassing or harmful to their future. Parents in all eight countries studied express preferences for far less data mining of students’ online activities than seems to be the current practice. Most importantly, aversion to data mining does not seem to be correlated with awareness of the extent to which data mining of teen’s activities occurs or the variety of forms that this data mining can exhibit. Only in the U.S. does teens’ aversion to an activity appear to be correlated with their individually engaging in that activity, and this appears to be true only for the most embarrassing or incriminating of online activities.

1. Introduction

Federal laws like FERPA (described in section 3) do not appear to provide the protection that they were intended to provide, nor do they appear to provide the protection that parents demand for their children. It is well known that teenagers and younger children engage in risky activities online [40,41]. It is well known that these groups often do not take adequate care to protect themselves online. Data-mining privileges that are now being granted to some providers of educational applications and services create new risks to pre-teen and teen privacy. Recent revelations by Google and a study by Law professors at Fordham demonstrate that these practices violate the spirit of FERPA and the explicit preferences of parents and students [31,32,55]. Recent legislation about the right to be forgotten [74] offer long term protection about unwanted information being found through search, but offer no protection against unwanted information being stored, analyzed, and used for ads by service providers.

The online privacy of teenagers and younger children is an increasingly important issue and an increasingly contentious one [10,53,60]. The very public failure of inBloom, the host of new laws addressing student and teen privacy, and the lawsuits alleging privacy violations of educational software companies all suggest that the future of online privacy is as yet unresolved [66,67,70]. Parents worry about the privacy of young Internet users, yet a significant fraction of young users cheerfully embrace the idea that “You have zero privacy. Get over it!” [54]. The use of social media technology and email among teenagers is pervasive [42], and the use of some technologies, like texting, is nearly universal [36], all of which increase the number of opportunities for a teen to share personal information, and in turn, increase the amount of information for applications and services to mine.

This paper addresses what parents believe their children are doing online, and what these students are actually doing. We determine what parental concerns are and what students’ concerns are, in order to assess what parents and students want from best practice in K-12 educational software. Our research is based on surveys of parents and students, conducted online in the US, Argentina, Brazil, Chile, Colombia, Germany, Japan, and Mexico.

Section 2 of this paper will describe the problems associated with the unprotected online behavior of young Internet users. Section 3 will describe FERPA, a Federal law intended to protect these users, at least in academic settings. Section 4 will discuss additional problems with data mining students. Section 5 will describe our research methodology. Section 6 and 7 will discuss the principal findings from the survey instruments. Section 8 will conclude with a recapitulation of the principal findings and discussion of future analyses and studies to be done.

This is exploratory work. We set out to learn what we could about contentious issues within the contentious topic of online privacy of students. We set out to learn the extent to which individual users were aware of current online practices, and the extent to which they approved of them. We set out to explore the attitudes of parents and of children towards online privacy. We set out to explore the differences and similarities among users online privacy preferences across different nations. We did not set out with a specific set of attitudes we wished to demonstrate, hypotheses we wished to test, or theories we wished to validate.
Since we did not begin with specific hypotheses, we did not begin with causal models of consumer behavior that we wished to explore. However, we did observe data on parental awareness of practices and their attitudes towards them and were able to test the extent to which awareness and attitudes were correlated. Likewise, we did observe data on students’ engaging in risky practices and their attitudes towards their being tracked, and were able to test the extent to which engaging in specific risky online practices were correlated with concern for tracking these practices.

2. Problems Associated with Online Behavior of Young Internet Users

Teenagers are spending more time online and texting [36,42]. Using this technology, teenagers engage in risky behaviors such as cyberbullying [12,31,37,48], sexting [16,25,38,46,71], and bragging about or describing inappropriate behaviors with drugs, alcohol, or sexual partners. Horror stories are frequently published about inappropriate behavior that may destroy students’ reputations or those of their friends and acquaintances [12,45].

Teenagers and children are vulnerable. They are less likely to understand the future ramifications of disclosing personal information, and the future implications of their actions on their careers or their social lives. They are less likely to understand the implications of their online actions for the lives of others. They are less likely to understand the risks of cyber-stalkers, or the risks of disclosing their identities to strangers online. Something once posted online may be online forever [2,15,44,56]; the net does not easily forget, and the net does not often forgive.

Parents are concerned about their children’s online activities [15,31,34,37,48], both because of the press surrounding the activities of young users, and because of their suspicions about the online activities of their own children. Parents worry about their children’s safety. They may also worry about the legal implications of their children abusing others. Increasingly, parents are concerned about what advertisers and online applications can learn about their children and their children’s activities, and they worry about how the information on their children may be stored, accessed, and used.

Schools increasingly are using email to communicate with their students and increasingly are using online apps, PCs, and tablets for instruction [11,18,26,77]. These apps often track users and amass large amounts of data [24,25,51,57,61,74], as do some providers of schools’ email systems. These vendors often violate the intent of FERPA, the legal requirements of FERPA, or both [17,69,72,74], in that they frequently obtain data related to schools and school activities, and combine it with other information and use it for commercial purposes that are in no way related to the provision of academic services [8,24,26,63]. Outside the US, American providers of educational software may believe themselves to be subject to little or no oversight. Such violations have become more public and more frequent. Google recently admitted that Google Applications for Education has been scanning the content of student’s emails, admitted that this may violate federal law, and pledged to stop the practice [7,31,58]. A lawsuit over the issue alleges that Google has been using the content gleaned from Google Apps for Education in order to build profiles of users that are used for targeting advertising across Google’s other products [32]. Another vendor, inBloom, a $100 million Gates-funded student information aggregator, failed because parents believed the information being collected was not being adequately secured [66,70].

There is very little explicit guidance for school administrators to deal with the privacy problems created by the increasing use of technology in K-12 education. Often, schools do not have the necessary resources for vetting contracts, and consequently, the schools are incapable of safeguarding students’ privacy. Common loopholes in these contracts allow software providers to collect a broad array of student’s personal information, and allow vendors to sell the information [55,64]. The FTC has requested that vendors adopt best practices [20], but the FTC’s reports suggest that app vendors do not consistently get consent for their data mining, do not explain their data mining practices to parents or school administrators, and in other ways do not observe FERPA requirements [72]. While FERPA permits the use of student data for purposes directly related to their education [17], it appears that many vendors also use data for a wide variety of commercial purposes unrelated to academic activities [8,24,63].

3. Protection Afforded by FERPA and Other Laws

FERPA (Family Educational Records Privacy Act) is designed to protect the privacy of students by preserving the confidentiality of all educational records [72]. Educational records are defined to be those directly related to a student’s performance, and are created and maintained by an educational institution. FERPA applies to all US schools that accept funds from the Department of Education, from elementary schools through secondary education and beyond. Certain personally identified information (PII) from these records is not considered to be harmful to privacy
if disclosed, such as a student’s name, address, email, and photographs. Other PII is considered to be harmful to privacy if disclosed, and is thus protected. Basically, FERPA is intended to restrict access to students’ academic records, performance records, and communications regarding academic activities. FERPA’s use of the term “potentially harmful to privacy” is extremely wide-ranging and all-inclusive; under FERPA, even a college student’s parents may not have access to the student’s grades or transcript without the student’s permission. We will substitute the less-judgmental but more accurate term, “private information” for “potentially harmful PII”.

In order for a K-12 educational institution to disclose private information about a student, a parent must give written and dated consent regarding which documents can be disclosed, for what purpose, and to whom the disclosure is being made. However, schools can disclose information to employees. Additionally, schools can disclose information to contractors working for the schools, to the extent that these contractors need access to information [72]. There is evidence that a large number of academic institutions are using this exemption to provide access to contractors like email providers, who do indeed need to store vast amounts of information [8,63]. Problems occur when contractors’ use is not consistent with serving the educational needs of students and goes well beyond the use envisioned by the educational institutions. It would not be consistent with the objectives of FERPA if the information services vender were to use information from students’ email, and to combine it with other information the services provider is able to obtain elsewhere, in order to implement targeted advertising programs directed at students. There is evidence that this practice, and others like it, are now widespread [4,24,59].

4. Additional Problems with Data Mining Students

This paper examines how parental concerns differ across nations, irrespective of national laws and regulations restricting or permitting online data mining of children.

It is useful to start with some potential bases for objection to data mining that are unrelated to FERPA:

1. First Degree Price Discrimination and The Myth of Anonymization — targeted ads are not safe, because they are not anonymous, at least not after you click on them.
2. Vulnerable Impulse Buying — ads targeted to children are not safe, which is why we regulate ads on children’s morning TV [3,13,21,35,39,68,75], and well-aimed, well-targeted ads may be particularly unsafe.
3. Vulnerable impulse buying — when your closest friends or your celebrity idols pitch directly to you, impulse buying may be even more dangerous to children.

4.1. First Degree Price Discrimination and The Myth of Anonymization

It is often argued that ads are harmless, and that invasion of privacy on the internet merely results in better ads, more interesting ads, and ads that come closer to performing a service for the viewer [1,22,49]. Indeed, this may sometimes be true. However, invasion of privacy can result in merchants who are better informed, and better positioned to perform first-degree price discrimination [5,50,52,76], and thus able to command more of the buyer’s surplus. In a recent study, Ben Shiller demonstrates that the use of big data can lead to first-degree price discrimination [62].

In order for a company to engage in effective price discrimination it is necessary that the company be informed about the buyer and be able to assess the buyer’s willingness to pay. We have addressed elsewhere the mechanisms by which advertisers are easily able to breach the wall of privacy allegedly provided by Google [14]. In brief, the advertiser knows why they sent you the ad and knows what combination of attributes recipients of the ad possess; as soon as you click on the ad you identify yourself and associate yourself with the collection of attributes that Google assures you are private.

4.2. Targeted Social Network Ads and Impulse Buying

Google Plus, Google’s social networking site, and Facebook have both launched similar ad capabilities that leverage user’s content and reviews for the purpose of targeting ads to members in their network [19,29]. For example, if a local grocery store wants to advertise through Google, they will have the option of using a Google Plus member’s positive review of the store. The ad will contain the member’s recommendation, word-for-word or abridged, and the member’s likeness, or picture [28]. This ad is not restricted to Google Plus; that is, the ad can show up during search queries involving Google search and Google Maps. While you may be able to prevent Google from using your likeness for ads, you cannot opt out of Google targeting you with ads involving your friends’ likenesses. Another dimension of harm relies on the inability of teens and children to resist impulse purchases, especially if peer pressure is involved [9,30,43,78].

The effects of targeting ads toward teens and children have been studied in depth: children and teens
are susceptible to undue influence and manipulation by ads [3,13,21]. Ads have been misinterpreted by youths as public service announcements, and others have been misinterpreted as commercials for an athlete when they are in fact sporting equipment commercials [23]. Initial studies of online advertising demonstrated that teens and children have difficulties distinguishing banner and display ads from the content belonging to the website [47]. And several studies have shown that ads targeted at youths lead to the purchase, adoption, and life-long use of products, sometimes even harmful products like alcohol and tobacco [3,13,21]. Moreover, teen purchasing habits are highly influenced by peer pressure and the appearance of fitting in [9,30,43,78]. The new type of ads developed by Google and Facebook can be misinterpreted as not an ad at all.

5. Our Study of Students’ and Parents’ Attitudes towards Privacy

- Our first study assessed parents’ attitudes towards a wide range of data mining of their children’s email accounts, including forms of detailed tracking and integration with search, texting, and other online activities. We also asked them to estimate the percentage of students who engaged in a range of risky online activities.
- Our second survey assessed what young internet users actually do online. We also asked for their awareness of other students’ online activities. We asked questions about their attitudes and their preferences concerning online data mining of their school email accounts, data mining of other email accounts, and the linking of information from various online sources. Space limitations prevent us from presenting these findings here, other than to say that parents’ are definitely justified in being concerned about the children’s online behaviors.
- Our third survey was a repeat of the first survey, except the parents in the third experiment were briefed about the percentages of students who do actually engage in a range of risky activities. Parents in this survey were asked the same questions as parents in survey 1 about their attitudes toward data mining of their children’s email accounts. We sought to determine if parents’ attitudes towards data mining of school provided email would change when informed of the prevalence of the risky behavior in which kids engage online.

The survey was conducted using Qualtrics, an online survey software company, and their associated panel companies in each of the surveyed countries. We ensured that we were only surveying relevant populations. We screened the survey of adults to determine that they had one or more children under the age of seventeen. We screened the survey of young users to include only subjects between 13 and 17 years old who use email and text. The number of parents surveyed is US: 200, Germany: 254, Japan: 246, Argentina: 340, Brazil: 327, Chile: 107, Columbia: 347, and Mexico: 332. We allowed Qualtrics to determine the criteria for a representative population in the US, Germany, and Japan. We were required to set our own criteria in the Latin American surveys, and the demographics of our population is described in tables 1A and 1B. The survey was conducted online until we achieved the number of subjects desired, with the percentage distributions of the populations we desired. Given the survey methodology, the concept of response rate of course has no meaning; the survey remains online until the desired number of responses is received. We suspect the population that responds to online surveys is always a bit skewed; obviously, only technology users respond to these surveys. We controlled the population as best we could, with breakdowns on age and educational level; we believe that the population is far more representative than the population that responds to surveys in universities’ behavior research labs.

The survey instrument is too long to include in this paper, but is available online on the author’s website at opim.wharton.upenn.edu/~clemons/consumer.html.

Table 1A-B. Table A gives the breakdown of the sample population by age and Table B provides the breakdown by education.

6. Summary of Findings

6.1 Parental Attitudes Towards Teen Privacy

Most parents in the U.S., Germany, and the Latin America countries generally do know that search engines track and retain individual users’ search history, while parents in Japan are mostly unaware that search engines tracking usage. Parents in the U.S. and Germany are more aware of tracking than their counterparts in Latin America countries which all have
similar degrees of awareness; this suggests that there may be a pattern in parental awareness. However, parents in every country we surveyed are much less aware of an email provider’s ability to scan their children’s email. Across every country, with the exception of Germany, less than half of parents are aware that some email providers are able to scan their children’s school-provided email for the purpose of targeting ads. Parents are even less informed of service providers’ ability to integrate information from numerous online sources. When a student has email provided by an online service provider with multiple offerings and limited regulation, emails provided by schools create even greater privacy risks.

Table 2 shows the number of parents whose children are provided with a school email account, across all of the countries we surveyed. The largest percentage of students with school provided email accounts is in the U.S., and the smallest percentage is in Japan. Table 3 shows that American and German parents have far greater awareness of data mining than do Japanese parents, with Latin American parents somewhat in between. Table 3 also shows that all parents have more limited awareness of the degree to which vendors of educational software and services can create integrated information profiles on their children.

Parents in all three countries are strongly opposed to having their children’s school-provided email scanned and linked to text and search in order to target ads. As shown in table 4, the vast majority of parents in all nations object to integration and data mining of their children’s school email accounts. This table also shows that these numbers are not greatly reduced even when vendors provide these services to the school district without charge. Table 5 shows that parents in all the countries believe that consent for data mining of school-provided email accounts should come either from themselves, or from themselves and the students. Almost without exception, parents do not trust school officials to make these consent decisions on behalf of their children. Only in Germany, do we see a significant number of parents trust school officials to make this decision, and even in Germany this group represents only 8%. This demonstrates that current practices violate the preferences of virtually all parents.

We did statistical testing to see the extent to which parental attitudes differed across nations. We found that the US and Germany were statistically indistinguishable from each other. The Latin American nations were indistinguishable from each other, but different from the US, Germany, and Japan. Japan differed from all other nations. Results for attitudes when email services are free are shown in table 4. Although Japan scored lowest on parental concerns for preventing data mining, 82% of Japanese parents still objected to data mining their children’s online activities for commercial purposes, even when vendors provided online services without charge. This is shown in table 6, which shows that when email services are free, Japan is statistically different from all other nations, the Latin American nations. For table 6, we tested the differences between countries using an independent samples t-test with unequal variance. We believe this is the preferred test because the data for each country was collected independent of each other, and while the distributions for each country may be the same, an inspection of bar graphs suggested unequal variances. Significant results are shaded in red.
Table 6.—Independent samples t-tests with unequal variances of differences in attitudes towards data mining free email, among parents in different nations.

6.2. Teen Attitudes Towards Teen Privacy

This study was performed only in the US, Germany, and Japan. Space limitations prevent full presentation of our numerical survey data, and we offer only a summary here. Not surprisingly, teenagers care about their own privacy. There are slight differences among the U.S. sample, the Japan sample, and the German sample. All of the teens, regardless of country, feel most strongly about text being tracked versus search and email. In general, the German teens are slightly more concerned than average, and the Japanese teens are slightly less concerned than average. However, while more U.S. teens express greater concern than do Japanese, a larger number of U.S. teens also express no concern at all.

Teenagers in the U.S., Japan, and Germany all object to linking their private email to their texts, their school email to their text, or any other combination of information sources that we explored. American students were the least concerned of the three populations when questions involved linking their text messages to other forms of online communications.

Although space prevents us from fully describing the risky online behavior of teenagers, our data shows that the risky online behavior of teenagers is quite extensive. A vast majority of teens have sent and forwarded emails regarding sexual behavior. In the U.S. there has also been significant texting about alcohol abuse by minors, illicit drug use, cheating in school, and even criminal behavior. The numbers are lower for email than for texting, and are lower for students outside the United States.

Nearly a quarter or more of American teenagers have received texts about all of the categories of inappropriate behavior we investigated. Email is used less frequently, which is consistent with other studies. Our numbers for cyberbullying and sexting are also consistent with other studies surveying U.S. teens [5,6]. Teenagers do engage in risky behavior, they do tell each other about it, and some appear to engage in all of the risky behaviors we studied. In all categories of risky behavior, Japanese teens are near the bottom, or very close, whereas U.S teens engage in online risky behaviors most frequently across all categories. The German teens are very similar to their U.S. counterparts, with the exception of illicit drugs and misdemeanors where German teens behave more similarly to their Japanese counterparts.

7. Further Analysis of Parental Attitudes

We did additional analysis and determined that there was almost no relationship between awareness of forms of data mining performed and attitudes towards performing that data mining. This is shown in tables 7 and 8. We initially found this surprising, but it becomes more easily understood after some introspection. If a parent believes an action is potentially dangerous to his or her children, or is in some sense morally repugnant, the negative attitude persists whether or not the action is currently being performed, or whether or not the parent is aware the action is currently being performed. Significant results are noted in red.

Table 7. p-values from Pearson χ² between parental awareness of search tracking and their attitudes toward data mining of school-provided email.

<table>
<thead>
<tr>
<th>Country</th>
<th>U.S.</th>
<th>Germany</th>
<th>Japan</th>
<th>Argentina</th>
<th>Brazil</th>
<th>Chile</th>
<th>Colombia</th>
<th>Mexico</th>
</tr>
</thead>
<tbody>
<tr>
<td>Awareness</td>
<td>0.57</td>
<td>0.23</td>
<td>0.31</td>
<td>0.81</td>
<td>0.59</td>
<td>0.91</td>
<td>0.25</td>
<td>9E-05</td>
</tr>
</tbody>
</table>

Table 8. p-values from Pearson χ² between parental awareness of email tracking and their attitudes toward data mining of school-provided email.

<table>
<thead>
<tr>
<th>Country</th>
<th>U.S.</th>
<th>Germany</th>
<th>Japan</th>
<th>Argentina</th>
<th>Brazil</th>
<th>Chile</th>
<th>Colombia</th>
<th>Mexico</th>
</tr>
</thead>
<tbody>
<tr>
<td>Awareness</td>
<td>0.007</td>
<td>0.14</td>
<td>0.49</td>
<td>0.99</td>
<td>0.70</td>
<td>0.23</td>
<td>0.46</td>
<td>0.0004</td>
</tr>
</tbody>
</table>

In the first three nations we studied, the US, Germany, and Japan, we conducted two additional surveys. We studied what students actually did with their email accounts and we studied how parental attitudes towards data mining changed when parents were fully briefed on the extent of student online risky behavior. We found that students’ behavior was largely what was observed in other studies. We found that parental attitudes towards data mining after being briefed on children’s activities were virtually identical to those of parents who had not been briefed. Therefore we did not conduct the study in the remaining five countries.

8. Conclusions and Directions for Future Research

The paper indicates that the behavior of educational software and service providers is not consistent with either parental attitudes towards privacy or with the attitudes of students themselves. This is consistent with other studies in other countries [2,3]. In all the surveyed countries, parents object to the data mining of their children’s school-provided email accounts. And these objections remain regardless of whether the parents are aware of the extent to which educational software and service providers actually do track their children’s online activity. Moreover, parents in all countries almost universally believe responsibility for giving consent to data mining does not rest with school district’s data.
processing directors, but with the parents and the children. That is, in all nations surveyed, current search engine practices violate the preference of a vast majority of the adult population. Teens in the U.S. and Germany engage in risky online behavior more so than their Japanese counterparts. However, teens in each country feel strongly about being tracked by service providers and having their account linked by service providers. That is, in all nations surveyed, current search engine practices violate the preferences of a vast majority of the student population.

Follow up work should investigate:
1. Understanding the extent to which individual providers of software and services do or do not actually violate preferences.
2. Developing appropriate policies for the use of big data in educational settings.
3. Developing deeper understanding of teen behavior and why, indeed, privacy may not be a concern for so many online users around the world.
4. Developing a deeper understanding of teen behavior and of why teens’ actual behavior towards protecting themselves online differs so greatly from their stated preferences towards privacy.
5. Additional statistical tests on the difference between countries, and the relationships between parental awareness of data mining and integration of activities and objections to data mining.

9. References


Research was funded in part by the Wharton Behavioral Research Lab, and by Microsoft.