



May 30, 2008

Privacy Commissioner of Canada
112 Kent Street
Ottawa, Ontario
K1A 1H3

Dear Commissioner Stoddart:

Re: **PIPEDA Complaint: Facebook**

This is a complaint under s.11 of Part I of the *Personal Information Protection and Electronic Documents Act (PIPEDA)* regarding the unnecessary and non-consensual collection and use of personal information by Facebook, a social networking website.

We submit that Facebook is violating Principles 4.1, 4.2, 4.3, 4.4, 4.5, 4.7, and 4.8 of *PIPEDA*, Schedule 1 by failing to:

- Identify all the purposes for which it collects Users' personal information (Principle 4.2);
- Obtain informed consent from Users and non-Users to all uses and disclosures of their personal information (Principle 4.3);
- Allow Users to use its service without consenting to supply unnecessary personal information (Principle 4.3.3);
- Obtain express consent to share Users' sensitive information (Principle 4.3.6);
- Allow Users who have deactivated their accounts to easily withdraw consent to share information (Principle 4.3.8);
- Limit the collection of personal information to that which is necessary for its stated purposes (Principle 4.4);
- Be upfront about its advertisers' use of personal information and the level of Users' control over their privacy settings (Principle 4.4.2);
- Destroy personal information of Users who terminate their use of Facebook services (Principle 4.5);
- Safeguard Users' personal information from unauthorized access (Principle 4.7); and
- Explain policies and procedures on the range of personal information that is disclosed to third party advertisers and application developers (Principle 4.8).

Statement of Facts

Background

Facebook, launched in February of 2004 by founder Mark Zuckerberg, is an online social networking company headquartered in Palo Alto, California with members from around the world. The website describes itself as “a social utility that connects people with friends and others who work, study and live around them.” Basically, Facebook is a free web based tool which allows members to “upload photos, or publish notes; get the latest news from your friends; post videos on your profile; tag your friends; use privacy settings to control who sees your info; join a network to see people who live, study, or work around you”. Initially membership of the social networking tool was restricted to Harvard students. However, Facebook soon expanded, providing membership to any student at a university recognized by its administration. In February of 2006, greater expansion occurred, during which membership became available to anyone with a valid email address.

Facebook now has more than 69 million active members across the globe and it is currently the fifth most-trafficked website in the world.¹ Canada is the third largest Facebook member base with more than 7 million active Canadian members.² New demographic studies indicate that over 700,000 Facebook members belong to the Toronto network alone, which represents approximately 25% of the city’s population.³

The information gathered below is taken from Facebook’s Privacy Policy and Terms of Use on March 27, 2008.

Sharing Personal Information

Facebook allows a Facebook user (a User) to share information through a profile page (a Profile) with other Users with whom they share a relationship. Information that can be shared on a User’s Profile includes birth date, phone numbers, email addresses, instant messaging addresses, place of employment, and place of education.

a) Friends and Networks

Initially when a User joins Facebook, his or her Profile is only viewable by other Users who have been designated as the User’s friend on Facebook (a “Friend”). Friends of a User can see all personal information that the User has provided to Facebook for the User’s Profile. To restrict the information that is shared with Friends, a User must take further action and change his or her privacy settings.

Most Users also choose to join a network based on their school, workplace or region (a “Network”). Once a User joins a Network, Facebook automatically begins sharing some of that

1 <http://www.facebook.com/press/info.php?statistics>

2 <http://www.facebook.com/press/info.php?statistics>

3 <http://www.thestar.com/News/Ideas/article/245217>

User's information with the other Users that have joined the same Network. This information that can be seen by other Users in the Network is the same information that can be seen by a User's Friend, except for any contact information. As with Friends, a User can also restrict information that is shared with other Users in his or her Network. However, to do so, the User must take further action and change his or her privacy settings.

A User may contact other Users through a poke, message, or Friend request. When a User contacts another User through a poke, message, or Friend request, Facebook lets the contacted User see part of the contacting User's Profile for 30 days, even if the User's privacy and Network settings would otherwise prevent the person from seeing the User's Profile.

A User may also search for other Users based on their name or other search criteria. Depending on the privacy settings of the User being searched, the User searching will be able to view either the User's name and Network or all of the User's personal information. Individuals that are not Users of Facebook may also search the Facebook website for Users. Information they receive as a result of this search includes the User's Name and a thumbnail of the User's Profile picture. Users must change their privacy settings to limit who can find them in a search and how much information the searcher will receive.

b) Facebook Wall

By default, every User's Profile includes an area in which other Users can post public messages (a "Wall"). These messages exist on the User's Profile until deleted by either the Profile User or the User who posted the public message, or until the Profile User deactivates his or her Facebook account. Messages posted on a User's Wall are not restricted. They may contain text, video, pictures, or links. Currently, Users cannot delete all Wall posts with a single click. Rather, they must be deleted one by one. Facebook allows the User to set which Users or groups of Users ("Friend Group") can see the User's Wall via the User's Privacy Settings.

c) Groups

Facebook allows Users to join or create a social group, which links that User with other Users (a "Group"). A User can be a member of up to 200 Groups. Groups can be created or joined on the basis of a Network or a type. Types of Groups are related to issues such as a business, a political cause, a school, and a place of employment. Given the wide variety of options available when creating a Group, a User can create a Group for essentially any purpose. A User can leave a Group at any time. Each Group has its own Profile Page and includes Group information, contact info, photographs, videos, posted items, a Wall, a list of member Users, related Groups, and a list of administrators and creators.

d) News-feeds

A User's Profile also includes a bulleted list of the most recent actions and items ("Stories") taken by that User ("Mini-feed"). By default, the Mini-feed broadcasts all available Stories. However, the User has the option of selecting which Stories are broadcasted in the Mini-feed. Stories can also appear in a bulleted list of all Users' actions which appears on a User's

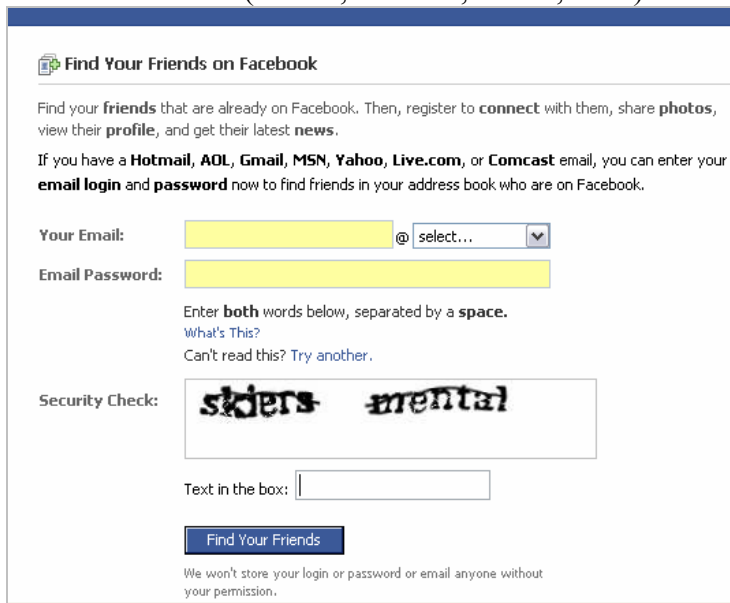
Homepage (“News-feed”). A News-feed includes the Stories of all Users that a User is Friends with. A User can set which type of Stories he or she will see more frequently.

e) Tagging

Users can add metadata tags to photographs. These tags can be identified to particular areas of the photograph. For example, a picture of a family in front of a landmark can have the individual faces of family members tagged with their names and the landmark tagged with its name. If the subject tagged is not a Facebook member, then the tag remains in plain text when published. However, if the subject tagged is a Facebook member, the tag becomes a hyperlink to his or her Profile. When a User is tagged in an image, they are given a brief notice. Upon viewing the image that has been tagged with that User's name by another, the User has the option of removing the tag. When photographs of Users are displayed, this display includes their own photographs and those published by others that are tagged with their names.

f) Contact Importer

Users are invited by Facebook to “[f]ind out which of your email contacts are on Facebook.” Facebook asks Users for their email address and password for many of the major providers of web mail services (Yahoo, Hotmail, Gmail, etc...) as shown in Figure 1.



The screenshot shows a web form titled "Find Your Friends on Facebook". The form contains the following elements:

- A header with the title "Find Your Friends on Facebook" and a small icon.
- Introductory text: "Find your friends that are already on Facebook. Then, register to connect with them, share photos, view their profile, and get their latest news."
- Instructions: "If you have a Hotmail, AOL, Gmail, MSN, Yahoo, Live.com, or Comcast email, you can enter your email login and password now to find friends in your address book who are on Facebook."
- Input fields: "Your Email:" with a text box and a dropdown menu, and "Email Password:" with a text box.
- Instructions: "Enter both words below, separated by a space. What's This? Can't read this? Try another."
- Security Check: A box containing the words "skiers" and "mental" in a distorted font.
- Text input: "Text in the box:" with a text box.
- Submit button: "Find Your Friends".
- Disclaimer: "We won't store your login or password or email anyone without your permission."

Figure 1

Once Facebook obtains the email address and password, it logs into the account and downloads all available contacts. Facebook can also import email contacts from applications such as Outlook and Thunderbird. Users are then shown a list of which of these contacts are current Facebook members and have the choice of sending friend requests to each of them. The screen has all the contacts pre-selected to be sent friend requests. The User may deselect contacts from the list.

The User is then given the option of inviting all of their other contacts to join Facebook. Again, all of the contacts are pre-selected. The default behavior is to send messages to all of one's contacts inviting them to become friends on Facebook.

g) Third Party Applications

On May 24, 2007, Facebook announced the Facebook Applications Platform, which provides access to the Facebook database to third party developers. Since the announcement, thousands of applications have been created on the open platform, gaining access to User information accessible from Facebook's database. The platform has become such a phenomenon that in the fall of 2007 a course at Stanford University was devoted to developing Facebook Applications.

h) Advertisements

Facebook employs two different methods of advertising, Social Ads and Facebook Pages, which contribute to its yearly revenues of roughly \$150 million. Facebook claims that "Social Ads allow your businesses to become part of people's daily conversations."⁴ Facebook Social Ads allow a business to create a Facebook Social Ad and target it to the audience that it chooses.⁵ Within the Social Ad method of advertising are two variations. The first and most common variation is the placement of an advertising banner in the left hand "Ad Space", which is "visible to Users as they browse Facebook to connect with their friends".⁶

The second variation of Facebook Social Ads is placed in the News-feeds. It is known as "Beacon". Beacon allows a business to broadcast actions taken by a User on their website to that User's News-feed. Beacon actions include "purchasing a product, signing up for a service, adding an item to a wish list, and more."⁷ In November of 2007, Facebook announced that 44 websites are using Beacon to allow Users to share information from other websites for distribution to Friends on Facebook.⁸

Terminating a Facebook Account

When a User wishes to terminate his or her Facebook account, Facebook offers a "deactivation" option. By deactivating, a User's account becomes dormant but can be reactivated upon request. Facebook retains all personal information in deactivated accounts for an unspecified length of time. Users who wish to terminate their accounts are offered no other option. In particular, Facebook offers no simple "delete" option, under which all account information is fully deleted.

In February of 2008, Facebook stated publicly that it would begin allowing Users to remove their accounts entirely, by simply emailing the company. However, Facebook still does not offer Users a one-click permanent "delete" option, alongside the temporary "deactivation" option.

4 <http://www.facebook.com/business/?socialads>

5 <http://www.facebook.com/business/?socialads>

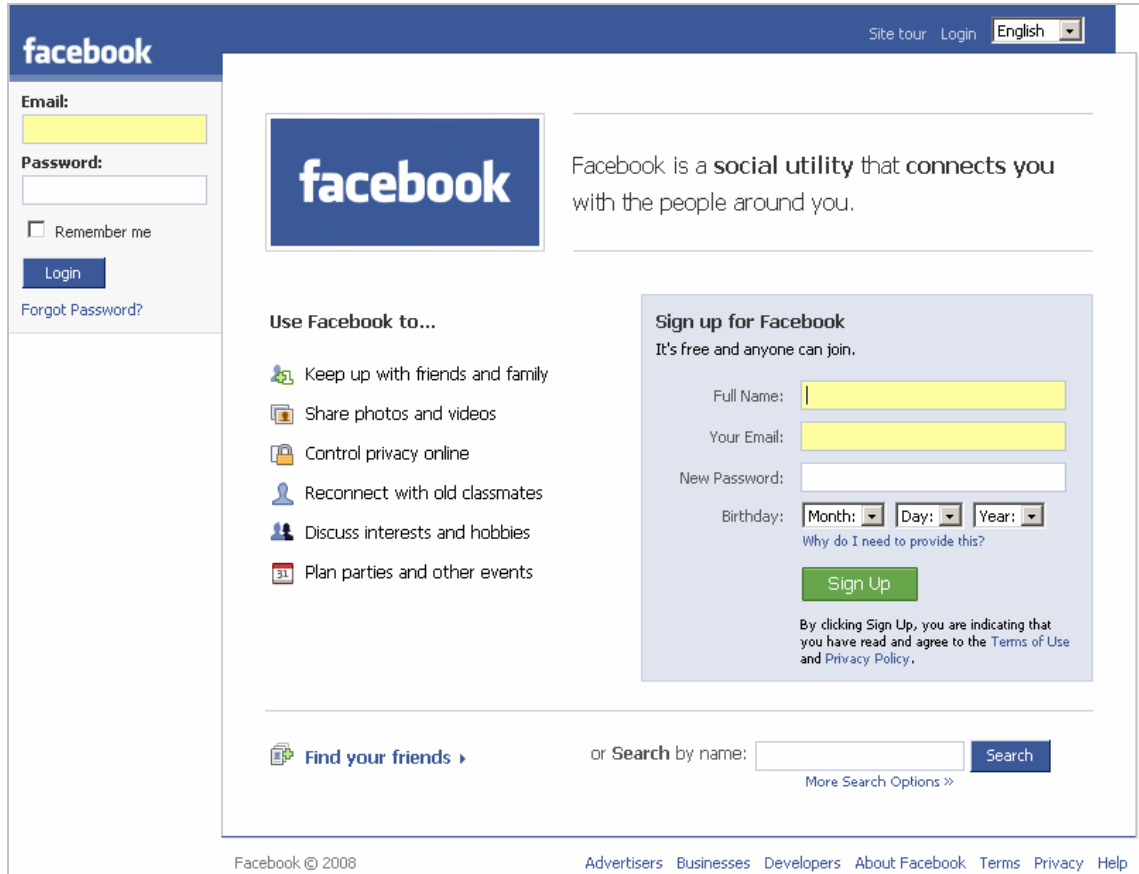
6 <http://www.facebook.com/business/?socialads>

7 <http://www.facebook.com/business/?beacon>

8 <http://www.facebook.com/press/releases.php?p=9166>

Registration Process

A new User is required to enter his or her name, email address and password in the sign-up box on Facebook's home page.



The screenshot shows the Facebook homepage with a registration form. On the left, there is a login section with fields for 'Email:' and 'Password:', a 'Remember me' checkbox, and a 'Login' button. Below the login section is a link for 'Forgot Password?'. The main content area features the Facebook logo, a tagline 'Facebook is a social utility that connects you with the people around you.', and a list of features under 'Use Facebook to...'. The registration form, titled 'Sign up for Facebook', includes fields for 'Full Name:', 'Your Email:', 'New Password:', and 'Birthday:' (with dropdown menus for Month, Day, and Year). A green 'Sign Up' button is prominently displayed. Below the button, a disclaimer states: 'By clicking Sign Up, you are indicating that you have read and agree to the Terms of Use and Privacy Policy.' At the bottom of the page, there is a 'Find your friends' link, a search bar with a 'Search' button, and a footer with copyright information and various links.

Figure 2

After the User has entered the required information and pressed the “Sign Up” box they are immediately sent a confirmation email to the email address that they provided in the sign-up page. By clicking the “Sign Up” button, the User acknowledges that they have read the Terms of Use (see Appendix 2 and below) and Privacy Policy (see Appendix 1). The User is then required to click the link provided in the email and sign into Facebook, in order to begin the 3 step registration process (with an intermediary step of entering two words as part of a security check).

The User is directed to a series of 3 registration screens after providing the required information on the initial sign up page. This 3 step registration process enables Users to confirm any current friends that they may have on Facebook (and subsequently invite them to be in their list of Friends), enter their affiliated educational institution or company and join a Network. However, all of these steps are optional and can be skipped (that is, the User can skip entering this information and proceed to their main Profile page).

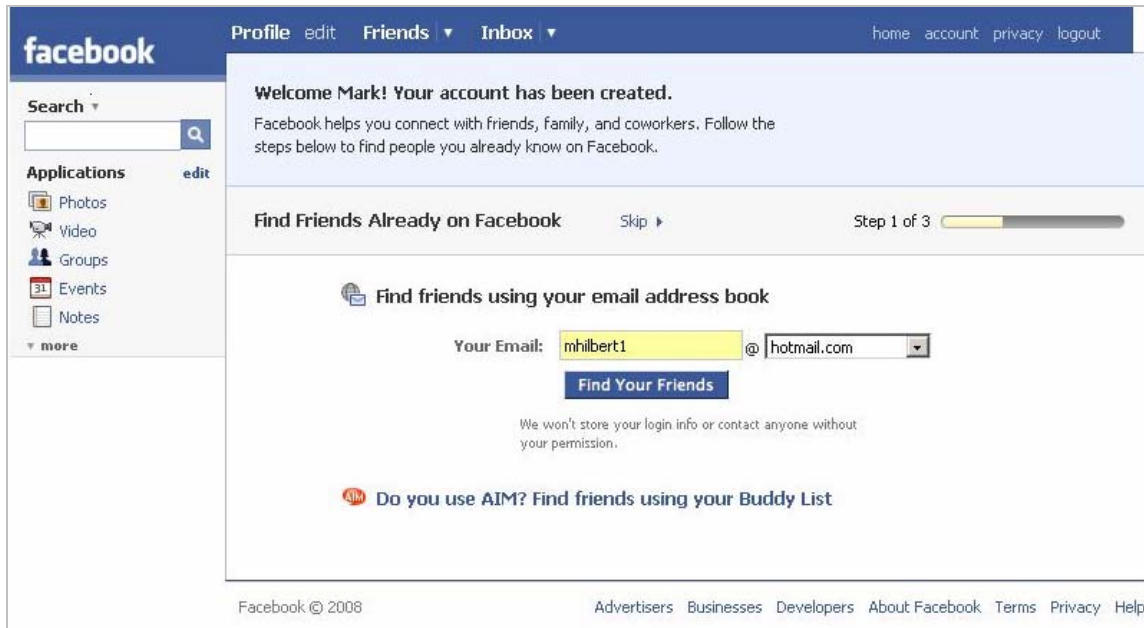


Figure 3



Figure 4



Figure 5

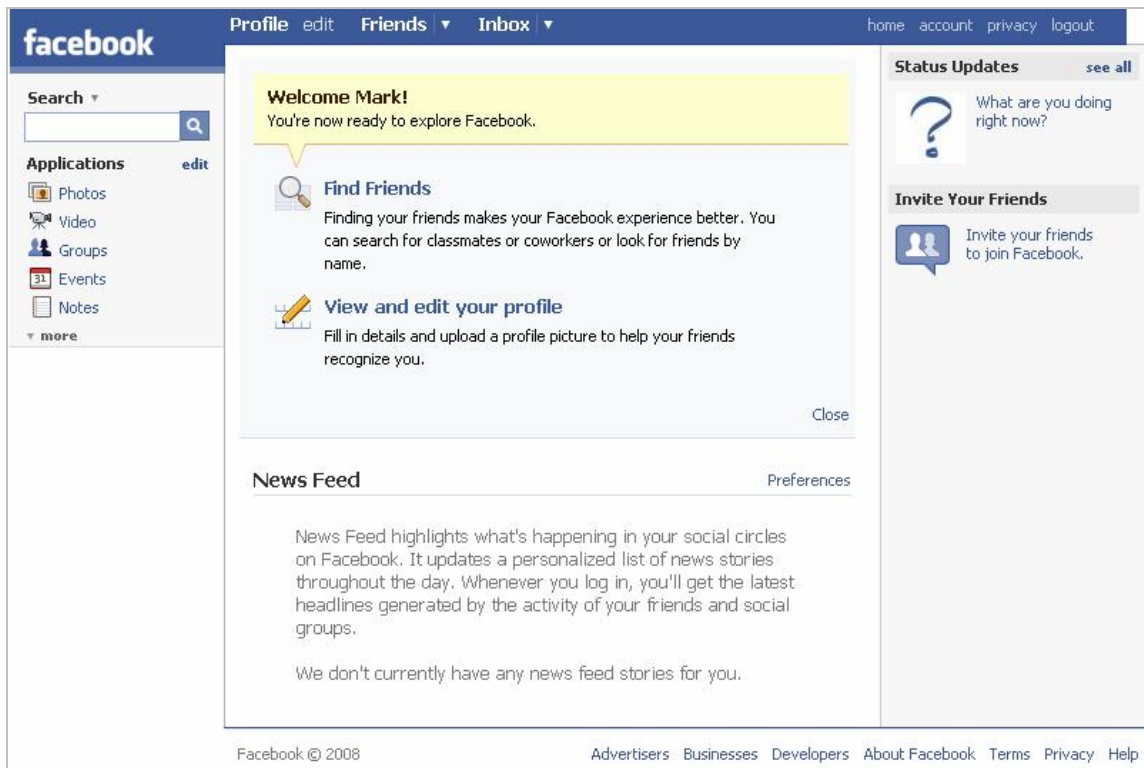


Figure 6

Terms of Use: Key Provisions

Facebook's Terms of Use include a number of provisions related to User privacy. Below are some excerpts.

Eligibility

The website states that it "is intended solely for users who are thirteen (13) years of age or older." In addition, anyone between the ages of 13 and 18 who is not in high school or college is prohibited from using the website. Their use is "unauthorized, unlicensed and in violation of these Terms of Use." In Facebook's "Customer Support: Security", Facebook focuses on the safety and security of young people. Facebook advises that "parents of children 13 years and older should consider whether their child should be supervised during the child's use of the Facebook site."

Authenticity of Registration Data

Facebook states in its Terms of Use that Users are required to "(a) provide accurate, current and complete information about you as may be prompted by any registration forms on the Site ("Registration Data")...[and] (c) maintain and promptly update the Registration Data, and any other information you provide to the company, to keep it accurate, current and complete."

Proprietary Rights in Site Content; Limited License

Facebook makes it clear in its Terms of Use that all the content on the site is the property of the company: "All content on the Site and available through the Service, including designs, text, graphics, pictures, video, information, applications, software, music, sound and other files, and their selection and arrangement (the "Site Content"), are the proprietary property of the Company, its users or its licensors with all rights reserved."

As a User, you are given a limited license to use your own information. However, this license does not extend to any data mining, robots or similar data gathering or extraction technology that you might use in connection with such information.

User Conduct

Facebook states that aside from the advertising provided by them on the site (e.g., Facebook Flyers, Facebook Marketplace), Facebook is for personal, non-commercial use. The Terms of Use also prevent Users from doing the following activities, which can impact User privacy. Users may not:

- harvest or collect email addresses or other contact information of other Users from the Service or the Site by electronic or other means for the purposes of sending unsolicited emails or other unsolicited communications;
- upload, post, transmit, share, store or otherwise make available any content that we deem to be harmful, threatening, unlawful, defamatory, infringing, abusive, inflammatory, harassing,

vulgar, obscene, fraudulent, invasive of privacy or publicity rights, hateful, or racially, ethnically or otherwise objectionable;

- upload, post, transmit, share, store or otherwise make available any videos other than those of a personal nature that: (i) are of you or your friends, (ii) are taken by you or your friends...
- impersonate any person or entity, or falsely state or otherwise misrepresent yourself, your age or your affiliation with any person or entity;
- upload, post, transmit, share, store or otherwise make publicly available on the Site any private information of any third party, including, addresses, phone numbers, email addresses, Social Security numbers and credit card numbers;
- solicit personal information from anyone under 18 or solicit passwords or personally identifying information for commercial or unlawful purposes;
- intimidate or harass another;
- use or attempt to use another's account, service or system without authorization from the Company, or create a false identity on the Service or the Site.
- upload, post, transmit, share, store or otherwise make available content that, in the sole judgment of Company, is objectionable or which restricts or inhibits any other person from using or enjoying the Site, or which may expose the Company or its Users to any harm or liability of any type.

Privacy Settings

Privacy settings are defaulted to share Users' personal information. If Users wish to restrict the information that they share, they must opt-out of most of the sharing settings. It is important to note that Users are not automatically directed to Facebook's privacy settings upon registering for Facebook. A thorough description of the privacy settings offered by Facebook is available in Appendix 3.

How Facebook Violates PIPEDA

1. Social Networking

Facebook's main purpose is to facilitate online social networking. Facebook makes this clear to Users upon registration. This purpose is also stated in Facebook's Privacy Policy and Terms of Use. Social networking involves sharing of photographs, messages and other personal information. However, the breadth and scope of what is shared is not clear.

Step 3 of the registration process allows Users to join Networks based on their geographical location, hobbies and interests. Although this is an optional step, joining Networks is encouraged and is a central feature of Facebook. When Users first joins a Network, they are informed that they will be sharing their Profiles with other Users in the Network. Users are also informed that they can change their privacy settings, but are not prompted to go this page (see Figure 5).

Before Users may begin the 3-step registration, they must provide their full name, email and birthday (see Figure 2). Users cannot continue the registration process unless they provide this information. Facebook claims to require a date of birth to serve as a safety precaution and to preserve Facebook's integrity. Facebook also claims that it helps to facilitate its birthday application. After the Users have inputted this information, they are immediately sent a confirmation email advising them of their request to join Facebook. Users may then click on the link provided in the confirmation email and begin the 3 step registration process.

Facebook fails to identify its purpose for collecting personal information beyond Users' names and email addresses

Facebook does not adequately explain why Users must provide their date of birth in order to use Facebook. Although a date of birth may be useful for applications, Facebook does not adequately explain why it is necessary for Users to provide this information for its social networking purposes. Facebook also does not make a reasonable effort to inform Users how their dates of birth will be used as required by Principle 4.3.2 of PIPEDA. Furthermore, Users are barred from continuing the registration process if they do not provide their dates of birth, which is a violation of Principle 4.3.3 of PIPEDA. Although Facebook does stipulate that Users must be older than thirteen years of age, this requirement does not necessitate that Users provide their date of birth.

In its Privacy Policy, Facebook states "When you register with Facebook, you provide us with certain personal information, such as your name, your email address, your telephone number, your address, your gender, schools attended and any other personal or preference information that you provide to us". The Privacy Policy also states that, "When you use Facebook, you may set up your personal profile, form relationships, send messages, perform searches and queries, form groups, set up events, add applications, and transmit information through various channels. We collect this information so that we can provide you the service and offer personalized features". Facebook fails to adequately explain the nature of the personalized features it offers which would necessitate personal information beyond email address and name.

continued.....

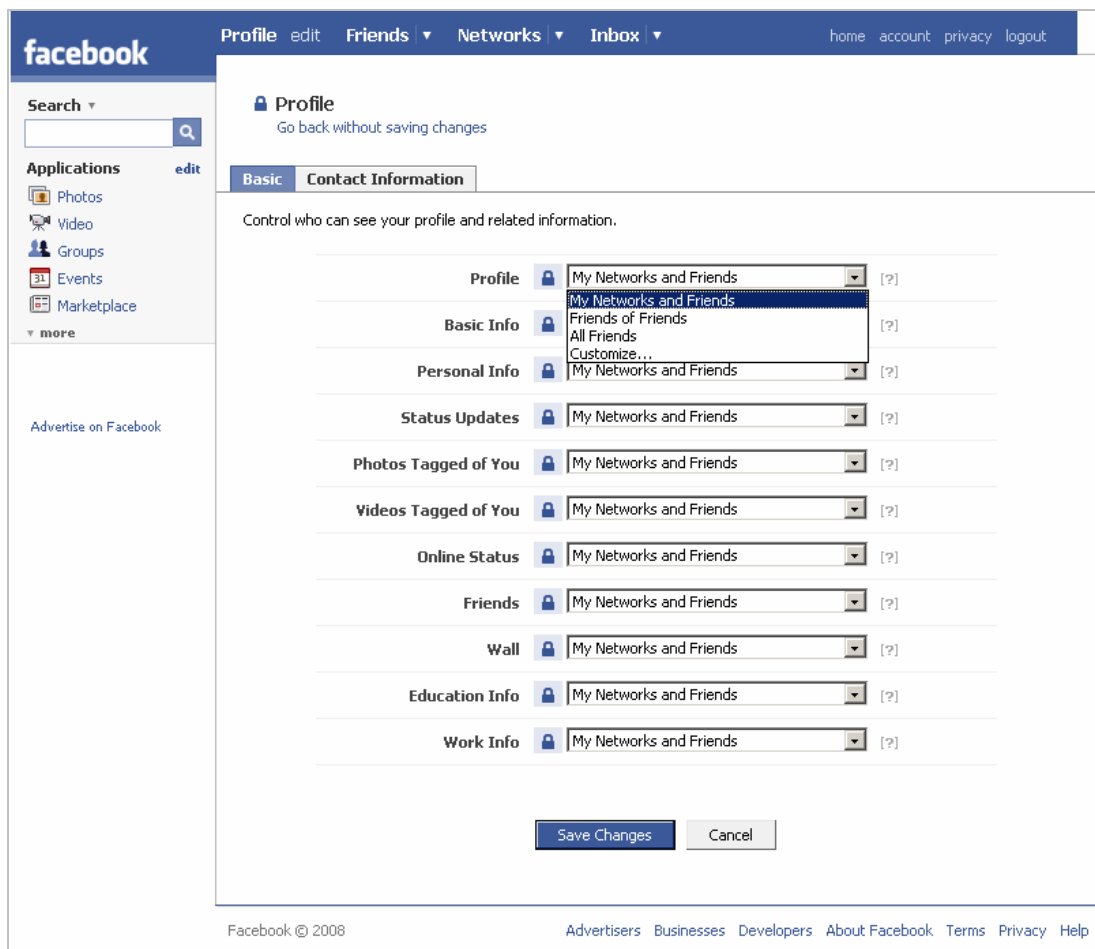


Figure 7

Facebook fails to obtain express consent to share Users’ sensitive personal information

Principle 4.3.4 of PIPEDA requires express consent for the sharing of sensitive information. Much of the information shared on Facebook could be sensitive, including marital status, age, hobbies and photographs. Given the advent of cyberstalking and cyberharrassment, the sharing of this information without express consent is especially problematic. Cyber stalkers could potentially target by age, hobbies or preferences.

When Users join Facebook and sign up for a Network (step 3 of the registration process, see Figure 5), the default privacy settings are set to share their personal information with everyone on the Network (Figure 7). This includes the sensitive information listed above. To restrict the information that they share, Users must opt out of the default privacy settings. However, an opt-in mechanism is required for the sharing of sensitive information under PIPEDA.

Principle 4.3.6 of PIPEDA states that an organization should generally seek express consent when the information is likely to be considered sensitive. Unless Users take action to “opt in” to sharing their sensitive information, Facebook cannot assume consent.

Facebook fails to provide adequate notice for Users' photo album privacy settings. If Users post photo albums on their Profiles, the default privacy settings for photo albums are set to share with everyone. Therefore, a User's non-Friends can view their photographs and any associated comments, even if that User's Profile is only searchable by their Friends. To restrict access to their photographs, Users must take action to "opt out" of the default settings. However, Users are not directed to their photo album privacy settings after uploading pictures. This is troubling considering that photographs and associated comments are often sensitive information.

Again, this is a violation of Principle 4.36 of PIPEDA, which states that an organization is required to seek express consent when the information is likely to be considered sensitive.

Facebook fails to notify Users of the uses and disclosures of their personal information

Facebook does not make a reasonable effort to advise Users of the purposes for which their personal information is used. Facebook also does not advise Users of the extent of their personal information that will be shared by joining a Network. Without this knowledge, Users cannot provide meaningful consent. Instead, consent should be achieved through an opt-in box in the privacy settings. Users can be directed to their privacy settings immediately after completing step 3 of the registration process. Users would then "opt-into" joining a Network, only after confirming that they understood the extent of their personal information that would be shared with Networks (by selecting to "opt out" of the default settings and "opt in" to new settings, see Figure 7)

Currently, Users are not directed to their privacy settings after completing the 3 step registration process. Instead, Users are directed to their own Profiles where they can initiate other activities (such as inviting friends, joining Networks or editing their Profile). If Users wants to alter their privacy settings, they have to take action themselves by clicking on the small privacy link in the right corner of their Profiles. Facebook's failure to direct Users to their privacy settings is especially troubling, because the default privacy settings are set to share all personal information with "all of my friends" and all personal information except contact information with "all of my networks." Further, Users' name and Profile picture are defaulted to be searchable by everyone. Even now, after Facebook has recently altered its privacy settings, Users still must take their own initiative to view the new privacy settings. Facebook only alerts Users by displaying a message on the welcome page, not by directing them to their settings.

Facebook fails to meet the requirements for valid opt-out consent

In the alternative to our argument above, that opt-in consent is required to share Users' personal information, we submit that Facebook fails to meet the requirements for valid opt-out consent. According to the Privacy Commissioner of Canada, opt-out consent is valid only if an organization offers individuals an opportunity to refuse sharing their information for the organization's identified purposes. Individuals should be informed that their failure to "opt out" will constitute consent to the proposed uses or disclosures of their personal information.

However, Users are not alerted or directed to their default privacy settings upon completing the registration process. As noted above, the default setting share Users' Profiles and applications

with “all my networks” and “all my friends”. Although the privacy settings pages allow Users to opt-out of certain sharing, these options are not adequately brought to the attention of Users.

2. Facebook Advertising

As mentioned above, Facebook employs two different methods of advertising: Social Ads and Facebook Pages. Social Ads, according to Facebook, “allow your businesses to become part of people's daily conversations.”⁹ Social Ads allow a business to create an advertisement and target it to its desired audience.¹⁰

Within the Social Ad method of advertising are two variations. The first and most common variation is the placement of an advertising banner in the “Ad Space” located to the left of Users’ Profiles. Ad Space is “visible to users as they browse Facebook to connect with their friends” (see Figure 8).



Figure 8



Figure 9

The business first creates the text of a Social Ad and may choose to add a picture. The business then selects the target group, searching by criteria related to location, sex, age, education status, workplace, political views, and relationship status and by any keyword chosen by the business (see Figure 10). The business lastly purchases ads by either number of clicks or impressions. While the advertisement is in circulation, the business will receive continuous performance metrics, which include comprehensive demographic data.

⁹ <http://www.facebook.com/business/?socialads>

¹⁰ <http://www.facebook.com/business/?socialads>

I want to reach liberal men between 18 and 25 years old who are single in Toronto, ON who like Britney Spears. fewer than 20 people

Location:
 Everywhere By State/Province By City

Cities:

Sex: Male Female

Age: -

Keywords:

Education Status: All College Grad In College In High School

Workplaces:

Political Views: Liberal Moderate Conservative

Relationship Status: Single In a Relationship Engaged Married

Figure 10

The second variation of Social Ads is known as Beacon. It involves the placement of ads in the News-feed. The News-feed is bulleted list of actions taken by a User's Friends ("Stories") and others (see Figure 9). These "social stories, such as a friend's becoming a fan of [a business'] Facebook Page or a friend's taking an action on [the business'] website, make [the] ad more interesting and more relevant." Beacon allows a business with a website to broadcast actions taken by Users on their site to the News-feed. Beacon actions include "purchasing a product, signing up for a service, adding an item to a wish list, and more."¹¹ In November of 2007, Facebook announced that 44 websites are using Beacon to allow Users to share information from other websites for distribution to Friends on Facebook.¹² When Users perform an action that the business wants to broadcast, they will be alerted that the business' website is sending a Story to their Profile and will be given a chance to opt out. If Users do not opt out, the Story is shared with Friends. For example, if Users log onto Facebook and then sign up for a new account at the website Epicurious.com, they will receive a popup requesting permission to broadcast this Story on their Profile (see Figure 11). If Users do not take action at the prompt, they are again prompted when they returns to their account (see Figure 12).



Figure 11

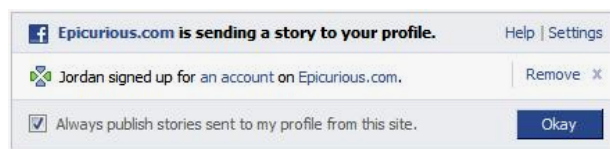


Figure 12

If Users accept the request, then the Story, signing up for a new Epicurious account, will be posted on their Profiles and will be visible to everyone who has access to their Profiles.

¹¹ <http://www.facebook.com/business/?beacon>

¹² <http://www.facebook.com/press/releases.php?p=9166>

Facebook fails to notify Users of its use of personal information for advertising purposes

PIPEDA Principle 4.3.2 states that “organizations shall make a reasonable effort to ensure that the individual is advised of the purposes for which the information will be used.” Principle 4.3.2 also states that “to make consent meaningful, the purposes must be stated in such a way that the individual can reasonably understand how the information will be used or disclosed”. Although Users must agree to the Privacy Policy, which states that personal information may be used for Social Ads,¹³ such notification is not sufficient given the nature of Facebook and its Users.

Firstly, a large percentage of Users are high school and lower school students. It cannot be assumed that they will comprehend the legal jargon and complicated wording in the Privacy Policy. Many of these Users are unaware of the potential dangers of sharing personal information. Further, the Privacy Policy is long and many Users will likely not read the clause that indicates that personal information is used for the purpose of Social Ads.

Secondly, the default setting includes the Users in both variations of Social Ads.¹⁴ If Users do not want personal information to be used for Social Ads, they must take additional steps to opt-out. Because the consent offered to Users is opt-out only, notice is especially important. Facebook is denying Users the extra notice that they would have received in an opt-in procedure. Furthermore, Users are not permitted to opt out of the Social Ads that appear on the left hand “Ad Space.” Users may only opt out of the News-feed Social Ads.

Therefore, Facebook does not make reasonable effort to ensure that Users are advised that their personal information is used for Social Ads, as PIPEDA Principle 4.3.2 requires. In order to provide sufficient notice to Users, Facebook must either require Users to opt-in to Social Ads or must provide a more obvious disclaimer to this use of personal information.

Facebook conditions its service on Users’ consent to sharing their personal information for the purpose of Social Ads

Principle 4.3.3 of PIPEDA states “an organization shall not, as a condition of the supply of a product or service, require an individual to consent to the collection, use, or disclosure of information beyond that required to fulfill the explicitly specified and legitimate purposes.” Facebook’s explicitly specified and legitimate purpose is social networking. However, Users may not opt-out of one variation of Social Ads, despite that these advertisements are not even remotely related to social networking. By requiring Users to agree to this use as a condition to its service, Facebook is violating Principle 4.3.3 of PIPEDA...

¹³ “Facebook may use information in your profile without identifying you as an individual to third parties . . . for purposes such as aggregating how many people in a network like a band or movie and personalizing advertisements and promotions . . .”

¹⁴ Users are also automatically included in the Beacon program; however, before any information is made public on the User’s Profile, specific consent must be given by the User. The User may also opt-out of the Beacon program completely.

Facebook fails to seek express consent from Users to share their sensitive information

PIPEDA Principle 4.3.6 states that “the way in which an organization seeks consent may vary, depending on the circumstances and the type of information collected. An organization should generally seek express consent when the information is likely to be considered sensitive.” Principle 4.3.6 applies to the collection and use of personal information.

The personal information used for Social Ads is sensitive information in some contexts. For example, the fact that a User is female, 13 years old, lives in a small town, and attends a certain school is likely sensitive information. Special precautions are needed to ensure the safety and well being of this young girl. Furthermore, Users’ Profiles may (and often do) contain a wealth of personal information, including favourite books, movie, and a general text box. Of the millions of Users, it is likely that some have posted sensitive information on their Profile. Facebook allows businesses to target their advertisements to Users based on a keyword search of their Profiles. Although Users may restrict their Profiles to very few Friends or none at all, their sensitive information will still be used for Social Ads.

Users consent to the use of their personal information for Social Ads by agreeing to the Privacy Policy. Facebook does not solicit consent by any other means. Consent to a lengthy, complex, privacy agreement is not express consent. Furthermore, Facebook requires the same level of consent from all Users regardless of the nature of their personal information. Therefore, Users’ sensitive information may be used by Facebook for Social Ads without express consent. Facebook is in breach of Principle 4.3.6 of PIPEDA.

Facebook fails to allow Users to withdraw consent to using their personal information for advertising purposes

Principle 4.3.8 of PIPEDA states that “an individual may withdraw consent at any time, subject to legal or contractual restrictions and reasonable notice. The organization shall inform the individual of the implications of such withdrawal.” Although Users may opt out and withdraw consent from both Beacon and Social Ads in the News-feed, Facebook does not allow Users to withdraw consent from Social Ads in the left hand “Ad Space” of Facebook. By not allowing the User to withdraw consent at any time, Facebook is in breach of Principle 4.3.8 of PIPEDA.

3. Third Party Applications

In the spring of 2007, the Facebook Platform (“FP”) began allowing third-party developers to create applications through its application programming interface (“API”). Examples of third party applications include a “Horoscope” application that adds daily horoscopes to their Profiles, a “Name Analyzer” game (see below), and a “SlideShow” application that displays a slideshow of Users’ photographs on their Profile.

To use an application, Users must “add” it to their Facebook account. As a condition of adding the application, Users must agree to “allow this application to...know who I am and access my

information”. The following screenshot shows the standard window that appears when Users seek to add an application to their account.

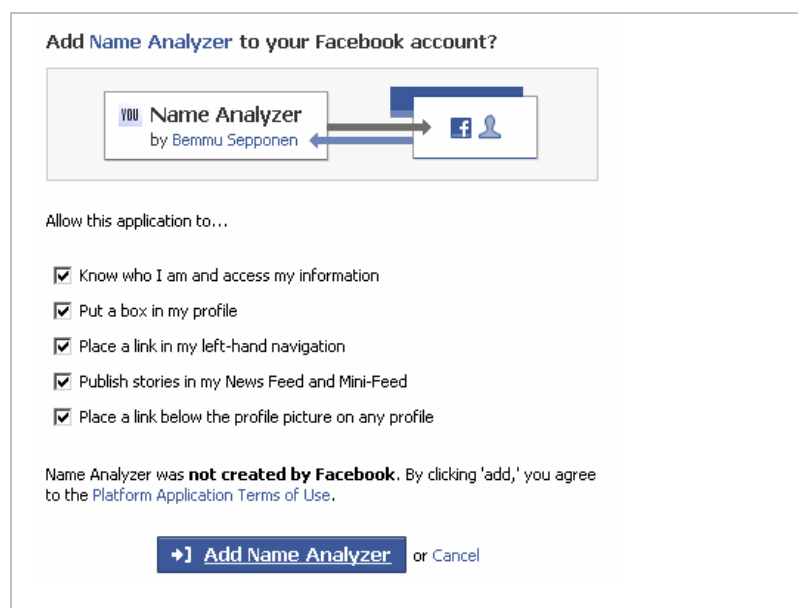


Figure 13

As indicated in the Figure 13, all five options are pre-selected. All but the first can be unselected. In other words, Users have no choice but to let the application developer “know who I am and access my information” should they want to use the application.

It is possible for Users to adjust the extent of personal information made available to third party application developers, but this is not made clear to Users when that they add an application. Rather Users must go into a separate section of the FP and read through their privacy settings. The process for accessing these settings is quite intricate: Users must first select the “Privacy” tab in the top right hand corner, then click on “Applications and Ads”, and finally click on “Other Applications”. This is the only way Users may gain access to the extent of their personal information third party developers are able to retrieve.

As a default setting, when Users adds an application, the developer gains access to their:

- Profile picture;
- Basic Info (name, email, birthday);
- Personal Info (address, religion, relationship status);
- Education Info;
- Work Info;
- Photos/Videos “Tagged” of them;
- List of Friends;
- Work history;
- Groups; and
- Events

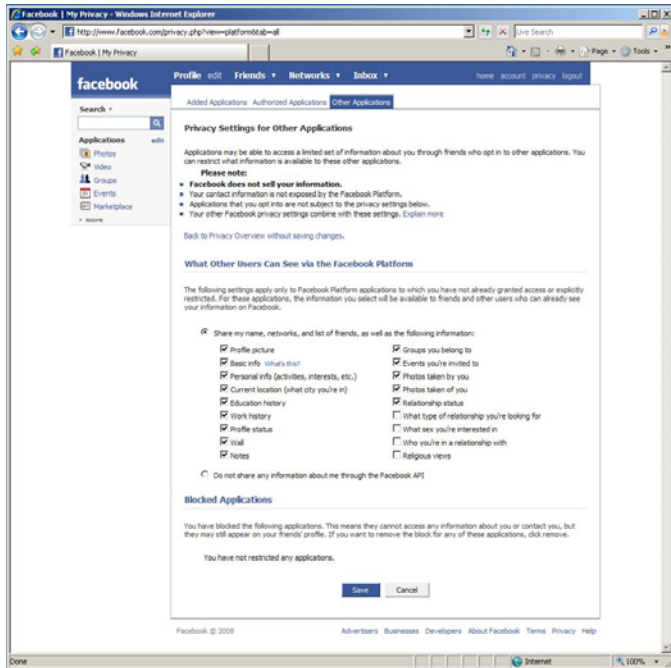


Figure 14

Facebook does not state the purpose behind supplying personal information to third party application developers

Principle 4.2.2 of PIPEDA states that not only shall the collecting organization identify the purpose for which personal information is being used at or before the information is collected, but that the organization shall not collect the information indiscriminately. As noted above, when Users wish to add any application to their account, they must first agree to “allow this application to...know who I am and access my information”. Facebook provides no additional information as to the purpose(s) or use(s) of providing access to these third parties to their personal information. PIPEDA Principle 4.2.5 goes on to recommend that the collector of information should be able to explain the purpose behind collection. Facebook is violating this provision by not providing such an explanation.

Facebook provides third party application developers with access to Users’ personal information beyond what is necessary

Principle 4.4.1 of PIPEDA states that the type and amount of information collected must be limited to what is necessary to fulfill the purpose. The information made available to third party application developers should be limited to what is necessary to carry out the application. For example, the “Horoscope” application developers only need access to the information necessary to deliver daily horoscopes to Users based on their date of birth. In this case, application developers would only need a User’s date of birth. However, when Users attempt to add a new application, such as the Horoscope, they are forced to share all their personal information with third party application developers, relevant or not to the application’s needs.

Facebook conditions the application services on Users consent to share their personal information with the third party application developers

Principle 4.3.3 of PIPEDA states that an organization “shall not, as a condition of the supply of a product or service, require an individual to consent to the collection, use, or disclosure of information beyond that required to fulfill the explicitly specified and legitimate purposes”. Yet, as noted above, Facebook requires that Users agree to share all their personal information with third party application developers in order to add an application. Figure 13 shows the prompt that Users must agree to in order to add an application. If a User deselects the box which states “allow the application to know who I am and access my information”, the User is unable to add the application. Facebook is thus in breach of Principle 4.3.3. Additionally, given that much of information being made available to third parties is considered sensitive, Facebook should obtain such express consent from Users rather than the opt-out permission currently employed.

Facebook does not advise Users of the consequences of withdrawing consent

Principle 4.3.8 of PIPEDA requires that an individual be permitted to withdraw consent at any time and be notified of any implications of this withdrawal. On the FP, when a User wishes to withdraw access by third party developers to his account, the User is presented with various options, as depicted in Figure 14.

The User is only provided with one option; “Do not share any information about me with the Facebook API (Application Programming Interface)”. If this option is selected, the User will immediately lose all applications including photographs, movies, “Gifts”, and other FP content. This consequence is not explained at the prompt page. Facebook is therefore in breach of Principle 4.3.8 by failing to advise Users of the consequences of withdrawing their consent to third party application developers to access to their personal information.

Facebook allows third party developers to retain a User’s personal information even after the User deletes the developer’s application

Principle 4.5 of PIPEDA states that personal information shall be retained only as long as is necessary to fulfill the purpose. Principle 4.5.3 further states that “personal information that is no longer required to fulfill the identified purposes should be destroyed, erased, or made anonymous”. Yet, Facebook’s Terms of Use state that it will not guarantee what personal information that it discloses to third party developers, nor does it offer any assurances that such information is destroyed once a User removes an application from the FP.

Even if Users do not add an application, third party developer may have access to their information through their Friends who may have added the application. Facebook’s Terms of Use state that “If your friends or members of your network use any Applications, such Platform Applications may access and share certain information about you.” This happens regardless of whether Users have installed the application themselves. Therefore, Users who have selected the highest privacy settings and not installed any third party applications may unknowingly add a Friend who has subscribed to a third party application. By adding this Friend, Users’ personal

information will be shared with the developer without their knowledge or consent. Facebook is therefore in direct violation of Principle 4.3.2 of PIPEDA, of the requirement for informed consent to the disclosure of personal information.

Facebook does not monitor the quality or legitimacy of third party applications

Facebook does an inadequate job of monitoring the development of third party platform applications. The developers are not properly authenticating access to their services. Hackers may easily penetrate into these poorly developed programs on the API. Because Facebook rarely reviews applications' level of security, rogue Users are able to "hack" into a User's Facebook account. Hackers may gain full access to Users' personal information, including information about the User's Friends. They also gain the ability to change settings on the Users' account.

Facebook's platform application guidelines state that: "Applications may not[...] contain functionality that permits any person to impersonate a user of the Facebook Site or obtain access to the Facebook Site without authorization [or] disregard or circumvent any technical measures instituted by Facebook to ensure that the application only provides users with access to Facebook Site content that they would otherwise be able to view on the Facebook Site in accordance with any user privacy settings". Yet applications, such as the Superwall, have vulnerabilities imbedded in their code, which allow rogue Users to send messages on behalf of anyone that they wish to exploit. Although third party application developers have a responsibility to create and maintain applications with ample security, Facebook is ineffectively monitoring them. Therefore, Facebook is effectively leaving unsecured applications on the FP.

Facebook fail to effectively notify Users of the extent of information that is shared with third party developers

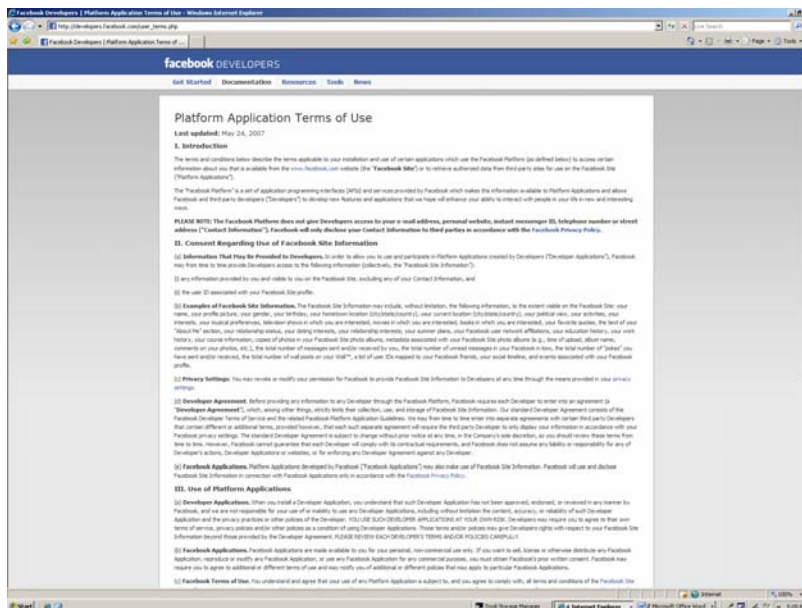


Figure 15

In the Platform Application Terms of Use, which is accessible from Developer's site rather than from the main Facebook page, Facebook discloses the extent of personal information that it gives to third party application developers. The following is an excerpt from this document. Note that the excerpt is drafted to address Facebook Users and not third party developers, even though it is only accessible through the Developers' site.

PLEASE NOTE: The Facebook Platform does not give Developers access to your e-mail address, personal website, instant messenger ID, telephone number or street address ("Contact Information"). Facebook will only disclose your Contact Information to third parties in accordance with the [Facebook Privacy Policy](#).

(a) Information That May Be Provided to Developers. In order to allow you to use and participate in Platform Applications created by Developers, Facebook may from time to time provide Developers access to the following information:

(i) any information provided by you and visible to you on the Facebook Site, excluding any of your Contact Information, and

(ii) the user ID associated with your Facebook Site profile.

(b) Examples of Facebook Site Information. The Facebook Site Information may include, without limitation, the following information, to the extent visible on the Facebook Site: your name, your profile picture, your gender, your birthday, your hometown location (city/state/country), your current location (city/state/country), your political view, your activities, your interests, your musical preferences, television shows in which you are interested, movies in which you are interested, books in which you are interested, your favorite quotes, the text of your "About Me" section, your relationship status, your dating interests, your relationship interests, your summer plans, your Facebook user network affiliations, your education history, your work history, your course information, copies of photos in your Facebook Site photo albums, metadata associated with your Facebook Site photo albums (e.g., time of upload, album name, comments on your photos, etc.), the total number of messages sent and/or received by you, the total number of unread messages in your Facebook in-box, the total number of "pokes" you have sent and/or received, the total number of wall posts on your Wall™, a list of user IDs mapped to your Facebook friends, your social timeline, and events associated with your Facebook profile.

Principle 4.8 of PIPEDA sets out that "an organization shall make readily available to individuals specific information about its policies and practices relating to the management of personal information." Facebook's description of the extent of personal information that is provided to third party developers is not readily available to Users. Users must login to the Developer's site (<http://developers.facebook.com/>) rather than Facebook.com. Principle 4.8.1 sets out that "individuals shall be able to acquire information about an organization's policies and practices without unreasonable effort." Clearly, Facebook is in violation of this provision.

Principle 4.3 of PIPEDA stipulates that "the knowledge and consent of the individual are required for the collection, use, or disclosure of personal information." Although Users are providing general consent to give third party developers access to their information, they are not providing consent for the particular types of personal information that are shared. Facebook

should provide the list above of the types of personal information that are made available to third parties when Users attempt to add applications.¹⁵

Surprisingly, the privacy information found on the Users' site does not include the types of personal information that are described in the Developers' section. The following is found on the Users' site, under "Sharing Your Information with Third Parties" in the Privacy Policy:

Facebook is about sharing information with others — friends and people in your networks — while providing you with privacy settings that restrict other users from accessing your information. We allow you to choose the information you provide to friends and networks through Facebook. Our network architecture and your privacy settings allow you to make informed choices about who has access to your information. We do not provide contact information to third party marketers without your permission. We share your information with third parties only in limited circumstances where we believe such sharing is 1) reasonably necessary to offer the service, 2) legally required or, 3) permitted by you.

For example:

Your news feed and mini-feed may aggregate the information you provide and make it available to your friends and network members according to your privacy settings. You may set your preferences for your news feed and mini-feed [here](#).

We may provide information to service providers to help us bring you the services we offer.

If you, your friends, or members of your network use any third-party applications developed using the Facebook Platform ("Platform Applications"), those Platform Applications may access and share certain information about you with others in accordance with your privacy settings. You may opt-out of any sharing of certain or all information through Platform Applications on the [Privacy Settings](#) page.

We occasionally provide demonstration accounts that allow non-users a glimpse into the Facebook world. Such accounts have only limited capabilities (e.g., messaging is disabled) and passwords are changed regularly to limit possible misuse.

We may be required to disclose user information pursuant to lawful requests, such as subpoenas or court orders, or in compliance with applicable laws. We do not reveal information until we have a good faith belief that an information request by law enforcement or private litigants meets applicable legal standards. Additionally, we may share account or other information when we believe it is necessary to comply with law, to protect our interests or property, to prevent fraud or other illegal activity perpetrated through the Facebook service or using the Facebook name, or to prevent imminent bodily harm. This may include sharing information with other companies, lawyers, agents or

¹⁵ If Facebook believes that the third party application developers are carrying out a Facebook service, we submit in the alternative that Facebook must assume responsibility for the information shared as per Principle 4.1.3. Principle 4.1.3 requires that the collecting organization is responsible for personal information in its possession, including information transferred out to third parties for processing. However, in its Terms of Use, Facebook does not "guarantee that all Platform Developers will abide by restrictions and agreements" with respect to information collected and User experience. They also state that "We are not responsible for the ...the privacy practices or other policies of Developers". To the extent that Facebook is "transferring" Users' personal information to third party developers "for processing," it is in breach of PIPEDA's requirement for accountability.

government agencies.

We let you choose to share information with marketers or electronic commerce providers through sponsored groups or other on-site offers.

We may offer stores or provide services jointly with other companies on Facebook. You can tell when another company is involved in any store or service provided on Facebook, and we may share customer information with that company in connection with your use of that store or service.

Facebook Beacon is a means of sharing actions you have taken on third party sites, such as when you make a purchase or post a review, with your friends on Facebook.

Facebook is providing Developers with significantly more detail about the collection and use of Users' personal information than it does to Users. This is highly inappropriate. At a minimum, Users should have access to the same information given to Developers.

4. New Uses

Facebook has continuously added new services, such as new advertising methods and third party applications. Many of these new services were added after Users had already agreed to the Terms of Use and Privacy Policy during the signup process. Facebook addresses the issue of new purposes in its Terms of Use as follows:

“We reserve the right, at our sole discretion, to change, modify, add, or delete portions of these Terms of Use at any time without further notice. If we do this, we will post the changes to these Terms of Use on this page and will indicate at the top of this page the date these terms were last revised. Your continued use of the Service or the Site after any such changes constitutes your acceptance of the new Terms of Use. If you do not agree to abide by these or any future Terms of Use, do not use or access (or continue to use or access) the Service or the Site. It is your responsibility to regularly check the Site to determine if there have been changes to these Terms of Use and to review such changes.”

Facebook fails to notify Users of new purposes

Principle 4.2.4 of PIPEDA states that “when personal information that has been collected is to be used for a purpose not previously identified, the new purpose shall be identified prior to use. Unless the new purpose is required by law, the consent of the individual is required before information can be used for that purpose.”

Facebook does not satisfy Principle 4.2.4. The Terms of Use explicitly state, “We reserve the right, at our sole discretion, to change, modify, add, or delete portions of these Terms of Use at any time without further notice.” Facebook cannot waive a PIPEDA requirement with a clause in the Terms of Use. In order to comply with PIPEDA, Facebook must provide notice to the User about the new purposes and obtain consent prior to using that information.

5. Collection of Personal Information about Users from sources other than Facebook

Facebook states in its Privacy Policy that it may also collect information from other sources, “such as newspapers, blogs, instant messaging services, and other users of the Facebook service through the operation of the service (e.g., photo tags) in order to provide you with more useful information and a more personalized experience”. The nature and scope of this practice is not disclosed.

Facebook fails to identify why it collects personal information from other sources

Facebook states that this information is collected to provide Users with “more useful information and a more personalized service.” However, this explanation lacks the specificity required by Principle 4.2 of PIPEDA. Facebook fails to explain exactly who the other sources are, how information is collected from them, and this collected information will help Facebook provide more personalized services to Users. Facebook does not meet the requirements of Principle 4.2.3, because it does not specify the purposes of collecting information from other sources.

To the extent that Facebook collects personal information from other sources, it is not acquiring the consent required by Principle 4.3 of PIPEDA. Because Facebook is not explaining how it uses and discloses information gathered from newspapers, blogs, and instant message services, Facebook cannot possibly acquire Users’ informed consent. Therefore, Facebook fails to meet the requirement stipulated under Principle 4.3.2

6. Retention of User Profiles after account deactivation

In order to terminate an account, Users must click on “Account” from their main page. A “Settings” window appears with the following options: “Name”, “Contact Email”, “Password”, “Security Question”, “Credit Cards” and “Deactivate Account”. If Users click on “Deactivate Account”, the following message will appear:

Confirm Facebook Account Deactivation
Please let us know why you are deactivating. (required)

I spend too much time using Facebook. [here](#)
One way to control your interaction with Facebook is to limit the number of emails you receive from us. You can control what emails you receive .
I don't find Facebook useful. [Friend Finder](#) , or [search](#) for them. Also try taking a [tour of Facebook](#)
You might find Facebook more useful if you connect with more of your friends. Check out our [tour of Facebook](#) to learn about features others find useful.
Facebook is resulting in social drama for me. You can prevent this by learning about how to [limit people](#) from accessing your profile.
I don't understand how to use the site. [A tour of Facebook](#) may help clarify how to best use the site. Or [email us with your questions](#)

. We'll respond within 24 hours.
I don't feel safe on the site. You can alter your [privacy settings](#) to make sure you are more protected.
I receive too many emails from Facebook. You can control what email you receive from us [here](#).

.
This is temporary. I'll be back.
Remember, you can reactivate at any time by logging in with your email and password. Just so you know, your admin status in any groups or events will not be automatically restored after activation.
I need to fix something in my account. [Let us know](#)
We can help you solve almost any problem. what the issue is and we'll help you fix it.
I have another Facebook account.
Other Please explain further:

Opt out of receiving emails from Facebook.
Note: Even after you deactivate, your friends can still invite you to events, tag you in photos, or ask you to join groups. If you opt out, you will NOT receive these email invitations and notifications from your friends.

You can reactivate your account at any time by logging in with your email and password.

Users can then deactivate their account by clicking Deactivate. The following message appears:

Your Facebook account has been deactivated.
To reactivate your account, simply log in as you normally would, and we'll send you a reactivation email.
Come back soon,
The Facebook Team

Facebook does not inform Users directly that all of their personal information that has collected over the course of their membership will indeed be retained. Users are simply informed that account reactivation is possible in the future. It left to them to realize what this implies.

Users are not given an express option to delete the account altogether. Instead, Users must contact Facebook directly and request an account deletion. The option is not readily brought to Users' attention. They must navigate through the Facebook Help page and search under Account Deletion in order to see the following message:

If you want to permanently delete your account, please contact us at privacy@facebook.com from the email address associated with your account.

The only way Users may ensure the deletion of personal information is to manually delete each item posted over the course of their membership. This is an unpractical option, given the high

volume of information that is shared on Facebook. Further, since this option is not clearly indicated, many Users would not know to undertake these steps on their own.

Facebook's Privacy Policy briefly mentions account deactivation and does not address account deletion:

Individuals who wish to deactivate their Facebook account may do so on the [My Account](#) page. Removed information may persist in backup copies for a reasonable period of time but will not be generally available to members of Facebook.

Facebook fails to destroy, erase or render personal information anonymous after Users terminate their accounts

Principle 4.5.3 of PIPEDA states that personal information that is no longer required to fulfill the identified purposes should be destroyed, erased, or made anonymous. Facebook's identified purposes when collecting personal information are social networking and information sharing. When Users choose to deactivate their accounts, they are effectively choosing to stop sharing information in a social utility. Facebook's identified purpose is therefore terminated. In accordance with Principle 4.5.3, when Users deactivate their accounts, Facebook should destroy, erase or render their personal information anonymous. Facebook presently fails to do any of this.

Facebook fails to obtain adequate consent for information retention after account termination. Principle 4.3 of PIPEDA states that the knowledge and consent of the individual are required for the collection, use, or disclosure of personal information. A reasonable person would assume that when they choose to deactivate an online account, all affiliation with that organization is severed. This assumption is reinforced by the fact that Facebook does not offer a permanent deletion of account option in an obvious manner. This leads Users to believe that account deactivation is the standard form of account deletion. Facebook should not be retaining User information in the event that the User might choose to reconsider and reactivate their account in the future, unless it has the User's express consent to do so. Facebook should provide a procedure whereby Users who decide to terminate their membership can choose between account deactivation and account deletion.

Principle 4.3.8 of PIPEDA states that an individual may withdraw his or her consent at any time to retention of personal information. When Users terminate their account, they are effectively withdrawing their consent for the continued sharing of personal information. Unless it has unambiguous instructions from Users to retain the information for possible future reactivation, Facebook should delete the information.

Facebook fails to obtain consent to keep a deceased User's Profile active

Facebook also retains the right to keep a deceased User's Profile active for memorial purposes:

"When we are notified that a user has died, we will generally, but are not obligated to, keep the user's account active under a special memorialized status for a period of time determined by us to allow other users to post and view comments." – Terms

Principle 4.2.4 of PIPEDA states that when personal information that has been collected is to be used for a purpose not previously identified, the new purpose shall be identified prior to use. Consent is required before information can be used for that purpose. Facebook states that it keeps a deceased's User's profile active for memorial purposes after the User has died. This is a different purpose than social networking. Unless Facebook has prior consent from the User to do so, it should not be retaining profiles of people after they die.

Facebook fails to provide retention periods for personal information after account deactivation

Principle 4.5.2 of PIPEDA states that "organizations should develop guidelines and implement procedures with respect to the retention of personal information. These guidelines should include minimum and maximum retention periods." Facebook does not indicate anywhere on its website how long User Profiles will be retained after account deactivation. Facebook states only that removed information may persist in backup copies for a reasonable period of time. This statement is unclear. Users have no idea what a "reasonable period of time" entails in this context: weeks, months, years? Facebook should establish a clear and upfront procedure, informing Users that their information will be kept on file for a determined amount of time after account deactivation, should they wish to reactivate their account in the future. This procedure would draw Users' attention to the fact that their information is being retained and not deleted. A direct link to a complete deletion option should be included in this procedure for those who do not consent to retention of their information.

6. Collection/use/disclosure of non-User personal information

Facebook allows Users to upload non-Users' personal information without their knowledge or consent. Personal information of non-Users that may be uploaded includes photographs or videos that are tagged with their names. A tagged non-User is searchable by Users on Facebook. A User can search a non-User by name in their Friends' albums and view all the photographs and videos in which the non-User has been tagged. Because non-Users do not have access to Facebook, they cannot untag themselves (Users do have this option). Non-Users have no control over the content that is being posted about them on Facebook nor can they prevent Users from searching them.

Users can also share non-Users' email addresses in order for Facebook to send them an invitation to join. Facebook states that it will remove non-User email addresses from its database upon request. The average non-User, however, would not be aware that this is necessary to keep their email address private, nor would they be aware that Facebook has retained their information.

Facebook fails to obtain non-User consent to post their personal information

Principle 4.3 of PIPEDA requires informed consent for the collection, use, or disclosure of personal information. Facebook is violating this principle by collecting non-User information without their consent. Facebook gathers this personal information by allowing Users to post

photographs, videos and other such personal information about non-Users, and renders it identifiable through the use of captions. Facebook then disseminates the information through their network.

Non-Users are not notified that their information has been provided to Facebook to be viewed by others. Therefore, they cannot possibly have consented to collection of their personal information. By collecting their personal information without their consent, Facebook is in violation of Principle 4.3 as it pertains to non-Users of the program.

Principle 4.3.4 indicates that in order for an organization to obtain sensitive information from the public, they must meet a higher threshold of consent. Medical and financial information are named as examples of sensitive information. It is submitted that videos and photographs identifying individuals by image and name ought to be considered sensitive as well. Facebook has a large amount of young Users who may not be fully aware of the consequences of providing personal information to a social networking site. Many of the videos and photographs submitted to Facebook by young Users depict alcohol consumption, parties and other such situations. In the context of privacy, videos and photographs should be considered sensitive, because they can tarnish an individual's reputation and can prevent them from obtaining potential employment. If it is accepted that the personal information collected by Facebook is sensitive, then Principle 4.3.5 of PIPEDA suggests that Facebook ought to obtain express consent when collecting the information. Facebook, however, does not seek express consent from Users who post videos and photographs, nor does it remind Users of the potential consequences of posting media of a sensitive nature. Furthermore, Facebook fails to obtain any kind of consent from non-Users who may be captioned in the videos and photographs. Facebook accepts a User's implied consent to post media as the User's express consent. They also allow this User's implied consent to act as consent for non-Users who appear in the videos and photographs.

Facebook fails to obtain consent to the collection and use of non-Users' email addresses

When Facebook collects non-Users' email addresses to send them invitations to Facebook, it collects this personal information from parties other than the individual in question. By retaining such email addresses for its own purposes, Facebook is violating the "knowledge and consent" principle outlined in Principle 4.3.3 of PIPEDA by not informing the individual why his or her email address is kept. The non-User has not consented to this retention of information, and is most likely unaware that it is taking place. The non-User only receives an automated email from their friend via Facebook, which encourages the individual to join the Network. The email gives no indication to the receiver that their information will now be kept on file or that they must contact Facebook directly to remove themselves from the list. Furthermore, if the individual has received more than one invitation to join Facebook, all past invitations will reappear on the new invitation. This is a clear example of how Facebook retains non-User's information.

Facebook should include a provision in its Terms of Use prohibiting posting of non-User information without consent. It should also institute a policy of terminating a User's membership if complaints about unauthorized postings are received. Facebook should also provide non-Users with an efficient method of searching the site and removing any of their own personal information that may have been posted by others.

7. **Monitoring User Activity**

According to a recent interview with Facebook's Chief Privacy Officer, Chris Kelly, Facebook currently uses technology to actively search for anomalous behavior.¹⁶ Facebook also has a dedicated customer service team which deals specifically with User reported anomalous behaviour and behaviour captured by the technology.

Facebook fails to inform Users that it monitors anomalous behaviour

Facebook does not inform Users that it employs technology to actively search for anomalous behaviour and that it has a dedicated customer service team which is involved in this activity. Principle 4.8 of PIPEDA obliges Facebook to make its policies and practices related to management of personal information readily available. Facebook is in violation of this principle since it does not disclose this practice in its Privacy Policy. Since this practice is not acknowledged in Facebook's Privacy Policy, Users would have to make unreasonable efforts in searching for information about this practice.

8. **Security Safeguards**

Facebook allows Users to access a mobile version of the Facebook website at <http://m.facebook.com> ("Mobile Facebook"). This webpage can be accessed using the web browser of mobile devices such as a blackberry or palm or mobile phones with internet browsing capabilities. When Users access Mobile Facebook, they are prompted to login. After Users log in, Facebook Mobile provides them with a "cookie" which appears to have no expiration date. A cookie is a parcel of text sent by a server to a web browser and then sent back unchanged by the browser each time it accesses that server, and is commonly used for authentication purposes. The purpose of the cookie in the Facebook Mobile context is to negate the necessity for Users to login every time they access Facebook Mobile from their mobile device. The cookie replaces a User login. If Users log in on Facebook Mobile, they will remain logged in indefinitely, regardless of whether they changes their Facebook Password or log in elsewhere.

Facebook Mobile fails to properly safeguard personal information

Principle 4.7 of PIPEDA states "personal information shall be protected by security safeguards appropriate to the sensitivity of the information." Furthermore, Principle 4.7.1 states "the security safeguards shall protect personal information against loss or theft, as well as unauthorized access, disclosure, copying, use, or modification. Organizations shall protect personal information regardless of the format in which it is held." Lastly, Principle 4.7.3 states "the methods of protection should include . . . technological measures, for example, the use of passwords and encryption."

The provision of a cookie of an indefinite length has several negative implications on security. Firstly, if a User uses another person's mobile device and forgets to log off, that other person

¹⁶ Juan Carolos Perez, IDG News Service, "Three minutes with Facebook's Privacy Chief", <http://www.peworld.com/printable/article/id.142324/printable.html>

will then have access to the User's personal information indefinitely. Secondly, if a User temporarily provides another person with their Facebook password, the other person may login with the User's information on a mobile device and have access indefinitely. Due to the indefinite duration of the cookie, the other person in both the instances described above will have indefinite access to the User's personal information, even after the User changes their password in an attempt to restrict the other person from accessing their personal information.

In order to provide an appropriate level of security, Facebook should set an appropriate duration on cookies provided upon login on Facebook Mobile. Furthermore, this cookie should expire when a User changes their password online.

9. **Misleading Statements / Deception**

Principle 4.4.2 states that "consent with respect to collection must not be obtained through deception." Furthermore, Principle 4.3.2 also requires that for consent to be meaningful, "the purposes must be stated in such a way that the individual can reasonably understand how the information will be used or disclosed." Facebook has violated Principles 4.4.2 and 4.3.2 by misleading Users over its primary purposes for collecting their personal information and over the level of control over their privacy settings.

Facebook misrepresents itself as solely a social networking site

Facebook presents itself as a social networking site. On the Facebook homepage, Facebook is described as "a social utility that connects you with the people around you." However, it has been demonstrated above that Facebook is involved in other activities. It shares Users' personal information with third party advertisers who serve Users targeted advertisements. It also shares Users' personal information with third party application developers for purposes beyond the functioning of the applications. This use needs to be made clear to Users who expect that Facebook is using their personal information solely to facilitate their social networking.

Instead, these other activities are relatively covert. Facebook often disguises its advertising activities as social networking activities. For example, in a Facebook blog, Mark Zuckerberg tells Users, "we released a new feature called Beacon to try to help people share information with their friends about things they do on the web."¹⁷ Beacon is primarily an advertising mechanism paid for by third party advertisers, but Zuckerberg represents it as a social activity. Facebook notes that it shares personal information with advertisers in its Terms of Use. These brief statements are buried among other Terms of Use and are unlikely to be noticed by Users. Facebook should make its advertising at least as transparent as its social networking.

¹⁷ Mark Zuckerberg, "Thoughts on Beacon," December 5, 2007, http://blog.facebook.com/blog.php?blog_id=company&blogger=4

Facebook misrepresents the level of control available to Users over personal information

Facebook also presents itself as a model for real world connections. In an interview with the *Time* magazine, Mark Zuckerberg relays:

People communicate most naturally and effectively with their friends and the people around them. What we figured is that if we could model what those connections were, [we could] provide that information to a set of applications through which people want to share information, photos or videos or events. But that only works if those relationships are real. That's a really big difference between Facebook and a lot of other sites.

To get Users to “understand the world around them,” Facebook claims to offer Users “granular” control over their privacy settings.¹⁸ Accordingly, the Facebook website identifies that one of two of Facebook’s core principles is: “You should have control over your personal information.”¹⁹ However, the actual level of control available to Users is firstly nowhere near the level of control available to people in the non-virtual world and is secondly not as granular as Facebook purports it to be.

As this submission has exposed, Users are not even permitted to opt out of certain kinds of information sharing. For example, third party application developers that Users have signed up for have access to all sorts of personal information about the Users’ Friends. Users would probably not share their personal information with strangers in the non-virtual world, but are doing so unwittingly in Facebook. Facebook needs to stop promoting itself as a model of the real world and needs to be upfront about the real limitations on the level of control available to Users.

These misrepresentations about Facebook’s use of personal information and about the level of control available to Users constitute violations of Principles 4.4.2 and 4.3.2.

continued....

¹⁸ David Kirkpatrick, “Why Facebook Matters,” *Fortune Magazine*, October 6, 2006, http://money.cnn.com/2006/10/06/magazines/fortune/fastforward_facebook.fortune/index.htm

¹⁹ <http://www.facebook.com/policy.php>

Summary of PIPEDA Complaint

To summarize, we submit that Facebook is in violation of the following *PIPEDA* provisions in the following regards:

Principle 4.2 – Identifying Purposes:

Principle 4.2.2

Principle 4.2.2 requires that an “organization identify the purpose for which personal information is collected at or before the time of collection” and that an “organization collect only the information necessary for the purposes that have been identified.”

- Facebook allows third party application developers to access User information that is beyond what is necessary to operate their applications.

Principle 4.2.3

Principle 4.2.3 sets out that “the identified purposes should be specified at or before the time of collection to the individual from whom the personal information is collected.”

- Facebook does not precisely identify why Users’ information is collected from other sources.

Principle 4.2.4

Principle 4.2.4 sets out that “when personal information that has been collected is to be used for a purpose not previously identified, the new purpose shall be identified prior to use. Unless the new purpose is required by law, the consent of the individual is required before information can be used for that purpose.”

- Facebook reserves the right to modify or add to its Terms of Use without notice.
- Facebook retains deceased Users’ profile for memorial reasons, a new purpose.

Principle 4.2.5

Principle 4.2.5 recommends that information collectors “should be able to explain to individuals the purpose for which the information is being collected.”

- Facebook does not explain to Users why third party application developers need access to all their User information.

Principle 4.3 – Consent:

Principle 4.3.1

Principle 4.3.1 sets out that “consent is required for the collection of personal information and the subsequent use or disclosure of this information.”

- Facebook does not obtain the consent of non-Users to collect their information from Users, to share their information with other Users, and to retain their information.

Principle 4.3.2

Principle 4.3.2 sets out that “organizations shall make a reasonable effort to ensure that the individual is advised of the purposes for which the information will be used” and that meaningful

consent requires that “the purposes must be stated in such a way that the individual can reasonably understand how the information will be used or disclosed”.

- Facebook does not make a reasonable effort to ensure that Users are advised of:
 - The purposes for which their dates of birth will be used;
 - The purpose of using User information for Social Ads;
 - All the types of information that are shared with third party application developers, including Friends’ information; and
 - The purpose behind retaining information of Users who have deactivated their accounts.

Principle 4.3.3

Principle 4.3.3 sets out that “an organization shall not, as a condition of the supply of a product or service, require an individual to consent to the collection, use, or disclosure of information beyond that required to fulfill the explicitly specified and legitimate purposes.”

- Facebook requires Users, as a condition of use of its service, to:
 - Provide their dates of birth despite that its purpose for doing so is not explicitly specified; and
 - Participate in one variation of Social Ads despite that this activity is beyond that required to fulfill Facebook’s explicitly specified and legitimate purpose of social networking.
- Facebook requires Users, as a condition to use of third party platforms, to:
 - Share personal information with third party application developers that is beyond what is required to fulfill the purposes of the applications.
- Facebook retains non-Users’ email addresses for purposes beyond sending them an email to invite them to Facebook.

Principle 4.3.6

Principle 4.3.6 sets out that “an organization should generally seek express consent when the information is likely to be considered sensitive.”

- Facebook does not obtain express consent to share sensitive information in the following ways:
 - Users’ information with other Users in joined Networks;
 - Users’ photo albums and associated comments with everyone;
 - Users’ name and picture searchable to everyone;
 - Users’ information with third party application developers and with third party advertisers;
 - Non-User’s information, including photographs, with Users; and
 - To retain Users’ information after they deactivate their accounts.

Principle 4.3.8

Principle 4.3.8 sets out that “An individual may withdraw consent at any time, subject to legal or contractual restrictions and reasonable notice.”

- Facebook does not permit active Users to withdraw consent from the Social Ads that are displayed in the left hand “Ad Space” of their Profiles.
- Facebook does not inform Users who withdraw consent to share their personal information with third party application developers that all their applications will be lost.

- Facebook does not permit Users who effectively withdraw consent to share their information by deactivating their accounts to do so.

Principle 4.4 – Limiting Collection:

Principle 4.4.1

Principle 4.4.1 sets out that “both the amount and type of information collected must be limited to what is necessary to fulfill the purposes identified.”

- Facebook allows third party application developers to collect information beyond what is necessary to run the applications.

Principle 4.4.2

Principle 4.4.2 sets out that “consent with respect to collection must not be obtained through deception.”

- Facebook deceives Users about its purposes for collecting personal information and about the level of User control over their personal information.

Principle 4.5 – Limiting Use, Disclosure, and Retention:

Principle 4.5.2

Principle 4.5.2 sets out that “organizations should develop guidelines and implement procedures with respect to the retention of personal information.”

- Facebook does not indicate the retention period for Profiles of Users who have deactivated their accounts anywhere on its Privacy Policy or website.

Principle 4.5.3

Principle 4.5.3 sets out that “personal information that is no longer required to fulfill the identified purposes should be destroyed, erased, or made anonymous”.

- Facebook does not guarantee that personal information that has been disclosed to third party application developers will be destroyed once a User removes an application from Facebook.
- Facebook retains Users’ personal information after they have terminated their accounts, when their information is no longer necessary to serve Facebook’s identified purpose of social networking.

Principle 4.7 – Safeguards:

Principle 4.7.1

Principle 4.7.1 sets out that an organization shall have security safeguards that “shall protect personal information against loss or theft, as well as unauthorized access, disclosure, copying, user, or modification.”

- Facebook enables a cookie of indefinite length on a User’s mobile device, which could potentially allow others to access the User’s Facebook account.

Principle 4.8 – Openness:

Principle 4.8.1

Principle 4.8.1 sets out that “individuals shall be able to acquire information about an organization’s policies and practices without unreasonable effort.”

- Facebook does not make its policies on the range of personal information that is disclosed to third party application developers available on their general website.
- Facebook does not disclose that it uses technology to actively search for anomalous behaviour.

We request that you investigate Facebook’s practices with a view to its compliance with *PIPEDA*. We await your findings. Should you have any questions, please do not hesitate to contact the undersigned.

Yours truly,

original signed

Philippa Lawson, on behalf of herself and the following law students:

Pradeep Chandrashekar
Harley Finkelstein
Carisa Gorrell
Jordan Plener
Lisa Feinberg

Attach - Appendices

cc: Facebook: privacy@facebook.com