SHOULD THE DEFAULT BE "SOCIAL"? CANADA'S PUSHBACK AGAINST OVER-SHARING BY FACEBOOK

Karen Tanenbaum[*]

TABLE OF CONTENTS

[*] J.D., University of Georgia, 2012; B.A., University of Georgia, 2008.

I. INTRODUCTION

With over 750 million active users worldwide,[1] Facebook has quickly become one of the most highly trafficked websites in the world.[2] Translated into more than seventy languages,[3] and with 70% of user access occurring outside of the United States,[4] the site has truly become an international sensation. As of July 2011, Facebook was worth an estimated $84 billion.[5] Along with others like MySpace, LinkedIn, and Twitter, the site has fueled the social networking revolution that is helping to define the new millennium.

Facebook's popularity, however, has not come without a price for its users. Although membership is up, privacy control is down.[6] As more and more users have joined the site, Facebook has decreased the amount of control users have over their personal data. This is particularly troublesome given the breadth of personal information that the site encourages users to make available (including photos, religious views, hometown, and address)[7] and the growing circle of third-party websites and application developers that can access much of this sensitive user information.[8]

Threats to user privacy have not gone unnoticed. Outcry over Facebook's privacy policies has echoed worldwide, backed by privacy advocates and a number of lawmakers.[9] As Facebook rapidly grows,[10] though, existing privacy and technology laws struggle to keep up with its innovations.[11]

---

[1] *Statistics*, FACEBOOK, http://www.facebook.com/press/info.php?statistics (last visited July 23, 2011) (document on file with author).

[2] *Factsheet*, FACEBOOK, http://www.facebook.com/press/info.php?factsheet (last visited July 23, 2011) (document on file with author).

[3] *Statistics*, *supra* note 1.

[4] *Id.*

[5] Shayndi Raice, *Is His Company Worth $100 Billion?*, WALL ST. J., July 14, 2011, at B1.

[6] *See infra* Part II.*B* (explaining how Facebook's privacy protections have weakened over time).

[7] *See infra* Parts II.*B*–*C* (describing the types of personal information that Facebook encourages users to share and makes publicly available).

[8] *See infra* Parts II.*B*–*C* (describing the types of personal user information that applications can access through Facebook).

[9] *See infra* Parts III.*C*, IV.*A* (illustrating some of the legal action thus far initiated against Facebook).

[10] James Grimmelmann, *Saving Facebook*, 94 IOWA L. REV. 1137, 1145 (2009) ("Facebook's pace of innovation is so blisteringly fast that it's not uncommon to log into the site and see that part of the interface has changed overnight to offer a new feature.").

[11] Miguel Helft & Claire Cain Miller, *Web Outruns Privacy Law*, N.Y. TIMES, Jan. 10, 2011, at A1; *see also* OFFICE OF THE PRIVACY COMM'R OF CAN., PRIVACY, TRUST AND INNOVATION—BUILDING CANADA'S DIGITAL ADVANTAGE 3–6 (2010), *available at* http://www.priv.gc.ca/infor

To date, Canadian law has proven one of the most effective tools for protecting user privacy on Facebook.[12] In 2009, the Canadian Office of the Privacy Commissioner (OPC or Commissioner) declared that Facebook violated Canada's private sector privacy law, the Personal Information and Electronic Documents Act (PIPEDA).[13] The OPC then successfully pressured Facebook to give users more knowledge and control regarding the site's use of users' personal information.[14] Significantly, because the site is transnational, the Facebook challenge allowed an ordinarily domestic law to provoke change on a massive international scale.[15] Privacy protections improved for users worldwide.[16]

Yet Facebook still has work to do. Since Facebook's work with the Commissioner, the site has continued to grow in ways that reveal its compliance with Canada's PIPEDA has not been as meaningful as it could and should be.[17] Users still do not have enough control over what information they share. They are also still not fully informed about what information they are sharing with third-party websites and application developers.[18] In July 2010, an Internet security consultant published personal data he collected from 100 million Facebook users.[19] The publication aimed to raise public awareness about the lack of user privacy on the site.[20] The amount of personal information compiled astounded users and

---

mation/pub/sub_de_201007_e.pdf (explaining the tension between technological innovation and privacy protections).

[12] *See Facebook Faces Up to Long-Awaited Privacy Upgrades*, 28 WESTLAW J. COMPUTER & INTERNET, Aug. 4, 2010, at 10, 10 ("Facebook users now have greater control over how much of their personal information is disclosed . . . . The changes were made in response to complaints from users, civil rights groups and governments, particularly Canada's privacy commissioner.").

[13] *See infra* Part IV.*A* (detailing the OPC's finding that Facebook was in violation of PIPEDA).

[14] *See infra* Part IV.*B* (explaining Facebook's improvements to user privacy that resulted from the OPC's findings).

[15] *See* Christine A. Carron & Martha A. Healey, *Privacy Laws and Regulations Around the Globe: The Impact on Doing Business Internationally*, 28 ACC DOCKET, Jan.–Feb. 2010, at S8, S9 ("Facebook recently indicated that it plans to amend worldwide practices to implement Canadian privacy requirements globally.").

[16] *Id.*

[17] *See infra* Part V.*A* (explaining how Facebook is currently not in compliance with PIPEDA).

[18] *See infra* Part V.*B* (giving examples of information sharing that likely occurs without full user consent).

[19] Daniel Emery, *Details of 100m Facebook Users Collected and Published*, BBC NEWS (July 28, 2010), http://www.bbc.co.uk/news/technology-10796584.

[20] *Id.*

advocates worldwide, leaving many asking—Should the default setting for information sharing on Facebook be *quite* so "social"?

This Note argues that sharing should *not* be quite so extensive on Facebook, at least in certain situations. Until Facebook gives users more meaningful control over their personal information and offers clearer, more specific disclosure of who has access to such information and how it is being used (particularly by third-party websites and applications), the site will continue to be out of step with Canada's PIPEDA and users' reasonable privacy expectations. Specifically, the site should: (1) ask permission before adding new features or settings that make user information more public than it was before, (2) offer users more information on how and why their information is being used by third parties, and (3) give users more control over their sharing with third parties.[21]

To accomplish these goals, Facebook must move closer to an "opt-in" privacy control model. An opt-in model is one that does not assume users' consent to sharing their information in new or more expansive ways without explicitly asking permission. Currently the site is built around an "opt-*out*" privacy control model.[22] This opt-out model assumes that users agree to new privacy settings or information-sharing features and adds them to users' accounts automatically.[23] User information is then shared until the user expressly opts-out of sharing.[24] Under an opt-in model, Facebook would have to ask a user's permission first.[25]

Given Canada's strong privacy law framework and the political will that enabled the OPC's recent success against Facebook, the country is in a strong position to further push the site toward an opt-in model in compliance with PIPEDA. PIPEDA's second mandated review is also set for 2011,[26]

---

[21] *See infra* Part V.*B* (explaining recommendations for Facebook in detail).

[22] *See infra* notes 49–51 and accompanying text (explaining Facebook's opt-out privacy model).

[23] *See infra* notes 49–51 and accompanying text (explaining Facebook's opt-out privacy model).

[24] *See infra* notes 49–51 and accompanying text (explaining Facebook's opt-out privacy model).

[25] *Determining the Appropriate Form of Consent Under the Personal Information Protection and Electronic Documents Act*, OFF. PRIVACY COMM'R CAN., http://www.priv.gc.ca/fs-fi/02_05_d_24_e.cfm (last modified Sept. 28, 2004) [hereinafter *Consent Under PIPEDA*].

[26] *See* Personal Information Protection and Electronic Documents Act, S.C. 2000, c. 5 § 29(1) (Can.) [hereinafter PIPEDA], *available at* http://laws-lois.justice.gc.ca/PDF/P-8.6.pdf ("The administration of this Part shall, every five years after this Part comes into force, be reviewed by the committee of the House of Commons, or of both Houses of Parliament, that may be designated or established by Parliament for that purpose.").

which will allow Canadian lawmakers to take an even closer look at the law. Lawmakers can then more effectively strengthen protections to combat online privacy challenges as needed.

To this end, part II of this Note provides a brief history of Facebook and an overview of its problematic privacy policies to demonstrate the origin of the key privacy issues. Part III examines Canada's PIPEDA, providing an overview of the privacy law and how it applies to Facebook generally. Part IV explains the Commissioner's success in using PIPEDA to pressure Facebook to make specific changes to protect user privacy. Part V argues that, despite changes, the site continues to violate PIPEDA principles and gives recommendations for modifying Facebook policies regarding privacy controls and third-party policies. Part VI concludes that Canada should re-launch an investigation of Facebook and pressure the site to incorporate changes that would put Facebook into compliance with PIPEDA and protect user privacy worldwide.

II. FACEBOOK AND ITS PRIVACY CHALLENGES: A BRIEF HISTORY

A. Facebook Is Born

Facebook was created in a Harvard University dorm room in 2004.[27] Initially dubbed "TheFacebook," the site was designed to help Harvard students share photos and communicate with their friends.[28] Within a month it was released to other universities and, by 2006, it was available to anyone with a functional e-mail address.[29] Facebook is now the number one social networking site in the world, and the most visited website in the world.[30]

Facebook describes itself as a "social utility that helps people communicate more efficiently with their friends, family and coworkers."[31] It has two fundamental interfaces or features: a member's profile and a member's home page.[32] The profile is customizable to feature anything from one's basic personal information to religious, sexual, or political preferences

---

[27] *Timeline*, FACEBOOK, http://www.facebook.com/press/info.php?timeline (last visited July 23, 2011) (document on file with author).

[28] Don Reisinger, *Facebook Six Years Later: From a Dorm Room Experiment to a Household Name*, L.A. TIMES (Feb. 4, 2010), http://latimesblogs.latimes.com/technology/2010/02/facebook-six-years-later-from-a-dorm-room-to-a-household-name.html.

[29] *Timeline*, *supra* note 27.

[30] *The 1000 Most-Visited Sites on the Web*, GOOGLE (July 2011), http://www.google.com/adplanner/static/top1000/.

[31] *Factsheet*, *supra* note 2.

[32] *Id.*

(all categories are suggested by the site and a user can choose whether to share the information).[33] Profiles also allow members to post pictures of themselves and of others.[34] Under this photo-sharing system, if a user clicks on a face in any photo posted on Facebook—even one posted by someone else—that user can enter any name to identify the face in the photo.[35] If the identified or "tagged" person is a Facebook user, the photo then also appears in the "tagged" user's personal profile.[36] Users can always "untag" themselves from a photo if they do not wish to be identified by name in that particular photo. Finally, users can also write public "posts," or messages, on one another's profile pages.[37]

The home page allows users to send private messages or to chat live with one another.[38] Its main feature, however, is a "News Feed" that keeps a running tab of any changes users' friends have made to their profiles, such as new groups, social events, or photos.[39] The News Feed also publishes up-to-date "statuses" of Facebook users.[40] For example, if Facebook user John Doe is going to Target to buy a new pair of socks and wants to notify his entire online friend network and allow them to comment, he can do so by posting a status update on Facebook. That update will appear both on his profile page and his friends' home pages.

---

[33] *Set up a Profile*, FACEBOOK, http://www.facebook.com/help/?guide=set_up_profile (last visited Dec. 15, 2010) (document on file with author).

[34] *See* Justin Mitchell, *Making Photo Tagging Easier*, FACEBOOK BLOG, http://blog.facebook.com/blog.php?post=467145887130 (last updated June 30, 2011) (illustrating the photo-tagging feature).

[35] *Tag Photos*, FACEBOOK, http://www.facebook.com/help/photos/tag-photos (last visited Nov. 21, 2011) (document on file with author) (offering a basic overview of the tagging feature on Facebook).

[36] *Id.*

[37] *Explore Facebook*, FACEBOOK, http://www.facebook.com/help/?guide=explore_facebook (last visited Dec. 15, 2010) (document on file with author).

[38] Nick O'Neill, *The New Facebook Home Page Guide That You Must Read*, ALL FACEBOOK: THE UNOFFICIAL FACEBOOK RESOURCE (Feb. 16, 2010), http://www.allfacebook.com/facebook-home-page-2010-02 (giving a general overview of the Facebook Home Page); *Messages Basics*, FACEBOOK, http://www.facebook.com/help/messages/basics (last visited Nov. 21, 2011) (document on file with author) (explaining the basics of sending private messages on Facebook); *Basics: How to Chat*, FACEBOOK, http://www.facebook.com/help/chat/how-to-chat (last visited Nov. 24, 2011) (document on file with author) (explaining the basics of chatting on Facebook).

[39] *Explore Facebook*, *supra* note 37.

[40] *Id.*

Users build online friend networks by sending "friend requests" to one another.[41] A friend request can be accepted or rejected once received.[42] As of June 2011, the average Facebook user had 130 friends.[43]

Facebook also features a "Platform," or interface that allows developers to create different "applications" or "apps" for use on the Facebook site.[44] Applications are software that allow Facebook users to play games and share common interests.[45] The applications range from games like hangman or scrabble to online celebrity quizzes, horoscopes, and classified ads.[46] Independent third-party developers can create applications, and the Platform feature enables those third parties to plug their applications into the Facebook site and present them to users with the Facebook look and feel.[47] As of October 2010, there are about 550,000 applications on the site, and 70% of Facebook users interact with at least one each month.[48]

B. Privacy Settings: Less Is More?

Facebook uses an opt-out model to protect user privacy on the site.[49] This means the site generally presumes a user's consent to share her information with the largest possible audience unless she deliberately opts-out.[50] When the site's privacy settings change or a new feature is added that requires more information sharing, Facebook automatically applies the new settings or

---

[41] *Adding Friends & Friend Requests*, FACEBOOK, http://www.facebook.com/help/?page=767 (last visited July 24, 2011) (document on file with author) (expand the "How do I add a Friend?" hyperlink).

[42] *Id.*

[43] *Statistics*, *supra* note 1.

[44] *Facebook Platform*, FACEBOOK, http://www.facebook.com/platform?v=info (last visited July 24, 2011) (document on file with author).

[45] *See generally App Directory*, FACEBOOK, http://www.facebook.com/apps/directory.php (last visited Dec. 15, 2010) (document on file with author) (featuring examples of different applications on the site).

[46] *Id.*

[47] Grimmelmann, *supra* note 10, at 1146.

[48] Emily Steel & Geoffrey A. Fowler, *Facebook in Privacy Breach—Top-Ranked Applications Transmit Personal IDs, a Journal Investigation Finds*, WALL ST. J., Oct. 18, 2010, at A1.

[49] Alexei Alexis, *House Panel Examines Privacy Concerns Surrounding Social Networking Websites*, 15 ELECTRONIC COM. & L. REP. 1211 (2010). Michael Merritt, assistant director of the Office of Investigations at the Secret Service, stated that " 'Facebook has changed its privacy controls several times, usually setting users' default preferences to maximum exposure, making users take the initiative to navigate the controls to restrict who may view their information.' " *Id.*

[50] *Id.*

shares user information without asking permission first.[51] As a result, users are more exposed to wider and wider circles of viewers.

To illustrate the privacy implications of this model, a hypothetical is useful. Imagine that the above Target shopper, John Doe, initially set up his Facebook account in 2005. Imagine further that he did so using the site's recommended, default privacy settings and made no adjustments to these privacy settings for five years. In 2005, John's profile information (photos, posts, and relationship status) is strictly available to other users that he has pre-designated on the site.[52] In fact, the site's privacy policy promises John it will not share his information with " 'any user of the Web Site who does not belong to at least one of the groups specified by you in your privacy settings.' "[53] The site has roughly 5.5 million active users.[54]

By 2007, however, Facebook applies new privacy settings that make John's once-protected information automatically available not only to his "friends," but to *any* Facebook user who is in his school network or registered in his geographic area.[55] A larger pool of users can see John's personal information regardless of whether John knows those users or they are his Facebook friends. By this time Facebook's user pool has jumped to 50 million.[56]

By November 2009, many of John's listed details, including his name, profile photo, friend list, city, and home address,[57] become available not only to users on Facebook, but to anyone searching the Internet, irrespective of Facebook membership. John's heightened exposure results from new Facebook policies that made his profile details mandatorily Publicly

---

[51] *Id.*

[52] Kurt Opsahl, *Facebook's Eroding Privacy Policy: A Timeline*, ELECTRONIC FRONTIER FOUND. (Apr. 28, 2010), http://www.eff.org/deeplinks/2010/04/facebook-timeline.

[53] *Id.* (quoting Facebook).

[54] *Timeline*, *supra* note 27.

[55] Opsahl, *supra* note 52 (" 'Profile information you submit to Facebook will be available to users of Facebook who belong to at least one of the networks you allow to access the information through your privacy settings (e.g., school, geography, friends of friends). Your name, school name, and profile picture thumbnail will be available in search results across the Facebook network unless you alter your privacy settings.' " (quoting Facebook)).

[56] *Timeline*, *supra* note 27.

[57] Opsahl, *supra* note 52 (" 'Information set to "everyone" is publicly available information, may be accessed by everyone on the Internet (including people not logged into Facebook), is subject to indexing by third party search engines, may be associated with you outside of Facebook (such as when you visit other sites on the internet), and may be imported and exported by us and others without privacy limitations. The default privacy setting for certain types of information you post on Facebook is set to "everyone." ' " (quoting Facebook)).

Available Information (PAI).[58] Facebook now exceeds 300 million active users.[59]

In December 2009, John Doe's PAI becomes accessible not only to other individuals on the Internet, but also to third-party applications and Facebook's partner websites.[60] Before this date, users could opt-out of sharing their personal data with application developers.[61] After the creation of the PAI category, however, this opt-out option disappeared.[62] Now if John plays a game of "Hangman" on Facebook, or takes a survey querying, "which '80s child actor are you?" he then (likely unwittingly) grants that application developer unrestricted access to his personal information.[63] Further, even if John never uses applications, the applications used by John's friends still have unrestricted access to his data.[64]

Finally, by April 2011, if John visits one of Facebook's partner websites, like Pandora Radio or the online directory Yelp,[65] Facebook's new Instant Personalization application gives that site access to some of his information.[66] John might log into Pandora, for example, and be surprised to see a list of his Facebook friends, accompanied by a link offering him access to those friends' Pandora playlists.[67] Like other new Facebook features, the

---

[58] Jane E. Kirtley, *Privacy Protection, Safety and Security*, *in* COMMUNICATIONS LAW IN THE DIGITAL AGE 2010, at 15, 122 (PLI Intell. Prop., Course Handbook Ser. No. 1027, 2010).

[59] *Timeline*, *supra* note 27.

[60] Opsahl, *supra* note 52 (" 'Certain categories of information such as your name, profile photo, list of friends and pages you are a fan of, gender, geographic region, and networks you belong to are considered publicly available to everyone, including Facebook-enhanced applications, and therefore do not have privacy settings.' " (quoting Facebook)).

[61] Kirtley, *supra* note 58, at 123.

[62] *Id.*

[63] *Facebook Sprung From Penalty Box by Canadian Privacy Czar*, 28 WESTLAW J. COMPUTER & INTERNET, Sept. 29, 2010, at 11, 11.

[64] Steel & Fowler, *supra* note 48.

[65] *See Instant Personalization*, FACEBOOK, http://www.facebook.com/instantpersonalization/ (last visited Oct. 24, 2011) (document on file with author) (listing Yelp, Pandora, and Facebook's other Instant Personalization partner sites); *see also* Chris Morrison, *A Look at Facebook's Three Instant Personalization Partners: Yelp, Pandora, Docs.com*, INSIDE FACEBOOK (Apr. 27, 2010), http://www.insidefacebook.com/2010/04/27/a-look-at-facebooks-three-instant-personalization-partners-yelp-pandora-docs-com/ (explaining Facebook's partnership with Yelp and Pandora).

[66] *See Controlling How You Share*, FACEBOOK, http://www.facebook.com/privacy/explanation.php (last visited July 24, 2011) (document on file with author) (generally explaining the Instant Personalization feature); *see also* Rose v. Facebook, Inc., No. CA 10-232 S, 2010 WL 2147928, paras. 1–5 (D.R.I. filed May 21, 2010) (explaining legally problematic aspects of Instant Personalization feature).

[67] Morrison, *supra* note 65 ("[T]here's an option called Friends' Music [on Pandora]. Clicking on this gives you a large box showing each [Facebook] friend and allowing you to

Instant Personalization application was added automatically, without John's permission.[68] At this point, Facebook has over 350 million active users.[69]

C. Opting-Out: A Meaningful Method of Privacy Control?

At any point, of course, John could choose to opt-out of much of this sharing by adjusting his privacy settings to restrict how much of his information is shared with others.[70] Facebook's Privacy Settings feature enables users to limit, in many cases, the accessibility of their private information.[71] The privacy settings page lists different categories of user information and allows the user to scale back from sharing a given category of information with "Everyone" to "Friends of Friends" or "Friends only."[72]

For example, in 2007, when John's details became available to all users, he could have visited his privacy settings and indicated that he did not want his profile information to be available to anyone other than friends.[73] Again in November 2009, he could have visited his privacy settings page and opted out of the public search feature so that his details were not available to third-party search engines and non-Facebook Internet users.[74] As of December 2009, there was nothing John could have done to avoid sharing certain information with his friends' applications.[75] Within several months, however, he would have the option to revisit his privacy settings and turn off the Platform feature entirely to avoid any unwanted sharing with applications.[76]

---

navigate through to look at their music and, if you'd care to, listen to their stations.").

[68] *Id.* ("The [Instant Personalization] service requires each partner site to display a prominent blue scroll-down bar allowing users to instantly opt-out. If users don't choose to opt out, the partner continues to be able to access general information.").

[69] *Timeline*, *supra* note 27.

[70] *See generally Facebook Privacy Policy*, FACEBOOK, http://www.facebook.com/policy.php (last visited July 24, 2011) (document on file with author) (explaining how users can control their sharing).

[71] *Choose Your Privacy Settings*, FACEBOOK, http://www.facebook.com/settings/?tab=privacy (last visited Dec. 15, 2010) (document on file with author).

[72] *Controlling How You Share*, *supra* note 66.

[73] Opsahl, *supra* note 52 (" 'Your name, school name, and profile picture thumbnail will be available in search results across the Facebook network unless you alter your privacy settings.' " (quoting Facebook)).

[74] PAI, however, would still be mandatorily available to other Facebook users. Kirtley, *supra* note 58, at 123; *see generally* Opsahl, *supra* note 52 (" 'The default privacy setting for certain types of information you post on Facebook is set to "everyone." You can review and change the default settings in your privacy settings.' " (quoting Facebook)).

[75] Steel & Fowler, *supra* note 48.

[76] Mark Zuckerberg, *Making Control Simple*, FACEBOOK BLOG (May 26, 2010), http://blog.

Facebook's manual opt-out method has a number of downsides for users. Namely, it puts the burden of privacy control on the user rather than on the site because users have to ask (via the privacy controls) the site to *stop* sharing their information rather than the site having to ask users' permission first.[77] This is problematic for several reasons. First, users do not always *know* when their information is being shared in new or undesired ways. Facebook does not always alert users of privacy changes or new features. When it does, Facebook's updates have been criticized as inadequate and untimely.[78] For example, if John did not visit Pandora after December 2009 and realize the Instant Personalization feature existed, he would likely be unaware that such information sharing with the site was ever authorized to occur. Without knowledge of a new feature, John cannot know to turn it off.

Moreover, even when a user does learn of a new feature and chooses to opt-out, that user can only do so *after* the unwanted sharing has occurred. Even the most privacy-literate and diligent users, then, still cannot prevent unwanted information sharing entirely. According to a class-action lawsuit pending in the United States, Facebook's method of adding new applications and sharing user information with third-party sites without prior consent, as Instant Personalization does, is a breach of the implied covenant of good faith and fair dealing in contract[79] and a violation of the federal Stored Communications Act.[80]

Second, Facebook's privacy settings and privacy policy have been criticized as unnecessarily complex and obscure.[81] Even if John becomes aware that he is over-sharing his information and wants to make changes, he may not be able to figure out how to do so. As of May 12, 2010, users would have to comprehend a 5,830 word policy—longer than the U.S. Constitution absent amendments—and wade through 170 options to make their

---

facebook.com/blog.php?post=391922327130.

[77] *See supra* notes 49–51 and accompanying text (explaining Facebook's opt-out privacy model).

[78] *See* Rose v. Facebook, Inc., No. CA 10-232 S, 2010 WL 2147928, paras. 2–3 (D.R.I. filed May 21, 2010) ("Facebook . . . broadcasts users' personal information through the network unless users affirmatively opt-out. . . . Facebook did not adequately warn users that their information would be posted to unrelated third party websites. . . . Therefore, Facebook, without permission, shared information about users with unrelated third party websites."); *see also infra* Part IV.*A* (detailing the allegations against Facebook).

[79] *Rose*, 2010 WL 2147928, paras. 24–31.

[80] *Id.* paras. 17–23; Stored Communications Act, 18 U.S.C.A. §§ 2701–2712 (2006).

[81] *Facebook Faces Up to Long-Awaited Privacy Upgrades*, *supra* note 12, at 10 ("The site faced complaints that the settings were too complex and made it too easy to inadvertently disclose personal information.").

information as private as possible.[82] Thus, the opt-out options that do exist may be less meaningful because of the time and energy it takes for users to understand and exercise those options. Users may inadvertently "agree" to share information they did not intend to share.[83]

Finally, there are limits on a user's ability to stop sharing certain information, even if the user wants to make the information private.[84] A prime example is the PAI category, which makes certain user information mandatorily available.[85] Several prominent privacy advocacy groups have already petitioned Facebook to eliminate the PAI category and give users full, "true control" over who sees their personal information.[86]

Given the drawbacks of Facebook's opt-out privacy control system, many privacy advocates and lawmakers have urged the site to shift to an opt-in model to give users more meaningful control over their information.[87] Using Canada's privacy law, PIPEDA, the Commissioner played an instrumental role in pressuring the site to move closer to such a model in May 2010.[88]

---

[82] Nick Bilton, *Price of Facebook Privacy? Start Clicking*, N.Y. TIMES, May 13, 2010, at B8.

[83] *Facebook Faces Up to Long-Awaited Privacy Upgrades*, *supra* note 12.

[84] *See infra* notes 209–16 and accompanying text (explaining the limits to the control users have over what information they share through Facebook applications).

[85] Kirtley, *supra* note 58, at 123.

[86] *Open Letter to Facebook: More Privacy Improvements Needed*, ELECTRONIC FRONTIER FOUND. (June 16, 2010), http://www.eff.org/press/archives/2010/06/16 [hereinafter *Open Letter to Facebook*].

[87] James G. Gatto & Seth A. Metsch, *Legal Issues with Virtual Worlds, Virtual Goods and Virtual Currencies*, *in* TECHNOLOGY AND ENTERTAINMENT CONVERGENCE 2010, at 837, 865 (PLI Intell. Prop., Course Handbook Ser. No. 1016, 2010); Press Release, Charles E. Schumer, U.S. Sen., et al., Schumer, Bennet, Franken, Begich Ask Facebook to Fix Privacy Policy to Keep Users' Data Private from Third-Party Websites—Facebook's Recent Decision to Share Personal Info Raises Major Privacy Concerns for Millions of Americans (Apr. 27, 2010), *available at* http://schumer.senate.gov/record.cfm?id=324226&; Rose v. Facebook, Inc., No. CA 10-232 S, 2010 WL 2147928, para. 30 (D.R.I. filed May 21, 2010) (alleging legal violations relating to aspects of Facebook's current privacy model); *Open Letter to Facebook*, *supra* note 86; *Facebook Reveals 'Simplified' Privacy Changes*, BBC NEWS (May 26, 2010), http://www.bbc.co.uk/news/10167143 (quoting Simon Davies, director of Privacy International as stating that "[t]he vast majority of people don't use privacy settings so the reforms are not likely to have as great an impact . . . . If the default is for less information then we've really made a step forward.").

[88] *See Facebook Faces Up to Long-Awaited Privacy Upgrades*, *supra* note 12, at 10 ("Facebook users now have greater control over how much of their personal information is disclosed . . . . The changes were made in response to complaints from users, civil rights groups and governments, particularly Canada's privacy commissioner.").

III. CANADA'S PERSONAL INFORMATION PROTECTION AND ELECTRONIC DOCUMENTS ACT (PIPEDA): AN OVERVIEW

A. Purpose and Scope

In July 2009, the Commissioner released a report declaring Facebook in violation of Canada's private sector privacy law, PIPEDA.[89] Signed into law on April 13, 2000,[90] PIPEDA was designed to protect Canadians' privacy in the new technological age of electronic storage, e-mail, and Internet[91] while still encouraging the free flow of data across borders.[92] PIPEDA's privacy model is premised on knowledge and consent.[93] PIPEDA thus seeks to protect an individual's personal information from being shared in ways that the individual does not know about or consent to.[94] When the Commissioner found aspects of Facebook in violation of PIPEDA in 2009, the cause was essentially for over-sharing users' personal information in unauthorized or undisclosed ways.[95]

---

[89] ELIZABETH DENHAM, REPORT OF FINDINGS INTO THE COMPLAINT FILED BY THE CANADIAN INTERNET POLICY AND PUBLIC INTEREST CLINIC (CIPPIC) AGAINST FACEBOOK INC. UNDER THE PERSONAL INFORMATION PROTECTION AND ELECTRONIC DOCUMENTS ACT (2009), *available at* http://www.priv.gc.ca/cf-dc/2009/2009_008_0716_e.pdf.

[90] PIPEDA, *supra* note 26. The Act was actually implemented in phases over a three-year period beginning on January 1, 2001. OFFICE OF THE PRIVACY COMM'R OF CAN., LEADING BY EXAMPLE: KEY DEVELOPMENTS IN THE FIRST SEVEN YEARS OF THE PERSONAL INFORMATION PROTECTION AND ELECTRONIC DOCUMENTS ACT (PIPEDA) 1 (2008) [hereinafter LEADING BY EXAMPLE], *available at* http://publications.gc.ca/collections/collection_2008/privcom/IP54-6-2008E.pdf.

[91] PIPEDA, *supra* note 26, § 3.

[92] *See OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, ORG. FOR ECON. CO-OPERATION & DEV., http://www.oecd.org/document/18/0,3343,en_2649_34255_1815186_1_1_1_1,00.html (last visited July 24, 2011) ("Privacy protection laws have been introduced . . . to prevent . . . violations of fundamental human rights, such as the unlawful storage of personal data, the storage of inaccurate personal data, or the abuse or unauthorised disclosure of such data. . . . Restrictions on these flows could cause serious disruption in important sectors of the economy . . . .").

[93] DENHAM, *supra* note 89, at 3 ("The central issue in CIPPIC's allegations was knowledge and consent. [The OPC] focused its investigation on whether Facebook was providing a sufficient knowledge basis for meaningful consent by documenting purposes for collecting, using, or disclosing personal information and bringing such purposes to individuals' attention in a reasonably direct and transparent way.").

[94] According to the OPC, the type of consent that must be given depends on the sensitivity of the information. The OPC differentiates between "Positive/Opt-in (Express) Consent" and a "Negative/Opt-out Mechanism." *Consent Under PIPEDA*, *supra* note 25.

[95] *See infra* Part IV.*A* (explaining in more detail the Commissioner's findings regarding Facebook's use of users' personal information).

PIPEDA generally requires an organization to get a person's consent[96] before it can collect, use, or disclose his personal information.[97] Even if an organization gets consent from an individual, use or disclosure of that individual's personal information is limited to the purposes to which that person consented.[98] Organizations must also limit the collection, use, and disclosure of a person's information to "purposes that a reasonable person would consider appropriate under the circumstances."[99] Finally, an individual also has the right to see the personal information that a given business has about that individual.[100]

PIPEDA is based on ten guiding principles: (1) accountability, (2) identifying purposes, (3) consent, (4) limiting collection, (5) limiting use, disclosure, and retention, (6) accuracy, (7) safeguards, (8) openness, (9) individual access, and (10) challenging compliance.[101] According to the principle of "accountability," an organization must protect personal information it holds or transfers to third parties, and ensure that personal information practices and policies are developed and implemented.[102] According to "identifying purposes," an organization must identify why it is collecting personal information and how it will be used.[103] "Consent" and "limiting collection" require an organization to honestly and meaningfully inform an individual and obtain consent for collection; the latter also requires limiting the information collected to what is necessary.[104] "Limiting use, disclosure and retention" puts limits on the use, disclosure, and length of retention of personal information, and "accuracy" encourages organizations to ensure that information is as accurate as possible before using or disclosing it.[105] "Safeguards" requires an organization to protect people's

---

[96] In certain cases, police may be exempt from the consent requirement under PIPEDA. Organizations that collect, use, or disclose personal information for solely journalistic, literary, or artistic purposes are also exempt. OFFICE OF THE PRIVACY COMM'R OF CAN., YOUR GUIDE TO PIPEDA 4 (2009) [hereinafter YOUR GUIDE TO PIPEDA], *available at* http://www.priv.gc.ca/information/02_05_d_08_e.pdf.

[97] *Complying with the Personal Information Protection and Electronic Documents Act*, OFF. PRIVACY COMM'R CAN., http://www.priv.gc.ca/fs-fi/02_05_d_16_e.cfm (last modified June 20, 2005).

[98] *Id.*

[99] *Id.*

[100] *Id.*

[101] *See* ASS'N XPERTISE, THE PIPEDA PRIVACY PRINCIPLES 2–7 (2001), *available at* http://www.axi.ca/resdocs/privacy_guide.pdf (outlining each of the principles in detail).

[102] *Id.* at 2.

[103] *Id.*

[104] *Id.* at 3.

[105] *Id.* at 4.

information from loss, theft, or unauthorized uses.[106] "Openness" refers to informing individuals of the organization's policies regarding personal information in a meaningful way.[107] Finally, "individual access" requires organizations to give people access to see and correct their own information, and "challenging compliance" requires organizations to develop a simple and accessible complaint process for those who feel their privacy has been violated.[108]

B. Who Is Covered and How Facebook Fits

For PIPEDA to apply,[109] the information at issue must be "personal"[110] and the allegedly unauthorized use, disclosure, or collection of that information must occur in the course of "commercial activity."[111] Personal information is defined as "information about an identifiable individual."[112] Currently, details such as a person's name, race, religion, marital status, education, email address, physical characteristics, medical information, income, spending habits, tax returns, and other identification numbers, like one's Social Insurance Number, all qualify as personal information under PIPEDA.[113] This definition is fluid, though, as it is largely shaped by case law.[114]

Many PIPEDA cases turn on whether the information at issue is "capable of identifying" the individual.[115] In one case, the Assistant Commissioner concluded a property manager violated PIPEDA when he photographed

---

[106] *Id.* at 5.
[107] *Id.*
[108] *Id.* at 6–7.
[109] Another threshold issue is that the Act applies only to an "organization," defined as "an association, a partnership, a person and a trade union," therefore, Facebook easily qualified. PIPEDA, *supra* note 26, § 2(1).
[110] *Id.* (defining "personal information").
[111] *Id.* (defining "commercial activity" broadly as "any particular transaction, act . . . course of conduct that is of a commercial character).
[112] *Id.* (noting also that personal information "does not include the name, title or business address or telephone number of an employee of an organization").
[113] YOUR GUIDE TO PIPEDA, *supra* note 96, at 2.
[114] *See generally* LEADING BY EXAMPLE, *supra* note 90, at 5–9 (providing a history and explanation of key case law under PIPEDA).
[115] *Id.* at 6. The Canadian Federal Court adopted the following test to determine personal information at the behest of the Commissioner: "Information will be about an identifiable individual where there is a serious possibility that an individual could be identified through the use of that information, alone or in combination with other available information." *Id.* (quoting Gordon v. Canada (Minister of Health), [2008] F.C.R. 258, para. 34).

tenants' apartments for insurance purposes.[116] The photographs revealed information about the dwellers' "likes," such as musical, art, culinary, and other lifestyle choices, and also included unit and building numbers.[117] The photographs thus violated PIPEDA because they had the potential to link a real-live individual with (otherwise generic) personal information.[118] The photos rendered the individual "identifiable" or "capable of being identified," irrespective of whether the individual was ever actually identified.[119]

In Facebook's case, the Commissioner similarly concluded that information that individuals post on the site qualifies as identifiable personal information under PIPEDA.[120] This is because a user's profile offers information about that user's race, religious and political preferences, and habits—all of which are capable of identifying the user. Moreover, such information is linked to an individual's photo and user ID, which is most often their real-world name.

Once the information in Facebook users' profiles qualified as personal, the next hurdle was to determine whether such information was actually used for commercial purposes. The Commissioner determined that it was.[121] She explained that even though the site is free for users and users voluntarily post information for "purely personal purposes," such information was also used for commercial purposes[122] because Facebook uses it to attract revenue from third-party advertisers and application developers.[123]

> [T]hose features of the site that do not have an obvious link to its business model are included to enhance the user's experience on Facebook. Enhancing the experience likely encourages existing members to continue to use the site and presumably encourages others to join as well—thereby indirectly contributing to the success of Facebook as a commercial enterprise. In that sense, collection, use and disclosure of personal information in relation to a feature without an apparent direct commercial link can still be

---

116 *Id.*
117 *Id.*
118 *Id.*
119 *Id.*
120 DENHAM, *supra* note 89, para. 11.
121 *Id.*
122 *Id.*
123 *Id.* para. 14.

> characterized as occurring 'in the course of commercial activit[ies]' in the sense required under the Act.[124]

Facebook thus qualifies for PIPEDA scrutiny because the information users post on the site is "personal,"[125] and any allegedly unauthorized use, disclosure, or collection of user information occurs in the course of "commercial activity."[126]

C. How Violations Are Caught and Enforced

The OPC provides oversight and helps to ensure compliance with PIPEDA.[127] The mission of the OPC is to protect and promote the privacy rights of individuals.[128] If an individual or group believes its privacy has been violated, it can file a written complaint with the Commissioner.[129] The Commissioner can also initiate a complaint on her own when she believes there are reasonable grounds to warrant an investigation.[130] The review of Facebook occurred because the Canadian Internet Policy and Public Interest Clinic (CIPPIC), a private legal clinic at the University of Ottawa,[131] filed a complaint with the OPC in May 2008.[132]

Once the complaint is filed, the Commissioner conducts an investigation.[133] Within a year after the original complaint is filed or

---

[124] *Id.* para. 12 (quoting PIPEDA, *supra* note 26, § 4(1)(a)).
[125] *Id.* para. 11.
[126] *Id.*
[127] LEADING BY EXAMPLE, *supra* note 90, at 2.
[128] *Id.*
[129] *Id.*; *see also* PIPEDA, *supra* note 26, § 11(1) ("An individual may file with the Commissioner a written complaint against an organization for contravening a provision of Division 1 or for not following a recommendation set out in Schedule 1.").
[130] LEADING BY EXAMPLE, *supra* note 90, at 2; PIPEDA, *supra* note 26, § 11(2) ("If the Commissioner is satisfied that there are reasonable grounds to investigate a matter under this Part, the Commissioner may initiate a complaint in respect of the matter."); *see also Information About Privacy Breaches and How to Respond*, OFF. PRIVACY COMM'R CAN., http://www.priv.gc.ca/resource/pb-avp/pb-avp_intro_e.cfm (last modified Nov. 5, 2008) (noting that the Commissioner only initiates an investigation "in exceptional circumstances, where, for example, the breach is very serious, appears to be systemic or the organization does not appear to be responding adequately").
[131] *See About Us*, CANADIAN INTERNET POL'Y & PUB. INT., http://www.cippic.ca/about-us/ (last visited July 25, 2011) (describing the clinic as a student-centered research and advocacy establishment on technology-related policy and law reform).
[132] Letter from Philippa Lawson, Dir., Canadian Internet Policy and Pub. Interest Clinic, to Jennifer Stoddart, Privacy Comm'r of Can. (May 30, 2008) (available at http://www.cippic.ca/uploads/CIPPICFacebookComplaint_29May08.pdf) [hereinafter CIPPIC Complaint].
[133] PIPEDA, *supra* note 26, § 12(1) (noting also that there are a few exceptions where an

initiated, the Commissioner must prepare a report containing her findings and recommendations, any settlement reached by the parties, and, if appropriate, a request that the organization give notice of any actions taken or intended to be taken to implement the Commissioner's recommendations.[134] After the Facebook investigation, the Commissioner wrote such a report explaining her findings and making recommendations to put Facebook in compliance with PIPEDA.[135]

The Commissioner's recommendations are nonbinding,[136] yet she may, at any reasonable time and with reasonable notice, investigate whether an organization is complying with OPC recommendations using the same methods PIPEDA grants to conduct the initial investigation.[137] If an organization is, after a reasonable or set time, not complying with the Commissioner's recommendations, the Commissioner (or the complainant) may then turn to federal court for legal enforcement.[138]

In Facebook's case, the Commissioner never actually turned to the federal courts, but she came very close after Facebook's initial refusal to comply with her recommendations and its subsequent delay in incorporating promised changes.[139] The threat of judicial action likely gave the Commissioner's recommendations the force they needed to compel Facebook's compliance efforts.[140]

---

investigation may not be the next step).

[134] *Id.* § 13(1).

[135] *See generally* DENHAM, *supra* note 89 (explaining Commissioner's findings and recommendations after the Facebook investigation).

[136] LEADING BY EXAMPLE, *supra* note 90, at 2.

[137] PIPEDA, *supra* note 26, § 18(1).

[138] *Id.* § 16 ("The Court may . . . (a) order an organization to correct its practices . . . (b) order an organization to publish a notice of any action . . . to correct its practices . . . and (c) award damages to the complainant . . . .").

[139] *See* Carron & Healey, *supra* note 15, at S9 ("Initially, Facebook resisted complete compliance with the Privacy Commissioner's recommendations. However, given the Commissioner's ability to submit the matter to the courts, Facebook ultimately proposed solutions satisfying Canadian privacy laws.").

[140] *Id.*

IV. HOW CANADA USED PIPEDA TO PUSH FACEBOOK TO IMPROVE USER PRIVACY

A. Specific Allegations Against Facebook

The CIPPIC complaint against Facebook contained twenty-four allegations of PIPEDA violations.[141] "The central issue in CIPPIC's allegations was knowledge and consent . . . [that is,] whether Facebook was providing a sufficient knowledge basis for meaningful consent by documenting purposes for collecting, using, or disclosing personal information and bringing such purposes to individuals' attention in a reasonably direct and transparent way."[142] Of the twenty-four counts, the Commissioner dismissed several and Facebook resolved several others.[143] Two unresolved issues were third-party applications and the length of time that Facebook stored personal information on current, deceased, and non-Facebook members.[144] Third-party application settings and policies were one of the most contentious issues.[145]

Regarding Facebook's third-party policies, the Commissioner said that Facebook was "in effect providing third-party application developers with the ability to retrieve the personal information of users (and their friends) who sign up for the applications."[146] This was problematic for two reasons.

First, Facebook was not doing enough to obtain meaningful consent from users when disclosing their personal information to application developers.[147] PIPEDA Principle 4.3 generally requires individuals' knowledge and consent for the collection, use, and disclosure of their personal information. Principle 4.3.2 requires organizations to make reasonable efforts to ensure the individual understands how that information will be used.[148] Principle 4.3.2 clarifies that, for consent to be meaningful, "the purposes must be

---

[141] *See* CIPPIC Complaint, *supra* note 132 (detailing CIPPIC's allegations against Facebook).

[142] DENHAM, *supra* note 89, at 3.

[143] *Id.*

[144] *Id.*

[145] *Id.* para. 194 ("Facebook objected strenuously to [CIPPIC's] preliminary treatment of the allegations relating to third-party applications. However, after considering Facebook's objections, [CIPPIC] remains concerned about the issues.").

[146] *Id.* para. 14 (explaining also that "in a traditional model, an organization may subcontract parts of its business to third parties (thus transferring personal information to another entity), or it may disclose personal information to another company that is purchasing customer lists for marketing, for example").

[147] *Id.* at 3.

[148] PIPEDA, *supra* note 26, princ. 4.3.2.

stated in such a manner that the individual can reasonably understand how the information will be used or disclosed."[149] In contravention of Principle 4.3.2, the Commissioner said Facebook was not informing users of the *purpose* of disclosing their personal information to third-party developers,[150] that it was giving developers more access than they needed to run their applications,[151] and that it was granting third-party developers access to users' personal information when their friends or members of their network added the application without giving adequate notice.[152]

Second, "the Assistant Commissioner determined that Facebook did not have adequate safeguards in place to prevent unauthorized access by application developers to users' personal information."[153] PIPEDA Principle 4.7 requires an organization to protect an individual's personal information from unauthorized use or access through "security safeguards appropriate to the sensitivity of the information."[154] In violation of Principle 4.7, the site was inadequately safeguarding personal information because it did not monitor the legitimacy or quality of third-party applications that were accessing user data.[155]

B. Facebook's (Delayed) Response

After initially refusing to comply with several of the Commissioner's recommendations, Facebook finally agreed to give users more control over how much of their personal information was shared by September 2009.[156] Specifically, Facebook agreed to the Commissioner's recommendation that applications only be allowed to access the personal information that users consented to disclose.[157] By February 2010, however, critics claimed the new policies exposed more, not less, user information and the Assistant Commissioner indicated that "[s]ome Facebook users are disappointed by

---

[149] *Id.*

[150] DENHAM, *supra* note 89, at 94 (indicating that this violated PIPEDA Principles 4.2.2 and 4.2.5, which require organizations to disclose the purposes for which personal information is being collected before it is collected).

[151] *Id.* (indicating that this violated PIPEDA Principle 4.4.1, which requires an organization to collect only the information necessary for the purposes it has identified).

[152] *Id.* at 95 (indicating that this violated PIPEDA Principle 4.3.2, which requires an individual's knowledge and meaningful consent with regards to collection).

[153] *Id.* at 3.

[154] PIPEDA, *supra* note 26, princ. 4.7.

[155] DENHAM, *supra* note 89, at 95.

[156] *Facebook Won't Face Off with Canada's Privacy Commissioner*, 27 ANDREWS COMPUTER & INTERNET LITIG. REP., Sept. 30, 2009, at 11.

[157] *Id.*

certain changes being made to the site—changes that were *supposed* to strengthen their privacy and the protection of their personal information" in a public statement.[158] After rumors about the Commissioner turning to the federal courts for enforcement, Facebook responded. On September 22, 2010, the Commissioner released a statement indicating, "The changes Facebook has put in place in response to concerns we raised as part of our investigation last year are reasonable and meet the expectations set out under Canadian privacy law."[159]

By September 2010, Facebook began to restrict an application from accessing user information without getting express consent for each category of personal information it wanted to access.[160] This is called a "permissions model."[161] When users add an application, they are notified that it wants to access certain types of information about them, and they can consent to sharing that data.[162] Facebook also created a panel in each user's privacy settings to reveal which applications have access to which bits of information about that user.[163] For example, the panel will indicate to a user if the application "Pandora" has access to the user's profile information. Information listed in a user's panel includes religious and political views, education history, work history, and Facebook Status, as well as a user's family and relationships, photos and videos, and all of the user's friends' personal information to which the user has access.[164]

The post-September 2010 privacy model still requires users to share personal information with an application before using it and there is no longer an opt-out option as there was before December 2009.[165] Users are, however, allowed to opt-out of the Facebook Platform entirely.[166] By turning off the Platform, users are no longer able to use any applications, but they can at least avoid sharing any information with them.[167]

---

[158] Randall Palmer, *Canada Investigates Facebook Again over Privacy*, REUTERS (Jan. 28, 2010), http://in.reuters.com/article/2010/01/27/us-facebook-canada-idINTRE60Q6M220100127 (emphasis added).

[159] Statement, Jennifer Stoddart, Canadian Privacy Comm'r (Sept. 22, 2010) [hereinafter Stoddart Statement], *available at* http://www.priv.gc.ca/media/nr-c/2010/nr-c_100922_e.cfm.

[160] *Id*.

[161] *Id*.

[162] *Id*.

[163] *Apps Settings*, FACEBOOK, http://www.facebook.com/settings/?tab=applications (last visited Dec. 15, 2010) (document on file with author).

[164] *Id*.

[165] *See supra* Part II.*B* (explaining the evolution of Facebook's privacy policies regarding applications before and after December 2009).

[166] Zuckerberg, *supra* note 76.

[167] *Id*.

Though the Commissioner was satisfied with these improvements and others, she emphasized, "to be clear, I am only speaking about those issues [related to the investigation] rather than the site as a whole."[168] Since her investigation concluded, the Commissioner has been investigating several other complaints.[169] There have also been several other developments in Facebook's privacy narrative that reveal Facebook's PIPEDA compliance is not as meaningful as it could be.

V. WHY FACEBOOK'S PIPEDA COMPLIANCE IS SUPERFICIAL AND HOW IT COULD BE MEANINGFUL

A. Red Flag Immediately Following Commissioner's "OK" of Facebook

Remarkably, roughly three weeks after the Commissioner completed her Facebook investigation, the *Wall Street Journal* reported on October 18, 2010 that Facebook applications had been leaking users' Facebook ID numbers to outside marketers and tracking companies.[170] Specifically, many applications that had access to user information were sharing users' names and, in some incidences, their friends' names, with dozens of Internet tracking and advertising companies.[171] The ten most popular applications were implicated.[172] The breach affected tens of millions of users, including those whose profiles were set to the strictest privacy settings.[173]

The leak occurred via referers, or bits of information that are sent when a user of one website clicks a link to another website.[174] The referer informs the new website from which website a user is arriving.[175] This practice is

---

[168] Stoddart Statement, *supra* note 159.

[169] *Facebook Investigation Follow-up Complete*, OFF. PRIVACY COMM'R CAN., http://www.priv.gc.ca/media/nr-c/2010/bg_100922_e.cfm ("[T]he Office has received several further complaints about issues that were not part of the initial investigation . . . . As a result of those complaints, the Office has opened investigations that are examining Facebook's invitation feature (the process by which Facebook suggests friends to new users) and Facebook social plug-ins (the Facebook 'Like' buttons that other websites can add to their sites).").

[170] Steel & Fowler, *supra* note 48.

[171] *Id.*

[172] *Id.* (indicating that implicated applications include FarmVille, Texas Holdem Poker, and FrontierVille, and that three of the applications, including FarmVille, were sharing personal information about users' friends).

[173] *Id.*

[174] Geoffrey A. Fowler & Emily Steel, *Referers: How Facebook Apps Leak User IDs*, WALL ST. J. (Oct. 18, 2010), http://blogs.wsj.com/digits/2010/10/18/referers-how-facebook-apps-leak-user-ids/.

[175] *Id.*

standard across the Internet and helps websites analyze the sources of their traffic and customize their information.[176] Privacy is also generally not a problem, because the referer information is not linked to any user's identity.[177] In the Facebook context, however, a referer may allow companies to connect otherwise "anonymous" data " 'to the very *non*-anonymous Facebook User ID, which is linked back to [one's] real-world name and identity.' "[178]

The leak violated Facebook's own policies that prohibit applications from sharing personal information about users with outside companies.[179] Its mechanics illustrate Facebook's unique and heightened responsibilities to protect user information relative to its online counterparts like MySpace. It also demonstrates that the issues the Commissioner sought to address in 2009—proper safeguards for data and user control over information—have not been meaningfully resolved.

A similar breach occurred when Facebook transmitted user IDs to advertisers in May 2010.[180] At the time, Facebook would not acknowledge that the user ID was personally identifiable information but promised to redevelop software to protect user data.[181] This "repeat-offense" in October—just weeks after the Commissioner ended her investigation—is a reminder that Facebook cannot be relied on to meaningfully self-correct or regulate without legal pressure.

B. The Path to Meaningful Compliance

Outside legal authorities like the Commissioner must police Facebook to ensure that it sets and follows its own policies to protect user privacy. The PIPEDA principles of accountability, limiting use and disclosure, and safeguarding sensitive personal information are ideal privacy guidelines for Facebook and are epitomized by an opt-in privacy model.[182] The following

---

[176] *Id.*

[177] *Id.*

[178] *Id.* (emphasis added) (quoting Peter Eckersley, a senior staff technologist for the Electronic Frontier Foundation).

[179] Kirtley, *supra* note 58, at 127–28.

[180] *Id.* at 127 (explaining that Facebook was sending user IDs to marketers when a user clicked on an ad from Facebook).

[181] *Id.* at 128.

[182] *See generally Consent Under PIPEDA*, *supra* note 25 (explaining how to determine the appropriate form of consent under PIPEDA, and that "[Positive/Opt-in (Express) Consent] is the strongest form of consent, and is in keeping with the spirit of PIPEDA").

recommendations create a blueprint for Facebook to move closer to an opt-in model by meaningfully complying with PIPEDA.

1. Recommendation I: Ask Permission Before Adding Information-Sharing Features

First, Facebook should not add new information-sharing features to user accounts without asking permission.[183] In its 2008 complaint against Facebook, CIPPIC alleged the site was not informing users when their personal information was being collected, used, or disclosed for new purposes in violation of PIPEDA Principle 4.2.4.[184] This Principle states, "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."[185] In other words, both a "new purpose" and failure to obtain consent must be present for a violation of Principle 4.2.4.

At the time of the Commissioner's investigation, CIPPIC did not offer any evidence of instances when Facebook violated PIPEDA Principle 4.2.4.[186] As a result, the Commissioner dismissed this particular allegation as not well-founded, explaining, "In the absence of any evidence . . . I am at present unable to find Facebook to be in contravention of the Act in this regard."[187]

The Instant Personalization application, however, is likely a valid example of a new information-sharing feature that uses personal information "for a purpose not previously identified"[188] because it exports information from Facebook to third-party websites previously unaffiliated with Facebook.[189] Instant Personalization was not examined in the Commissioner's investigation because the application was launched after the

---

[183] *See generally id.* ("Unless the individual takes action to 'opt out' of the purpose—that is, say 'no' to it—the organization assumes consent and proceeds with the purpose. The individual should be clearly informed that the failure to 'opt out' will mean that the individual is consenting to the proposed use or disclosure of the information.").

[184] DENHAM, *supra* note 89, para. 215.

[185] PIPEDA, *supra* note 26, princ. 4.2.4.

[186] DENHAM, *supra* note 89, para. 221.

[187] *Id.*

[188] PIPEDA, *supra* note 26, princ. 4.2.4.

[189] *See supra* notes 66–68 and accompanying text (explaining the mechanics of the Instant Personalization feature).

Commissioner completed her review.[190] The application likely qualifies as a new use of a user's personal information under Principle 4.2.4 of PIPEDA, and because Facebook added the application automatically without user consent, it likely contravenes Principle 4.2.4.

Asking user permission before adding a new feature like Instant Personalization, or any application that increases information sharing, will align Facebook with PIPEDA's requirement that an organization procure an individual's permission before putting that individual's personal information to new uses.

2. Recommendation II: More Meaningful Disclosure in the Third-Party Context

Asking user permission, as suggested above, is only effective when users are given enough information to make informed decisions. As of October 6, 2010, Facebook's control panel allows users to see which applications have access to which pieces of information about them.[191] The application privacy settings page also indicates to users when an application accesses that information.[192] This page, however, does not provide a comprehensive or clear picture of exactly how, why, or how frequently user information is used.[193]

PIPEDA Principle 4.3.2 notes that an organization must "make a reasonable effort to ensure that the individual is advised of the purposes for which the information will be used" and that "[t]o make the consent meaningful, the purposes must be stated in such a manner that the individual can *reasonably understand* how the information will be used or disclosed."[194]

Under these criteria, Facebook's application control panel is not a meaningful source of information unless users also have access to *how* and *why* their data is being used by applications. The current control panel does not offer this information. For example, the panel does not indicate to users the information that a user's friends' applications have accessed about that

---

[190] *See* Josh Constine, *Introduction Page Explains Facebook Instant Personalization to Users*, INSIDE FACEBOOK (Dec. 20, 2010), http://www.insidefacebook.com/2010/12/20/instant-personalization-intro-page/ (noting that Instant Personalization began in April 2010).

[191] Steel & Fowler, *supra* note 48.

[192] *Id.*

[193] *See Apps Settings*, *supra* note 163.

[194] PIPEDA, *supra* note 26, princ. 4.3.2 (emphasis added).

user.[195] Privacy advocates have termed this phenomenon the "app gap"—the fact that your friend's applications get access to your information even if you have never used nor installed the application.[196] Thus, users who take the time to examine their application privacy settings may think they "reasonably understand"[197] exactly who (or what) is accessing their information, but they are missing this critical piece of the puzzle.

Giving users a more comprehensive and accurate picture of how much information they are sharing with applications will include a panel that indicates how much information is going to the applications their friends have installed. It will list users' friends' applications, and tell users which bits of information those applications are accessing. Finally, in addition to telling users which applications can access which information about them, a comprehensive panel will tell users how often their information is accessed and exactly how it is used. Providing such information allows users to make more informed choices when deciding whether to use applications on the Platform. Enabling such informed decision-making is key to meaningful compliance with PIPEDA Principle 4.3.2 on obtaining user consent.

Although many users may not go through the trouble of looking at the details to determine which application is accessing what information about them, making such statistics publicly accessible will act as a deterrent to over-sharing by applications (either by design or by accident) as happened in the November 2010 application leak incident.[198]

3. Recommendation III: More User Control in the Third-Party Context

Users should also be given more control over what information they share with applications. Without turning off the Facebook Platform entirely, users are currently unable to block applications from accessing their information to varying degrees,[199] although the option existed prior to December 2009.[200] According to Facebook's policies as of January 2011, "apps and websites

---

[195] Steel & Fowler, *supra* note 48; Chris Conley, *Facebook Application Privacy Breach Exposed*, ACLU N. CAL. (Oct. 18, 2010), http://www.aclunc.org/issues/technology/blog/facebook_application_privacy_breach_exposed.shtml.

[196] Kurt Opsahl, *Facebook Moves Closer to EFF Bill of Privacy Rights*, ELECTRONIC FRONTIER FOUND. (Oct. 6, 2010), http://www.eff.org/deeplinks/2010/10/facebook-moves-closer-eff-bill-privacy-rights.

[197] PIPEDA, *supra* note 26, princ. 4.3.2.

[198] *See supra* Part V.*A* (explaining the November 2010 application leak).

[199] Zuckerberg, *supra* note 76.

[200] *See infra* Part II.*B* (explaining Facebook's Platform privacy policies before December 2009).

you and your friends use already have access to your name, profile picture, gender, networks, friend list, user ID, username, and any other information you share with everyone."[201]

In practice, this list of information available to applications is quite extensive. For example, to use the application "Graffiti," a nifty feature which allows a user to "spray paint" pictures or messages and post them on friends' walls, a user must allow the application to access her basic information (full name, profile picture, gender, networks, user ID, and list of friends); profile information (music, movies, books, quotes, activities, interests, groups, events, notes, birthday, hometown, current city, websites, religious views, political views, education history, work history, and Facebook status); family and relationships (significant other and relationship details, family members, and relationship status); photos and videos in which the user appears (whether those photos are originally posted by the Graffiti user or one of her friends); and, finally, her *friends*' information (including all information listed above that the user has access to about her friends).[202] The Graffiti application can also detect a user's online presence (i.e., whenever the user is signed in) and send emails directly to that user's personal email address.[203]

Given the imbalance of the tradeoff—an extensive array of personal details in exchange for electronic spray paint—this information sharing may violate PIPEDA Principle 4.3.3 that "[a]n 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 fulfil the explicitly specified, and legitimate purposes."[204] Subsection 5(3) also requires such personal information only be collected for "purposes that a reasonable person would consider are appropriate in the circumstances."[205]

Giving an application access to a user's likes, hobbies, or social groups may indeed be a legitimate use of user information, as it could help software developers to better define their target audiences and tailor their applications accordingly. Access to a user's relationship status, photographs, videos, and family members, though, may be unnecessarily excessive and in contravention of the "legitimate purposes" requirement of Principle 4.3.3.[206]

---

[201] *Controlling How You Share*, *supra* note 66.
[202] *Apps Settings*, *supra* note 163.
[203] *Id*.
[204] PIPEDA, *supra* note 26, princ. 4.3.3.
[205] *Id.* § 5(3).
[206] *Id.* princ. 4.3.3.

Facebook could counter that, irrespective of how "reasonable"[207] or extensive the tradeoff, users are still knowingly making the decision to provide their information and get something in return. Facebook could argue that the user is aware of the deal, as the information available to the application is "explicitly specified"[208] as required by Principle 4.3.3, and the user gives permission before any information sharing occurs. So this aspect of third-party sharing—when users make an explicit tradeoff with a specific application they wish to use—may not be alone sufficient to violate PIPEDA.

The case for a PIPEDA violation is more compelling, though, because other applications also gain access to user information even when users are *not* signed up or have not explicitly agreed to use them.[209] As long as a user has not disabled the Platform feature entirely, even applications a user has *not* signed up for can still see some of that user's information. So even if a user's application privacy settings are set to the maximum possible and he has never even used an application before,[210] that user cannot keep applications from seeing information that is publicly available to fellow Facebook users.[211] If a user's friend uses the Graffiti application, for example, that application can then access any information that the friend can see about the user.[212]

As of January 2011, there is a tab on the application privacy page that gives users some control over what information their friends' applications can access about them.[213] If users click onto the "Info Accessible Through Your Friends" option, they should see eighteen checked boxes, each representing a bit of their own personal information.[214] Assuming users make it to this point in the privacy controls process, they then have the opportunity to manually uncheck each of the eighteen boxes so that their friends' applications cannot have access to these eighteen categories of information.[215] However, users will then read three lines of text at the bottom of the page explaining the parts of information they *cannot* control

---

[207] *Id.* § 5(3).
[208] *Id.* princ. 4.3.3.
[209] Zuckerberg, *supra* note 76 (indicating that applications can still see information the user makes available to everyone).
[210] Short of entirely disabling the Platform, that is.
[211] Zuckerberg, *supra* note 76.
[212] *See supra* text accompanying notes 202–03 (explaining the Graffiti application and the information a user must make available to use it).
[213] *See Apps Settings*, *supra* note 163.
[214] *Id.*
[215] *Id.*

access to: "your name, profile picture, gender, networks and user ID (along with any other information you've set to everyone)" because that information "is available to friends' applications unless you turn off platform applications and websites."[216]

In the words of the Commissioner, "One of the key concepts of [PIPEDA] is that of one's control of their personal information."[217] To better comply with this fundamental PIPEDA concept, Facebook should give users more meaningful control over their personal information. Rather than the all-or-nothing option of either turning off the Platform or submitting to extensive sharing with third parties, the site should offer a middle ground. Users should only have to share information with the applications they are actually using, not with applications generally or the applications of their friends. When a user is sharing information with an application, the user should have more input regarding how much information the application uses, and applications should be limited to accessing information that truly enables them to better provide a service to their users. Details like "Relationship Status" and photos from the user's most recent holiday party are likely unnecessary bits of information. Giving users more control over their personal data comports with the "legitimate purposes" requirement of PIPEDA Principle 4.3.3, and also with the "reasonable expectations of the individual" under Principle 4.3.5.

VI. CONCLUSION

Canada has played an instrumental role in the global pushback against over-sharing by Facebook. Given the strength of its privacy laws and the resolve of its current Commissioner, though, Canada can do more. Facebook has still not meaningfully complied with PIPEDA in letter or in spirit, and thus the Commissioner should re-launch an investigation pushing for more holistic changes to the Facebook site. Namely, she should demand the site shift closer to an opt-*in* information-sharing structure that enables users to choose when and what they want to share, rather than the current opt-out model that allows the site to assume users' consent to share everything. This can be achieved by offering individual users more specific control over what information is publicly available by default, and by increasing disclosure so users better understand how their information is being used before they make

---

[216] *Choose Your Privacy Settings: Apps, Games and Websites*, FACEBOOK, http://www.facebook.com/settings/?tab=privacy&section=apps&h=c2ce0f0f5f389375a502b5477dbdd33a (last visited Dec. 15, 2010) (document on file with author).

[217] *See* DENHAM, *supra* note 89, para. 13.

information-sharing decisions. Urging an opt-in privacy mode for Facebook keeps with the spirit of PIPEDA and the current movement in Canada to encourage "privacy by design" by making users' personal data private by default.[218] It will also, as it did in 2009, give Canada the chance to tackle a global problem with global ramifications for Facebook's 750 million plus users around the world.

[218] *Why 'Privacy By Design' is the New Corporate Hotness*, FORBES (July 28, 2011), http://www.forbes.com/sites/kashmirhill/2011/07/28/why-privacy-by-design-is-the-new-corporate-hotness/.