Grip Your Information So That It Does Not Expose You: Facebook's Privacy Shortfalls and Their Solutions

by Dmitrij Borscs

Over 160 million Americans have a Facebook account and over 50% of them update their profile every month (Quentin Fottrell, 1). Due to such robust social media activity, young adults in the United States need to reevaluate the worth of privacy, as it has become an intangible possession of users that can be unnoticeably collected by employers or marketing firms. According to Harvey Jones, over 91% of users had not read the terms of service at the time they registered and 89% had never read the privacy policy (Harvey Jones & Jose Soltren, 20-21). The high rates of negligence show that the American youth takes privacy for granted and assumes Facebook and federal privacy laws protect it. Despite contrary belief, Facebook can indeed share one's information with companies for advertising or other purposes, as indicated in their privacy policy (Jones & Soltren, 20-21). Few people realize that Facebook and its partners are regular businesses, making profits by collecting and selling the personal data of their users.

There is substantial grey area when it comes to making federal privacy laws: the social media industry is a novelty for which the government has not yet fully mastered regulation. Therefore, there are many loopholes in the legislative system. Privacy laws remain weak: the recent incidents surrounding Edward Snowden and the government's increasing desire to collect information about its citizens are not reassuring. Furthermore, the federal Privacy Act, amended forty years ago, remains stale and outdated, thus failing to regulate the concealed exploitation of Facebook and its third-party marketing partners. Although the socioeconomic consequences of privacy loss can be hard to identify, there are many steps an individual can take to reinforce information security. I believe that personal information can be effectively controlled by the individual who releases that information. We should not be relying on privacy laws or Facebook's promises to protect us; we should be proactively monitoring the types of information we are putting on display and recognizing the effects it might have on our friends, family, and future or current employers.

Where do privacy problems stem from and where do they grow?

A Facebook profile can be as minimal as an e-mail address, a name, a birth date, and a gender. However, if one wants to enhance their social experience by going beyond this basic point (as most users do), there are many other types of information a user can disclose. Additional data could include education, a relationship status, visuals like pictures and videos, one's previous work experience, and interests such as music, cinematography, and many others. If you synchronize your life events with Facebook by checking into places and/or attending Facebook events, marketing companies can predict your likes/dislikes and future behavior. This analysis is enhanced by unseen data collection, which an average user might not immediately recognize. Login information, such as time of day and frequency of logging into Facebook, is recorded and analyzed. Every click and every website visit is documented and used to strengthen the marketing algorithms of Facebook and its third-party marketing partners. Despite the fact that information exchange practices between the Facebook platform and its apps have received a tremendous amount of scrutiny and criticism, most Facebook users tend to ignore these warnings

and continue to use the applications (Jennifer King, Airi Lampinen & Alex Smolen, 10). Another vulnerable point of Facebook is the application platform which adds an additional layer of complexity for privacy statements and terms of use. Application developers usually collect data by leeching onto players' Facebook profiles. Perhaps not all users have the above mentioned types of information disclosed. Nevertheless, once the data appears on Facebook, it is saved forever, meaning that all information is historically searchable even after deletion.

The content that a user shares affects different social groups in different ways. A user might have 600 "friends", but not all of those friends belong to the same social circle. Some of them are family, some of them are close friends, possibly some they have only met once, and some perhaps coworkers or employers. The best way to analyze how one post impacts social circles differently is to separate them into personal and professional.

Personal effects may include arguments with family about inappropriate emotional statuses or compromising pictures, a quarrel with a loved one because of a misrepresented hug or "poke," or even jealousy from friends after revealing memories of an activity enjoyed without them. There is substantial evidence supporting the idea that young adults are the most concerned about controlling their personal information. For instance, young adults explore their identity online, but try to control what their parents can see of that online identity (Emily Christofides, Amy Muise & Serge Desmarais, 343). However, from my personal experience, it is only a small portion of young adults who recognize this problem and try to actively filter information from one social circle or another, whereas the rest of the demographic group still fails to differentiate information dissemination. The constant struggle to filter information may consequently hurt one's popularity as it is one of the main reasons why young adults disclose so much information in the first place. According to Emily Christofides, Facebook makes information disclosure the key factor in assessing a person's popularity. Having a presence on Facebook requires that a person posts many pictures, has active discussions, and shares many personal interests (Christofides, Muise & Desmarais, 343). One's Facebook experience is formed by the responses of their "friends": they like and comment on the activities or pictures that the person shares. The more popularity a user wants, the more they need to disclose. Christofides' study also concluded that general disclosure was a significant predictor of information control, and the two were inversely correlated (Christofides, Muise & Desmarais, 343). This means that the more a user wants to enjoy Facebook, the more they will share and subsequently the less control they will have over it. On the other hand, the individual's family can become more involved as one posts more. The two social circles, friends and family, are inversely correlated so if one wants to get positive attention from his or her peers then he or she might get criticized by family, and vice versa. If one wants to concentrate on family, some of his or her friends might find those posts to be less fun. Eventually, the social balance between friends and family can be disturbed, and the person can suffer the negative personal effects of posting information on Facebook.

Likewise, from a professional standpoint, one's Facebook profile is visible to recruiters. An employer can easily find out more about a Facebook user than they might want to share before a potential interview. For example, if someone "liked" a company page previously and is now applying for work with that company's competitor, their Facebook may convey the wrong message to an interviewer. Similarly, many people do not get a chance for an interview after being Facebook scanned. Employers can observe an individual's social behavior by simply

looking through their shared information. If they find something unfitting, then that might tip the scales to the unfavorable outcome. Christofides concluded that 20% of users would not be comfortable with employers seeing certain information on their Facebook site. However, most of those participants also admitted to not controlling who sees what information because they did not want to give up their exposure to popularity (Christofides, Muise & Desmarais, 343). Again, this finding is an extension of the friend-family balance. As a result, it becomes even harder to find the perfect combination of information to share in order to satisfy the three branches of the social balance. Internet services, such as Facebook, are in between helping users connect and share information, while preventing them from unintentionally exposing sensitive or embarrassing information to other users or third-parties (King, Lampinen & Smolen, 10). In the same way, individuals provide third-party marketing and data collecting companies with valuable information without realizing it.

How is privacy being publicly sold?

As the amount of total information shared has rapidly increased, marketing companies have recognized the opportunity to capitalize on this enormous pool of data. Currently, Facebook sells targeted advertising to many users of its site, and cooperates with firms such as Apple, Nike, and JetBlue to assist in marketing their products to college students (Jones & Soltren, 5). Many companies whose target market coincides with Facebook's have seized the opportunity to advertise through the site. The advertisements are constructed by very complex and sophisticated algorithms that harvest all data from one's profile page and predict the types of products that the individual might be interested in. Harvey Jones and Jose Soltren found that connected users disclose more personal information, especially commercially valuable information (Jones & Soltren, 18). The popularity contest, with such a large network and so much information, is a goldmine for data collecting and advertising companies. Furthermore, the marketing algorithms are constantly enhanced because users who frequently update their profiles, tend to be even more open (Jones & Soltren, 16). However, the data is not only impressive in quantity, but also valuable in quality. Jones' study showed that users put real time and effort into their profiles, making the data accurate and desirable (Jones & Soltren, 13).

In one particular research study, Harvey Jones and Jose Hiram Soltren successfully downloaded the majority (over 70%) of personal data provided by students from four different universities by applying simple algorithms (Figure 1.0). This only shows how simple it is to collect data without even having specific technology or technical knowledge.

Figure 1.0 Success Rates In Downloading Profiles

School	Number Profiles	Number Downloaded	Percentage
MIT	10063	8021	79.71%
Harvard	25759	17704	66.16%
Oklahoma U.	28201	24695	70.54%
NYU	32250	24695	77.41%
Total	97273	70311	72.28%

Moreover, Facebook has become one of the most valuable sources of information, as its users have an incentive to make the information accurate. Generally speaking, profiles used for social networking are likely to be almost 100% accurate, as they are maintained by their subjects who want to reflect fresh and truthful data (Jones & Soltren, 26). To be more exact and show how much the data that Facebook users provide is worth, we can observe the graph below (Figure 1.1). The chart shows that each user in the United States provides approximately $9 in data and actual sales revenue. This is an enormous amount of money if you multiply that by the number of Facebook users in the United States. Also note the difference between the United States and other countries: Americans use Facebook more frequently and update their information more accurately. As a result, marketing firms gain a higher value out of each individual. If one did not experience any direct impacts of such privacy exploitation, then this would probably not be significant, but users are bombarded by advertisements in a manner we cannot ignore.

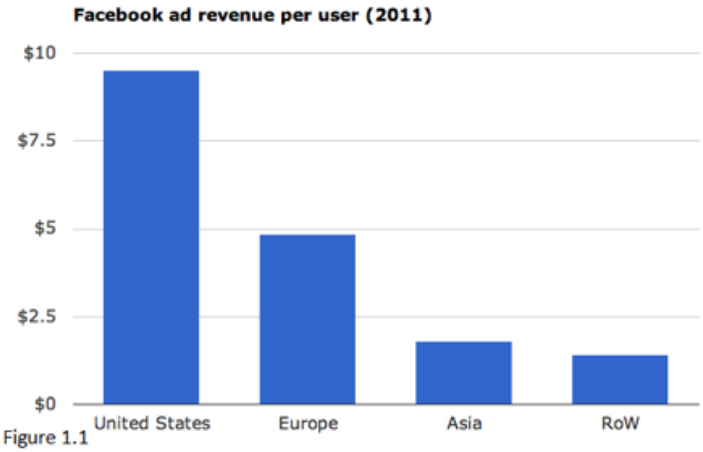

Figure 1.1

The newsfeed of Facebook users is increasingly saturated with advertisements that an individual cannot bypass because of the customized approach of ads. If a user likes a rock band's page, advertisements in their newsfeed might recommend buying that band's music, or a similar band's music. The purpose of being on Facebook is to enjoy the social experience. As users are constantly interrupted by these advertisements; they take away the smooth experience of social networking. Moreover, e-mail provided upon registration is used to send advertisements that are well-tailored to users. The amount of e-mails a user recieves is overwhelming and quickly turned into spam. Once a user receives the first couple of e-mails, it is very hard to stop the e-mail flow, even after unsubscribing from mailing lists. Spam quickly fills up personal e-mail accounts and prevents users from effectively managing their inboxes.

Another frustrating aspect of privacy loss is that third-party companies set cookies on browsers. The blanket statement of Facebook regarding information disclosure allows the company to disclose any personal data to advertisers. It also allows advertisers to set cookies that are not governed by the privacy policy, introducing a hidden threat (Jones & Soltren, 20-21). Cookies are used to track and record website activities and cause periodic pop-ups and other bothersome browser activities that alter the online experience. According to Luigi Dumirescu, in this new internet era--due to Google searches, e-mail traffic, commercial transactions, cookies and public information on social networking sites-- personal privacy is under attack (Luigi Dumirescu,

Oana Stanciu, Mihai Tichindelean & Simona Vinerean, 41). The wide spectrum of effects has a significant socioeconomic consequence on young adults in the United States. As the number of Facebook users increase daily, there is a call for recognition and treatment.

How can privacy be appreciated and protected?

Another interesting finding shows that Facebook users are significantly more likely to disclose information on Facebook than they would elsewhere (Christofides, Muise & Desmarais, 343). Still, this information affects social circles, e-mail and browsing experiences, as well as employment. We need to realize that Facebook is very closely interconnected with our actual lives and that we need to protect our privacy online as we already do in person. There are several steps an individual can take to protect one's privacy. These steps can be separated into precautions during registration and behavioral changes.

When a user creates a Facebook account, they are asked for an e-mail address. I advise creating a new e-mail address just for the purpose of that registration. The separate e-mail will be accessible if changes need to be made to account settings, but will not pollute a working mailbox, thus preventing the user from receiving spam. Also, refrain from sharing cellphone number or home address. These are very sensitive types of information that would rarely be shared even in face-to-face communication. Furthermore, when sharing content, a user should think about who will see that content. Is it only close friends, or family as well? Remember that an employer can easily look up any information shared at any point, so that should instigate a shift in posting behavior. It is generally a good idea to stay conservative in terms of sharing behavior. If you want to separate friends and family, I recommend creating separate Facebook accounts for the two or not adding family at all. After all, the main focus of Facebook is to connect with one's school and college friends. In addition, I advise one not to post pictures from parties or drinking occasions. There is a review option that one can setup which will prompt the tagged person to review any visual material before it is displayed on their timeline. Pictures of get-togethers are acceptable, as long as they do not involve alcohol, any indication of drinking, or other irresponsible activities. Also, do not post frequently: think quality rather than quantity. One's friends do not want their walls flooded by his or her posts. Moreover, do not like any pages of companies or other entities within your industry of profession. Usually business is conducted over LinkedIn and not Facebook, but a bad "like" or comment can have a serious impact on the hiring process.

The approach I am offering makes a profile clean and equally applicable to all social circles from the start. There are many claims that users cannot protect themselves from employers anymore: Facebook has announced new changes to its privacy settings that means users can no longer choose to hide their profile from searches on the site (Vincent, 1). This would have a serious impact if the person was trying to change his or her name in order to hide from the employer, but since the profile I propose is clean, it has no impact on the user's privacy whatsoever. In addition, some researchers claim that users are not protected from criminal surveillance because it is fair play to credit everything that a person says and thinks to his or her posts. Anything a person announces publicly can be used against them. Facebook is not an exception. However, if a reasonable and healthy profile is maintained and consequences are considered, it is not likely for illegal content or criminal evidence to be shared.

Unfortunately, the most consistent factor that correlates with increased user privacy concern is the experience of an adverse privacy event on a social networking site. Users learn about privacy risks the "hard way" by experiencing an unwanted information disclosure event first-hand (King, 9). By following the directions listed above users will not engage in any activity that might hurt their privacy in the long run. I offer a constantly proactive approach to increase young adults' control over their privacy. Such information security will result in a more stable social balance between family, friends, and workplace. It might also eliminate some of the concealed barriers against getting hired for jobs that offer young adults financial stability.

Works cited

Bowling, Drew. Facebook International Ad Revenue Is Pretty Bad. WebProNews, 21 May 2012. Web. Sept.-Oct. 2013.

Christofides, Emily, Amy Muise, and Serge Desmarais. Information Disclosure and Control on Facebook: Are They Two Sides of the Same Coin or Two Different Processes? Cyberpsychology & Behavior Volume 12, 1 Mar. 2009. Web. Sept.-Oct. 2013.

Dumirescu, Luigi, Oana Stanciu, Mihai Tichindelean, and Simona Vinerean. Disclosing the promising power of Social Media – an important Digital Marketing Tool. Studies in Business and Economics Volume 6, Apr. 2011. Web. Sept.-Oct. 2013.

Fottrell, Quentin. "Facebook loses 1.4 million active users in U.S." Market Watch, 15 Jan. 2013. Web. Oct.-Nov. 2013.

Jones, Harvey and Jose Hiram Soltren. Facebook: Threats to Privacy, 14 Dec. 2005. Web. Sept.-Oct. 2013.

King, Jennifer, Airi Lampinen, and Alex Smolen. Privacy: Is There An App for That? Proceedings of the Seventh Symposium on Usable Privacy and Security (SOUPS), 20-22 July 2011. Web. Sept.-Oct. 2013.

Vincent, James. Facebook tells users they can't hide from searches. The Independent, 11 Oct. 2013. Web. Oct.-Nov. 2013.