Samuelson-Glushko Canadian Internet Policy and Public Interest Clinic
Clinique d'intérêt public et de politique d'internet du Canada Samuelson-Glushko

Statement of Concern
Re: Facebook's new Privacy Approach

Tamir Israel, Staff Lawyer, CIPPIC

February 20, 2010

Samuelson-Glushko Canadian Internet Policy and Public Interest Clinic (CIPPIC)
University of Ottawa – Faculty of Law, Common Law Section
57 Louis Pasteur Street, ON., K1N 6N5
Tel: (613) 562-5800 ext. 2553
Fax: (613) 562-5417
www.cippic.ca

Table of Contents

Executive Summary

This document serves two distinct purposes. First and most importantly, it highlights CIPPIC's most immediate concerns with respect to privacy dangers raised by recent changes made by Facebook to its site , primarily in early December of 2009 (the "Transition"). Second, it gauges Facebook's more general compliance with the resolution it entered into with the Privacy Commissioner, as described in a Letter of Resolution ("Resolution"),[i] with the Assistant Privacy Commissioner's Report of Findings ("Findings"),[ii] and with PIPEDA generally.

The Transition has prompted international rebuke from privacy advocates[iii] as well as a complaint to the US FTC by EPIC and others,[iv] a renewed investigation by our own Privacy Commissioner,[v] and a review of EU data protection laws by EU Justice Commissioner Viviane Reding to ensure these remain capable of protecting privacy rights.[vi] Viewed within the context of the Finding and the Resolution, CIPPIC is most concerned that the Transition fails to meet a number of clear standards set out in the very Finding with which it was intended to comply. As a result, Facebook has taken the vast amounts of personal information its users had invested into it and made much of it available to everyone. It did so without the adequate, informed consent of those users, many of whom are not aware of the degree to which their personal information has now been disclosed. CIPPIC views the resulting risks to be immediate, and asks Facebook to respond to CIPPIC's concerns with respect to the Transition, in particular, within 30 days so that CIPPIC may assess the need for further action.

CIPPIC has additional concerns, less urgent in nature, but nonetheless troubling as they appear to signal an ongoing lack of compliance with PIPEDA. In some cases, Facebook has failed to make specific changes it undertook to make. In others, Facebook's violations are of the spirit or the letter of the Finding and of PIPEDA. CIPPIC offers suggestions on how these violations can be addressed, and asks that Facebook remedy these concerns as well.

---

[i] E. Denham, "Letter from OPC to CIPPIC outlining its resolution with Facebook", ["Resolution"], Office of the Privacy Commissioner of Canada, August 25, 2009, available online at: <http://www.priv.gc.ca/media/nr-c/2009/let_090827_e.cfm>.

[ii] PIPEDA Case Summary #2009-008, *Report of Findings into the Complaint Filed by the Canadian Internet Policy and Public Interest Clinic (CIPPIC) against Facebook Inc.*, [Finding] July 15, 2009, available online at: <http://www.priv.gc.ca/media/nr-c/2009/let_090827_e.cfm>.

[iii] See, for example, K. Bankston, "Facebook's New Privacy Changes: The Good, The Bad, and the Ugly", Electronic Frontier Foundation, December 9, 2009, available online at: <http://www.eff.org/deeplinks/2009/12/facebooks-new-privacy-changes-good-bad-and-ugly>, and N. Ozer, "Facebook Privacy in Transition – But Where is it Heading?", American Civil Liberties Union, Blog of Rights, December 9, 2009, available online at: <http://www.aclu.org/blog/technology-and-liberty/facebook-privacy-transition-where-it-heading>.

[iv] EPIC *et. al.*, Complaint before the Federal Trade Commission, *In re Facebook*, December 17, 2009, available online at: <http://epic.org/privacy/inrefacebook/EPIC-FacebookComplaint.pdf>.

[v] Office of the Privacy Commissioner of Canada, "Privacy Commissioner launches new Facebook probe", News Release, January 27, 2010, available online at: <http://priv.gc.ca/media/nr-c/2010/nr-c_100127_e.cfm>.

[vi] M. Newman, "Facebook's Privacy Changes Being Watched by European Commission", Business Week, February 5, 2010, available online at: <http://www.businessweek.com/news/2010-02-05/facebook-s-privacy-changes-being-watched-by-european-commission.html> and L. Phillips, "New EU Privacy Laws Could Hit Facebook", Business Week, January 29, 2010, available online at: <http://www.businessweek.com/globalbiz/content/jan2010/gb20100129_437053.htm>. Commissioner Redding described her reaction to Facebook's Transition changes with the term 'astonishment'.

A. The Transition

The Transition resulted in a number of users changing their privacy settings to adopt Facebook's 'recommendations'. CIPPIC argues that Facebook's Transition was in violation of both the spirit and the letter of the initial Finding, and as such is invalid at law and, viewed within the context of the Resolution, difficult to justify in practice. First, section II of the Finding set out legal principles and standards governing the manner in which new privacy settings can be presented to users. It did so in the context of new users, but applies equally to circumstances such as the Transition. Applying these standards, and PIPEDA generally, consent gained by Facebook for Transition changes was deficient in both form and substance. It failed to properly inform users and pre-selected settings far out of line with reasonable expectations. Second, the core of the Finding was to enhance user knowledge, and also to increase user control over personal information in ways that supplement reasonable expectations of users with respect to default settings. Far from doing so, the Transition expressly removed the ability of users to control how much of their information will be disclosed. Finally, the Transition makes it difficult if not impossible for Facebook to effectively carry out some of its remaining obligations under the Resolution with respect to third party developers.

Moving forward, the Transition has implemented a general approach to privacy that CIPPIC does not think can be upheld under PIPEDA. It takes the basic premise, central to data protection, that it is the *user* who knowingly controls her information and upends it. Its starting point is to extract 'limitless' user consent to do as it sees fit with broad categories of personal information, and then attempts to supplement this limitless release with piecemeal protections where it sees fit. Data protection typically starts from the opposite extreme – with user knowledge and consent required for each specific collection, use and disclosure of personal information. CIPPIC highlights in its Statement of Concern below a number of ways in which it believes Facebook's piecemeal protections and user explanations are currently inadequate, but, ultimately, it holds little hope that this new approach to privacy, which begins with 'public availability' to 'Everyone', can be saved by any piecemeal protections. The process is, in its view, inherently flawed.

i. The Transition violated user expectations, the Finding and PIPEDA

The Finding held, quite clearly, that if Facebook is to pre-select default privacy settings for its users, even if it is to do so in the presence of readily available opt-out mechanisms, such defaults must be in line with reasonable expectations of Facebook users.[vii] The rationale for this requirement is that most users will not take the time to understand and adjust their settings. They will trust Facebook to act in ways that are reasonable, and to recommend settings that most users would find acceptable. Because of this trust, if Facebook is to recommend settings to its users through pre-selection, it must do so in ways that meet reasonable expectations. On Facebook, users generally expect information to be shared with 'only friends'[pages 27-31].[viii] The Transition failed to meet this requirement as Facebook's recommended settings, chosen by default for the vast majority of its users [pages 13-27], allow it to disclose its user's information beyond 'only friends' in most cases.

[vii] Finding, *supra* note ii at paras. 87-98.
[viii] Finding, *supra* note ii at paras. 80-81.

'Only friends' user expectations emerge from a number of sources. They are recognized in Facebook's user-oriented site literature, which begins on its home page where its motto of "help[ing] you connect and share with the people in your life" is prominently emblazoned. This motto is reinforced throughout the site – 'to help you find and connect with your friends' is the golden thread that runs through all of Facebook's user-oriented documentation. But this is not the true source of such expectations, which emerge from the character of interactions on Facebook and from the friend-based architecture of the site, where the primary control over access to user profile items is the 'friend' request. It is on the basis of *these* expectations that users have felt sufficiently secure to invest vast amounts of personal information in Facebook's service [pages 27-31]. As stated in its developer materials:

> Facebook users create rich profiles with Facebook in order to share information with their friends. We offer rich privacy settings that allow people to feel secure sharing highly personal information including interests, thoughts, and contact information. Given this rich set of control [sic.], a significant number of Facebook users have filled out information on their profile.[ix]

Facebook failed to set reasonable user defaults for the majority of users in the Transition. But that is not the limit of its transgressions. The Finding additionally held that merely setting reasonable user defaults is not on its own sufficient to meet consent requirements.[x] This is because, at its core, privacy is subjective and control-oriented – different users will have different sensitivities. Only individual users will know the contexts in which they wish to expose their information. For such reasons it is necessary to take steps to ensure users are aware of privacy issues in a meaningful way. To meet this requirement, Facebook had undertaken to put in place a 'privacy wizard' or 'privacy tutorial'.[xi] The rationale behind this requirement was to better inform users as to what was behind the privacy settings – that is, to provide meaningful information on what privacy settings would look like for different levels of privacy sensitivity, always keeping reasonable expectations in mind as a baseline.

A sample, balanced, and reasonable explanation of a setting might look like this:

> Facebook recommends settings that make your name available for everyone on Facebook to see and search for. This will help your friends find you and send you friend requests so you can decide whether to share more with them or not. Since many users share names, you may in addition to your name wish to make your profile picture available as well.
>
> Some may be more protective of their privacy, and may wish to limit who can find them. For these people, Facebook recommends that you adjust your settings so as to allow friends of friends to find your name and perhaps even your profile picture. As, on its own, your name only provides limited information about you, we recommend you at the least make that available. It will be difficult for friends to find you otherwise.
>
> Some users may wish to use Facebook to meet new people who are not yet their friends. For these users, we provide the option of adding other details about themselves, such as their

[ix] Facebook Developers, "Understanding User Data and Privacy", ["Facebook, Understanding Privacy"] wiki.developers.facebook.com, last modified October 30, 2009, online at: <http://wiki.developers.facebook.com/index.php/Understanding_User_Data_and_Privacy>, my emphasis (last accessed January 20, 2010).

[x] Finding, *supra* note ii at para. 89.

[xi] Finding, *supra* note ii at para. 100; Resolution, *supra* note i.

> favourite movies, or pages they are 'fans' of, to their search listings. Others who find them but do not know them may wish to 'friend' them based on similar interests. You can even choose to make this information available on the internet and on search engines. However, Facebook warns that once information is released beyond your friends in this way, it may be used in contexts you have not foreseen, such as by potential or current employers.

Instead of a balanced and meaningful explanation of this nature, Facebook's Transition 'guide to privacy on Facebook' ("Privacy Guide" – see Figure 3, page 15) was at best uninformative and at worst misleading.[xii] Uninformative as it drastically understated the impact of selecting its 'everyone' recommended setting – a setting which permits it (and 'others') to import and export data attached to it "without privacy limitation" and at times effectively override express user choices *not* to share, particularly with respect to developer access to personal information [pages 13-22 and 51-68].

Additionally uninformative with respect to Facebook's public search opt-out. It failed to provide users with either insight into the expanded role this control would play post-Transition, or an opportunity to address this change within the Transition, preferably through opt-in consent [pages 16-18 and 24-25]. The public search opt-out now apparently controls profile association with indexed fan page and group comments (as public groups and fan pages are now all publicly indexed and available to 'Everyone') [pages 24-25 and 37-45].

The Privacy Guide is misleading in that its stated purpose for recommending users share a vast range of information including employment history, 'interested in' (sexual orientation) and all postings with **Everyone** is to "make it easier for **friends** to find, identify and learn about you."[xiii] CIPPIC cannot see how such information is demonstrably necessary in the circumstances for Facebook's stated purpose. All a *friend* needs to find and identify a user is that user's name and, perhaps, a profile picture. Once found, identified and approved through Facebook's friend request mechanism, a true friend can then proceed to 'learn more'. The rationale offered in support of Facebook's 'friends of friends' recommendation is equally baffling to CIPPIC [pages 22-23].

The Transition failed to meet standards set in the Finding with respect to meaningful consent and additionally with respect to the form of consent, which must be either express or – if it is to rely on pre-selected privacy settings – set defaults generally in line with what users reasonably expect. CIPPIC is not surprised that 65% of Facebook users reportedly did not customize their settings at all when presented with the Transition screens. Many users trust Facebook. They trust it to act generally in accordance with their reasonable expectations. They trust its recommendations. Many would not have taken the time to turn a critical eye to the Transition and adopted its recommended settings without hesitation. Where Facebook's recommendations ignore these expectations, there is no basis for informed consent under PIPEDA as articulated in the Finding.

ii. The Transition took away user control without any legitimate reason for doing so

Far from enhancing user control over personal information as required by the Finding, post-Transition Facebook has altogether taken away the ability of its users to control the availability of certain items of personal information – still, presumably, for the purpose of helping

[xii] See pages 12-13 below for a description of the 'Privacy Guide' Transition screen, as well as a screenshot at Figure 3, below.
[xiii] "Privacy Guide" Transition screen. See Figure 3 below.

to make it easier for friends to find, identify and learn more about you. Users can no longer control whether Facebook will disclose certain types of activities or to whom it will disclose other types [pages 45-49]. This change is problematic for its inclusion of sensitive information such as change in relationship status, geo-location or what applications a users uses and when, but equally due to the lack of any legitimate justification for it. Certainly users can decide for themselves whether to share such information with their 'friends' or 'everyone' or anyone at all, as the case may be. What legitimate purpose does Facebook have for imposing such sharing on everyone?

More egregious – much of its newly designated 'publicly available' information, for which Facebook claims to have 'no privacy settings', is extremely sensitive and indicative of, for example, a wide range of political expression, religious views, and personal preferences such as sexual orientation. By taking from its users the ability to hide this information, Facebook has severely limited their ability to control the context in which this information is used, exposing hundreds of millions to the whims of oppressive governments,[xiv] of current and even potential employers (a recent study notes that 70% of employers admit to rejecting candidates based on information found online),[xv] of spiteful peers or even teachers,[xvi] of identity thieves,[xvii] of child predators,[xviii] of commercial data miners,[xix] of banks seeking to assess financial credibility of customers,[xx] and of its own third party developers, to name but a few [pages 42-45 and 51-68]. Again, CIPPIC can see no legitimate reason for forcing users to share such data against their will. This is in direct contradiction to the spirit and the letter of the Finding, which was intended to provide more knowledge and control over user information. The 'publicly available' designation goes further then merely mis-setting defaults, as even the most conscientious and well-informed of users can no longer hide such data [pages 37-49].

iii. Facebook's post-Transition capacity to meet its third party developer obligations

CIPPIC is of the opinion that Transition changes have made it highly unlikely that Facebook will adequately meet its Resolution and Finding commitments to limit the exposure of its users to third party developers. In the Resolution, Facebook undertook to:

- "improve[ing] consent…around third party application developers' access to users' personal information";

[xiv] See EPIC, *supra* note iv.

[xv] Microsoft, "Research Shows Online Reputations Matter", Microsoft Data Privacy Day, online at: <http://www.microsoft.com/privacy/dpd/research.aspx>, (last accessed February 7, 2010). See also, I. Byrnside, "Six Clicks of Separation: The Legal Ramifications of Employers Using Social Networking Sites to Research Applicants", (2008) 10 Vand. J. Ent. L. & Prac. 445.

[xvi] M. Masnick, "Students Given Detention Just for Becoming 'Fans' of a Page Making Fun of Teacher", TechDirt, February 1, 2010, available online at: <http://techdirt.com/articles/20100126/0810057903.shtml>.

[xvii] B. Evangelista, "Too Much Info on Social Media Aids ID Thieves", SFGate, Monday 25, 2010, available online at: <http://www.sfgate.com/cgi-bin/article.cgi?f=/c/a/2010/01/25/BU581BMB2F.DTL> notes how identity thieves can piece together data such as birthplace or school name (recommended: Everyone for both) to gain access to bank accounts, etc.

[xviii] See in particular page 40, Figure 10 and accompanying text, below.

[xix] R. Singel, "Rogue Marketers Can Mine Your Info on Facebook", Wired, Epicenter, January 5, 2010, online at: < http://www.wired.com/epicenter/2010/01/facebook-email/>, (last accessed February 5, 2010).

[xx] M. Finney, "Banks Mining Social Media Sites for Personal Info", abc7 News, February 17, 2010, available online at: <http://abclocal.go.com/kgo/story?section=news%2F7_on_your_side&id=7283384>.

- "implementing significant changes to its site (namely, retrofitting its API) in order to give its users granular control over what personal information developers may access and for what purposes"; and
- adopting technical measures to ensure that third party developers will only be able to access information they are authorized to access [pages 68-74].[xxi]

It appears to be Facebook's intention to provide *any and all* 'publicly available' and 'Everyone' information to developers whose service is added by a user or even one of her friends and, moreso, to make such authorize such access. If this is the case, given the broad range of data now classified as 'publicly available' and defaulted to 'Everyone', Facebook's promised protections would be effectively meaningless if they did not also prevent developers from accessing such data, by any means, without express authorization.

Forcing developers to improve consent by clarifying to users what items of data they intend to collect is not helpful if such developers are given blanket authorization by Facebook to access all 'publicly available' and 'Everyone' information. These developers are likely to state just that: 'we may collect any 'publicly available' or 'Everyone' information' [pages 62-68]. Clarity of consent is further muddied by Facebook's inconsistent approach to what developers can and cannot legitimately consider as 'required' to operate their service [54-58]. Providing users with granular controls over what information will be provided to specific developers upon connecting to their services is equally meaningless if such controls do not override an 'Everyone' default or 'publicly available' designation [pages 52-58 and 70-72]. Additionally, it is not clear that Facebook intends to apply its granular controls so as to permit users to opt-out of secondary purposes (such as marketing) it permits developers to make of information otherwise legitimately collected for other primary purposes [pages 56-58]. Finally, technical safeguards that do not protect those informational categories are at best a marginal improvement. Under such circumstances, none of these improvements would bring Facebook closer to complying with PIPEDA nor remedy the issues that led the Assistant Privacy Commissioner to conclude in the Finding that "express opt-in consent should be sought in each case" involving disclosure of personal information to third party developers [pages 68-74].[xxii]

CIPPIC premises its belief that Facebook's intended limitations on developer access to user data will not extend to 'publicly available' and 'Everyone' data on a number of indications. First, Facebook clearly and unambiguously defines 'publicly available information' data items as "considered publicly available to everyone, including Facebook-enhanced applications, and therefore do not have privacy settings."[xxiii] 'Everyone' information is similarly defined as publicly available information that can be "imported and exported by [Facebook] and others without privacy limitations."[xxiv] In addition, in an informational screen on developers and privacy included among its new privacy settings, Facebook informs users that application and connect website developers "May access any information you have made visible to Everyone…as well as your

[xxi] Resolution, *supra* note i.
[xxii] Finding, *supra* note ii at para. 193.3.
[xxiii] Facebook, "Privacy Policy", Dec 9, 2009, (accessed on December 14, 2009).
[xxiv] *Ibid*.

publicly available information" [page 52].[xxv] While Facebook places general contractual limitations on developers to respect privacy settings, it is not clear how these interact with the 'limitless' releases it attaches to 'publicly available' and 'Everyone' information. From a practical perspective, it is not difficult for developers to gain access to user profile URLs. Post-Transition, this is all that is required to collect all 'publicly available' and 'Everyone' [pages 52-62]. It appears to CIPPIC that Facebook might intend to authorize developer access to such information 'without privacy limitation' [pages 51-68].

Second, and irrespective of intended authorization, CIPPIC has no confidence that Facebook's promised granular controls will be implemented with sufficient precision. In particular, our concern is that these will not apply to 'publicly available' and 'Everyone' data. In support of this notion:

- Facebook's new 'learn more about application privacy' page informs users that developers will be given access to all publicly available and 'Everyone' data, and need only request express user permission "to access any **additional** information it needs" [page 52];[xxvi] this is bolstered by Facebook's developer materials, which tell developers that while they must respect user privacy settings, public and 'everyone' data can be display unconditionally; [pages 70-72];[xxvii]
- Second, Facebook currently allows developers to access user profile URLs through a sessionless API call, meaning developers are authorized to request such data at any time (although there are storage limitations). Post-Transition, a developer armed with a user's URL can access her 'publicly available' and 'Everyone' data directly by visiting her profile page [pages 61 and 70-72];
- Third, Facebook currently ignores granular privacy limitations expressly placed through its new granular Publisher tool on posted items such as wall photos in favour of more general defaults such as that for the wall photo album (recommended: Everyone) [pages 70-72; and
- Finally, while Facebook will allow a user to signal their express intent to opt distinct items of data out of general developer access, it will ignore such input if the default setting for that distinct item is 'Everyone' [see Figure 18 at page 81, and pages 70-72].

In addition, in the Resolution, Facebook undertook to improve granular user control "over what personal information developers may access *and for what purposes*."[xxviii] CIPPIC has seen a number of indications suggesting that Facebook does *not* intend its promised granular control tool to apply to secondary purposes such as marketing or internal analytics [pages 53-58]. This, too is a failing to live up to its Resolution obligations, in CIPPIC's opinion.

[xxv] Facebook, Settings>Privacy Settings>Applications and Websites>Learn More ["Applications>Learn More"], (accessed January 2, 2010).
[xxvi] *Ibid*.
[xxvii] Facebook Developers, Understanding Privacy, *supra* note ix: "Users may choose to make some of this data public, which you can then use to display publicly as well"; and "You may not display any of this data outside the user's specified privacy settings which control exactly what other users can see a piece of information. This setting ranges from everyone, to all friends, or even just a selected group of friends. The APIs have ways to help you determine this – see the implementation details below. If you do not want to display information conditionally, you should only use information available to everyone."
[xxviii] Resolution, *supra* note i, my emphasis.

It seems that Facebook will authorize developers to access 'publicly available' and 'Everyone' data 'unconditionally' and 'without privacy limitation', that its promised granular control will not effect an 'Everyone' default setting nor will it permit users to opt out of secondary uses, and that its promised technical safeguards will be of marginal benefit at best as they will not protect broad categories of information now publicly available to Everyone. Under these circumstances, Facebook will be in compliance with neither its undertakings in the Resolution, nor the Finding.

Of additional concern to CIPPIC in this respect is Facebook's apparent willingness to facilitate developer access to 'publicly available' and 'Everyone' data of random users upon the merest pretence of 'interaction' with a developer's product. CIPPIC notes, for example, that application developers are apparently given access to Facebook user IDs and profile URLs of any visitor to their canvas pages, regardless of whether those users have authorized the application in question or not [pages 18-22 and 75-78]. As noted above, post-Transition, a profile URL is all a developer needs to gain access to all 'publicly available' and 'Everyone' user data. As stated in Facebook's privacy policy:

> To help those applications and [connect websites] operate, they receive publicly available information automatically when you visit them, and additional information when you formally authorize or connect your Facebook account with them.[xxix]

Of greatest concern to CIPPIC is the implication in this statement that Facebook apparently reserves itself the right, not currently exercised, to our knowledge, to disclose similar data to *external* connect website developers when random, otherwise anonymous users visit these. This threatens to turn what users believe to be anonymous browsing into rich data mining expeditions.

Finally, CIPPIC is also concerned at Facebook's apparent intention to begin extending developer like information access to Fan Page owners and, in addition, to provide external web pages with Fan Page functionality. In CIPPIC's view, the conditions placed on developers in the Finding apply at least as stringently to Fan Page owners.

iv. Requested Remedy

In light of all of this, CIPPIC regards Facebook in direct violation of the Finding, the Resolution, and PIPEDA. As the Transition itself formed part of an ongoing process to bring it *into* compliance with the Finding, and as Facebook was well aware of the requirements therein, CIPPIC finds the result indefensible. It finds public statements justifying the Transition through a shift in reasonable expectations away from 'friend' sharing and towards 'Everyone' sharing unconvincing and in direct contradiction of both the Privacy Commissioner's Finding of not six months ago as well as Facebook's own representations to the Commissioner [pages 6-8 and 27-31]. It is further belied by the continued prevalence of the 'Friend' concept in its very architecture and its materials, including its prominent motto, its privacy policy, and the following statement still present in its explanation of privacy to its connect developers:

> Facebook users create rich profiles with Facebook in order to share information with their friends. We offer rich privacy settings that allow people to feel secure sharing highly personal

[xxix] Privacy Policy, *supra* note xxiii.

> information including interests, thoughts, and contact information. Given this rich set of control, a significant number of Facebook users have filled out information no their profile.[xxx]

Social norms such as expectations of privacy do not change overnight. Nor is privacy as trivial as a social norm. It is based in the need to control one's environment, which includes one's personal information. Some users may choose to release their information out into the world, but when it is released without their informed knowledge and control – when it is taken from the context in which it was disclosed and used for other purposes – unforeseen harm often ensues, as well as a sense of invasion and violation. Further, that a large proportion of users have accepted Facebook's recommendations is not indicative of such a shift in norms, but rather of the trust these users had placed in Facebook.

CIPPIC asks that Facebook immediately and without delay revert its settings to their pre-Transition status quo. If, as it claims, its users wish to share more broadly, the incentive is there for Facebook to provide them with quick and easy .

Specifically, CIPPIC asks Facebook to take the following immediate and short-term remedial measures:

- Undue any user changes made to privacy settings as a result of the Transition before direct harm results [page 31];
- Revert new users from the post-Transition period to pre-Transition default settings [page 37];
- Eliminate the mandatory 'publicly available information' category you have created and seek opt-in user consent if you wish to make such information publicly available [page 44]; and
- Opt users out of public search as this now exposes far more information than it once did [page 31 – with respect to public search, see in addition pages 16-18, 24-25, and 37-45].

With respect to these changes, CIPPIC has asked Facebook to respond within 30 days to indicate its willingness or lack thereof to comply with our request so that we can assess what further action to take. CIPPIC notes that none of the changes it requests here would prevent users who want to share information more publicly from doing so by opting in to less private settings.

B. General non-Compliance with PIPEDA

Included in this statement of concern are other ways in which CIPPIC believes Facebook remains in violation of the Resolution, the Finding and PIPEDA. These violations are of less immediate urgency, in CIPPIC's view, but nonetheless important. These can be grouped into different categories of violations, some of which are violations of direct undertakings Facebook committed to in the Resolution, others involve situations where Facebook has failed to live up to either the spirit or the letter of the initial Finding. CIPPIC is concerned by the general trend of backwards progress these violations indicate, and hopes that Facebook will address them.

To begin with, Facebook has failed to meet specific and direct obligations it undertook in the Resolution, including:

[xxx] Facebook Developers, "Understanding User Data and Privacy", *supra* note ix.

- A failure to set all photo posting defaults (particularly wall photo albums and photo postings) to 'Friends of Friends' as opposed to 'Everyone' [page 32];
- A failure to put in place a promised privacy wizard or tour/tutorial intended to supplement its common sense defaults by explaining privacy to new users [page 32];
- A failure to provide users with control over currently limitless exposure of their friends' information to third party developers when adding developer services [page 81];
- A failure to embed an account deletion option within the account deactivation flow screens, so as to ensure users are aware their information will be stored indefinitely and that they have the alternative option of deletion[page 91]; and
- A failure to ensure users are adequately aware of their obligation to obtain non-user consent for collection and retention of non-user personal information such as Email address [page 96].

All of these changes should now be in place. Given Facebook's recent privacy overhaul, there is no excuse why they are not. Indeed, some of Facebook's Transition changes represent a step back from these obligations. One clear example of this is its decision to default photo wall postings and the Wall photo album to 'Everyone'.

Another example, already touched upon above, is Facebook's promised privacy wizard/tutorial/tour. Such a tool was intended to supplement Facebook's then common sense default settings. Post-Transition, these defaults no longer reflect the common sense reasonable expectations that the Finding required, making the need for the promised wizard or tutorial all the more pressing. In fact, in light of the Transition, CIPPIC is now of the belief that the issue of meaningful consent should be addressed through express opt-in consent upon sign up [pages 31-37; see particularly Figure 8 and Figure 9].

Another example relates to Facebook's commitment to provide a modicum of user control over when and under what circumstances information of that user's *friends* will be disclosed to an application developer. In justifying the amount of information it discloses to developers whose applications a user's *friend*, but not the user herself, has added, Facebook relied in the Resolution on the fact that "a user can now choose if they want to share their friends' data with a particular application".[xxxi] This appears to have been Facebook's attempt to form a basis of consent for such disclosures [pages 31-37]. However, if such a control exists, CIPPIC is unable to locate it. Worse, Facebook appears to have broadened exponentially what it will disclose to developers in cases where a user's friend but not the user herself has added an application or connect website – all publicly available and 'Everyone' data is now apparently available, regardless of user input [page 81].

In CIPPIC's view, this backwards progress on explicit commitments made by Facebook is troubling. Of additional concern is Facebook's disregard for the spirit of the Resolution and the Finding. In CIPPIC's view, the Resolution signalled not only Facebook's adherence to the specific, itemized obligations it contained, but to the legal requirements in the Finding as well and,

[xxxi] Resolution, *supra* note i.

more so, the principles embodied therein. Post-Transition Facebook remains in violation of a number of these, including:

- It has, in CIPPIC's view yet to adequately inform its users, particularly upon signup, that any information provided it will be used for commercial purposes [pages 1-6];
- It has yet to adequately and meaningfully notify users that adding a network will override existing privacy settings, as it agreed to do in the initial Finding [pages 9-11];
- Its post-Transition default settings for new users are in direct contradiction of those required by the Finding [pages 31-37];
- It allows general default and 'publicly available' privacy designations to override and conflict with user input to the contrary [pages 16-21, 38-42, 52-62 and 81];
- It still fails, in CIPPIC's view, to diligently ensure it has the implied consent of non-users for personal information of theirs that it collects and retains [pages 96-99];
- It continues to retain data of users and non-users alike for indefinite and hence unreasonable periods of time [pages 95-99];
- It appears as though Facebook may retain data expressly deleted by users, such as when a user deletes records of an action taken and even after a user deletes her entire account. Such retention must be both justified and better clarified to users [pages 90-91]; and
- CIPPIC is concerned by indications that it is potentially retaining far more data than it requires, such as internal pages visited by users [pages 90-91] and, more troubling, browsing habits on external websites visited by users while logged in [pages 74-90]

CIPPIC makes suggestions on how it believes these and other similar concerns should be addressed by Facebook in the document below. These are summarized in the following table. It is our hope that Facebook will give these due consideration.

Summary of Concerns

Potential Violation	Requested Fix
I. Transparency of Facebook's Advertising Agenda	
1. Facebook requires users to provide gender as a condition of service though it is not necessary for its purpose of encouraging authenticity, in violation of Principles 4.3.3 and 4.4.	Remove 'Gender' as a requirement for opening a new Facebook account;
2. Facebook requires phone number as a condition of some services for authentication purposes although this is not necessary as there are alternatives, in violation of Principles 4.3.3 and 4.4.	Facebook should provide alternative options for authentication;
3. Facebook requires provision of certain personal data but fails to provide time-of-collection, explicitly specified notification that this information is being collected in part for advertising purposes, in violation of Principles 4.2.3, 4.3, 4.3.2, 4.3.3.	▪ Expand the current time-of-notification popup to expressly mention advertising as a purpose for the collection of DOB and gender, as well as for phone numbers; ▪ Alternatively, let users know near the top of the privacy policy that DOB and Gender, once provided, shall be used for advertising purposes regardless of later user preferences.
4. Controls for opting out of social ads are no longer located in the privacy settings, where reasonable users would expect them, in violation of Principles 4.3.4, 4.3.5 and 4.3.6	Move Social Ad opt out controls back amongst the Privacy Settings;
II.A. Facebook ignores direct user input as to expectations when setting defaults	
1. In setting defaults for new controls, Facebook makes decisions based on assumed expectations of users that are difficult to uphold as reasonable in light of past similar user actions, in violation of Principles 4.2.4, 4.3, 4.3.2, 4.3.4, 4.3.5, and 4.3.6	▪ When introducing new privacy controls, Facebook must take greater steps to notify users of their existence; ▪ Facebook should force users to expressly consider new settings upon adding these; ▪ Alternatively, if setting defaults for new settings, Facebook should take into account previous user actions taken to restrict disclosure of similar personal information;
2. Facebook unreasonably assumes its users would expect it to disclose highly sensitive information when a user adds a network, ignoring past user controls on limiting information sharing and thus in violation of Principles 4.2.3, 4.3, 4.3.2, 4.3.4, 4.3.5, and 4.3.6.	▪ Force users to expressly consider what information they wish to share with newly added networks; ▪ Alternatively, take into account previous user limits placed on information sharing when formulating assumptions as to how a user expects information to be shared with networks; and ▪ Improve the current misleading notification to ensure meaningful consent is gained;
II.B. The Transition	
1. Facebook's Transition did not adequately explain to users the full impact of new terms such as 'Everyone' and it relied on misleading or deceptive explanations of the purposes for its	CIPPIC asks that Facebook immediately reverts its users to its pre-Transition privacy settings. An immense amount of personal information is currently available to 'Everyone' on Facebook and much is also available more

Potential Violation	Requested Fix
recommended changes. As such it failed to gain meaningful consent of its users for Transition changes, and is in violation of Principles 4.3, 4.3.2 and 4.3.5.	broadly. The risks associated with the continued status quo are, in CIPPIC's view, large and difficult to calculate. Facebook does not have meaningful, informed consent for any of its post-Transition disclosures. As these disclosures are currently with a much broader community than most Facebook users would reasonably expect, CIPPIC believes many of Facebook's users are not aware of their exposure and will not be until after any potential harm manifests. In addition, CIPPIC asks that Facebook immediately opts all of its users out of public search.
2. Facebook's Transition did not include opt-in consent to expanded public search capabilities and for the vast majority of users did not employ an adequate opt-in mechanism for its changes. As such it failed to gain express consent for its recommended changes, and is in violation of Principles 4.3.4, 4.3.5 and 4.3.6.	
3. Facebook's recommended opt-out changes were a violation of its users reasonable expectations as well as of Principles 4.3.4, 4.3.5 and 4.3.6.	
4. Facebook's transition in total failed to provide its users with the accurate information they required to make informed decisions and further failed to employ the proper method of consent. In CIPPIC's view, the Transition was not conducted in a manner that a reasonable person would find appropriate in the circumstances and is in violation of Section 5(3).	
5. Facebook's 'Everyone' privacy category is excessively broad and is not an adequate basis for meaningful consent as required by Principle 4.3.2;	Better define the 'Everyone' setting so as to take account for actual limitations placed on sharing such information;
II.C. Default Settings for New Users	
1. Facebook's current process for new users does not gain express user consent and subjects users to default settings far out of line with their reasonable expectations. It is therefore in violation of Principles 4.2.3, 4.3, 4.3.2, 4.3.4, 4.3.5, 4.3.6 as well as s. 5(3) of PIPEDA.	▪ Alter the signup and information input flow screens as suggested above in order to ensure users provide express opt-in consent to Facebook disclosures; ▪ Alternatively, change default settings to ones that users would reasonably expect – only friends for most settings and opt-in for public search;
III.A. Publicly Available Information	
1. Facebook's 'publicly available' designation is unclear and may leave many users with mistaken impressions as to how broadly their personal information will be disclosed by it. It is not gaining meaningful express consent, nor are its users able to acquire information about its policies and practices in this respect without unreasonable effort. It is thus in violation of Principles 4.3.2, 4.3.4, 4.3.5, 4.3.6 and 4.8.1.	▪ Eliminate the 'publicly available' designation and provide users with opt-in control over when and under what circumstances Facebook will disclose their data; ▪ Alternatively, eliminate the 'publicly available' category, default such information to 'only friends', and provide users with opt-in control over when and under what circumstances Facebook will disclose such data to non-friends such as third party developers;
2. Facebook has taken away most user control over how information it deems 'publicly available' will be disclosed and as such requires user consent to such disclosure as a condition of service with no legitimate purpose for doing so. It also fails to gain	

Potential Violation	Requested Fix
opt-in consent and discloses information it designates as publicly available in ways users would not reasonably expect. As such it is in violation of Principle 4.3.3, 4.3.4, 4.3.5 and 4.3.6.	
III.B. Facebook combines broad categories of data forcing users to share all or none	
1. Facebook groups together broad categories of information, forcing users to consent to sharing item x if they are to share item y in violation of Principles 4.3.4, 4.3.4 and 4.3.5.	Provide a mechanism for finer adjustments to global categorical privacy settings;
III.C. Facebook no longer provides user control over activity disclosure	
1. Facebook forces users to consent to disclosing Facebook activity to all those able to see their 'Wall' as a condition of carrying out that activity, and is therefore not acquiring the proper form of consent required under the circumstances by Principles 4.3.4, 4.3.5 and 4.3.6.	Return user control over what activity will and will not be displayed on the Wall;
2. Facebook is requiring those users who wish to share application-generated actions with some of their friends to also share it with everyone who has access to their wall and this is therefore not a reasonable and appropriate form of consent as required by Principle 4.3.4, 4.3.5 and 4.3.6.	Provide users with more granular controls over who Facebook will disclose application generated actions, especially with respect to locational data;
3. Facebook no longer allows users to hide their 'add me as a friend' button from everyone, and thus uses an improper form of consent with respect to resulting disclosures of information, in violation of Principles 4.3.3 and 4.3.4.	Add an 'Only me' option to the existing 'add me as a friend' privacy setting;
4. Facebook's new Applications Dashboard informs friends what applications and games a user is interacting with and when she has last done so as a condition of service and is thus an improper form of consent in violation of Principles 4.3.3, 4.3.4, 4.3.5 and 4.3.6.	Provide users with an opportunity to opt-out of being displayed in the Applications/Games Dashboard, either globally or on a per-Applications basis.
IV.A. Privacy, one piece at a time - does it work?	
1. Facebook is not meaningfully notifying users what information it will disclose to developers upon connecting in violation of Principles 4.2, 4.2.3, 4.3, 4.3.1 and 4.3.2.	Facebook should require developers to list what items of data they intend to collect from it directly at time of collection – as part of the connect or add application flow screens;
2. Facebook now provides a great deal of information publicly, to 'Everyone', through its user profiles but does not make it clear that restrictions placed on information provided to developers through its API apply equally to the collection, use, disclosure and retention of data harvested directly from user profiles; without such	Clarify that all data protection restrictions limiting developer collection, use, disclosure and retention of user data apply equally to data acquired through direct harvesting from sources such as user profile URL;

Potential Violation	Requested Fix
clarification, developers appear authorized to access all 'publicly available' and 'Everyone' data 'without privacy limitation'; such authorization is extremely broad and in violation of Principles 4.2 and 4.3.4.	
3. Facebook will disclose user information to developers who 'require it to operate their service' but does not adequately prevent excessively broad definitions of 'need', resulting in refusal to deal requests for unnecessary information, which violate Principles 4.3.2, 4.3.3 and 4.3.4.	▪ Facebook should better define in its terms of use what user information its developers are able to require as a condition of service; ▪ Specifically, Facebook should clarify that 'advertising' and 'internal analytics' are not 'necessary' to operate a service; ▪ Alternatively, if Facebook wishes to permit developers to collect 'unnecessary' user data, it must require them to gain express consent before doing so, such as through its Independent data policies;
4. Facebook currently contractually limits developers from *collecting* user information they do not require, but fails to limit them from *using* otherwise collected information for purposes not strictly necessary to the operation of their service, in violation of Principles 4.3.2, 4.3.3, 4.3.4, 4.3.5, 4.3.6, 4.5 and 4.5.1.	▪ Facebook should clarify its SRR so as to ensure developers are limited to *using* information they collect only for the purposes for which it is collected; ▪ Alternatively, Facebook should ensure developers gain opt-out or opt-in consent for secondary uses, using Facebook's promised granular control tool;
5. It is not clear the extent to which Facebook authorizes connect website developers to disclose personal information of users in new contexts on their external websites and to public search engines, potentially in violation of Principles 4.3, 4.3.3, 4.3.4, 4.3.5, 4.3.6, 4.5 and 4.5.1	Facebook should clarify that connect website developers cannot disclose information gained from it on their websites and to public search without express user consent to such disclosures;
IV.B. Can Facebook still meet its Resolution obligations?	
1. Facebook's new notification requirements do not appear to meet its obligation, undertaken in the Resolution, to improve clarity of consent gained by developers for information it discloses to them;	Require developers to inform users, at time of collection (during the connect or add application flow screens), each category of data (including 'publicly available' data) they intend to collect directly from Facebook and why;
2. It is no longer clear that Facebook intends its promised granular control tool to apply to *all* user data disclosed, including 'publicly available' and 'Everyone' data, as required by the Resolution;	Clarify that the granular control tool will allow users to opt-out/in of each item of data disclosed to a developer that is not required for the service that developer is offering;
3. It is no longer clear that Facebook intends its promised granular control tool to apply to *purposes* for which the information is collected, as stated in the Resolution;	Clarify that the granular control tool will permit users to opt-out/in of any secondary uses a developer intends to make of collected data;
4. It is not clear that the technical safeguards Facebook intends to provide to meet its Resolution obligations reflect a proper understanding of what developers can and cannot legitimately access;	Ensure that the promised technical safeguards apply to *all* personal information, including publicly available and 'Everyone' data and user activity data, as well as means of accessing such data;

Potential Violation	Requested Fix
IV.C. What developers get before you interact with them	
1. Facebook's Privacy Policy reserves it the right to provide external websites with "publicly available information automatically when you visit them"; while it does not appear to do so at this time, any such disclosures would violate section 5(3) of PIPEDA;	Facebook should clarify in its Privacy Policy that it does not, will not and can not identify otherwise anonymous users to external websites "when you visit them";
2. Facebook appears to authorize and facilitate developer collection of some user data for users when neither they, nor even their friends have interacted with the developer's services in any way, in violation of Principles 4.3, 4.3.3, and 4.3.4 of PIPEDA;	▪ Facebook should prevent developers from accessing user data unless a user has specifically interacted with their services, and then only with express user consent; ▪ Alternatively, if Facebook is to rely on global controls for consent, these must be opt-in, and must apply to *all* user data;
3. Facebook appears to disclose user data to applications and external website developers upon the mere visitation of such sites by a user, without any authorization or substantial interaction with those services and without opt-out or express user consent, in violation of Principles 4.3, 4.3.3, and 4.3.4 of PIPEDA;	▪ Facebook should not provide developers with user information simply because a user has viewed their website or canvas screen; ▪ Facebook should ensure its otherwise anonymous users cannot be identified by developers upon visiting their external websites or canvas screens;
4. Facebook fails to get user consent before disclosing personal information to developers when a friend of that user adds an application or connects to a website, in violation of Principle 4.3 and section 5(3) of PIPEDA;	Facebook should gain opt-in express user consent before disclosing *any* information to applications a user's *friends* have interacted with, but with which a user has not.
IV.D. Facebook and the open web	
1. Facebook's Privacy Policy does not clearly articulate what information it provides owners of Fan Pages; specifically, such owners now have access, at the least, to all 'publicly available' and 'Everyone' information; Principle 4.3.2 requires clearer articulation of what users provide such individuals;	Clarify what information Fan Page owners have access to in the Privacy Policy and 'Help' FAQs;
2. Facebook's new logout button is no longer readily accessible, and this is problematic as users are more likely to close their Facebook tab/browser without logging out, potentially exposing their accounts to other passers by; this constitutes a violation of Principle 4.7	Return the logout button to a prominent location on Facebook pages;
3. Facebook now has access to significant browsing activity of its users but does not clarify whether such activity is collected, stored or used, and if so, how and for what purposes; collection, retention and use of such data without opt-in user consent would constitute a violation of Principles 4.3 and 4.3.6 of PIPEDA; Principle 4.8 further requires Facebook to explicitly specify in its	▪ Facebook should clarify its policies around collection, retention and use of external browsing activity; ▪ If Facebook wishes to retain or use such data, it must gain informed, meaningful opt-in consent;

Potential Violation	Requested Fix
Privacy Policy what its data practices are with respect to such information;	
V.A. Retention of user data manually deleted from active accounts	
1. If Facebook is retaining personal information that users have manually removed from its site, it must notify them gain their informed consent for doing so, as required by Principles 4.8 and 4.3.	If Facebook retains manually deleted information, it should notify its users precisely what will be retained, under what conditions and for how long; If it is retaining such information for a legitimate purpose, it should gain its users informed consent for doing so.
2. If Facebook is retaining personal information that users have manually removed from the site, this is a violation of Principle 4.5 as the initial purpose for which it was provided is no longer applicable.	If Facebook is retaining personal information manually deleted by its users, it should cease doing so within a reasonable period of time.
V.B. Deletion and deactivation	
1. Facebook relies on the deletion option as a mechanism for facilitating user withdrawal of consent, but this option remains obscured, placing Facebook in violation of Principle 4.3.8 as well as its undertakings in the Resolution.	▪ The deletion option should be displayed beside the deactivation option on the account settings page; ▪ An explanation of and a link to the deletion option should be included in the deactivation flow screens, as Facebook undertook to do in the Resolution.
2. Facebook is employing an improper form of consent by requiring users to opt-out of ongoing Facebook activity such as communications while deactivated, in violation of both their reasonable expectations and Principles 4.3.4, 4.3.6 and especially 4.3.5.	Gain opt-in consent for any specific uses of personal information from deactivated accounts Facebook wishes to make.
3. Facebook indefinitely retains user data from deactivated accounts and continues to make such information available to others long after it can be reasonably implied that the initial purposes for its provision remain, in violation of Principles 4.5 and 4.5.3.	▪ Facebook must set a reasonable retention period for deactivated account information; ▪ Facebook should notify users upon deactivation that their data will only be retained for x period of time.
4. Facebook retains personal information of users who have deleted their accounts for the stated purpose of 'preventing identity theft', but fails to explain what information it will keep, why it is required for preventing identity theft, and why it should be retained indefinitely, in violation of Principles 4.3.2, 4.5, 4.5.3 and 4.8. Facebook additionally requires users to consent to such retention as a condition of service, in violation of Principle 4.3.3.	▪ Facebook should explain to users what information it retains after an account is deleted, why it feels this is necessary to prevent identity theft, and why it feels it should be retained for an explicitly stated period of time; ▪ Facebook should provide users with the opportunity to refuse retention of their deleted information for the purpose of protecting them from identity theft.
V.C. Retaining Personal Information of Non-users	
1. Facebook does not adequately advise users they must gain non-user consent before permitting it to retain non-user Emails indefinitely, and as such cannot imply non-user consent to such retention	▪ Facebook must explain in its SRR precisely what consent users must gain from non-users before providing it with their Emails; ▪ Facebook must add a similar notification to its Privacy

Potential Violation	Requested Fix
and use and violates Principle 4.3.	Policy explanations of the friend finding process, as well as to the friend finding flow screens;
2. Facebook retains non-user Emails provided by users, as well as a 'friend' association between sending users and recipient non-users, indefinitely, but does not exercise due diligence before implying consent of non-users of such activities, despite having direct access to them, as required by Principle 4.3 and section 5(3) of PIPEDA.	▪ Emails sent at the behest of users must inform non-user recipients, prominently, that such Emails shall be retained by Facebook and associated with the sending user unless the non-user informs it otherwise; ▪ Preferably, neither Emails of non-users, nor accompanying associations to sending users, should be retained at all unless the non-user recipient provides express opt-in consent to such retention;
3. Regardless of how expressly and directly non-users are initially informed that their Email shall be retained by it, Facebook's indefinite retention policy for such data becomes unreasonable after a certain period of time and can no longer be justified under Principles 4.5 and 4.5.3 of PIPEDA.	Facebook should develop a reasonable period of time after which Emails of non-users as well as the association of those Emails to sending users will no longer, barring additional input, be retained and clearly notify non-users and users alike of that period;
4. Facebook implies non-user consent to collection, use and retention of Email address and its association to existing users in situations where it is unreasonable to do so, in violation of Principle 4.3, 4.5 and 4.5.3.	▪ Facebook should not retain Email addresses of non-users or their association with sending users in circumstances where it is clear either or both does *not* intend such connections to manifest; ▪ Specifically, it should not retain non-user Emails or associate them with users who have imported contact lists, but expressly decided *not* to send invitations to particular individuals; ▪ Additionally, it should not retain non-user Emails or associate them with sending users where these Emails have been ignored by recipient non-users, particularly where they have been repeatedly ignored.

Introduction

Our concerns track in organization categories in the Assistant Privacy Commissioner's, initial *Report of Findings* (the "Finding")[1] and are laid out as follows. First, CIPPIC addresses the transparency of Facebook's commercial agenda. It is a commercial entity and for this reason, all of its activities are captured by PIPEDA. In fact, given the primary and central role advertising plays in Facebook's business model, its obligations to expressly disclose this as an animating purpose behind its activities are high, and in CIPPIC's view it is not doing a sufficient job of addressing these.

Second, CIPPIC points to a number of ways in which Facebook is fails to make reasonable inferences with respect to the expectations of its users. Of central concern is its handling of recent privacy adjustments to its site (the "Transition"), where Facebook changed user settings in ways they would not reasonably expect. As it did not gain their express consent for these changes, and, additionally, as it failed to meaningfully notify them of the changes it was asking them to make, it has no basis for consent to these changes.

Third, in the Transition, Facebook eliminated user control over personal information in a number of ways. Most troubling among these are its new mandated publicly available information category and its removal of user control over which of their Facebook and Facebook-enhanced actions will be disclosed by Facebook and to whom. CIPPIC sees no justification for forcing users to share information in this manner and against their will.

Fourth, CIPPIC reassess Facebook's obligations with respect to placing limitations on third party developer access to personal information of its users in light of recent Transition changes. It finds cause to believe Facebook will not adequately meet these obligations. It also addresses how these obligations should apply to services such as Facebook connect and Facebook's new Open Graph API.

Finally, CIPPIC addresses shortcomings it sees in Facebook's retention policies. It is particularly concerned that Facebook does not present users with clear deletion options for their accounts, is retaining too much information for longer than can be reasonably justified, and is not taking adequate steps before implying non-users consent to at times indefinite retention their personal information.

I. Transparency of Facebook's Advertising Agenda

Facebook's core operations are dual, encompassing not only its often touted mission to "help[] you connect and share with the people in your life",[2] but also its "prominent and essential" advertising agenda.[3] Essential because monetizing the personal information of its users is Facebook's primary source of revenue, and this fact impacts on PIPEDA's application to Facebook.[4]

---

[1] PIPEDA Case Summary #2009-008, *Report of Findings into the Complaint Filed by the Canadian Internet Policy and Public Interest Clinic (CIPPIC) against Facebook Inc.*, [Finding] July 15, 2009, available online at: <http://www.priv.gc.ca/media/nr-c/2009/let_090827_e.cfm>.

[2] Facebook Homepage, www.Facebook.com, (accessed January 20, 2010).

[3] Finding, *supra* note 1 at para. 139.

[4] Finding, *supra* note 1 at para. 131.

Under PIPEDA, marketing is typically viewed as a 'secondary purpose', meaning not necessary to the service for which the individual provided the information. Under Principle 4.3.3, it is not legitimate for organizations to force customers to consent to secondary purposes as a condition of service.[5] Indeed, Jon Leibowitz, Chairman of the U.S. Federal Trade Commission, recently noted in an interview discussing social networks such as Facebook that he sees privacy requirements in the U.S. potentially "head[ing] towards opt-in", a more restrictive standard, in the near future.[6]

In Facebook's case, monetizing the personal information of its users is its primary source of revenue. Under such circumstances, it is reasonable to treat marketing purposes as a 'primary' purpose.[7] Given the central role marketing plays in Facebook's business model, the Assistant Privacy Commissioner has determined that it need not obtain opt out consent for some of its less intrusive marketing activities.[8] However, there are other implications that arise from operating a business model wherein monetization of personal information plays such a central role. For one thing, it means that most if not all of Facebook's activities can be characterized as "of a commercial character" and are therefore capture by PIPEDA.[9] In CIPPIC's view, if marketing is to be treated as a primary purpose for Facebook, it must also be 'explicitly specified' in proportion to its primacy. This entails that Facebook inform users early and often that their personal information will be used and is being collected, in part, for advertising purposes. CIPPIC finds support for this conclusion in the Finding, which relies in part on the 'explicitly specified' component of Principle 4.3.3 to impose such obligations on Facebook.[10] This is how the 'appropriate balance' can be struck between Facebook's legitimate business model and the privacy rights of those whose personal information that business model relies upon.

The Finding notes Facebook's commitment to address this issue by ensuring "full disclosure as to the collection and use of information for advertising purposes."[11] In this respect, Facebook has added the following paragraph in a bullet point near the top of its privacy policy:

> Facebook is a free service supported primarily by advertising. We will not share your information with advertisers without your consent. We allow advertisers to select characteristics of users they want to show their advertisements to and we use the information we have collected to serve those advertisements.[12]

---

[5] Finding, *supra* note 1 at para. 130. Also, see PIPEDA Case Summary #2005-308, available online at: <http://www.priv.gc.ca/cf-dc/2005/308_20050407_e.cfm>; PIPEDA Case Summary #2002-83, available online at: <http://www.priv.gc.ca/cf-dc/2002/cf-dc_021016_1_e.cfm>; and PIPEDA Case Summary #2003-238, available online at: <http://www.priv.gc.ca/cf-dc/2003/cf-dc_031204_01_e.cfm>.

[6] S. Clifford, "F.T.C.: Has Internet Gone Beyond Privacy Policies?", New York Times, January 11, 2010, available online at: <http://mediadecoder.blogs.nytimes.com/2010/01/11/ftc-has-internet-gone-beyond-privacy-policies/>.

[7] Finding, *supra* note 1 at para. 131.

[8] Finding, *supra* note 1 at para. 134.

[9] Finding, *supra* note 1 at para. 12.

[10] Finding, *supra* note 1; See paras. 51 and 56.4, especially, as well as paras. 135 and 140.2.ii. In both cases, the Assistant Privacy Commissioner relied in part on the 'explicitly specified' component of Principle 4.3.3 to recommend Facebook take great steps in ensuring users are well aware of its advertising purposes.

[11] Finding, *supra* note 1 at para. 141.

[12] Facebook, "Privacy Policy", Dec 9, 2009, (accessed on December 14, 2009)

CIPPIC commends Facebook for this addition, as well as for the greatly increased clarity of its privacy policy. However, CIPPIC believes there are a few outstanding points Facebook must address if it is to be in compliance with PIPEDA.

A. Facebook does not adequately inform users of its advertising purposes when requiring information as a condition of service

Facebook collects Date of Birth ("DOB") and Gender as a condition of service at time of signup. Users are not permitted to open a Facebook account without providing these pieces of information, yet Facebook fails to 'expressly specify' to users at time of collection that such data is collected in part for marketing purposes. It additionally collects mobile phone numbers as a condition of service for account authentication.

With respect to DOB, the time-of-collection notification Facebook currently provides to users to explain its mandatory collection is incomplete and therefore misleading:

> Facebook requires all users to provide their real date of birth to encourage authenticity and provide only age-appropriate access to content. You will be able to hide this information from your profile if you wish, and its use is governed by the Facebook Privacy Policy.[13]

While CIPPIC agrees that it may be legitimate and necessary to require DOB for the purposes of preventing under-aged children from joining Facebook and encouraging authenticity, CIPPIC does not find the inclusion of the reference to Facebook's privacy policy as sufficient time-of-collection notification to users that their DOBs are being collected for advertising purposes as well. As recently noted by David Valdeck, Chief of the U.S. Federal Trade Commission's Bureau of Consumer Protection, "'[t]he literature is clear' that few people read privacy policies," and relying such policies to gain meaningful consent is a "fiction".[14]

Once provided, users must allow Facebook to use DOB for marketing purposes. In addition, as advertising permeates all of Facebook's activities, it is not merely a 'use', but also an animating purpose behind its collection of DOB. Time-of-collection notification that DOB is being collected not just to encourage authenticity and monitor user age but also for marketing purposes is required in such circumstances.[15] Without such notification, its current time-of-collection notification is at best incomplete.

As currently structured, Facebook's DOB notification may leave many users with the misleading impression that such data is not being collected for marketing purposes and that they will have the option later to "hide this information." The notification gives the impression of providing a complete picture of the purposes for collection and merely refers to 'use' as governed by the privacy policy. It also expressly states users will be able to hide DOB. While the privacy policy

---

[13] Finding, *supra* note 1 at para. 57.

[14] S. Clifford, "F.T.C.: Has Internet Gone Beyond Privacy Policies?", New York Times, January 11, 2010, available online at: <http://mediadecoder.blogs.nytimes.com/2010/01/11/ftc-has-internet-gone-beyond-privacy-policies/>.

[15] Finding, *supra* note 1 at para. 53. The Finding states at para. 52 that:

> having adopted what it has itself described as the "best practice" of time-of-collection notification regarding DOBs, Facebook should endeavour to make the very best of the practice by notifying users, at the time of registration, of all purposes for which it intends to use their DOBs.

See also para. 56.4: "indicate, in the pop-up in which it specifies the purposes for collection of DOBs, that DOBs are collected also for the purpose of targeted advertising."

now notes that users cannot hide 'DOB' from Facebook's internal advertising platform, even upon changing their privacy settings, this notification is only revealed several pages into the document.[16] As a result, neither the full purposes for DOB collection nor the inability to opt out thereof are 'expressly stated' as required by Principle 4.3.3. In addition, through this lack of meaningful time-of-collection notice Facebook remains in violation of Principles 4.2.3, 4.3, and 4.3.2, as held in the Finding.[17] In CIPPIC's view, this notification must be incorporated into the existing popup. If, in the alternative, Facebook is to continue to rely on its privacy policy, it cannot inform users that it will ignore they will not be able to opt out of advertising targeting DOB so far into its document.

In addition, users attempting to manually select a user name through their account settings page are now informed that:

> **Before you can set your username, you need to verify your account.**
> If you have a mobile phone that can receive SMS message, you can verify via mobile phone. If not, please try to register your username at a later time.[18]

Users are then prompted to provide Facebook with a phone number to which a confirmation number is sent by SMS. They are informed that "Facebook uses security tests to ensure that the people on the site are real. Having a mobile phone helps use establish your identity."[19] Users are not provided with any alternative method of authenticating their account. Facebook does not make clear what, if any, additional purposes animate this mandatory collection or its retention policy with respect to phone numbers. If Facebook indeed only collects phone numbers for authentication, this should be a one-time process and the numbers should not be retained once the account has been authenticated. Further retention would violate Principle 4.5. If Facebook *does* have additional purposes for collecting and using such data, it should be explicitly stated at time of collection as required by Principles 4.3.3 and 4.2.3, 4.3 and 4.3.2. CIPPIC does not view mandatory collection of phone number as a legitimate reason for authentication at all. There are far less invasive industry standards for doing so, such as the Email verification system Facebook already utilizes, as well as the above mentioned required DOB and gender. Facebook should not require such data as a condition of service, as there are equally viable alternatives to authentication.

With respect to the mandatory collection of gender, Facebook provides even less explanation for why it requires this data as a condition of service. There is no popup explanation at all, as there is for DOB. Even the privacy policy fails to expressly notify users that, once provided, gender will be used for marketing purposes regardless of user settings,[20] as required by the Finding with respect to other types of mandatorily collected information such as DOB.[21] Further, with respect to gender, CIPPIC is not convinced that 'encouraging authenticity' or marketing are sufficiently

---

[16] Privacy Policy, *supra* note 12.
[17] Finding, *supra* note 1 at para. 56.4.
[18] Account Settings>Settings>Username>change, (last accessed February 14, 2010).
[19] *Ibid*., 'Continue'.
[20] There is notice relating to 'publicly available' information (including gender) which states that such information "do[es] not have privacy settings." (Privacy Policy, *supra* note 12). However, Facebook *does* provide users with the opportunity to hide gender by editing their info tab and opting out of the 'show my sex in my profile' box.
[21] Finding, *supra* note 1 at para. 54.

legitimate reasons to force users to collect this type of data. With respect to authentication, Facebook already collects three pieces of authentic data: Email address, real name and DOB. This should be sufficient for identification purposes, in CIPPIC's view, and as such requiring gender as a condition of service violates Principles 4.3.3 and 4.4.[22]

B. Use of personal information in advertisements

A second concern relates to Facebook's opt out settings for more invasive forms of advertisement. As required by the Finding, advertising that uses personal information to endorse products is more invasive and, in the context of Facebook, requires opt out consent.[23] To its credit, Facebook has provided such opt out controls for advertisements of this type.

However, in the recent transition, these opt out controls have been relocated from their previous home amongst other privacy settings to a tab in the account settings interface. In addition, the privacy policy currently states that users can opt out of such ads through the help page. A hyperlink is provided, but merely leads to the main privacy settings page.[24]

Mistaken hyperlink aside, this setting is now found in a counterintuitive and obscure location. As these controls relate to uses Facebook may make of a customer's personal information, they should be located in the privacy settings where users will find them. A reasonable user hoping to adjust how their information is shared would turn to the privacy controls and, having canvassed these, be left with the impression that their work is complete. This fairly reasonable expectation would be fortified in the case of previous users by the fact that the social ad opt outs were in fact previously located in the privacy settings.

In placing these controls under the account settings tab and not in the privacy settings, Facebook is in violation of Princples 4.3.4, 4.3.5 and 4.3.6, which hold that in deciding the method by which consent is obtained, consideration will be given to the general circumstances of the collection, the reasonable expectations of users, as well as the sensitivity of the information. Under the circumstances, this requires locating the opt out controls in the privacy settings.

Potential Violation	**Requested Fix**
Facebook requires users to provide gender as a condition of service though it is not necessary for its purpose of encouraging authenticity, in violation of Principles 4.3.3 and 4.4.	Remove 'Gender' as a requirement for opening a new Facebook account;
Facebook requires phone number as a condition of some services for authentication purposes although this is not necessary as there are alternatives, in violation of Principles 4.3.3 and 4.4.	Facebook should provide alternative options for authentication;
Facebook requires provision of certain personal	▪ Expand the current time-of-notification popup to

[22] On this point, see PIPEDA Case Summary #2005-288, available online at: <http://www.priv.gc.ca/cf-dc/2005/288_050201_e.cfm>, PIPEDA Case Summary #2002-45, available online at: <http://www.priv.gc.ca/cf-dc/2002/cf-dc_020411_e.cfm>; and PIPEDA Case Summary #2002-46, available online at: <http://www.priv.gc.ca/cf-dc/2002/cf-dc_020426_e.cfm>.

[23] Fiding, *supra* note 1 at para. 133.

[24] Privacy Policy, *supra* note 12. The URL currently provided through the 'help page' hyperlink in the privacy policy is: <http://www.facebook.com/privacy/?view=feeds&tab=ads> (accessed January 12, 2010).

data but fails to provide time-of-collection, explicitly specified notification that this information is being collected in part for advertising purposes, in violation of Principles 4.2.3, 4.3, 4.3.2, 4.3.3.	expressly mention advertising as a purpose for the collection of DOB and gender, as well as for phone numbers; ▪ Alternatively, let users know near the top of the privacy policy that DOB and Gender, once provided, shall be used for advertising purposes regardless of later user preferences.
Controls for opting out of social ads are no longer located in the privacy settings, where reasonable users would expect them, in violation of Principles 4.3.4, 4.3.5 and 4.3.6	Move Social Ad opt out controls back amongst the Privacy Settings;

II. Facebook is Violating the Reasonable Expectations of Users

People join Facebook and provide it with information for the purpose of sharing it. Because of this, it is reasonable for Facebook to make assumptions on behalf of its users in deciding how to make that information available to others.[25] But such assumptions must reflect the reasonable expectations of those users if they are to comply with PIPEDA consent requirements. Following Facebook's recent transition, CIPPIC is concerned that it is no longer in touch with the reasonable expectations of its users. This is not surprising, as privacy is at its core a subjective right.

On December 9, 2009, Facebook put its users through a process ("Transition") intended to introduce them to some changes to Facebook's privacy settings, purportedly intended to give users "more control of [their] information and help [them] stay connected."[26] This Transition implemented Facebook's commitment, made in the Resolution, to put in place a new privacy tool intended to give users more granular control over posts they make. This tool, in CIPPIC's opinion, is an important and effective step that will give users a greater degree of control. However, Facebook appears to have also used the transition as a platform to move its customers away from a friend/community centered model and towards one where 'Everyone' is now your 'Friend', privy to the intimate details of your profile.

There has been much speculation regarding the purpose for this push towards expanded sharing. Some have seen it as an integral component in an attempt by Facebook to increase its market share by capturing a greater portion of the growing 'real-time search' market from competitors such as Twitter.[27] Facebook has noted in public statements that that the changes were calculated to reflect changing social norms which, apparently, have evolved beyond privacy.[28] CIPPIC takes no position as to what the true animating factor behind this transition may have been, except to note that Facebook remains primarily a profit-making enterprise and all of its activities including the transition can be viewed as "of a commercial character" within the meaning of PIPEDA, and so

[25] Finding, *supra* note 1 at paras. 88-89.

[26] "Privacy Announcement" popup screen. See Figure 1, below.

[27] J. Kincaid., "Facebook to Roll Out New Privacy Controls to its 350 Million Users, Kills Regional Networks", TechCrunch, December 1, 2009, online at: <http://www.techcrunch.com/2009/12/01/facebook-privacy-controls/>; R. Tate, "Facebook's Great Betrayal", Valleywag, December 14, 2009, online at: <http://gawker.com/5426176/facebooks-great-betrayal>.

[28] M. Kirkpatrick, "Why Facebook Changes Its Privacy Strategy", ["Kirkpatrick, Why Facebook Changed"] ReadWriteWeb, December 10, 2009, online at: <http://www.readwriteweb.com/archives/why_facebook_changed_privacy_policies.php> and E. Barnett, "Technology and Digital Media Correspondent", *Telegraph.co.uk*, January 11, 2010, available online at: <http://www.telegraph.co.uk/technology/facebook/6966628/Facebooks-Mark-Zuckerberg-says-privacy-is-no-longer-a-social-norm.html>.

that Act applies. In addition CIPPIC notes that social norms typically change quite gradually over time, and it is not evident to us that society has indeed evolved to the point where privacy is no longer a norm.

CIPPIC is particularly skeptical that the changes made by Facebook in the Transition are in line with the expectations of its users. According to Mr. Zuckerberg, privacy controls were integral to Facebook – the "vector around which Facebook operates" – as recently as two years ago.[29] This was repeated more forcefully more recently by Facebook in its representations to the Privacy Commissioner defending its pre-Transition defaults, as recorded in the Finding.[30] To this date, Facebook's own materials, targeting connect website developers, state:

> Facebook users create rich profiles with Facebook in order to share information with their friends. We offer rich privacy settings that allow people to feel secure sharing highly personal information including interests, thoughts, and contact information. Given this rich set of control, a significant number of Facebook users have filled out information no their profile. […]
>
> Once a user connects to your site or application, you are able to access and use information that the user has shared on their profile to provide a richer experience. In addition, you can access information about the user's friends and others on behalf of the user of your app – basically any information that is available to that user on Facebook can be used through the lens of your site or application. […]
>
> Beyond just providing a better user experience to target content and experiences to users, some of the information made available via Facebook APIs may help you better target advertisements to users. You may use this information locally within your systems to help better target advertisements, but you may not transfer this information to any 3rd party ad networks whatsoever.[31]

As this and Mr. Zuckerberg's statements of a year ago explain, the large community of users who have invested a great deal of their "highly personal" information into Facebook have done so largely because Facebook provided them with a secure environment to, as the prominent motto on its homepage still proclaims "connect and share with the people in [their lives]".[32] share [this] information with their friends." Post-transition, however, Facebook is more reflective of an environment where much of this highly sensitive information is now available to "Everyone".

Many of the changes made in the Transition reflect this view, expressed by Mr. Zuckerberg, that Facebook customers no longer have the same high expectations of privacy they once had on the site. However, in its Finding, the Assistant Privacy Commissioner found quite differently, holding that:

---

[29] M. Kirkpatrick, "Mark Zuckerberg on Data Portability: An Interview", [Kirkpatrick, Data Portability] *ReadWriteWeb*, March 10, 2008, available online at: <http://www.readwriteweb.com/archives/mark_zuckerberg_on_data_portab.php> (accessed January 12, 2010).

[30] Finding, *supra* note 1 at paras. 80-81.

[31] Facebook Developers, "Understanding User Data and Privacy", ["Facebook Developers, Understanding Privacy"] wiki.developers.facebook.com, last modified October 30, 2009, online at: <http://wiki.developers.facebook.com/index.php/Understanding_User_Data_and_Privacy>, my emphasis (last accessed January 20, 2010).

[32] Facebook Homepage, www.Facebook.com, accessed December 12, 2010.

> Since Facebook is structured upon the "friend" concept, I think it reasonable to assume that users expect their personal information to be shared with the people they have "friended"…This seems at odds, however, with making the default privacy setting "Everyone"…As Facebook has suggested, its users see themselves as a community…it should be left up to the individual user to decide for himself or herself whether to make information available outside the community.[33]

The Ontario Superior Court of Justice, citing the Assistant Privacy Commissioner and the Finding, reinforced this view in a recent judgment, holding that the plaintiff in that case had joined Facebook to share information with her friends. She had "not created her profile for the purpose of sharing it with the general public."[34]

In CIPPIC's view, Facebook has acted and is currently acting contrary to the reasonable expectations of its users in a number of ways that violate PIPEDA. First, in making its assumptions about reasonable expectations of users, it ignores past actions of specific users that directly contradict these assumptions. Second, the Transition itself, in its employment of default settings, effectively made decisions on behalf of users that were not reasonable in the circumstances. Finally, the default settings it has set for future users do not reflect the 'community' atmosphere that still pervades its network of users. That Facebook has taken actions that are not in line with privacy expectations is not surprising. Privacy is a subjective right, and what its users reasonably expect may be quite different from what its officers expect. Ideally, Facebook should require input from its users with respect to their expectations so it need not make such assumptions. While at the time of the Finding, Facebook cited practical restrictions on gaining this type of input, in CIPPIC's view, it has demonstrated in its handling of the Transition that it is quite possible to get such input in a non-intrusive way. The following sections examine ways in which Facebook has made changes contrary to the expectations of its users and ways in which those can be corrected.

A. Facebook ignores direct user input as to expectations when setting defaults

The Finding notes that Facebook is free to make assumptions when pre-setting default privacy levels – as long as these assumptions are reflect the reasonable expectations of users.[35] It may, for example, be reasonable for Facebook to provide opt out consent for Social Ads and to assume that, when adding a new network, its users expect to share some of their information with that network.[36] However, these types of assumptions become far less reasonable in light of contrary user input as to actual expectations and the lack of notice users receive with respect to these changes. In addition, Facebook has demonstrated there are simple ways to get direct user input so it need no longer make assumptions with respect to their reasonable expectations.

i. Existing Settings and Social Ads

Facebook has long provided users with the opportunity to opt out of its more invasive Social Ads program. Sometime after CIPPIC's initial complaint, Facebook added a new option which provides much the same opt-out functionality as its Social Ads, but applies to ads served by

[33] Finding, *supra* note 1, at paras. 90-94.
[34] *Schuster v. Royal & Sun Alliance Insurance Company o f Canada*, [2009] O.J. No. 4518, 2009 CanLII 58971 (Ont. S.C.) at paras. 51-53.
[35] Finding, *supra* note 1, at para. 89.
[36] Finding, *supra* note 1, at paras. 133 and 90, respectively.

application developers as opposed to Facebook itself. As with Social Ads, the default selection for this new control was opt-in, which in and of itself may be reasonable. The Finding has noted that Facebook can assume users will accept such ads as long as they are informed and given a chance to opt out.[37] However, it becomes less reasonable when the same assumption is made with respect to someone who has already opted out of regular Social Ads, as was the case. This is especially so as Facebook did not adequately notify users of the new control.[38]

By not fine-tuning its newly introduced controls, Facebook is making assumptions about the expectations of some of its users that are difficult to reasonably uphold. Especially in light of the intrusive nature of the advertising in question, this is in violation of Principles 4.3.4, 4.3.5 and 4.3.6. Facebook should default new settings in a manner that is consistent with similar pre-existing ones or force users to decide for themselves upon introducing new controls.

ii. Existing settings and adding a new 'network'

A similar problem occurs when users add networks. To begin with, the Finding held that Facebook must take significant steps to ensure its users are aware it is making assumptions on their behalf upon adding a new network. To this effect, Facebook was to insert clear user notification, as part of its 'add a network' flow screens, that user "profile information can be seen by other members of the network."[39]

Facebook has now attempted to include such notification – the words "profile privacy settings may have changed" appear at the top of user's screens when a new network had been added through the account settings menu. However this notification is misleading in two ways. First, it notifies users that their profile information settings *may have changed* not, as the Finding required, that "their profile information *can be seen by other members of the network*."[40] Unless *all* of a user's profile information was set to 'Everyone' (and even by default, information such as birthday and religious/political views is set only to 'Friends of Friends'), adding a network will indubitably change her profile information settings as all profile information appears to be shared with the entire network regardless of the pre-set level (Only Friends, Friends of Friends or Everyone). Second, it is not just profile information settings that are changed when a new network is added, as most contact information,[41] photo albums, and even the ways in which other non-friend network members can interact with the user change.[42] In light of the inherent inconsistencies contained in this notification, CIPPIC is of the opinion that it fails to meet the meaningful consent requirements imposed on Facebook in the Finding with respect to networks.[43] Facebook remains in violation of Principles 4.2.3 and 4.3.2.

---

[37] Finding, *supra* note 1 at para. 133.

[38] CIPPIC notes that Facebook no longer permits developers to conduct this type of advertising at this time, however the control is in place and will indicate how such activity is governed in the future (see Account Settings>Facebook Ads: "Facebook does not give third party applications or ad networks the right to use your name or picture in ads. If this is allowed in the future, this setting will govern the usage of your information.").

[39] Finding, *supra* note 1 at para. 97

[40] *Ibid.*

[41] One tester who had previously limited her profile information to 'only friends' found most of her contact information being disclosed to the 80,000 plus members of the Harvard network upon joining. Interestingly, the one item of information that was kept private was the email address she used to join the network.

[42] For example, when adding a new network, one tester found that anyone on the new network could add her as a friend, whereas she had set her preferences to only 'friends of friends.' Similarly, people in the new network could now send her a message, whereas previously only her friends could do so.

[43] Finding, *supra* note 1 at paras. 97-98.

However CIPPIC questions whether clarifying this consent is enough in circumstances where a user has manually limited their privacy controls. In such cases, adding an initial network overrides the pre-existing settings. So, even if I have changed my defaults away from the now prevalent 'Everyone' setting to share 'only with friends', adding a network will ignore this for most of my settings, resulting in 'friends and networks'. In CIPPIC's view, it is not reasonable to imply from the addition of a network that users who have deliberately limited information sharing to 'only friends' are suddenly expecting highly sensitive items of data to be shared with entire networks of people they have never met. Such assumptions become even less reasonable when applied to users who have already adjusted sharing controls with respect to existing *networks*. Adding a second network on top of a pre-existing one will ignore not only regular changed defaults ('Everyone' to 'Friends of Friends' or to 'Only Friends') but even custom designed settings applied to pre-existing networks. So, even items of data from which a user had explicitly excluded networks and non-friends will be shared by default upon the addition of another network. While assuming such expectations may be reasonable, as held in the Finding, without any user input, they becomes far less reasonable after a user has already adjusted her settings to exclude non-friends or pre-existing networks and, in CIPPIC's opinion, violates Principles 4.3.4, 4.3.5 and 4.3.6.

This inability to properly assess the reasonable expectations of its users is reflected in many other aspects of Facebook's recent decisions. Its decisions on what to share and what not to share are difficult for CIPPIC to understand from a privacy perspective. In deciding what to share with added networks by default, it provides them with wide swaths of sensitive data, including DOB, which is often used for identity theft purposes, but withholds the network specific Email address required to join that network in the first place – the one piece of data individuals in the network are most likely to be able to access independently. It classifies 'interested in' (its shorthand for sexual orientation) as "basic information" that will "make it easier for friends to find, identify and learn more about you", but designates "hometown" as "more personal" information that should not be shared as broadly.[44] It now, as detailed below, believes that users reasonably expect extremely sensitive information to be shared with 'Everyone' in spite of the Friend-centric makeup of the site. In light of this, it is CIPPIC's position that Facebook should, instead of attempting to make assumptions regarding the expectations of its users, simply ask them for direct input as to how they would like their information to be shared.

In the past Facebook has cited practical constraints on doing so, complaining that its users would be deterred from using its site if forced to consider the "sheer number of screens" involved in selecting privacy settings.[45] Thankfully, Facebook has developed clever and effective mechanisms that, if properly applied, will allow it to get this input from users with minimal time delay. The method by which Facebook handled its Transition demonstrates, in CIPPIC's view, that it is not only possible, but practical and relatively easy to force users to consider or reconsider their privacy settings. As detailed below, CIPPIC believes there is now evidence of an effective means of gaining express consent from users upon signup. Before this, however, we turn to a consideration of the Transition itself, which we believe to have been exceptionally flawed in several key but correctible ways. With respect to the need to account for past user actions in

[44] Facebook, "A Guide to Privacy on Facebook", (Figure 3 – "Privacy Guide"), online at: <http://www.facebook.com/privacy/explanation.php>, (accessed January 20, 2010).
[45] Finding, *supra* note 1 at para. 66.

making new assumptions, clear notification can go some way towards alleviating this issue. However, CIPPIC notes that in the Transition screen, Facebook demonstrated quite clearly that it is capable of applying different sets of defaults based on past user decisions. In light of this, CIPPIC believes such past inputs should be taken into account when users add networks, or when Facebook adds new controls that mimic pre-existing ones, as was the case with Social Ads. Alternatively, Facebook can force users to reconsider their privacy settings expressly upon making such changes to gain direct input from them.

Potential Violation	**Requested Fix**
In setting defaults for new controls, Facebook makes decisions based on assumed expectations of users that are difficult to uphold as reasonable in light of past similar user actions, in violation of Principles 4.2.4, 4.3, 4.3.2, 4.3.4, 4.3.5, and 4.3.6	▪ When introducing new privacy controls, Facebook must take greater steps to notify users of their existence; ▪ Facebook should force users to expressly consider new settings upon adding these; ▪ Alternatively, if setting defaults for new settings, Facebook should take into account previous user actions taken to restrict disclosure of similar personal information;
Facebook unreasonably assumes its users would expect it to disclose highly sensitive information when a user adds a network, ignoring past user controls on limiting information sharing and thus in violation of Principles 4.2.3, 4.3, 4.3.2, 4.3.4, 4.3.5, and 4.3.6.	▪ Force users to expressly consider what information they wish to share with newly added networks; ▪ Alternatively, take into account previous user limits placed on information sharing when formulating assumptions as to how a user expects information to be shared with networks; and ▪ Improve the current misleading notification to ensure meaningful consent is gained;

B. The Transition

The Transition was problematic in a number of ways, and failed to live up to the clear standards set out in the Finding for privacy changes of this nature. First, the changes it was asking users to make were not meaningfully explained – information on the impact of requested changes was hard to come by and, when located, was incomplete and misleading.

Second, the accounts of users who accepted Facebook's recommended changes in the Transition are now operating in ways that violate the reasonable expectations of those users. The counter-intuitive nature of Facebook's recommendations will mean that those operating under these new settings will not have a clear idea of how their information is being disclosed once they place it on Facebook. It is for this reason that the Finding articulated in detail the necessity for gaining express opt-in consent when putting in place settings that conflict with user expectations. The rationale is that if the settings are reasonable and people are meaningfully informed of their impact, then Facebook can impose them on users by default and assume that the majority of users will not be surprised by how their information is then disclosed. Where, as here, Facebook's default settings contradict these expectations directly, greater efforts must be taken to ensure it gains the express consent of users. The Finding made it clear that providing readily available opt-out mechanisms was *not* sufficient to meet consent requirements where defaults violated user expectations. Yet this is precisely the form of opt-out consent 80% of Facebook users were presented in the Transition.

While Facebook may attempt to defend the Transition on the basis that reasonable expectations have changed since the Finding was issued (a period of six months), CIPPIC sees no justification for this. Such claims are belied by Facebook's own materials, by the reality of user interactions on Facebook, by the very nature in which users approach information sharing. CIPPIC sees now support for such claims.

Given these deficiencies in consent, CIPPIC is not surprised that fully 60% of users faced with its recommended defaults did not customize their settings at all.[46] Given its failure to gain meaningful and express consent, any changes resulting from the Transition are void under PIPEDA. Facebook doe not have the informed consent of its users to disclose their information in accordance with its current defaults. CIPPIC views this failure as quite serious when taken in the context of the current process Facebook is undergoing with the Privacy Commissioner. The Resolution established this one year process during which Facebook was to bring itself into compliance with the Finding. The manner in which the Transition was carried out directly conflicted many aspects of the Finding. Now Facebook has put its users information at grave risk. The longer the situation continues, the greater the risk to its users. In light of this, CIPPIC asks that Facebook immediately commit to undue any changes resulting from the Transition.

i. The Transition process

The Transition was comprised of three screens: a 'Privacy Announcement' popup (figure 1), the "Main Transition" screen (Figure 2) and an optional "Privacy Guide" screen ["Transition Screens", collectively]. The first time a user logged in after Wednesday, Dec 9, 2009, she was confronted with the 'Privacy Announcement' popup:

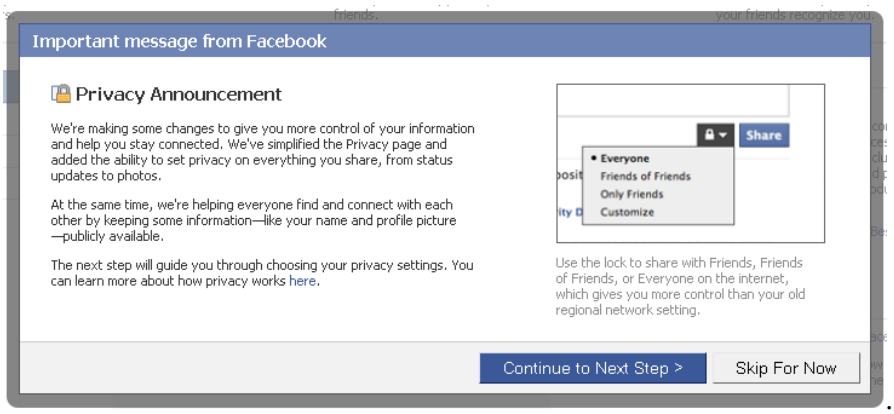


Figure 1 – Transition Popup – Privacy Announcement

Users were given the option to 'learn more', to 'continue to next step' or to 'skip for now'. The 'skip for now' option was soon dropped, at which point users faced with the Privacy Announcement were prevented from interacting with the site until they had completed the Transition. The 'Next Step' button leads directly to the Main Transition page, where users were prompted to change their existing settings in favour of Facebook's recommendations. Users could not use their Facebook account until completing the main transition screen unless they logged out

[46] B. Prince, "Facebook Privacy: Just How Much Do Users Want?", *eWeek.com*, December 20, 2009, online at: <http://www.eweek.com/c/a/Security/Facebook-Privacy-Just-How-Much-Do-Users-Want-222378/> (accessed January 14, 2010).

and logged back in. Nor could users navigate to other areas of Facebook such as their privacy settings or to Facebook's privacy policy.

ii. Facebook failed to get meaningful consent for Transition changes

In CIPPIC's view, users were not provided with sufficient and clear explanations with respect to changes Facebook was asking them to make in the Transition. The recently redefined 'Everyone' privacy setting – central to the Transition – was not clearly explained to users and it failed to provide clear and reasonable purposes for its recommendations. Given this lack of clarity, it is not apparent to CIPPIC that Facebook gained the meaningful consent of its users to any changes that resulted from the Transition. Users reading Facebook's explanations would not have been left with a sufficient and accurate understanding of the impact of the recommendations they were being asked to follow or why they were being asked to follow them. This is not, in CIPPIC's view, an acceptable basis for user consent, nor does it meet the standards set out in the Finding.

Is Everyone your Friend?

Central to Facebook's recommended Transition settings was its 'Everyone' setting. This setting had been recently redefined – where 'Everyone' once meant 'everyone on Facebook', it now means 'everyone on the Internet'. This in itself would be confusing for users, especially users in a rush. A small print notice at the very bottom of the Main Transition screen stating that "[i]nformation you choose to share with Everyone is available to everyone on the internet" could be easily missed:

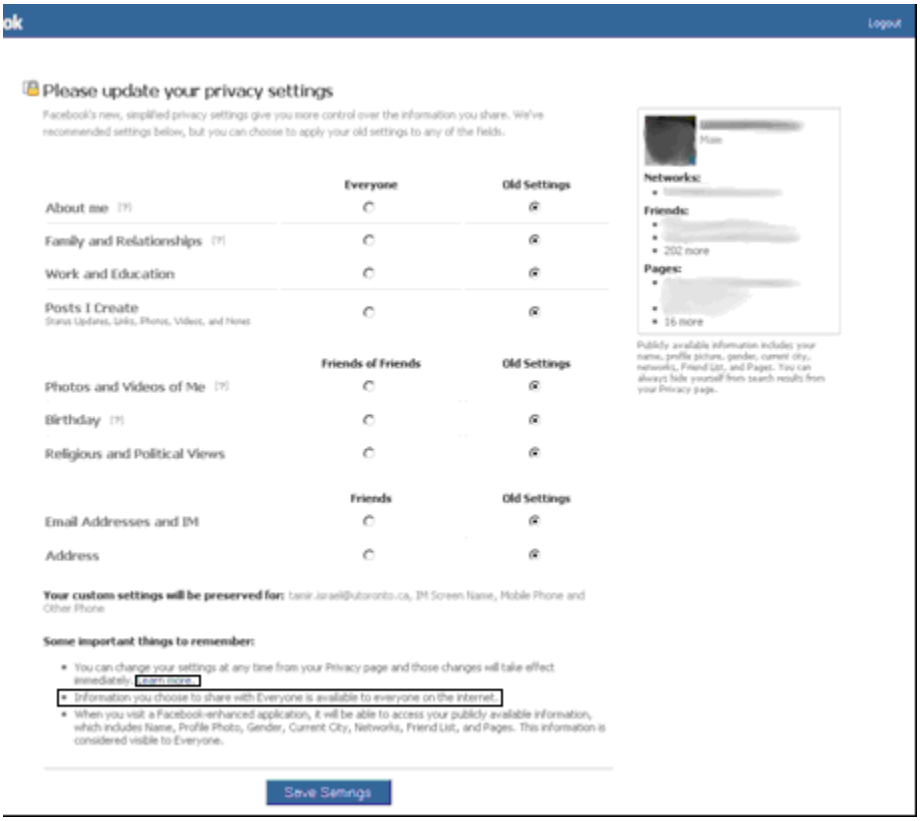


Figure 2 – Main Transition Window (my emphasis)

Also easily missed from the bottom of the main transition page is the 'Learn more' link, which leads a user to another new screen – the 'Guide to Privacy' ("Privacy Guide") page where more details on this setting are provided. Even those users who discovered this Privacy Guide may not have been sufficiently enlightened, as the 'Everyone' now means 'the Internet' reminder is conspicuously missing from the nicely arranged set of highly visible bullet points entitled 'What these changes mean to you' found at the top of the Privacy Guide. It is only found near the bottom of the screen under a section labelled 'Recommended Settings" that users are 'reminded' that Everyone now means, truly, Everyone:

Figure 3 – Privacy Guide; Excerpts

An expanded description of 'Everyone' is also contained in Facebook's new privacy policy, but not in the Transition documentation itself. A closer examination of the full definition of 'Everyone' in the privacy policy reveals that making information available to Everyone amounts to far more than merely making it available to the Internet:

> **"Everyone" Privacy Setting.** 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.[47]

It actually means permitting Facebook and 'others' to make it publicly available "without privacy limitations". This broad release appears to be the basis of Facebook's new approach to privacy, which begins with all-encompassing consent from its customers permitting it to do whatever it wants with 'Everyone' (as well as 'publicly available') data, coupled with piecemeal attempts to build in safeguards ex post in order to provide a reasonable level of protection.

In that respect, there are 'some' privacy limitations on what Facebook and others can do with such data. In CIPPIC's view, these piecemeal limitations are neither sufficiently clear, nor sufficiently protective. In some cases, an 'Everyone' designation appears to override such limitations. In others it does not. Some such limitations provide assurances of protection that are more apparent then real. In general, however, and as detailed below, it appears to CIPPIC that 'without privacy

[47] Privacy Policy, *supra* note 12, my emphasis.

limitations' will often mean, without privacy limitations. The full impact of the resulting, at times limitless, release is serious and difficult to estimate. The bland Transition reminder that "[i]nformation you choose to share with Everyone is available to everyone on the internet" does not fully capture it, in CIPPIC's view. In particular, the extent to which an 'Everyone' designation will override other expressly selected privacy controls is not made clear to users.

It is unclear to CIPPIC how such an imprecise and overly broad definition can withstand scrutiny under PIPEDA, as there are always residual privacy limitations on personal information such as, for example, if an organization wishes to use it for a purpose other than that for which it was originally collected. In addition, this description is imprecise in that it does not make it clear what 'others' may import or export such information from Facebook and under what conditions.

Indeed, CIPPIC finds Facebook's new approach to privacy problematic regardless of whether it succeeds in sufficiently insulating user information through piecemeal protections or not. Starting with a limitless release in this manner is flawed. It simply does not lead to an informed understanding of how information will be collected, used, disclosed and retained. The limitless claims that are its starting point are, in and of themselves, far too broad to ever uphold as they lack precision in definition and are not sufficiently limited to the purposes they intend to achieve. Users are then presented with often conflicting and at other times inadequate reassurances that their privacy will be protected in specific ways. In net, this is not an effective, nor meaningful method of acquiring consent as required by Principle 4.3.2.

Further, if Facebook *truly* sought to classify user data as 'without privacy limitation' and 'publicly available' in general, this in itself would be a violation of PIPEDA. PIPEDA defines 'publicly available' in its regulations.[48] Moreover, few would find it acceptable in the circumstances for Facebook to import and export their data 'without privacy limitation'. So broad and unwarranted a disclaimer is in and of itself a violation of s. 5(3). In this regard, CIPPIC asks that Facebook amend its definition of 'Everyone' information to exclude the 'without privacy limitation' disclaimer.

Regardless, the full impact of accepting Facebook's 'Everyone' recommendations would not have been clear in a number of ways.

When is Google Everyone?

Indicative of this is Facebook's 'Public Search' privacy control – a control that the Transition never mentions, but which purports to remove 'publicly available' and 'Everyone' data from search engine indexing. Diligent users attempting to understand the full extent of their Google exposure post-Transition, may well have been confounded. To begin with, soon after the Transition, Facebook added this 'Important Privacy Announcement' pop-up ("Google Search popup"), which users must read before given access to their privacy search controls:

[48] Personal Information and Protection of Electronic Documents Act ["PIPEDA"], S.C. 2000, c.5, at s. 7(1)(d), as well as *Regulations Specifying Publicly Available Information*, SOR/2001-7 13, December 13, 2000.

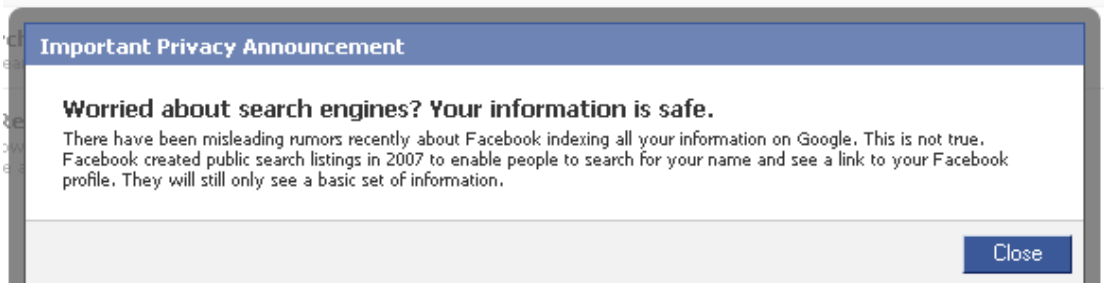


Figure 4 – Privacy Settings>Search – Important Privacy Announcement [Google Search Popup]

This 'privacy' announcement is itself and in combination with the search settings themselves misleading in a number ways. To begin with, it does not inform users that the "basic set of information" now exposed to Google is in effect far broader than it once was, in that it now includes anything posted to a public group or fan page and other types of activities not previously exposed (see Section II.B.iii: Google exposure, below at pages 24-25). This has less to do with the 'Everyone' setting, however, and more to do with 'publicly available information'.

It creates a great deal of confusion surrounding 'Everyone' data. First, by Facebook's recommendation, the 'Everyone' setting is now applied to a wide range of Facebook activity, including the user Wall, which documents most user activity on Facebook – far more than a 'basic set of information'. Facebook does *not* at this time expose all 'Everyone' data to Google. Only to its own internal search engines. However it clearly reserves the right to do so, in its privacy policy (quoted above), in its Transition Privacy Guide explanation of 'Everyone' (see Figure 3), and, indeed, in the very description attached to the public search opt-out control, which purports to "allow search engines to access your publicly available info (*sic*.) and any information visible to Everyone":

Figure 5 – Privacy Settings > Search ("Privacy Search") – emphasis added

It is not clear to CIPPIC whether Facebook need provide any further notification to its users before allowing such indexing – besides, perhaps, removing its ambiguous Google Search Popup. The confusion resulting from this approach is indicative of Facebook's entire new approach to privacy. It asks for unlimited consents, and then attempts to reassure users with misleading descriptions of what it is not currently doing. Users are not left with a clear answer – if I do not opt-out of public search, is my Everyone data available to Google?

Third, the privacy search control screen further confounds general user understanding of 'Everyone' as, on this screen at least, the 'Everyone' setting appears to mean 'everyone on Facebook' not 'Everyone' in its new, limitless sense. Making "Facebook Search Results" available to 'Everyone' does not, within the context of this screen, mean making them available to 'Everyone on the internet', as that disclosure is purportedly governed by the public search opt-out.

In all these ways a user attempting to understand the full extent of Google exposure attached to the 'Everyone' setting would find it difficult to do so. She would be left with a sense that 'Everyone' might *not*, after all, mean Google or the Internet at large. She would be mistaken, however, as Facebook clearly reserves itself the right to disclose this data to 'Everyone' including Google as long as a user has yet not opted out of public search.

Even with respect to users that have opted-out of public search, it appears that an 'Everyone' designation *will* permit Facebook to *indirectly* expose 'Everyone' data to indexing by exposing it to enhanced connect websites and authorizing *them* to display it unconditionally and without privacy limitation. Facebook's instructions to connect website developers describe this authorization as such:

> Users may choose to make some of this data public, which you can then use to display publicly as well (often the case for name, picture)…You may not display any of this data outside the user's specified privacy settings which control exactly what other users can see a piece of information. This setting ranges from everyone, to all friends, or even just a selected group of friends. The APIs have ways to help you determine this – see the implementation details below. *If you do not want to display information conditionally, you should only use information available to everyone*.[49]

This explanation appears to permit connect websites to display 'Everyone' information *unconditionally* and without privacy limitation. It makes no mention of the public search opt-out. To this extent, it appears that the public search opt-out has only limited effect on Facebook's and others' ability to export user information "without privacy limitation".

In CIPPIC's view, the broad Transition disclaimer that 'Everyone' information will be available to developers and "may be visible" to search engines or RSS feeds is incomplete in and of itself, but is further undermined by misleading "Important Privacy Announcements" and inconsistent indexing controls and disclosure policies. It is not clear to CIPPIC that users accepting Facebook's 'Everyone' recommendations would have had any clear idea of what type of indexing Facebook can or will subsequently permit.

When are Enhanced Developers Everyone?

The answer to this question appears to be whenever and without privacy limitation. The Transition Privacy Guide notifies users that:

> Facebook-enhanced applications and websites now have access to a limited set of information when you use and interact with them: your publicly available information and information you've made visible to Everyone.[50]

This appears to be in direct contradiction of what actually occurs. First, the privacy policy clearly and unambiguously states that:

> by default, every application and website, including those you have not connected with, can access "everyone" and other publicly available content[51]

[49] Facebook Developers, Understanding Privacy, *supra* note 31, my emphasis.
[50] Privacy Guide, *supra* note 44.

Meaning that enhanced developers will have access to 'publicly available' and 'Everyone' data *regardless* of whether "you use and interact with them". They will have seemingly unrestricted access to such data all the time. Indeed, Facebook will even ignore a user who has expressly told it, through its privacy settings (page 81: Figure 18), *not* to share certain data with developers it has never interacted with – just as long as such data is defaulted to 'Everyone'. This is especially troubling given Facebook's apparent intention to expand API access to external websites with Fan pages.[52]

Second, once a developer has a user's profile URL, it can now access any and all 'Everyone' data directly by merely visiting that user's page. It need no longer rely on the API to call data. Even if a user has completely hidden herself from search (on and off Facebook), her 'Everyone' and 'publicly available' data will always be available to a developer who has her direct URL (see pages 38-42 below for more details on Facebook search opt-out and discoverability)

Perhaps of greatest, concern, however, is Facebook's willingness to provide 'Everyone' and 'publicly available' data to developers in particular contexts and in combination with other information, such as when a user visits their site. As noted in the Privacy Policy:

> To help those applications and [connect websites] operate, they receive publicly available information automatically when you visit them, and additional information when you formally authorize or connect your Facebook account with them.[53]

In its developer's materials, Facebook expressly authorizes application developers to access 'publicly available' and 'Everyone' data for any user who *visits*, but does not *interact* with their canvas page:

> When a user who hasn't authorized your application visits your application's canvas page, Facebook sends you some user data and lets your application take a number of actions. The following occurs:
>
> - Facebook passes the viewing **user's ID** to your application.
> - Facebook passes the viewing **user's friend UIDs**.
> - **You can call any API method that doesn't require a session.**
> - You can **get user information that's publicly available via search** (except for any users who have chosen to not display a public search listing).
> - You can use FBML tags to show a **user's profile pic** and **name** based on the UIDs passed.
> - You can publish Feed stories by the user via Feed forms.
> - You can send requests on behalf of the user via request forms.[54]

---

[51] Privacy Policy, *supra* note 12. See also Facebook, Settings>Privacy Settings>Applications and Websites>Learn More ["Applications>Learn More"], www.facebook.com, (last accessed January 2, 2010):

> When you **visit** a Facebook-enhanced application or website, it may access any information you have made visible to Everyone...as well as your publicly available information…The application will request your permission to access any additional information it needs. (my emphasis).

[52] See Section IV.C, pages 74-90 , below.

[53] Privacy Policy, *supra* note 12.

[54] Facebook Developers, "Authorizing Applications", ("Facebook Developers, Authorizing Applications") wiki.developers.facebook.com, last modified January 13, 2010, online at:

A list of 'user information' that is 'publicly available via search' and that 'doesn't require a session' includes:

> This call no longer requires a session key. However, if you call this method without a session key, you can only get the following information:
>
> - uid
> - first_name
> - last_name
> - name
> - locale
> - current_location
> - affiliations (regional type only)
> - pic_square
> - **profile_url**
> - sex
>
> You can call this method as soon as a user interacts with your application, before she has authorized your application to access her information. If you do so, you can get the same information as you can without a session (see above).[55]

These are considered 'Sessionless' API calls, meaning the user need not be actively engaged with the developer's service for the developer to make such a call.[56] It is not clear to CIPPIC why an application developer would 'require' *any* of this data from users who are merely *visiting* its canvas pages. Further, if a developer wishes to make such calls to the API when a user is *no longer* visiting their canvas page, it appears to CIPPIC they could do so as long as they retained that user's Facebook ID, which Facebook classifies as 'permanently storable' data.[57] As Facebook appears to permit "every application and website" to access 'Everyone' and 'publicly available' data "by default",[58] it appears that developers are authorized to access such data at will, and can do so once they have this Facebook User ID (UID). With the addition of the 'Everyone' category, a developer now has the option of visiting the user's profile page if it wished to gain all such data by entering her URL directly.

Most troubling is the suggestion in the Privacy Policy that external Connect websites also "receive publicly available information automatically when you visit them". As it clearly does with application canvas pages, this Privacy Policy statement appears to authorize Facebook to disclose UIDs of otherwise anonymous visitors to external connect websites to the developers of those sites. Armed with UIDs, connect developers can also, with ease, gain user profile URLs and, now, access and collect all 'Everyone' data on each user that visits them. Fortunately, it appears as though Facebook currently does *not* disclose UID or any other identifier of unconnected visiting

---

<http://wiki.developers.facebook.com/index.php/Authorizing_Applications>, (last accessed February 1, 2010), my emphasis. Note this document has been updated (February 4, 2010) and currently states:

> When a user who hasn't authorized your application visits your application's canvas page, Facebook sends you some user data (known as automatic authentication) and lets your application take a number of actions.

[55] Facebook Developers, "Users.getInfo", ("Facebook Developers, Get Info") wiki.developers.facebook.com, last modified January 20, 2010, online at: <http://wiki.developers.facebook.com/index.php/Users.getInfo>, (last accessed February 1, 2010).

[56] Facebook, Authorizing Applications, *supra* note 54: "About Session Keys".

[57] Facebook Developers, "Storable Data", wiki.developers.facebook.com, last modified January 20, 2010, online at: <http://wiki.developers.facebook.com/index.php/Users.getInfo>, (last accessed February 1, 2010).

[58] Privacy Policy, *supra* note 12. See also note 51, above.

users to external connect websites. It appears, however, that Facebook's current Privacy Policy encompasses such disclosures, as Facebook relies on the same clause to provide Application developers with information on otherwise anonymous users visiting their canvas pages. It is not clear to CIPPIC that, were Facebook to start making such disclosures, it would need to provide further notification to users. Accepting an 'Everyone' recommendation could, then, amount to consenting to such disclosures.

Facebook's Transition notified users in the Privacy Guide that developers will only have access to such data if and when a user uses and interacts with their application or website. This does not appear to be the case. Facebook authorizes developer access to 'Everyone' data – at the very least – whenever a *friend* of a user interacts with an application or connect website (see page 81, *Figure 18* below for more details). It appears to authorize access any time, regardless of any interaction between a user or a user's friend, seemingly leaving the API open to random queries for 'Everyone' and 'publicly available' data from anyone with an API key.[59] It appears to further authorize access to such data in connection with visits to sites, such as application developer canvas pages, or even external websites. Further, as noted below, it is not clear to CIPPIC that Facebook intends to provide technical safeguards that prevent developer access to 'publicly available' or 'Everyone' data.

Who else can be 'Everyone'?

It appears that 'anyone' can be 'everyone'. More to the point, where anyone gathers data from Facebook and uses it for non-commercial purposes (research) or, say, for journalistic purposes, PIPEDA will not necessarily apply.[60] In such cases, the only protections provided to such data will be through Facebook's internal contracts, terms and policies. As 'Everyone' data "may be imported and exported by [Facebook] and others without privacy limitation", this protection appears scant at best. This limitless access is confirmed in Facebook's Privacy Policy, which states:

> **Exporting Information.** You (and those you make your information available to) may use tools like RSS feeds, mobile phone address books, or copy and paste functions, to capture and export information from Facebook, including your information and information about you.[61]

PIPEDA is intended to protect privacy in commercial contexts, and does not apply to such collection, user and disclosure for good reason. However, these exceptions contemplate that the manner in which the data was first released is acceptable in the circumstances. CIPPIC is of the opinion that Facebook users are not aware that their 'Everyone' data can now be collected, used and disclosed in such contexts without limitation. A reasonable user sharing information on Facebook expects it to be shared with friends, not with random researchers,[62] or, perhaps, with the New York Times. These profiles are now a rich source of data, "just waiting to be analyzed and cross referenced".[63] Without privacy limitation.

---

[59] *Ibid*.

[60] See Personal Information and Protection of Electronic Documents Act, S.C. 2000, c.5, ss. 4 and 7. CIPPIC notes that PIPEDA continues to apply to Facebook's *disclosure* of data for such purposes, which, along with all its other activities, is of a commercial nature (Finding, *supra* note 1 at para. 12).

[61] Privacy Policy, *supra* note 12.

[62] M. Kirkpatrick, "The Man Who Looked Into Facebook's Soul", ["Kirkpatrick, Facebook's Soul"] ReadWriteWeb, February 8, 2010, available online at: <http://www.readwriteweb.com/archives/facebook_user_data_analysis.php>.

[63] *Ibid*.

In sum, it does not appear to CIPPIC that users appraising Facebook's recommended 'Everyone' defaults would have had a meaningful understanding of the full impact of this 'limitless' designation on their personal information. Certainly, the difficult to locate Transition reminders that "any information that's visible to Everyone may be seen by everyone on the Internet" do not, in CIPPIC's view, completely capture the import of the redefined setting. Users attempting to gain a better understanding post-Transition would be further confounded by contradicting controls and third party contractual obligations whose impact on an initial authorization that is "without privacy limitations" is questionable.

Facebook did not provide clear and reasonable purposes for its recommendations

Further, the justifications that Facebook offered its users for its recommended settings were at best meaningless and at worst misleading. The Transition begins with the Privacy Announcement, which notifies users that some changes are being made "to provide you more control of your information and help you stay connected." Next, the Main Transition asks users to "Please update your privacy settings", explaining that "Facebook's new, simplified privacy settings give you more control over the information you share. We've recommended settings below, but you can choose to apply your old settings to any of the fields."

Those users searching for an explanation of Facebook's recommendations may have discovered the Privacy Guide screen, which begins with an explanation of 'Privacy on Facebook:

> Privacy is built around a few key ideas: You should have control over what you share. It should be easy to find and connect with friends. Your privacy settings should be simple and easy to understand.[64]

In a section entitled "Recommended Settings", Facebook then justifies its 'Everyone' recommendations as such:

> We recommend **Everyone** be able to see information that will make it easier for friends to find, identify and learn about you. This includes basic information like your About Me description, Family and Relationships, Work and Education Info, and Website, as well as posts that you create, like photo albums and status updates.[65]

It is not clear to CIPPIC how making *any* of this information, including past employment, 'interested in' (sexual orientation), or status updates available to **Everyone** helps "make it easier for **friends** to find, identify and learn about you."[66] All a user needs to find a friend is their name and perhaps their profile picture (now designated 'publicly available' by Facebook irrespective of privacy settings). Upon locating these basic pieces of information, a friend request can be sent, after which any **real** friend of the user will be able to 'learn more' about them. CIPPIC finds it highly unreasonable in the circumstances to recommend to users that they should share such a broad category of sensitive information with 'Everyone' for the purpose of helping their friends find, identify and learn more about them.

---

[64] Privacy Guide, *supra* note 44.
[65] Privacy Announcement, *supra* Figure 1.
[66] Privacy Guide, *supra* note 44, Figure 3, my emphasis.

Facebook's purposes for the 'Friends of Friends' recommendations are even more problematic. It presents these recommendations as a form of 'privacy protection', informing users that:

> Some information is more personal, so we recommend **Friends of Friends** be able to see that type of info. This includes the settings for your Birthday, Religious and Political views, Hometown, and Photos and Videos of Me, which his all the photos and videos you've been tagged in.[67]

While CIPPIC finds Facebook's rating of the relative sensitivity of categories of information puzzling in itself, its rationale for the 'Friends of Friends' recommendation is more so. It appears to still rely on the over-arching purpose of sharing information with **friends**, but recommends **Friends of Friends** as a method of achieving that purpose in a privacy protective manner. It is unclear to CIPPIC why anyone who is not a **friend** requires access to any of the information in this category of recommendations in order for one's friends to find, identify and learn more about her.

To CIPPIC, it appears as though Facebook now intends to equate 'friend' with 'Everyone', but that is not borne out by its materials. If Facebook wished to attempt to convince its consumers to disclose their highly personal information for the purpose of sharing it with 'Everyone', it should not do so by telling them such sharing will facilitate sharing with 'friends'. Having read the Transition materials, many users facing the Main Transition screen would be under the mistaken impression that, in light of the new privacy settings (aimed at providing users more control over personal information), they should follow Facebook's recommendations so as to make it "easy to find and connect with friends".[68]

Under such circumstances, it is CIPPIC's view that users who changed their settings in order to follow Facebook's recommendations cannot be held to have provided consent as required by principles 4.3, 4.3.2 and 4.3.5. Many of Facebook's users trust them and would have accepted their justifications and recommendations at face value. Such consent is not meaningful, as users are not provided with a clear sense of the purpose of the disclosures and is deceptive in that it is likely to misled users into thinking the recommended disclosures are necessary to help them find and interact with their friends. CIPPIC does not believe reasonable people would find it appropriate in the circumstances to request individuals to share so much sensitive data with 'Everyone' for the purpose of facilitating interactions with their friends.

iii. Facebook failed to get express consent from users for Transition changes

The Transition also failed to meet express consent standards set out in the Finding, where it was made clear that express consent involves an opt-in, not an opt-out choice. The Transition greatly expanded the role played by Facebook's public search control. Facebook is now relying on that opt-out consent to cover a broad range of public search disclosures. However this control was not included or even linked to in the Transition.

Further, the design of the Main Transition screen, where users were asked to adopt Facebook's recommendations, did not meet requirements for express consent. It did not provide users with the full range of options available to them and, for the majority of users, it pre-selected Facebook's

[67] *Ibid*., emphasis in original.
[68] *Ibid*.

recommendations by default. As noted in the Finding, where express consent is sought, it is not sufficient to merely offer a user an easy method of opting out of a default choice.[69]

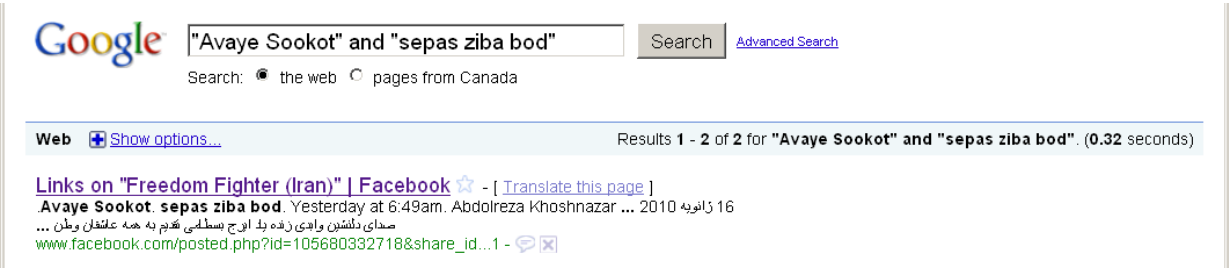
Overall, Facebook failed to get express consent for changes resulting from the Transition. And, as explained in the Finding, where requested changes are not in line with reasonable expectations of privacy, an express form of consent is required by PIPEDA.[70] This section will demonstrate that Facebook failed to gain express consent, while the next will show how its recommended changes violated the reasonable expectations of privacy of its users.

Google exposure

Users were not provided with an opportunity to opt-out of public search indexing within the Main Transition screens. Whereas before the Transition, Facebook acquired opt-out consent from users to display publicly searchable profiles containing a limited and at that point optional list of data, this same control now covers much more.

For one thing, the 'optional' list is no longer optional as the data involved is now deemed 'publicly available' by Facebook. Users who had, for example, expressly removed fan pages from their public search listings would find them suddenly returned post-Transition.

More troubling, however, is Facebook's decision to allow public search indexing of public groups and fan pages, which are now considered available to 'Everyone', with all the implications that term carries post-Transition.[71] But it is not only the pages themselves that are indexed, but also every comment, link, picture, etc., posted to these pages, regardless of whether the user posting them is doing so under the default 'Everyone' publisher setting or not. For users who have opted out of public search, these comments appear and are indexed along with their first name alone. For those users who have *not* opted out of public search listings, all of these postings are now indexed along with their full names, and the posts themselves are now accompanied by their profile pictures as well as a link to their public profile which, of course, now includes a list of their friends, fan pages, gender, etc.:



[69] Finding, *supra* note 1 at paras. 92-93.
[70] Finding, *supra* note 1 at paras. 89-95.
[71] As the Facebook "Statement of Rights and Responsibilities", ["SRR"] December 21, 2009, (accessed January 20, 2010) states at s.12.3: "Pages can only post content and information under the "everyone" setting."

Figure 6 – Public Searches

Given search result hierarchy, results of this nature are often the first to appear when a user's name is entered into Google. As noted by EPIC in its complaint to the FTC, this type of expanded visibility is not only privacy invasive, but can have serious and harmful consequences.[72]

In CIPPIC's view, in order to gain the express consent of users to disclosures of this nature, Facebook would have had to include an opt-in public search control in its Main Transition screen.

Design of Main Transition screen

The design of the Main Transition screen itself was not appropriate in form to meet express consent standards. To Facebook's credit, it attempted to tailor its Transition to past user action to some extent. So, for users who had previously changed their privacy settings, the Main Transition controls were defaulted to 'Old Settings'. Even so, the Main Transition screen was deficient in form. Instead of offering users the full range of available privacy controls,[73] the screen only provided users with the option of dropping their pre-existing settings in favour of Facebook's typically far less protective 'recommendations'. Users were not even provided with a visible method of identifying what their previous settings were – the buttons are merely labelled 'old settings'.[74]

As deficient as the form of consent was for this first class of users, a second class of users, those who had been operating their Facebook accounts under the old pre-existing default settings, were not even required to opt in to the new recommendations. For such users, the Main Transition appeared as such:

---

[72] EPIC *et. al.*, Complaint before the Federal Trade Commission, *In re Facebook*, December 17, 2009, available online at: <http://epic.org/privacy/inrefacebook/EPIC-FacebookComplaint.pdf> at paras. 45-53. See also F. Fassihi, "Iranian Crackdown Goes Global", Wall Street Journal, December 3, 2009,, available online at: <http://online.wsj.com/article/SB125978649644673331.html>.

[73] Including 'Everyone', 'Friends of Friends', 'Only Friends' and 'Custom', which includes limited profile lists and 'only me'.

[74] After extended testing, CIPPIC discovered that hovering over an 'old setting' button would reveal what that old setting was. However this is not an intuitive means of notification. No indication is provided in the Main Transition that hovering would reveal these old settings. Further, a user who wished to change her settings away from 'old settings' would hover over the 'recommended setting' button, not the 'old setting' button.

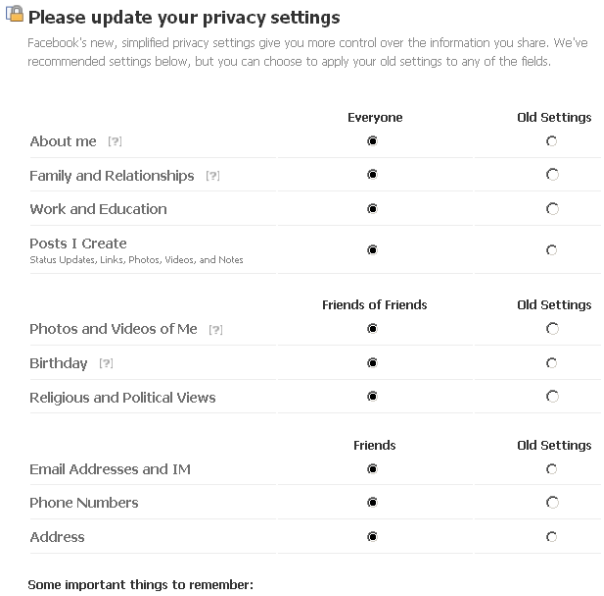


Figure 7 – Main Transition Screen – For Accounts still functioning under Facebook's initial defaults

As 70-80% of users never change their default settings, this would have been the screen confronting the vast majority of Facebook users.[75] The Main Transition effectively opted such users in to Facebook's recommendations. In this scenario, all a user need do is trust Facebook enough to hit 'Save Settings' without further investigation, and highly sensitive data such as 'interested in' (sexual orientation), past occupations, education history, status updates, posted links, posted photos, posted videos, and posted notes would be broadcast to 'Everyone'. Other highly sensitive pieces of data such as Birthday, Political views, and Religious views would now be shared with 'Friends of Friends' – an uncontrollable and potentially quite large group of people – whereas before they were only shared with 'Friends'.

While it is true that users were provided with a readily available means of opting out of these default settings in favour of their undefined 'Old Settings', the Finding clearly set a higher standard than this for express consent in the social networking context:

> Since Facebook is structured upon the "friend" concept, I think it reasonable to assume that users expect their personal information to be shared with the people they have "friended"…with regard to the ["Everyone"] setting for photo albums, I commend Facebook for its privacy-sensitive practice of automatically presenting users uploading photos with…an easy means of changing the privacy setting if they wish. This seems at odds, however, with making the default privacy setting "Everyone".[76]

As noted in this passage, it is not sufficient to provide users with an 'easy means of changing' pre-selected privacy settings if such settings are not in alignment with their reasonable expectations. For this reason, Facebook cannot rely on its new 'Publisher' tool to justify recommended 'Everyone' defaults either. The reality is that few users take the time to change defaulted settings, even with an "easy means" readily available. They typically trust organizations

[75] Finding, *supra* note 1 at para. 66.
[76] Finding, *supra* note 1 at paras. 90, 92.

such as Facebook to make decisions that are in line with their reasonable expectations. They trust their 'recommendations' to be in line with their interest. This is why PIPEDA and other data protection statutes require express, opt-in consent in such situations. As stated in a recent opinion adopted by the EU Article 29 Data Protection Working Party addressing the application of EU data protection laws to SNSs such as Facebook:

> An important element of the privacy settings is the access to personal data published in a profile. If there are no restrictions to such access, third parties may link all kinds of intimate details regarding the users, either as a member of the SNS or via search engines. However, only a minority of users signing up to a service will make any changes to default settings. Therefore, SNS should offer privacy-friendly default settings which allow users to freely and specifically consent to any access to their profile's content that is beyond their self-selected contacts in order to reduce the risk of unlawful processing by third parties. Restricted access profiles should not be discoverable by internal search engines, including the facility to search by parameters such as age or location. Decisions to extend access may not be implicit, for example with an "opt-out" provided by the controller of the SNS.[77]

Members of the US FTC have made similar comments suggesting that data protection laws require more than the opt-out approach utilized by Facebook in the Transition.[78] The global consensus that appears to emerge is in support of the Assistant Privacy Commissioner's initial Finding – that where Facebook seeks to make disclosures that deviate from what people would normally expect, it must get their express opt-in consent. In the Transition, it has failed to do so.

CIPPIC does not, under these circumstances, find surprising reports that as of Dec 14, more than 60% of users presented with Facebook's pre-selected recommended defaults in the Main Transition screen did not customize these at all.[79] It is its position these pre-selected defaults did not meet the express consent standards set out in the Finding and cannot be relied upon under Principles 4.3.4, 4.3.5 and 4.3.6 for subsequent disclosures. As noted in the Finding, PIPEDA requires Facebook to gain express consent where it is to disclose the personal information of its users in a manner that violates their reasonable expectations.[80] The next section will demonstrate that Facebook's recommended settings were *not* in line with user expectations.

iv. Facebook's recommended Transition changes violated reasonable user expectations

Privacy has been a central and integral component of Facebook since its early days.[81] Its users have come to expect it, and that is why they "feel secure sharing highly personal information including interests, thoughts, and contact information."[82] On Facebook, where users join, as its motto states, to "connect and share with the people in [their] life",[83] privacy does not mean hiding

---

[77] Article 29 Data Protection Working Party, *Opinion 5/2009 on Online Social Networking*, [EU Working Group] (2009) 01189/09/EN, WP 163, available online at: <http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2009/wp163_en.pdf>, at p. 7.

[78] Clifford, *supra* note 6. FTC Chair Jon Leibowitz recently commented with respect to potential regulation of social networks such as Facebook that the FTC is "head[ing] towards opt-in."

[79] Prince, *supra* note 46.

[80] Finding, *supra* note 1 at paras. 89-95.

[81] Kirkpatrick, Data Portability, *supra* note 29.

[82] Facebook Developers, Understanding Privacy, *supra* note 31.

[83] Facebook HomePage, *supra* note 2.

information away from everybody whatsoever. But it also does not mean disclosing it to 'everyone'. It means, of course, disclosing it to 'the people in your life'. Your friends.

This expectation – that information users provide Facebook will be shared with their friends – is reinforced from the moment a user enters Facebook. The motto above remains emblazoned on Facebook's homepage and is the golden thread that still permeates most of Facebook's customer oriented explanations of the purpose of its site and its privacy controls. By CIPPIC's count, its Privacy Policy mentions the justification "Facebook is about sharing information with…friends" or some variation of it nine times.[84] In addition, its new Privacy Guide, which was incorporated into the Transition and is now presented to users who follow the 'privacy' hyperlink at the bottom of any Facebook page, explains under the heading "Privacy on Facebook" that "[p]rivacy is built around a few key ideas: You should have control over what you share. It should be easy to find and connect with friends."[85]

Yet site literature is not, in CIPPIC's view, a determinant of user expectations. It is, rather, more a recognition thereof. Users respond to this type of literature precisely *because* it reinforces their reasonable expectations. As recently stated by Facebook CEO Mark Zuckerberg, Privacy has been the "vector around which Facebook operates".[86] As still noted in Facebook's own developer materials, it is Facebook's rich and intuitive privacy settings that have "allowed people to feel secure sharing highly personal information" with it.[87] As few users ever directly interact with the privacy settings (only about 20%-30%),[88] however, it is not the settings themselves that have attracted so much trust in Facebook, but rather the architecture itself that the settings are built around.

As stated by the Assistant Privacy Commissioner in the Finding, "Facebook is structured upon the "friend" concept."[89] The EU Article 29 Data Protection Working Party similarly would require express opt-in consent for any SNS disclosures beyond a user's "self-selected contacts".[90] PIPEDA protects privacy by ensuring user knowledge and control over personal information. Reasonable users expect to have this type of control. The Friend architecture is an intuitive method of achieving this knowledge and control. Users build their information profiles and, upon receiving friend requests, can decide who may access these and who may not. Through such controls, the expectation that only friends can see most user information is reinforced at every stage of the Facebook experience and is rooted in this need for control of one's personal information. Both the 'Friends of Friends' and the 'Everyone' categories fail to provide users with the same level of control, as both represent an undefined and effectively unknowable category of individuals.

CIPPIC finds little support for comments, publicly made by Facebook representatives, that "[p]eople have really gotten comfortable not only sharing more information and different kinds,

---

[84] Privacy Policy, *supra* note 12.
[85] Transition Privacy Guide, *supra* note 44.
[86] M. Kirkpatrick, "Facebook's Zuckerberg Says The Age of Privacy is Over", [Kirkpatrick, No More Privacy] *ReadWriteWeb*, January 9, 2010, online at: <http://www.readwriteweb.com/archives/facebooks_zuckerberg_says_the_age_of_privacy_is_ov.php>
[87] Facebook Developers, Understanding Privacy, *supra* note 31.
[88] Finding, *supra* note 1 at para. 66.
[89] Finding, *supra* note 1 at para. 90.
[90] EU Working Group, *supra* note 77 at p. 7.

but more openly and with more people. That social norm is just something that has evolved over time."[91] In CIPPIC's view, enduring social norms such as privacy do not change at such a rapid rate. Facebook's stated view that users no longer expect privacy on its site conflicts with both its own fairly recent statements as well as the bulk of its user-oriented materials.[92] Pointing, as Facebook Director of Corporate Communications and Public Policy Barry Schnitt recently did, to the rise of blogging and Twitter as evidence to the contrary is not sufficient, in CIPPIC's view.[93] Indeed, it has been CIPPIC's experience that users *do* care about privacy as long as they are adequately informed of it and its implications.[94]

Context is the key that defines what users expect to occur with their personal information. Users on Twitter, for example, are far more aware that they are not merely interacting with their 'friends'. They have a list of 'followers' that is often not reciprocal. They themselves follow a list comprised of different people. In many cases, they will have met few of these people in real life. Even when interacting with their friends, they do not invest immense quantities of personal information into their Twitter accounts as their purpose on Twitter involves far simpler interactions – the types of conversations one would have in a crowded café as opposed to the types of more intimate information exchanges one would have in the privacy of one's home. Danah Boyd describes the majority of social interactions on Twitter as primarily phatic – serving an important social purpose, but conveying little that could be deemed 'informational' to third parties.[95] A far cry from the "rich profiles" Facebook prides itself upon.[96]

As noted by many, even when disclosing information in a far more public forum than Facebook such as a blog or on Twitter, users still have high expectations of privacy. These are rooted in a need to control the context in which the information is used and disclosed. When such information is taken from that medium and used in contexts other than as it was intended, harm can often occur and, regardless, users often experience a sense of personal invasiveness. Helen Nissenbaum has described this sense of invasiveness as such:

> Most people have a robust sense of the information about them that is relevant, appropriate, or proper to particular circumstances, situations, or relationships. When information is judged appropriate for a particular situation it usually is readily shared; when appropriate information is recorded and applied appropriately to a particular circumstance it draws no objection. People do not object to providing to doctors, for example, the details of their physical condition, discussing their children's problems with their children's teachers, divulging financial information to loan officers at banks, sharing with close friends the details of their romantic relationships. For the myriad transactions, situations and relationships in which people engage, there are norms—explicit and implicit—governing how much information and what type of

[91] Kirkpatrick, No More Privacy, *supra* note 28

[92] Finding, *supra* note 1 at paras. 80-81; Kirkpatrick, No More Privacy, *supra* note 28:

> This is a radical change from the way that Zuckerberg pounded on the importance of user privacy for years. That your information would only be visible to the people you accept as friends was fundamental to the DNA of the social network that hundreds of millions of people have joined over these past few years.

See also Kirkpatrick, Data Portability, *supra* note 29.

[93] Kirkpatrick, Why Facebook Changed, *supra* note 28.

[94] W. Davis, "Flash Cookies Could Become Hot-Button Privacy Issue", Media Post News, January 15, 2010, available online at: <http://www.mediapost.com/publications/?fa=Articles.showArticle&art_aid=120673>.

[95] D. Boyd, "Twitter: "Pointless babble" or peripheral awareness + social grooming?", apophenia, August 16, 2009, online at: <http://www.zephoria.org/thoughts/archives/2009/08/16/twitter_pointle.html> (accessed January 18, 2010).

[96] Facebook Developers, Understanding Privacy, *supra* note 31.

> information is fitting for them. Where these norms are respected I will say that contextual integrity is maintained; where violated, I will say that contextual integrity has been violated.[97]

On Facebook, with its 'share with the people in your lives' clarion call and 'Friend'-centric architecture, users are willing to provide information because they reasonably expect it to be shared with their friends alone. Disclosing it to 'Everyone' violates these expectations to begin with, as the initial context of disclosure is 'between friends'. But it is also problematic in that it is likely to lead to further violations and a sense of lost control as, it being publicly available, the likelihood that the information will be used and re-used in other contexts increases exponentially. It is for this reason that most individuals would not expect so much personal and sensitive information to be made available so broadly. It is the loss of control that results. It is to reduce the risk of this type of uncontrolled data processing that lead the EU Data Protection Working Party to advocate 'friends only' defaults.[98] As a recent survey affirmed, Canadians, too, still care about this control a great deal.[99] Facebook's Transition defaults and recommendations effectively take that friend-based control away from the user and release her information to 'Everyone'.

Users may reasonably expect some basic information to be shared beyond 'only friends' for some purposes. Helping friends of a user locate her is the only such purpose that CIPPIC views as legitimate. However, only a very limited amount of data is required to meet this objective. Name, and perhaps profile picture. Nothing more is required. Anything further can be shared with a true friend after that friend has been granted access to the user's profile. Nor does CIPPIC see any justification for public search profiles. Users come to Facebook to share information with their friends within the Facebook community.[100] While some users may wish to share more broadly, most will not reasonably expect this to occur by default. In addition, those users that do wish to share more broadly are not prevented from doing so. All they need do is change their privacy settings. In CIPPIC's view, it appears far more reasonable to ask individual users who wish to share more broadly to adjust their settings then the opposite.

Most of Facebook's Transition recommendations involved pushing users to sharing information well beyond their 'friends'. Given the central and integral role played by the 'share with your friends' concept on Facebook, CIPPIC is of the opinion that the majority of Facebook users do not reasonably expect Facebook to share their information more broadly than with their friends. Given that Facebook failed to gain the express, informed and meaningful consent of its users for changes resulting from the Transition and given that these changes violated user's reasonable expectations, it is CIPPIC's view that Facebook is in violation of Principles 4.3.4, 4.3.5 and 4.3.6 of PIPEDA and the consent standards set in the Finding. The majority of its users will not be aware of the full extent to which their personal information is now available. The risks associated with such exposure are great.

---

[97] H. Nissenbaum, "Protecting Privacy in an Information Age: The Problem of Privacy in Public", (1998) 17 *Law and Philosophy* 559., available online at: <http://www.nyu.edu/projects/nissenbaum/papers/privacy.pdf>.

[98] EU Working Group, *supra* note 77 at p. 7.

[99] Phase5 Consulting Group, *Research Related to Privacy and the Use of Geospatial Information*, Natural Resources Canada, November 2009, available online at: <http://epe.lac-bac.gc.ca/100/200/301/pwgsc-tpsgc/por-ef/natural_resources/2009/091-08/report.pdf>, at p. ii: "Privacy of personal information is a sensitive issue with more than half of all respondents indicating that they are 'very concerned ' about the privacy of their personal information in general and over 80% stating they are 'concerned' or 'very concerned'.

[100] Finding, *supra* note 1 at para. 94.

Further, assessed in the context of the broader Resolution process that the Transition occurred within, CIPPIC does not find it to have been conducted in a manner that a reasonable person would consider appropriate in the circumstances. Facebook was aware of the Finding and was in the process of complying with it. As the changes it was requesting of its customers were a dramatic departure from the Finding, it should have consulted with the Commissioner with respect to these. Taking the Commissioner's recent decision to reopen her investigation of Facebook with a particular focus on the Transition,[101] CIPPIC does not believe that she would have approved of such changes. Taken within this broader context, CIPPIC views the Transition as a violation of s. 5(3) of PIPEDA as well. It therefore asks that Facebook return user settings to their pre-Transition defaults immediately, before any harm results to its users.

Potential Violation	**Requested Fix**
Facebook's Transition did not adequately explain to users the full impact of new terms such as 'Everyone' and it relied on misleading or deceptive explanations of the purposes for its recommended changes. As such it failed to gain meaningful consent of its users for Transition changes, and is in violation of Principles 4.3, 4.3.2 and 4.3.5.	CIPPIC asks that Facebook immediately reverts its users to its pre-Transition privacy settings. An immense amount of personal information is currently available to 'Everyone' on Facebook and much is also available more broadly. The risks associated with the continued status quo are, in CIPPIC's view, large and difficult to calculate. Facebook does not have meaningful, informed consent for any of its post-Transition disclosures. As these disclosures are currently with a much broader community than most Facebook users would reasonably expect, CIPPIC believes many of Facebook's users are not aware of their exposure and will not be until after any potential harm manifests. In addition, CIPPIC asks that Facebook immediately opts all of its users out of public search;
Facebook's Transition did not include opt-in consent to expanded public search capabilities and for the vast majority of users did not employ an adequate opt-in mechanism for its changes. As such it failed to gain express consent for its recommended changes, and is in violation of Principles 4.3.4, 4.3.5 and 4.3.6.	
Facebook's recommended opt-out changes were a violation of its users reasonable expectations as well as of Principles 4.3.4, 4.3.5 and 4.3.6.	
Facebook's transition in total failed to provide its users with the accurate information they required to make informed decisions and further failed to employ the proper method of consent. In CIPPIC's view, the Transition was not conducted in a manner that a reasonable person would find appropriate in the circumstances and is in violation of Section 5(3).	
Facebook's 'Everyone' privacy category is excessively broad and does not a good basis for meaningful consent as required by Principle 4.3.2.	Better define the 'Everyone' setting so as to take account for actual limitations placed on sharing such information.

C. Default Settings for New Users

CIPPIC finds Facebook's post-Transition signup process for new users to be in direct violation of both the spirit and the letter of the Finding and Facebook's undertakings in the Resolution. The Finding was premised on the basic concept, central to Facebook's philosophy and the majority of its materials, that Facebook is about helping users find, connect and share with *friends* note with *everyone*.

[101] Office of the Privacy Commissioner of Canada, "Privacy Commissioner launches new Facebook probe", News Release, January 27, 2010, available online at: <http://priv.gc.ca/media/nr-c/2010/nr-c_100127_e.cfm>.

Facebook relies on setting pre-selected defaults for new users, in effect deciding for them how their information will be disclosed. Facebook described this process, pre-Transition, stating it:

> believe[d] that users should be empowered to make their own choices about sharing personal information. [Facebook] facilitate[d] this choice by setting powerful defaults that reflect common sense views about availability and allowing users to change settings if they wish.[102]

The vast majority (70%-80%, by its own estimates] of its users trust Facebook enough not to examine or change these pre-selected defaults.[103] Facebook justified its reliance on defaults on pragmatic grounds, stating "it would not be practical to force users to pick all their privacy settings before being allowed to register. The sheer number of screens they would have to go through would deter them from ever signing up for the service."[104] The Finding approved this scheme, in general terms, on the grounds that the 'powerful defaults' at the time did indeed reflect 'common sense' views. Most were limited to 'only friends' for most users. Where Facebook's defaults deviated from this norm, the Assistant Privacy Commissioner demanded that it adjust these so that they were more in line with the reasonable expectations of its users.[105]

Facebook's default settings for new users mirror its 'recommendations' from the Transition which, as stated in the preceding section, are in line neither with "common sense views about availability", nor with the reasonable expectations of its users. Particularly troubling to CIPPIC is the expansion of public search capacities from, at the time of the Finding, a limited, optional but already problematic list of data to much broader amounts of information without the express opt-in consent of its users.[106] CIPPIC additionally views the default settings for posting photos as well as the wall photos album ("Everyone") to be in direct violation of Facebook's undertaking in the Resolution to change the default for photos to 'friends of friends'.[107] The new 'Everyone' and 'Friends of Friends' defaults as well as the opt-in for public search are all, in CIPPIC's view, in violation of PIPEDA as Facebook lacks express consent for these disclosures, none of which is in line with reasonable user expectations.

In addition, Facebook has adopted neither the global "Privacy Wizard" tool it had initially promised to include, nor the privacy tutorial it mentioned in the Resolution.[108] Unless Facebook intends the Privacy Guide screen from the Transition (currently available through the 'Privacy' link at the bottom of all Facebook pages) to function as its tutorial. CIPPIC would find the latter possibility problematic, as the Privacy Guide as it currently stands is misleading and inaccurate.

Further, CIPPIC is no longer convinced that any form of consent short of express consent is appropriate in the circumstances. It is difficult for organizations such as Facebook to estimate the reasonable expectations of its users, and ineffective to initiate legal processes ex-post every time Facebook wishes to make changes to its site. Perhaps more importantly, Facebook has

---

[102] Finding, *supra* note 1 at para. 66.
[103] *Ibid*.
[104] *Ibid*.
[105] Finding, *supra* note 1 at paras. 87-98.
[106] Finding, *supra* note 1 at paras. 76, 94.
[107] E. Denham, "Letter from OPC to CIPPIC outlining its resolution with Facebook", ["Resolution"], Office of the Privacy Commissioner of Canada, August 25, 2009, available online at: <http://www.priv.gc.ca/media/nr-c/2009/let_090827_e.cfm>.
[108] Finding, *supra* note 1 at para. 100; Reslution, *supra* note 107.

demonstrated that there are numerous effective mechanisms for acquiring time-of-collection express consent from its users. It has also shown that it does not deem such mechanisms overly intrusive as it is willing to utilize them where it deems appropriate.

For example, the Transition Screens demonstrated that forcing users through a few extra screens in order to address privacy settings is not inappropriate. While CIPPIC has noted above the deficiencies it perceived in this process, the Transition as a concept could provide an effective mechanism for gaining express user consent at signup. Inserting a similarly designed process into the current signup flow would hardly be intrusive. The new settings could be contained in a single screen. Facebook can even include and explanation of its privacy controls as part of this page, as long as this explanation is accurate.

To ensure proper consent, these settings should be defaulted to 'Only Me', so that Facebook can be certain any disclosure it makes are further to express opt-in consent of its users. Such a mandatory privacy setting screen could look something like this:

A guide to privacy on Facebook

Understand and control how you share information

Privacy on Facebook

Privacy is built around a few key ideas: You should have control over what you share. It should be easy to find and connect with friends. Your privacy settings should be simple and easy to understand.

On Facebook, there are three basic levels of privacy: **Friends**, **Friends of Friends**, **Everyone**.

What does sharing with 'Everyone' mean?

- Information shared with 'Everyone' will be available not just to everyone on Facebook, but to everyone on the Internet.
- Information shared with 'Everyone' will be available to all Facebook enahnced application and website developers.
- Information shared with 'Everyone' will be available to search engines for indexing.
- Facebook enhanced applications and websites will be able to display any information shared with 'Everyone' in any way, without limitation.

Select your privacy settings

Please take a few minutes to review your privacy settings below. By default, these are set not to share your personal information with anyone. This will impact on your ability to connect with your friends and on their ability to learn more about you. Facebook recommends that you adjust your privacy settings now, so that your friends will be able to find you and see information you post on the site. Facebook has some recommendations that will help your friends find you and learn more about you.

Recommended Settings

- You should make your Facebook Search Results available more broadly so that your friends on Facebook can find you. We suggest you adjust this setting to 'Everyone on Facebook'.
- You should adjust many of your other settings to 'Only Friends' so that your friends on Facebook will be able to see the items you post and learn more about you.
- Some information may be more sensitive or persoanl. For such information, Facebook recommends that you create custom limited profiles of specific friends who will have access.
- You will be able to readjust these settings at any time by visiting your privacy settings.

Editing your settings

The Privacy page is designed to make it easy to edit your settings. Any changes you make will go into effect immediately. You can select a privacy level or choose to customize your privacy. For example, you may have some information that you only want your family to see. You can easily do this by creating Friend Lists from the Friends page and selecting "Custom Setting" any time you set your privacy.

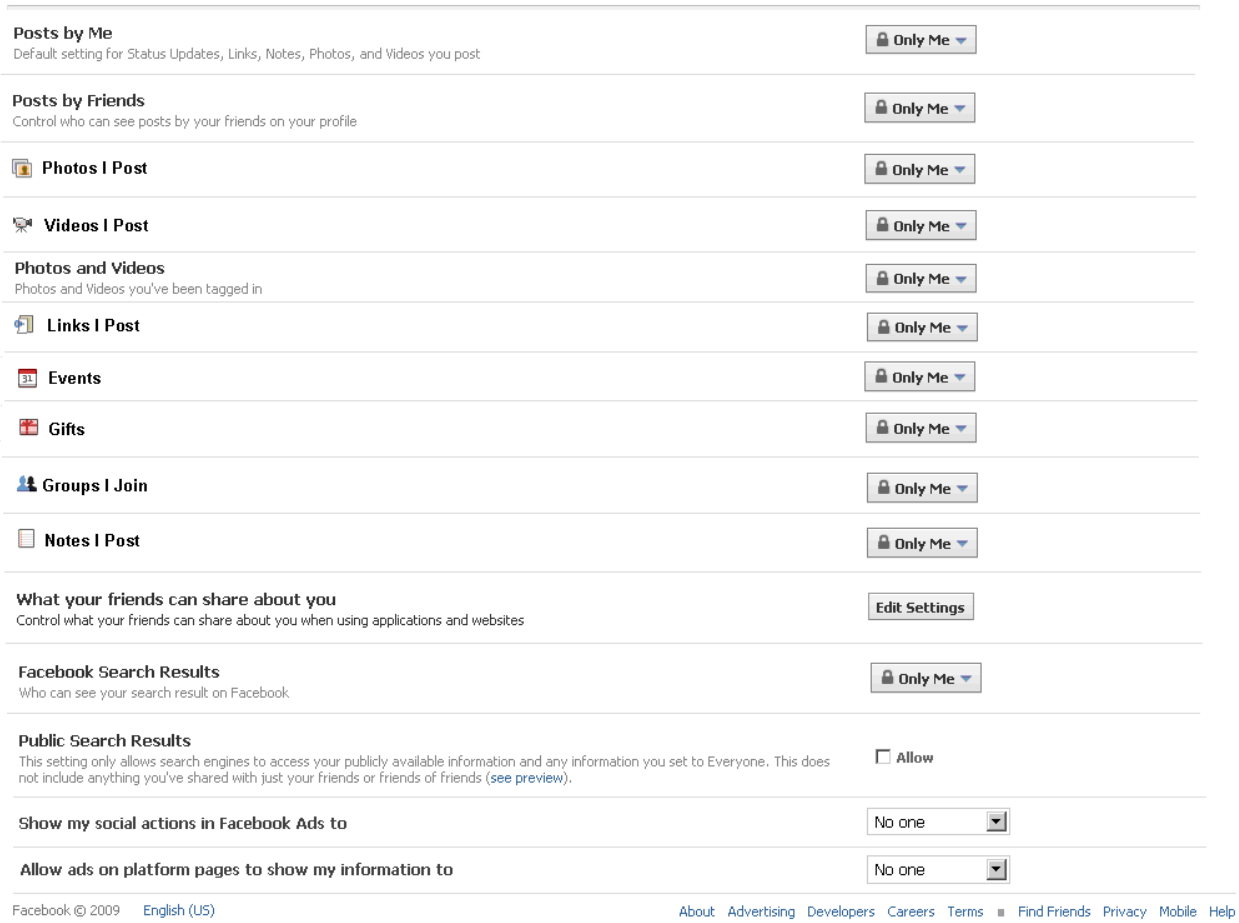


Figure 8 – Mandatory Privacy Signup Screen – Visualization[109]

Those would address the majority of Facebook's current default settings and ensure that its users are making choices with respect to how their information will be disclosed.

Facebook has additionally developed a mechanism to address any remaining privacy settings such as those relating to profile and contact information. Facebook now includes small lock icons in its contact information input screen. These locks provide users with a non-intrusive, readily accessible manor of changing their contact information from the defaulted 'Only Friends' if they wish to share that information more broadly. It is not clear to CIPPIC why Facebook does not already include similar controls as part of its other input screens.

CIPPIC suggests that this 'lock' mechanism could easily be adopted so as to get express user consent without intruding at all on the user signup experience. The information input screens would look like this:

[109] Visualizations in Figure 8 and Figure 9 composed of various screens and features taken from www.facebook.com.

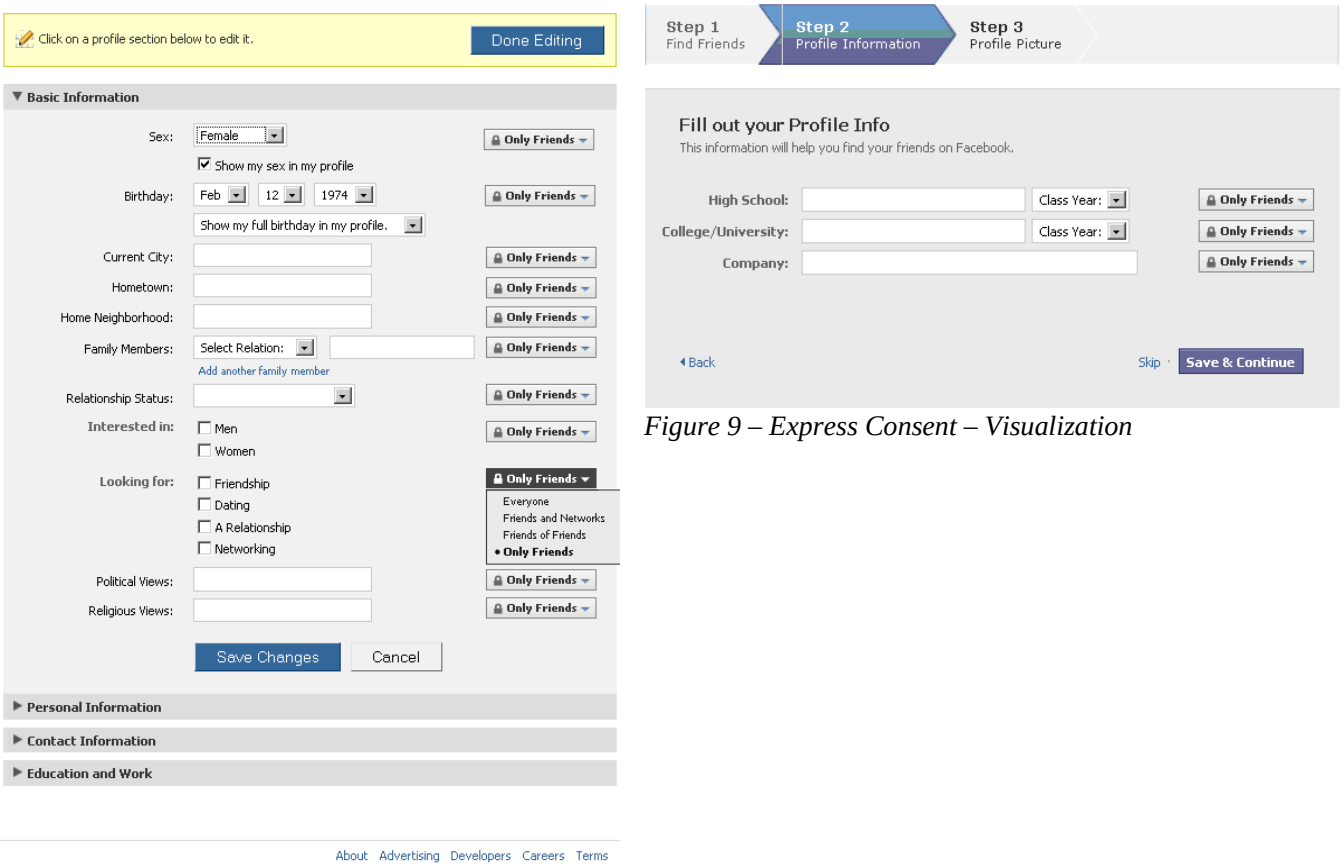


Figure 9 – Express Consent – Visualization

As before, the settings should, ideally, default to 'Only Me'. Only in that way can Facebook be certain that it has the express opt-in consent of its users to the disclosures it makes and that it is giving it effectively empowers its users "to make their own choices about sharing personal information", as it states it wishes to do.[110] It cannot be argued that the process above will be so burdensome on new users as to make deter them from signing up. It is hardly more intrusive than Facebook's Transition was on the user experience, and increases the signup process by only a single screen or 20%. If, as Facebook claims, "many users do wish to be searchable" or to share the intimate details of their lives with 'Everyone', then with such simple controls in place there will be nothing preventing them from doing so upon signup. If, as CIPPIC suspects, few users will take the time to customize these settings in any case, then the incentives are in place for Facebook to provide its users with later opportunities to share more broadly.

Regardless, the current defaults are not in line with reasonable expectations and as such are in violation of the Finding as well as, in particular, Principles 4.2.3, 4.3.2 and 4.3.5 of PIPEDA. Users are not aware that under the current scheme much of the information they provide Facebook will be shared with 'Everyone' or 'Friends of Friends'. Nor are the default settings consistent with what they would reasonably expect them to be. In this respect, Facebook must restore its pre-Transition 'Only Friends' defaults and, in addition, opt users out of public search. Under such conditions, users will have a sense of who they are sharing with, as they will be asked to approve

[110] Finding, *supra* note 1 at para. 66.

any new 'friend' before that friend can gain access to their information. Given the current drastic disconnect between Facebook defaults what a reasonable person would find acceptable in the circumstances, CIPPIC is of the view that Facebook is currently in violation of s. 5(3) as well.

In addition, CIPPIC contends that there are no longer any practical limitations preventing Facebook from getting express opt-in consent for any of its sharing. Given the highly sensitive nature of the information its users entrust it with, CIPPIC believes that in order to comply with Principles 4.3.4, 4.3.5 and 4.3.5 it must gain such consent in a manner similar to that suggested above.

Potential Violation	**Requested Fix**
Facebook's current process for new users does not gain express user consent and subjects users to default settings far out of line with their reasonable expectations. It is therefore in violation of Principles 4.2.3, 4.3, 4.3.2, 4.3.4, 4.3.5, 4.3.6 as well as s. 5(3) of PIPEDA.	▪ Alter the signup and information input flow screens as suggested above in order to ensure users provide express opt-in consent to Facebook disclosures; ▪ Alternatively, change default settings to ones that users would reasonably expect – only friends for most settings and opt-in for public search;

III. Control – Forcing users to share information

Recent changes to Facebook have also significantly reduced the level of control users are able to exert over how and when it will disclose their personal information. Facebook has designated a significant amount of information as 'publicly available', creating confusion over the capacity of users to control some while removing that capacity altogether with respect to other items of data. In addition, Facebook has bundled together categories of information, often in unintuitive ways, and forced users to share all or none of the data captured by them. Finally, Facebook has diminished or removed the capacity of users to control what and to whom actions on Facebook and enhanced applications and websites will be disclosed.

User control over information is an essential component of privacy as it is protected by PIPEDA and it is particularly essential in the context of social networking, where few if any disclosures can be legitimately classified as 'necessary' unless the user expressly desires them. The diminished user control that has resulted from the Transition is puzzling to CIPPIC, especially in light of Facebook comments as well as statements in the Privacy Announcements that it was intended to and has *increased* user control.[111] CIPPIC finds little legitimate justification for the lack of control Facebook currently provides its users.

A. Publicly Available Information

Facebook has recently designated a fairly broad category of information as 'publicly available information'. Its privacy policy explains in a bullet point near the top of the page:

> 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

[111] Kirkpatrick, "The Facebook Privacy Debate: What You Need to Know", ["Kirkpatrick, Privacy Debate"] ReadWriteWeb, February 18, 2010, online at: <http://www.readwriteweb.com/archives/facebook_privacy_explanation_debate.php>, quoting Chris Kelly, then Chief Privacy Officer, Facebook. See also, Privacy Announcement, *supra* Figure 1: "We're making some changes to give you more control of your information and help you stay connected."

> available to everyone, including Facebook-enhanced applications, and therefore do not have privacy settings. You can, however, limit the ability of others to find this information through search using your search privacy settings.[112]

Its Help FAQ supplements this definition as follows:

> **What is considered publicly available information?**
> Publicly available information includes your name, profile picture, gender, current city, networks, friend list, and Pages. This information makes it easier for friends, family, and other people you know to connect with you.
>
> Publicly available information is visible to people visiting your profile page, and Facebook-enhanced applications (like applications you use or websites you connect to using Facebook) may access this information. It does not allow people without Facebook accounts to contact you.[113]

Facebook's application of this designation is confusing. To begin with, Facebook states, in the bullet above, that such information does "not have privacy settings". However there are a number of settings located at various places that could be construed as 'privacy settings' and do control, to various extents, publicly available information. This in itself provides users with an incomplete picture of what they can and cannot do with respect to data of this type. Second, to the extent that Facebook has removed control over publicly available information from its users, this is problematic in that this category contains highly sensitive information. The impacts of this lack of control are potentially significant.

i. Is publicly available information indelibly public?

The answer to this question is, once again, difficult to discern as Facebook provides users with partial measures that may provide the illusion that their data is hidden. The privacy policy informs users that publicly available information is considered available to everyone and therefore has no privacy settings. This is inaccurate, as some items of publicly available information *do* have privacy controls. Users can limit search indexing of such information, or hide items of 'publicly available' information such as gender or friends lists, only in a limited fashion and through difficult to find controls not located in the privacy settings. The end result, in CIPPIC's view, is that user may be left with the impression that they are hiding some of their publicly available information, but in reality they are not.

Users can, for example, hide their 'gender' from view by editing their 'Basic Information' page and opting out of the 'show my sex in my profile'.[114] As to Friends' list, in response to substantial user complaint, this data can now be hidden by de-selecting the 'Show Friend List to everyone' opt-out on the Profile Wall home page Edit Box. Confusingly, removing other items such as 'Networks' from the Profile Wall home page Edit Box does *not* prevent 'Everyone' from seeing these. Further confusing matters, users can edit the profile pictures album privacy settings in order to make it visible to only friends, but this will have no effect on their current profile picture, even though this picture is part of that album. In spite of these controls, Facebook will continue to

[112] Privacy Policy, *supra* note 12.
[113] Facebook, "Privacy: Update to settings – What is considered publicly available information?", ["Facebook, What is publicly available?"] Help Center, online at: <http://www.facebook.com/help/?faq=16374>, (last accessed February 10, 2010).
[114] Profile>Info>Basic Information 'Edit Information'.

disclose Friends' lists and genders to 'others' such as connect website and application developers regardless of user input. In CIPPIC's view this is problematic. Reasonable users may mistakenly believe that in spite of the fact that Gender will be "available to everyone, including Facebook-enhanced applications" and that it has no privacy settings,[115] changing its privacy settings so as to not "show sex in my profile" may indeed have the impact of hiding gender from 'everyone'.

More confusing is the extent to which the Privacy Search controls can override a publicly available designation. Opting out of public search listings, for example, appears to not only remove an individual's name from indexing by public search engines, but to remove a user's entire profile from the Internet altogether. Entering the URL of an opted-out public search profile will lead to an internal Facebook error page, and Facebook will prevent logged out users from linking through to a user's profile from their profile in a public group or fan page.[116] This feature appears to do far more than preventing search engines from "access[ing] your publicly available info and any information visible to Everyone."[117]

Setting Facebook search to 'Only Friends', however, does far less, as 'everyone' can still access an opted-out users' publicly available information in a number of ways. This setting prevents Facebook's internal search engine from indexing user name and other profile attributes such as location and school. Non-Friends may still access this data in multiple ways. They can link through from a group or fan page or from the profile of an *actual* Friend of the user, for example, or, if they have the user's URL, they can link through directly. In addition, given that many Facebook URLs are formulaic (www.facebook.com/USER.NAME),[118] it may well be possible to guess URLs of specific individuals or, alternatively, to guess and test in order to gather data on random users.

For those users who have not personally selected a user name in the Account Settings>Settings tab, Facebook utilizes a Facebook ID number to generate URLs. However, this is no safety. As a recent article documented, third party advertisers can gain access to Facebook ID numbers as such numbers often leak from the site.[119] In addition, others can guess and test URL numbers to reach random profiles in order to collect information on those users. In addition, Facebook's contact importer can be utilized to mine random accounts by inserting multiple Email addresses.[120] This can currently be done, apparently, even without logging in to Facebook.[121]

---

[115] Privacy Policy, *supra* note 12, 'publicly available' bullet point.

[116] That is, entering the user's URL (http://www.facebook.com/tamir.israel) into a browser while logged out of Facebook will lead to an error page from Facebook if the User has opted out from public search settings. Alternatively, if anyone (including non-friends of friends) enters that same URL into her browser while on Facebook, it *does* grant access to the full profile in question, regardless of search result settings for either Facebook or the Public.

[117] Privacy Settings>Search, *supra* page 17, Figure 5, 'Public Search Results' caption.

[118] Mine, for example, is http://www.facebook.com/tamir.israel.

[119] B. Krishnamurthy and C.E. Wills, On the Leakage of Personally Identifiable Information Via Online Social Networks, ACM SIGCOMM 2009 Workshop on Online Social Networks (WOSN '09), August 17, 2009, available online at: <http://conferences.sigcomm.org/sigcomm/2009/workshops/wosn/papers/p7.pdf>.

[120] R. Singel, "Rogue Marketers Can Mine Your Info on Facebook", Wired, Epicenter, January 5, 2010, online at: < http://www.wired.com/epicenter/2010/01/facebook-email/>, (last accessed February 5, 2010).

[121] P. Warden, "How to harvest Facebook profiles from emails without logging in", PeteSearch, February, 2010, online at: <http://petewarden.typepad.com/searchbrowser/2010/02/how-to-harvest-facebook-profiles-from-emails-without-logging-in.htm>, (last accessed February 10, 2010).

Perhaps most disturbing, Facebook will provide a user setting up an account and adding any local high school under 'education' (recommended default: Everyone) with lists of high school students, some as young as 14, as well as their 'publicly available' and 'Everyone' information including friends lists as 'recommended friends':

Figure 10 – 'Recommended friends' from fake account[122]

Such access can be a potential treasure trove for child predators who need do no more then peruse the profiles presented to them upon signing up to get the data they need. One researcher has, apparently, already taken it upon himself to the fan page, friends, and name data of hundreds of millions of users and made it "available to the academic research community".[123]

Also, Facebook now apparently authorizes anyone with access to its API to collect the publicly available (and "Everyone") information of *any and all* of its customers, without privacy limitations and regardless of whether the user or any of her friends has interacted with the service in any way, or if her profile is hidden from search:

> by default, every application and website, including those you have not connected with, can access "everyone" and other publicly available content[124]

CIPPIC finds this troubling, but more so suggestions that such access may extend much further. Facebook seems, for example, to give external websites access to publicly available (and 'Everyone') data of any user visiting that website as long as the user is logged in to Facebook at the time of the visit:

---

[122] CIPPIC opened a fake account using a fake email address. The age was set to 14. Facebook offered no 'recommended friends' upon completion of signup. However, when a real secondary school was added under 'education', this list of suggested friends appeared. CIPPIC was able to click through to these profiles and access all publicly available and 'Everyone' data, including things these kids were interested in (fan pages), friends lists and, in some cases, family members.

[123] Kirkpatrick, Facebook's Soul, *supra* note 62.

[124] Privacy Policy, *supra* note 12.

> That means that when you visit Facebook-enhanced applications and websites you are making your Facebook information available to someone other than Facebook. To help those applications and sites operate, they receive publicly available information automatically when you visit them, and additional information when you formally authorize or connect your Facebook account with them.[125]

Meaning, if true, that any Facebook user visiting an external connect website while logged in is essentially forfeiting their 'publicly available' data to that website, including their identity.

It further appears to be Facebook's intention to broaden the category of external websites able to access such data by extending API access of this type to external non-connect websites who adopt its new Open Graph API functionality.[126]

Further, researchers have documented the ease by which external websites can de-anonymize visiting Facebook users through a basic browsing history attack.[127] Whereas before, this technique would furnish malicious websites with only limited information, they can now collect user URLs, log onto Facebook, and collect all 'publicly available' and 'Everyone' data with ease. All of this has potential to transform anonymous visits to external websites into data mining expeditions. Even if such external sites are merely provided with user name or profile ID, that is now sufficient for them to find profiles of visiting users through Facebook and collect 'publicly available' (and 'Everyone') information on all their visitors. Nor is it clear that Facebook limits these developers' ability to market based on such information or to disclose such information on their own sites (see pages 53-62, below). So, in effect, the publicly available designation appears to carry serious implications along with it.

Removing information such as 'Friends' lists' from visibility to 'Everyone' neither removes its 'publicly available' character nor its availability to developers through the API.[128] Neither does the search opt-out prevent access to such information in the ways enumerated above. However, many users may be under the impression that it does, as testing for such availability is a time consuming task. This belief will be reinforced by the more readily verifiable results of opting out of public search, which *does* hide user profiles from the Internet altogether.

In CIPPIC's view, this lack of clarity emerges from Facebook's new apparent approach to privacy, which begins with full disclaimers (information is 'publicly available' to 'Everyone') and attempts to build in piecemeal protections where it sees fit. This approach, in relation to its 'publicly available' category and its 'Everyone without privacy limitation' setting, does not leave users with a clear, meaningful and informed view of when Facebook intends and does not intend to disclose

---

[125] Privacy Policy, *supra* note 12. See pages 18-22 above for more details.

[126] Facebook Developers, "Roadmap Open Graph API", ["Facebook Developers, Open Graph API"] wiki.developers.facebook.com, last modified January 27, 2010, online at: <http://wiki.developers.facebook.com/index.php/Roadmap_Open_Graph_API>, (last accessed February 2, 2010). See section IV.C, below for more details.

[127] G. Wondracek, T. Holz, E. Kirda, and C. Kruegel, "A Practical Attack to De-Anonymize Social Network Users", February 1, 2010, to be presented at 31st IEEE Symposium on Security & Privacy, available online at: <http://honeyblog.org/archives/51-A-Practical-Attack-to-De-Anonymize-Social-Network-Users.html>.

[128] L. Magid, "How to Hide Your Facebook Friends List", CNet news, December 16, 2009, available online at: <http://news.cnet.com/8301-19518_3-10416524-238.html>.

their personal information. This in and of itself is a violation of Principles 4.3.2, 4.3.4, 4.3.5, 4.3.6 and 4.8.

ii. Facebook forces users to share too much

More troubling than the lack of clarity surrounding universal disclosure of 'publicly available' information is the lack of control over such data. CIPPIC can find no reasonable justification for forcing users to disclose information to 'Everyone' – be it other non-friend users, application developers, or other websites. Facebook can claim that providing some details such as full name and profile picture is necessary in order to help a user's friends find them. It is CIPPIC's view that users can make use of Facebook's services *without* making it easier, or even possible, for friends to find them. If a users chooses to remain so hidden, or to make her name and network but not her profile picture available so others can find her, that is her choice. Facebook cannot force users to share such information as a condition of service as such sharing is not necessary and is a violation of Principle 4.3.3, nor is it reasonable or acceptable in the circumstances.

Further, in CIPPIC's view, no more is needed for Facebook's stated purpose of identifying an individual and sending her a Friend request than that individual's name and perhaps her profile picture.[129] Anything beyond that is *not* necessary. Many of the items now designated as 'publicly available' by Facebook are far more than is necessary for identification while others can only be rationally linked to the concept of identification by thinnest of threads.

In addition, much of the information Facebook has now designated as irrevocably 'public' can be highly sensitive. Name and profile, for example, are highly sensitive if attached to comments that are politically or socially questionable in, say, a Facebook group:

Figure 11 – Screenshot – From Facebook Group: 100 Million Facebook members for Democracy in Iran – Taken January 18, 2010; names, profile pictures blurred.

Whereas before, users could limit their visibility on such pages to first name (no profile picture, no link to profile), this is now impossible. Further, following profile links on Facebook now leads to an indelible amount of information consisting at a minimum of full name, profile, networks, fan

[129] Facebook, What is publicly available?, *supra* note 113.

pages and geographic region. Given the unintuitive, difficult to locate opt-out provided for friends' lists and gender, these too will be present in many cases. Post-Transition, much of a user's 'Everyone' information will also be visible, as well as their Wall. This facilitates data mining by group or fan page on a scale that was not previously possible.

The information being disclosed, in addition, is not trivial. Facebook fan pages can be equally revealing of a user's political, social or ethical views. As noted by the Electronic Frontier Foundation, users may wish to support a cause and signal that support to a select group of their friends without, for example, letting their co-workers know of this support.[130] EPIC notes in its complaint to the FTC the risks that can emerge when statements of political support are taken out of the context in which they were initially intended.[131] Even a list of a user's friends can be extremely revealing.[132] Not to mention the less serious social embarrassment that can occur from even the most innocuous of informational items. By designating such information as 'publicly available', Facebook has put it and its users at the whims of oppressive governments,[133] of current and even potential employers (a recent study notes that 70% of employers admit to rejecting candidates based on information found online),[134] of spiteful peers or even teachers,[135] of identity thieves,[136] of child predators,[137] of commercial data miners,[138] of banks seeking to assess financial credibility of customers,[139] and of its own third party developers, to name but a few. The longer this information is exposed, the greater the threat that it will become indelibly public as it is collected in more and more databases – two examples have already emerged.[140]

While, as privacy is subjective, preferences will vary with respect to the degree an individual is willing to take such risks, forcing them to do so is, in CIPPIC's opinion, unacceptable. Further, Facebook has no legitimate purpose for taking away user control over information of this nature.

---

[130] K. Bankston, "Facebook's New Privacy Changes: The Good, The Bad, and the Ugly", Electronic Frontier Foundation, December 9, 2009, available online at:
<http://www.eff.org/deeplinks/2009/12/facebooks-new-privacy-changes-good-bad-and-ugly>.

[131] EPIC et. al., *supra* note 72.

[132] An MIT experiment revealed, for example, that it is possible to determine the sexual orientation of many individuals purely through an analysis of their friends' lists: C.Y. Johnson, "Project 'Gaydar'", boston.com, September 20, 2009, available online at: <http://www.boston.com/bostonglobe/ideas/articles/2009/09/20/project_gaydar_an_mit_experiment_raises_new_questions_about_online_privacy/>.

[133] See EPIC *supra* note 72 and Fassihi, *supra* note 72.

[134] Microsoft, "Research Shows Online Reputations Matter", Microsoft Data Privacy Day, online at: <http://www.microsoft.com/privacy/dpd/research.aspx>, (last accessed February 7, 2010). See also, I. Byrnside, "Six Clicks of Separation: The Legal Ramifications of Employers Using Social Networking Sites to Research Applicants", (2008) 10 Vand. J. Ent. L. & Prac. 445.

[135] M. Masnick, "Students Given Detention Just for Becoming 'Fans' of a Page Making Fun of Teacher", TechDirt, February 1, 2010, available online at: <http://techdirt.com/articles/20100126/0810057903.shtml>.

[136] B. Evangelista, "Too Much Info on Social Media Aids ID Thieves", SFGate, Monday 25, 2010, available online at: <http://www.sfgate.com/cgi-bin/article.cgi?f=/c/a/2010/01/25/BU581BMB2F.DTL> notes how identity thieves can piece together data such as birthplace or school name (recommended: Everyone for both) to gain access to bank accounts, etc.

[137] See previous section, and particularly page 40, Figure 10 and accompanying text.

[138] Singel, *supra* note 120.

[139] M. Finney, "Banks Mining Social Media Sites for Personal Info", abc7 News, February 17, 2010, available online at: <http://abclocal.go.com/kgo/story?section=news%2F7_on_your_side&id=7283384>.

[140] Finney (*Ibid*.) describes the operations of RapLeaf, a US company that collects online user profiles and sells these to organizations such as banks in order to help them assess debt eligibility. In addition, Pete Warden, a researcher, has collected 'publicly available' information on hundreds of millions of Facebook users and intends to make this all available to researchers and others (Kirkpatrick, Facebook's Soul, *supra* note 62).

It may wish to make it easier for users to share with people in their lives, but certainly it cannot force them to share all of this information with everyone if they do not wish to do so.

Given the potential harms that can result from Facebook's mandatory disclosures, CIPPIC does not believe a reasonable person would find it acceptable to require such broad disclosures of users. If Facebook wishes its customers to share their information more broadly, and if it believes that these users wish to do so as well, it should give them the opportunity to decide this for themselves. Principle 4.3.3 of PIPEDA requires that it gain users opt out consent for these types of disclosures, as they are not necessary for Facebook's services. In addition, as the information in question is often highly sensitive and most users would not reasonably expect it to be disclosed to "Everyone", Principles 4.3.4, 4.3.5 and 4.3.6 require opt-in consent to any disclosures of such data or, at the least, that such disclosures are limited to confirmed Friends unless express consent is gained for broader disclosures.

The only exception CIPPIC can see to this requirement is user name. However, following the model Facebook is now using for displaying comments made by users who have opted out of public search in public groups or fan pages. These comments are still indexed by Google and available on the public Internet. However, the user's last name and profile picture are removed, so only her first name is displayed:

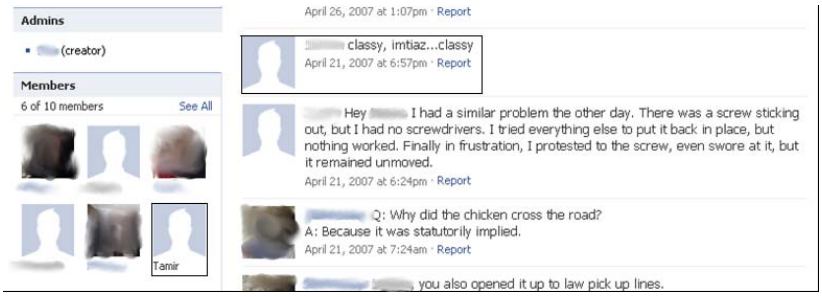


Figure 12 – Screenshot – Group accessed on public Internet – emphasis added

To CIPPIC, this demonstrates that it is not necessary to display more than a user's first name to 'Everyone' in order to participate in Facebook. Many users may wish to share more information, but they should not be forced to do so against their will.

Potential Violation	**Requested Fix**
Facebook's 'publicly available' designation is unclear and may leave many users with mistaken impressions as to how broadly their personal information will be disclosed by it. It is not gaining meaningful express consent, nor are its users able to acquire information about its policies and practices in this respect without unreasonable effort. It is thus in violation of Principles 4.3.2, 4.3.4, 4.3.5, 4.3.6 and 4.8.1.	▪ Eliminate the 'publicly available' designation and provide users with opt-in control over when and under what circumstances Facebook will disclose their data; ▪ Alternatively, eliminate the 'publicly available' category, default such information to 'only friends', and provide users with opt-in control over when and under what circumstances Facebook will disclose such data to non-friends such as third party developers;
Facebook has taken away most user control over how information it deems 'publicly available' will be disclosed and as such requires user consent to such disclosure as a condition of service with no legitimate purpose for doing so. It also fails to gain opt-in consent and discloses information it designates as publicly available in ways users would not reasonably expect. As such it is in violation of	

Principle 4.3.3, 4.3.4, 4.3.5 and 4.3.6.	

B. Facebook combines broad categories of data forcing users to share all or none

Another manner in which Facebook's recent transition has led to diminished user control over personal information is with respect to its new practice of bundling categories of information together into one privacy setting. Examples of this include its 'Posts by me' setting, its new 'Religious and Political Views', 'Family and Relationship' and 'Education and Work' categories, and its 'profile' and 'wall' photo albums, each of which now have global settings.

Posts by me is a broad category covering status updates, links, notes, photos and videos an individual posts. Users should, ideally, be provided with an opportunity to address these diverse types of posts individually. This is mitigated to some extent by Facebook's new Publisher tool which allows users to override defaults on a per object basis, but that is not sufficient, especially when default settings for objects such as the Wall photo album will override more specific, granular settings applied through the Publisher tool.[141]

This is not the case for other broad categories such as "Religious and Political Views", "Family and Relationship" and "Education and Work". Many users may not view religious and political views as similar at all. Users wishing to share what high school they went to with friends of their friends or with 'Everyone' (as Facebook recommends they do) may not wish to also share their current occupation with so broad and uncontrolled a category of people. Forcing them to do so as a condition of service (that is, saying if you want to share 'family members', you have to share 'interested in' [sexual orientation]) is unnecessary and counter intuitive.

Such bundling forces some users to share items of information more broadly if they wish to share at all. As a result, the form of consent sought in these circumstances violates Principles 4.3.4, 4.3.5 and 4.3.6, especially in light of the highly sensitive items of information being bundled together.

Potential Violation	**Requested Fix**
Facebook groups together broad categories of information, forcing users to consent to sharing item x if they are to share item y in violation of Principles 4.3.4, 4.3.4 and 4.3.5.	provide a mechanism for finer adjustments to global categorical privacy settings;

C. Facebook no longer provides user control over activity disclosure

Facebook has taken away the ability of users to control which of their actions are broadcast to their Wall (recommended default: 'Everyone'). A recent informational block appearing at the top of the profile Privacy Settings page now informs users that:

[141] So, for example, a photo posted through the 'only friends' Publisher tool privacy setting may only be visible to 'friends' on the poster's wall. However, 'Everyone' will nonetheless be able to access the photo through the posting user's wall photos album (default: Everyone). Even deleting a posted wall photo from a user's wall will not remove it from 'Everyone' availability, as it will be retained in the user's wall photos album.

Information about Recent Activity

> Whether we display a story on your profile is now controlled by the privacy of the content itself, rather than an additional setting. For example, only people who can see both your Wall, and the Wall to which you posted would be able to see a story about you writing on a friend's Wall. You cannot completely turn off recent activity stories anymore. However, if you want to remove a particular story that currently shows up, simply click the "Remove" button that appears to the right of the story after you move your mouse over it. Learn more about privacy here.[142]

Pre-Transition, users who wished to do so could hide the following Facebook activity through the Privacy>News Feed and Wall controls:

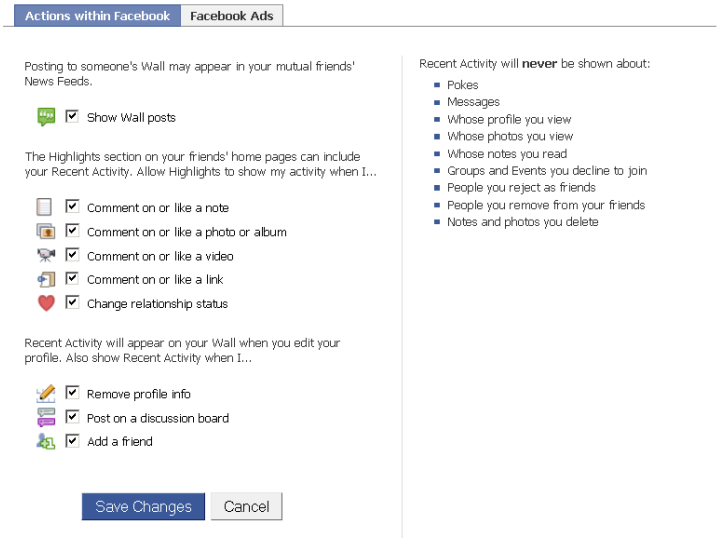


Figure 13 – Old 'Actions within Facebook' controls

Informing users that they can still remove such activity, they need "simply click the "Remove" button" is not sufficient. By the time users 'remove' such activity, it may have already been disclosed to others. In addition, it is impractical for users not wishing to allow others to follow all of their Facebook activity to remove notices of such actions one by one. Users should not be forced to share all of this Facebook activity as a condition of service. Someone should be able to change, for example, their relationship status without notifying 'Everyone' or even anyone for that matter. Such information can be sensitive, and implying consent to disclose it to 'Everyone' from the action itself is not a reasonable form of consent in the circumstances. It therefore violates Principles 4.3.4, 4.3.5 and 4.3.6.

Far more troubling, Facebook appears to apply this approach to certain types of third party applications as well. Much application activity and, in the future, Connect website activity can be posted to user's Wall. However it is not possible to limit visibility of specific developer activity to a sub-set of those able to see one's Wall (a limited profile friends list, for example).[143] This is especially problematic as locational information is incorporated into Facebook to greater

[142] Facebook, Privacy Settings>Profile, "Information about Recent Activity", Popup at top of page, January 18, 2010.
[143] C. McCarthy, "Facebook App Privacy: It's Complicated", CNet News, December 22, 2009, online at: <http://news.cnet.com/8301-13577_3-10420499-36.html>, (accessed January 18, 2010).

degrees.[144] Such information can be quite sensitive and disclosing it to 'Everyone' through Facebook can lead to harm. An example of the potential issues is FourSquare, which discloses real-time user location to FourSquare approved contacts only by default. When a user connects FourSquare to Facebook and permits it to post to her Wall, these locational real-time updates will now be available to everyone who can see that user's Wall (recommended default: Everyone). And the user apparently has no capacity to limit that disclosure to a smaller subset of individuals able to see her Wall. The purpose of services such as FourSquare is to share location with a select list of individuals, not with all a user's Facebook contacts or 'Everyone'. By forcing users to share such locational updates with anyone who can see a their Wall, Facebook is also not gaining the appropriate form of consent as required by Principles 4.3.4, 4.3.5 and 4.3.6.

Additionally, Facebook has removed the ability of users to hide their 'add me as a friend' button. This button has a privacy control (Privacy Settings>Contact Information), but can now only be set to 'Everyone' or 'Friends of Friends'. Users should be given the choice of whether they wish to provide other users the opportunity to request to be added as a friend. Some may wish, for example, to avoid spam. Others may wish to avoid having to reject 'friends' who are not real 'friends'. In CIPPIC's view, forcing users to either ignore or accept 'add friend' requests is revealing of their intention towards those 'friends'. The proper form of consent to displaying the 'add friend' button under Principles 4.3.3 and 4.3.4, then, is one that permits users the option to hide it from everyone.

Finally, Facebook has taken to disclosing to friends what applications and games a user has added, as well as when such applications and games have last been used:

[144] *Ibid.*

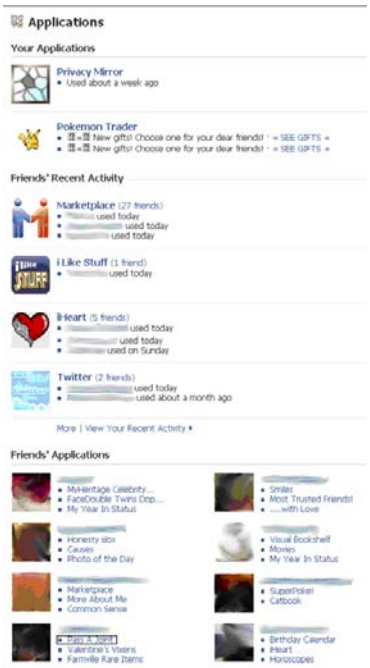


Figure 14 – Applications Dashboard, emphasis added

Applications can be quite revealing. Many users will not want all of their friends to know every time they play a game or take a Facebook quiz. There is no legitimate purpose to force them to do so as a condition of service, and as such this new Facebook of feature violates Principles 4.3.3 and 4.3.4, 4.3.5 and 4.3.6.

Potential Violation	**Requested Fix**
Facebook forces users to consent to disclosing Facebook activity to all those able to see their 'Wall' as a condition of carrying out that activity, and is therefore not acquiring the proper form of consent required under the circumstances by Principles 4.3.4, 4.3.5 and 4.3.6.	Return user control over what activity will and will not be displayed on the Wall;
Facebook is requiring those users who wish to share application-generated actions with some of their friends to also share these with everyone who has access to their wall and this is therefore not a reasonable and appropriate form of consent as required by Principle 4.3.4, 4.3.5 and 4.3.6.	Provide users with more granular controls over who Facebook will disclose application generated actions, especially with respect to locational data;
Facebook no longer allows users to hide their 'add me as a friend' button from everyone, and thus uses an improper form of consent with respect to resulting disclosures of information, in violation of Principles 4.3.3 and 4.3.4.	Add an 'Only me' option to the existing 'add me as a friend' privacy setting;
Facebook's new Applications Dashboard informs friends what applications and games a user is interacting with and when she has last done so as a condition of service and is thus an improper form of consent in violation of Principles 4.3.3, 4.3.4, 4.3.5 and 4.3.6.	Provide users with an opportunity to opt-out of being displayed in the Applications/Games Dashboard, either globally or on a per-Applications basis;

IV. Facebook Enhanced Applications and Websites

In its settlement with the Privacy Commissioner, Facebook undertook to ensure "improve[d] consent and safeguards around third-party application developers' access to users' personal information." While, under the terms of the settlement, Facebook need not comply with this obligation until September 2010, CIPPIC believes some of the recent changes on the site will make it difficult for Facebook to comply with its undertaking. A number of the problematic documents referred to in this section have emerged on Facebook quite recently, and most form part of its "Roadmap Principles", announced in October, 2009.[145] The Roadmap applies to all developers of Applications or Connect websites and seems to be aimed at bringing Facebook into compliance with the developer-specific segments of the Finding.[146] It and its subsidiary documents appear to not yet be binding on developers because, as Facebook states, "adapting to certain increased requirements may take some time."[147] The Roadmap goes on to ask developers to familiarize themselves with the new requirements, and that a compliance deadline will be forthcoming. It is not clear what privacy protections are offered users in the meanwhile, which is especially problematic in light of the new broad 'Everyone' and 'publicly available' information categories now in effect on Facebook. Regardless, it does appear that these documents will form the basis of Facebook's response to the Finding. Given that, CIPPIC believes that it would be productive to point out some issues it has come across with these documents now, so that any future measures taken by Facebook in refining or adding to this 'Roadmap' will be built on solid ground.

The Transition put in place a new general approach to privacy. It begins with seemingly limitless user consent to treat certain informational items as 'publicly available' to 'Everyone' – to be imported and exported "without privacy limitation". A genuine attempt to treat data as 'without privacy limitation' would be an egregious transgression of data protection laws, especially given the broad range of sensitive information now 'classified' or 'recommended' to such treatment by Facebook. In acknowledgment of this, Facebook attempts to stem the informational tide that would result from such limitless disclosures with piecemeal privacy controls, through the method by which it makes information available to developers and others, and by contractual terms. The result is that 'publicly available'/'Everyone' information is at times protected to certain extents, while at others treated as truly 'without privacy limitation'. Users – even those diligent enough to explore Facebook privacy in detail – are faced with limitless disclosures followed by lists of often conflicting reassurances, to the extent that it is often difficult to tell precisely what will be disclosed when, to whom and under what circumstances. Confusion aside, CIPPIC views the piecemeal protections *currently* in place on Facebook as wholly in adequate in mitigating the initial 'limitless' consent extracted from users.

---

[145] Facebook Developers, "Roadmap Principles Policies and Verification", ("Facebook Developers, Roadmap Principles") "wiki.developers.facebook.com, online at: <http://wiki.developers.facebook.com/index.php/Roadmap_Principles_Policies_and_Verification>, (last accessed January 20, 2010). The Roadmap refers to the 'Developer Principles and Policies' (Facebook Developers, "Developer Principles and Policies", ["Facebook Developers, Principles and Policies"] last revised December 1, 2009, online at: <http://developers.facebook.com/policy/>, (last accessed January 20, 2010)) which includes the SRR, (*supra* note 71) the 'Principles' and the 'Policies' contained in the Developers Principles document itself. The Roadmap additionally includes a number of examples, which are also incorporated into the Developer Principles through a hyperlink.

[146] Facebook Developers, Roadmap Principles, *supra* note 145.

[147] *Ibid*.

But this is just one facet of the problem. Facebook's new approach to privacy *in toto* appears inherently flawed from a privacy protection. It attempts to reverse the entire data protection scheme put in place by PIPEDA and other privacy legislation around the world. Such data protection begins with the assumption that information is private, belongs to the individual, and cannot be collected, used, disclosed or unreasonable retained without the individual's knowledge and consent. Privacy on Facebook now *begins* with user consent to 'everything' 'without privacy limitation', then provides such limitations where it sees fit. Granted, users come to Facebook to share their personal information, and perhaps some tailoring of data protection rules to this reality is necessary. However, the wilful sharing occurs in a specific context – people come to share with their friends. They do not wilfully share 'without privacy limitation'. Adopting a privacy starting point that ignores this reality is doomed to fail, in CIPPIC's opinion. Facebook will never succeed in plugging all the holes in the proverbial information dam that 'publicly available to Everyone' designations cut. Even if it does so to a reasonable extent, users will be required to track down each plugged hole one by one before truly understanding what is happening with their information. It is for these reasons that data protection norms start with targeted user consent to specific purposes, not obligations on organizations to protect information on their user's behalf.

Nowhere is the failure of Facebook's new approach more evident, in CIPPIC's view, than in the context of application and connect website developers. CIPPIC's specific concern is that this new approach as it currently stands will make it difficult for Facebook to meet its obligations under the Resolution, the Finding and PIPEDA generally. Specifically, Facebook committed to:

- "improve[ing] consent…around third party application developers' access to users' personal information";
- "implementing significant changes to its site (namely, retrofitting its API) in order to give its users granular control over what personal information developers may access and for what purposes"; and
- adopting technical measures to ensure that third party developers will only be able to access information they are authorized to access.[148]

CIPPIC is no longer certain post-Transition Facebook is capable of meeting these requirements. Much of this emerges from the new 'limitless' information categories, but there are other issues as well, as articulated below. Primarily, our concern is that 'publicly available to Everyone' data can be accessed with ease through a user's profile URL, which is developers can currently get with ease. In addition, Facebook appears to be expanding its developer capabilities to external websites and to other entities such as owners of Fan pages. These developments raise additional potential issues, in CIPPIC's view.

With the addition of 'Everyone' and 'publicly available' settings, it becomes far more difficult to 'improve consent' gained by developers. Such consent was too broad at the time of the Finding.[149] If it is, as Facebook's current materials imply, to permit developers to access all 'publicly available' and 'Everyone' data without limitation, CIPPIC suspects developer consent may get even *broader* post Transition. In addition, Facebook relies on ambiguous terms it does not

[148] Resolution, *supra* note 107.
[149] Finding, *supra* note 1 at paras. 151, 193.2.

adequately define in explaining to developers what they are and are not authorized to do.[150] This confounds disclosure that is already unclear

A. Privacy, one piece at a time - does it work?

There are a number of issues related to clarity of consent and what contractual limitations Facebook places on developer access to user data – especially, but not limited to 'publicly available' and 'Everyone' information. As noted above, Facebook's new post-Transition approach to privacy beings with limitless consents and attempts to supplement these where it deems appropriate and necessary with specific contractual limits. This approach is analogous to sticking fingers in the proverbial bursting dam and, in CIPPIC's view, as effective. The resulting problems, some of which have been canvassed above, are especially salient in the context of developer access to user data. CIPPIC is concerned that the limitless disclaimers Facebook collects with respect to disclosures to developers are not sufficiently counteracted by the piecemeal contractual restraints it then attempts to put in place. The result is that it authorizes developer collection, use and disclosure of information for non-legitimate purposes, but does not permit users opportunities to opt-out from these purposes. In addition, as Facebook's notification requirements currently stand, CIPPIC is concerned developers, and especially connect website developers, will not sufficiently notify users as to how they intend to collect, use and disclose personal information requested from Facebook. Piecemeal privacy protections to the contrary are simply not sufficient as they currently stand.

i. Privacy – now 'publicly available without limitation'

Facebook's new privacy documents appear to grant developers of applications and connect websites potentially limitless access to all 'publicly available' and 'Everyone' information. Its new 'publicly available' designation is described as follows in a bullet point near the top of its privacy policy:

> Certain categories of information…are considered publicly available to everyone, including Facebook-enhanced applications, and therefore do not have privacy settings. You can, however, limit the ability of others to find this information through search using your search privacy settings.[151]

Its new 'Everyone' privacy setting is described as such:

> **"Everyone" Privacy Setting.** 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…If you delete "everyone" content that you posted on Facebook, we will remove it from your Facebook profile, but have no control over its use outside of Facebook.[152]

From these descriptions alone, it appears as though such data is "considered publicly available to everyone, including Facebook-enhanced applications" and "may be imported and exported by [Facebook] and others without privacy limitation." 'Others', presumably, includes developers.

[150] Facebook Developers, Open Graph API, *supra* note 126.
[151] Privacy Policy, *supra* note 12.
[152] *Ibid*.

In addition to these extremely broad disclosures, Facebook additionally notifies users in a new privacy settings page ('learn more about what you share when using applications and websites' ["Applications>Learn More"]) that:

> When you visit a Facebook-enhanced application or website, it may access any information you have made visible to Everyone...as well as your publicly available information…The application will request your permission to access any additional information it needs. [153]

This strongly suggests that developers need not 'request your permission' before accessing such data. Additionally, in describing privacy and developers, the privacy policy states that:

> by default, every application and website, including those you have not connected with, can access "everyone" and other publicly available content.[154]

As a starting point, at least, it appears that Facebook seeks authorization to disclose 'Everyone' and 'publicly available' data to any and all developers without limitation. Facebook's terms of use *do*, however, place some limitations on these releases. CIPPIC is of the view that these limitations do not have any tangible effect in limiting the broad consent now attached to 'publicly available' and 'Everyone' information.

ii. Form of Consent – what are developers authorized to access and how?

CIPPIC does not believe it does. The primary contractual limits Facebook places on developers are found in the Statement of Rights and Responsibilities ("SRR"), to which Facebook, developers and users are all privy. In particular, s. 9.2 of the SRR states:

> Your access to and use of data you receive from Facebook, will be limited as follows:
> 1. You will only request data you need to operate your application.
> 2. You will have a privacy policy or otherwise make it clear to users what user data you are going to use and how you will use, display, or share that data..
> 3. [sic.] You will make it clear to users what user data you are going to use and how you will use, display, or share that data.
> 4. You will not use, display, or share a user's data in a manner inconsistent with the user's privacy settings. […]
> 9. You will not transfer the data you receive from us (or enable that data to be transferred) without our prior consent.[155]

This *appears* to limit developers to requesting only data they "need to operate" their service. It additionally requires developers to "make it clear" to users what data will be used ("going to use", not "going to collect", CIPPIC notes) and how it will be used, displayed or shared. PIPEDA requires no less – organizations are typically limited to collecting what they require as a condition of service, and must expressly state what data they intend to collect, how they intend to use and disclose it, and why.

These requirements are undermined in a number of ways that make it apparent to CIPPIC that they do not apply at all or adequately to 'publicly available' and 'Everyone' data. To begin with, they

[153] Applications>Learn More, *supra* note 51.
[154] Privacy policy, *supra* note 12.
[155] SRR, *supra* note 71, at s. 9.2.

starkly contradict the limitless consents described in sub-section i above. Second, even if they are *intended* to apply to such data, the lack of clarity around terms such as 'need to operate' is not likely, in CIPPIC's view, to adequately protect such data, especially given that developers need only 'request user permission' when accessing *other* data.[156] Third, the SRR only limits 'collection' to necessary data, but places no limits on 'use' of such data for additional, secondary purposes. Fourth, the SRR and supporting Facebook documents do not appear to place adequate limitations on further disclosure of 'publicly available' and 'Everyone' data collected by developers and particularly connect website developers. Fifth, the SRR and supporting documentation fail to adequately explain to developers the precision with which they must 'make clear' to users what information they intend to collect, use and disclose and for what purposes.

Three main concerns emerge from these issues. First, with respect to 'publicly available' and 'Everyone' data, CIPPIC is not convinced developers are in fact limited, whether in intention or in practice, from collecting all such data, regardless of whether it is 'required' to operate their service or not. Second, regardless of restrictions on collection, it is not clear that developers are prevented from forcing users to consent to *uses* and *disclosures* of legitimately collected information for secondary purposes such as advertising as a condition of service. Under PIPEDA, collection, use and disclosure of information that is not strictly necessary or primary to the service must be at least opt-out, and opt-in when sensitive. Third, CIPPIC is not convinced that, as currently phrased, developers are required to provide users with sufficiently precise notification of what they will collect. As described in the next section, CIPPIC feels these concerns, if realized, will undermine Facebook's ability to address its Resolution obligations undertaken with respect to developers.

Publicly available without limitation or necessary to operate your service?

The SRR requirement to "only request data you need to operate your application" does not appear to survive the limitless releases described in sub-section i, which state that developers need not "request"[157] 'publicly available' and 'Everyone' data, and that it will be disclosed to developers, "without privacy limitation",[158] and by any and "every application and website".[159]

CIPPIC points in particular to the notification provided in Facebook's new Privacy Settings 'Applications>Learn More' screen reproduced above, which states explicitly that applications need only "request" "additional" (meaning non- 'publicly available' and 'Everyone') information. The SRR limitation to "request" only necessary data, in light of this, appears meaningless and not even intended to apply to data of this type. It therefore appears that developers are authorized to collect such data without limitation of any kind.

If this is indeed the nature of Facebook's new privacy framework – where developers are permitted to access any and all 'publicly available' and 'Everyone' information without privacy limitation and regardless of need, then it can hardly form a basis for meaningful consent as required by Principles 4.3, 4.3.2, 4.3.3, and 4.3.4 of PIPEDA.

[156] Applications>Learn More, *supra* note 51. See note 153 above, and accompanying text.
[157] Applications>Learn More, *supra* note 51.
[158] Privacy Policy, *supra* note 12, description of 'Everyone' (see note 152 and accompanying text, above).
[159] *Ibid*. See note 154 and accompanying text, above.

Information disclosed to developers – what do they need and what can they request?

Assuming for the moment that the SRR term limiting developer information request to 'only what they need to operate their services' applies to 'publicly available' and 'Everyone' information, that term is not defined by Facebook with sufficient precision to prevent over-collection of user data by developers.

While under PIPEDA, the term 'need' is strictly defined, that term in common usage can be far broader. A recent 2007 survey found that, with respect to applications, only approximately 9.3% required more than rudimentary personal information such as name and network to conduct the strict operations of the application.[160] Many might believe they 'need' more than this to operate their service, but the Finding has held that not to be the case.[161] The ambiguous and overly broad privacy releases Facebook obtains with respect to 'publicly available' and 'Everyone' information from its users would only support any such confusion if, indeed, they do not intend to legitimize it.

CIPPIC can foresee numerous potential misunderstandings that may manifest as a result. For example, some applications or websites may have social networking components similar to Facebook, in which case the term 'need' in its broader sense can be quite ambiguous and might include information such as "interested in" (sexual orientation) or the type of relationship one is seeking (recommended defaults: Everyone). While such information may not be strictly necessary to provide the service, it could be treated as such by the developer both in practice and in the policy/notification. However this would not qualify as 'necessary' for a legitimate purpose under PIPEDA in most cases. This is reflected in Facebook's own explanation of what information it will provide developers, which states that 'Everyone' and 'publicly available' information will be available to all, but a developer seeking "any additional information *it needs*" must expressly request it.[162] Such problems are particularly salient with respect to connect websites, who may redefine 'need' based more on what may be available than on what is 'necessary'. The Digg.com example noted in sub-section iii, at pages 64-68 below is illustrative of potential issues that may arise in such cases.

A second potential problem that may arise from this unclear definition of 'need' is that some developers may find that 'need' covers verification of personal information collected from other sources. While the SRR and other surrounding documentation place clear boundaries around how a developer can convert customer information it receives from Facebook into 'Independent Data' (data with far less restrictions as to collection, use, disclosure and retention under the SRR and surrounding developer's documentation),[163] it is not clear that using Facebook-acquired data to verify 'Independent Information' acquired either from the user herself or from another source is restricted. This is problematic as, while Facebook is not premised upon an atmosphere of anonymity, other external websites or applications may be.

---

[160] Finding, *supra* note 1 at paras. 182-183.
[161] *Ibid*.
[162] Applications>Learn More, *supra* note 51 and excerpt accompanying note 153, above.
[163] Facebook Developers, "Policy Examples and Explanations/Data and Privacy", wiki.developers.facebook.com, last modified November 18, 2009, online at:
<http://wiki.developers.facebook.com/index.php/Policy_Examples_and_Explanations/Data_and_Privacy>, (last accessed January 20, 2010).

CIPPIC is especially concerned that Facebook, or many developers, will mis-classify marketing purposes as 'necessary' to operate their applications or websites. Advertising is *not* typically considered a legitimate 'need' under PIPEDA.[164] Yet, as described in the next section, Facebook clearly deems marketing to be a legitimate *use* of personal data collected. It appears to CIPPIC as though it might be considered by it, or at least by some developers, as an equally legitimate purpose for *collecting* personal data. PIPEDA requires users to be given the opportunity to opt-out of such collection, at the very least. Opt-in is preferred where the information in question is sensitive. But, for 'publicly available' and 'Everyone' information in particular, there is no requirement to 'request user permission' before collecting, if a developer deems it 'requires' such data.[165]

Indeed, in its developer materials, Facebook appears to authorize collection of data by developers of connected websites and added applications at any time (regardless of whether a connected user is logged in, or interacting with the developer at the time or not) for "internal analytics".[166] For this purpose, developers are authorized to collect the following data: "UID, first_name, last_name, name, timezone, birthday, sex, affiliations (regional type only), locale, profile_url, proxied_email, current_location, and allowed_restrictions."[167] Data collected in this manner cannot be displayed. Aside from User ID (UID), it cannot even be stored for longer than 24 hours at a time. However this can hardly be viewed as an impediment, as it can be perpetually renewed by the developer at any time if it "needs analytic information".[168] Facebook appears to approve, if not outright endorse this practice:

> **Connect Auth - What information can I use in my application once a user connects? Can I make it part of their public profile?**
>
> When a user connects, you can use information provided via the API to help provide a richer user experience to that user. You can cache this data for up to 24 hours, but may not store or transfer it. […]
>
> You should refresh your version of the data at least every 24 hours to make sure you are using the most up-to-date versions of the information.[169]

Most websites do not typically have access to such detailed demographic information on their visitors and users, nor are such analytics typically 'necessary' to provide their services. Yet Facebook appears to deem collection of data, for such purposes at least, as wholly legitimate. It is not. Further, as explained in greater detail below (on page 61), there appears to be *nothing* preventing developers from taking this temporary data, visiting Facebook, entering data such as

---

[164] Finding, *supra* note 1 at para. 130.

[165] See Applications>Learn More, *supra* note 51 and excerpt accompanying note 153, above and SRR, *supra* note 71.

[166] Facebook Developers, "Connect/Accessing User Data and Privacy Settings", ("Facebook Developers, Connect/Access Data") wiki.developers.facebook.com, last modified January 23, 2010, online at: <http://wiki.developers.facebook.com/index.php/Connect/Accessing_User_Data_and_Privacy_Settings>, (last accessed February 1, 2010), 'standard_user_info'; see also Facebook Developers, "Users.getStandardInfo", [Facebook Developers, Get StandardInfo"], wiki.developers.facebook.com, last modified January 13, 2010, online at: <http://wiki.developers.facebook.com/index.php/Users.getStandardInfo>, (last accessed February 7, 2010).

[167] Facebook Developers, Get StandardnInfo, *supra* note 166.

[168] *Ibid*.

[169] Facebook, "Platform and Developer Support: What information can I use in my application once a user connects? Can I make it part of their public profile?", ["Facebook Help Center, What can I make public?"] Facebook Help Center, available online at: <http://www.facebook.com/help/?page=888#!/help/?faq=15334>, (last accessed February 8, 2010).

profile_url (which, on its own, cannot be 'stored'), and visiting all user profiles to gather 'publicly available' and 'Everyone' information directly. Data collected in such a manner is not, in CIPPIC's view, subject to any of the restrictions Facebook places on data acquired through the API.

Under PIPEDA, users must at the very least be given an opportunity to opt out of such collection. Given that much of this data is not in any way necessary for the *actual* services performed by the developer, and that, moreover, a user will never really know when such data is 'requested', CIPPIC believes opt-in consent is necessary under Principle 4.3.4 before Facebook can authorize developers to collect such data, as CIPPIC does not believe users would reasonably expect such broad disclosures at all. Indeed, it appears to conflict directly, at least with respect to birthday, to contradict Facebook's assurances that developers will 'request user permission' before accessing 'additional information' (i.e. information not 'publicly available' or 'Everyone').[170]

What can developers to do with requested information?

While Facebook at least putatively limits information requests to 'what is required to operate a service', the only general limitation on *use* of data that CIPPIC could find is that such uses be 'made clear' to users.[171] Compare this with an older version of the SRR:

> When users add your application or connect it to their Facebook account, they give permission for you to receive certain data relating to them. Your *access to and use* of that data will be limited as follows:
>
> 2. You will only *use* the data you receive for your application, and only use it in connection with Facebook.
> 3. You will make it clear to users what user data you are going to use and how you will use, display, or share that data.
> 4. You will not use, display, or share a user's data in a manner inconsistent with the user's privacy settings without the user's consent. […][172]

In contrast to this, nothing in the new SRR appears to limit developer data usage to the primary and necessary purposes for which it was initially retrieved. It only mandates notification of such uses. Indeed, whereas marketing is typically seen as a secondary and 'non-necessary' purpose under PIPEDA, Facebook appears to deem it legitimate for developers to use (if not also collect) information for such purposes. As its connect developer materials explain:

> *Advertising Considerations*
>
> Beyond just providing a better user experience to target content and experiences to users, some of the information made available via Facebook APIs may help you better target advertisements to users. You may use this information locally within your systems to help better target advertisements, but you may not transfer this information to any 3rd party ad networks whatsoever.[173]

[170] Applications>Learn More, *supra* note 51, see excerpt accompanying note 153, above.
[171] SRR, *supra* note 71. See also excerpt accompanying note 155, above.
[172] Finding, *supra* note 1 at para. 199, my emphasis.
[173] Facebook Developers, Understanding Privacy, *supra* note 31.

Facebook's Advertising Guidelines, applicable to application developers serving internal ads on Facebook itself, take a similar view as to the legitimacy of marketing purposes:

> **Targeting**
>
> a. Any targeting of ads based on a user attribute, such as age, gender, location, or interest, must be directly relevant to the offer, and cannot be done by a method inconsistent with privacy and data policies.
> b. Ads with adult themes, including contraception, sex education, and health conditions must be targeted to individuals at least 18 years old. Platform ads should do this via Demographic Restrictions, not by obtaining user data.
> c. Ads for dating sites, services, or related content must follow these targeting criteria (does not apply to ads on Facebook Platform):
> i. the Relationship Status targeting parameter must be utilized and set to Single;
> ii. the Sex targeting parameter must be utilized and a single value of Male or Female must be selected;
> iii. the Age targeting parameter must be utilized and the age range selected must start at least at 18 years old;
> iv. the Interested In targeting parameter must be utilized and a single value of either Men or Women must be selected.[174]

Facebook's help center answers this question even more explicitly:

> **Can I use user information to better target ads?**
>
> Yes -- for your ads or content you may run and control completely within your own site. You may not in any way send user information pulled from Facebook's APIs to a third party.[175]

In CIPPIC's view, this authorized use may well apply not only to information expressly provided by user to developer, but also potentially to data requested for 'analytical purposes' (see previous sub-section). Indeed, given the legitimacy these documents seemingly confer on marketing purposes, it is not clear to CIPPIC that Facebook, or perhaps many of its developers, do not consider such purposes to be 'required' to operate websites and applications in general, and therefore an acceptable purpose for *collection* as well as use of information. All of this is wrong.

Marketing is not typically a legitimate purpose in the context of Principle 4.3.3 of PIPEDA.[176] Consent collection *and* use of information for such purposes must at the very least be opt-out, regardless of how expressly these purposes are 'made clear'.[177] Moreover, whereas Facebook requires 'user permission' for the *collection* of 'additional information' (i.e. information not 'publicly available' or 'Everyone'),[178] there does not appear to be such a requirement for secondary *uses* of data such as marketing, meaning these concerns apply to any and all information collected by developers. As much of this information will be sensitive, Principles 4.3.4, 4.3.5 and 4.3.6 users should be asked to opt-in to these secondary purposes, even where data is collected for otherwise legitimate purposes. Finally, if Facebook indeed intends to authorize such secondary

---

[174] Facebook, "Facebook Advertising Guidelines", last revised January 4, 2010, online at: <http://www.facebook.com/ad_guidelines.php>, (last accessed January 20, 2010).
[175] Facebook, "Platform and Developer Support: Can I use user information to better target ads?", Facebook Help Center, online at: <http://www.facebook.com/help/?page=888#!/help/?faq=14973>, (last accessed on February 8, 2010).
[176] Finding, *supra* note 1 at para. 130.
[177] *Ibid*.
[178] Applications>Learn More, *supra* note 51 and excerpt accompanying note 153, above.

uses, it is also in violation of its obligations under Principles 4.5 and 4.5.1 as it is not adequately informing users of the new purposes for which their information is being disclosed and used.

How may developers disclose data they have collected?

CIPPIC is additionally concerned that developers and particularly connected website developers are not sufficiently prevented from further disclosing much of the personal information Facebook will disclose to them. Our specific concern is that they may be able to disclose such data on publicly on external websites, in contexts far different from those in which it was first collected by Facebook and without sufficiently express user consent. Consistent with Facebook's new approach to privacy, the license it provides developers to make subsequent disclosures of such information begins with an all-encompassing disclaimer that 'Everyone' information can be 'imported and exported' from the site by anyone 'without privacy limitation'.[179] Publicly available information, similarly, is deemed "publicly available to everyone, including Facebook-enhanced applications, and therefore do[es] not have privacy settings."[180] Facebook then attempts to limit these broad categorical waivers on disclosure in specific ways.

As noted above, s. 9.2 of its SRR (reproduced for convenience) states:

> Your access to and use of data you receive from Facebook, will be limited as follows:
>
> 1. You will only request data you need to operate your application.
> 2. You will have a privacy policy or otherwise make it clear to users what user data you are going to use and how you will use, display, or share that data..
> 3. You will make it clear to users what user data you are going to use and how you will use, display, or share that data. [sic.]
> 4. You will not use, display, or share a user's data in a manner inconsistent with the user's privacy settings. […]
> 9. You will not transfer the data you receive from us (or enable that data to be transferred) without our prior consent.[181]

Further, its Developers Principles and Policies includes these restrictions under section III:

> Storing and Using Data You Receive From Us
>
> 1. You must not store or cache any data you receive from us for more than 24 hours unless doing so is permitted by the offline exception, or that data is explicitly designated as Storable Data.
> 2. You must not give data you receive from us to any third party, including ad networks.
> 3. You must not use user data you receive from us or collect through running an ad, including information you derive from your targeting criteria, for any purpose off of Facebook, without user consent.
> 4. Unless authorized by us, your ads must not display user data - such as users' names or profile photos - whether that data was obtained from us or otherwise.
> 5. You cannot convert user data you receive from us into Independent Data (e.g., by pre-filling user information with data obtained from the API and then asking the user to save the data). […][182]

[179] Privacy Policy, *supra* note 12.
[180] *Ibid*.
[181] SRR, *supra* note 71.
[182] Facebook Developers, Principles and Policies, *supra* note 145, at section III.

Sections 9.2.9 of the SRR and III.2 of the Developer's Principles provide strongly stated prohibitions against disclosing or 'enabling' disclosure of data to third parties, including ad networks. In addition, there are explicit prohibitions against disclosing user data in advertisements (s. III.3, Developer's Principles). In addition, Facebook requires developers to 'make it clear' to users how their information will be disclosed (ss. 9.2.2, 9.2.3, SRR) and must respect user privacy settings (s. 9.2.4).

Taking each of these in turn, CIPPIC notes to begin with that prohibitions against disclosing or 'enabling' data transfers to third parties are not prohibited outright, but made subject to explicit authorization, not from the user, but from Facebook (s. 9.2.9 SRR; s. III.2, Developers Principles). That such permission emerges from Facebook and not from users is extremely problematic in light of the overbroad releases relating to 'publicly available' and 'Everyone' information already required of users.

With respect to prohibitions against developer disclosures of Facebook customer data in advertisements, these, as well, are subject to Facebook (not user) permission. In this case, the effect is less harmful, as Facebook is presumably bound by user controls against these types of disclosures (which it states it currently does not permit).[183]

Most problematic are statements allowing developers to make disclosures as long as they gain user consent (SRR, s. 9.2.2-9.2.3; Developers Principles and Policies, s. III.3). It appears to CIPPIC that, in conjunction with the 'limitless' definitions of some data categories, these provisions can be taken to legitimize *any* retention or disclosure of such information, as long as the user is informed. As noted above, the SRR only restricts *collection* of information to what is 'necessary', but places no general restriction on subsequent use or disclosure of such data for secondary purposes.[184] Disclosure for such purposes must be opt-out, regardless of how well informed the user is. The only other direct restriction placed on public developer disclosures is users' privacy settings which, with respect to publicly available and 'Everyone' information, is more or less meaningless.

Some other limitations may indirectly prevent developers from posting user data on an external website. First, posting information on an external website may "enable" such data to be indirectly transferred to third parties such as advertising networks (as prohibited by SRR s. 9.2.9 and Developers Principles and Policies s. III.2).[185] Second, to do so would presumably require a developer to store such data on its website servers. Where such data is not designated 'storable data', this appears to violate s. III.1 of the Developers Principles and Policies.[186] Third, posting information on external websites will in most cases expose such data to public search. Where users have opted out of public search, this may violate terms requiring compliance with user's privacy settings (SRR s. 9.2.4).[187] CIPPIC is uncertain how these limitations interact with 'publicly available' and 'Everyone' designations.

---

[183] However, these controls are currently *not* located in the privacy settings, but rather hidden in the account settings. In addition, they are opt out and not opt in, as they should be pursuant to principle 4.3.4 and 4.3.6 and in light of the often sensitive information in question, the fact that these controls appear to apply to off-Facebook (i.e. connected website) disclosures, and the fact that much of the information in question has been released to the world 'without privacy limitation'. (See Account Settings>Facebook Ads).
[184] SRR, *supra* note 71, ss. 9.2.2 -9.2.3.
[185] SRR, *supra* note 71 and Facebook Developers, Principles and Policies, *supra* note 145.
[186] Facebook Developers, Principles and Policies, *supra* note 145, see excerpt accompanying note 182, above.
[187] SRR, *supra* note 71.

While it appears clear that Faebook prohibits direct transfers of data developers receive from it, it is less clear the extent to which it prohibits indirect transfers. The Developers Principles and Policies appears to absolutely prohibit 'giving' data received from Facebook to any third parties, including advertising networks.[188] It is not clear to CIPPIC that this would include merely making it available on an external website. Third parties are not, in that case, explicitly 'given' information, though, certainly, it would not be difficult in that case for them to collect it. The SRR offers greater protection, restricting 'enablement' of data transfer without Facebook consent.[189] However, Facebook does *not* make clear that such consent must be express, and given the limitless descriptions of 'Everyone' and 'publicly available' information, it would not, in CIPPIC's view, be unreasonable for a website developer to believe it *has* consent with respect to such data.

Additionally, while Facebook requires developers to respect privacy settings, it is not clear the extent to which it envisions public search opt-out to be included in this requirement. Facebook's API architecture, for example, has built in mechanisms to inform developers about user privacy settings so these can be respected. However, it appears that developers are not provided with a list of settings. Facebook provides developers with a specific data request command – 'Users.getInfo' – with built-in privacy settings, that is to be used when a developer wishes to disclose collected information on its website or application.[190] When a Facebook user (Bob) is viewing a connect website, a developer wishing to display another user (Alice)'s data to Bob will request Alice's information with the Users.getInfo command. It will include in that request Bob's unique session parameter identifying Bob to Facebook, as well as a list of data it wishes to display to him. Facebook will only return, in these cases, information Alice has authorized Bob to see through her privacy settings.[191]

What happens, however, if a developer wishes to display information 'without privacy limitation'? Facebook explains, in various places:

> "You may not display any of this data outside the user's specified privacy settings which control exactly what other users can see a piece of information. This setting ranges from everyone, to all friends, or even just a selected group of friends. The APIs have ways to help you determine this – see the implementation details below. If you do not want to display information conditionally, you should only use information available to everyone."[192]

> "The session key will determine exactly which information will be returned based on what the viewing or active user has access to see. If the current viewer is not signed in, you can use "null" as the session parameter and get information available to **everyone**…"[193]

---

[188] *Ibid*., at s. III.2.

[189] SRR, *supra* note 71.

[190] Facebook Developers, Users.getInfo, *supra* note 55. Not to be confused with Users.getStandardInfo, *supra* note 166, which provides greater data, but is not to be 'displayed'.

[191] *Ibid*. See also, for more details, Facebook Developers, Connect/Access Data, *supra* note 166:

> You can access most all information for a user of your application when you have an active session for that user, and a limited amount of data that is considered publicly viewable if you do not have an active session. For data about other users that you wish to display to an active user, you must request this using the session key of the active user which will determine what information is available for that user to view. Friends usually have greater access to each other's information than strangers.

[192] Facebook Developers, Understanding Privacy, *supra* note 31.

[193] Facebook Developers, Connect/Access Data, *supra* note 166, emphasis in original.

> "In addition, if you are ever displaying information about one user to another user, you must use the viewing user's session key to request the data about the person being viewed. This will determine whether or not the viewing user has access to see the information. In the case where the viewing user is not connected with Facebook, use "null" for the session key, and you will be able to access public information."[194]

The Users.getInfo command can be requested by developers at any time, and the information contained therein can be displayed to any random website visitor, regardless of whether she is a Facebook user or not. If she *is* a Facebook user, the Users.getInfo request will disclose any and all 'Everyone' and 'publicly available' data. If not it is limited to: "UID, first_name, last_name, name, locale, current_location, affiliations (regional type only), pic_square, **profile_url**, and sex."[195] It appears as though a 'null' request will display all "everyone" data on that list, which, post-Transition, includes much of that data. There is no indication that a public search opt-out will be signalled to requesting developers.

Another, non-API method of accessing data (FQL) appears to return *all* "information available to **everyone**" when sent with a null session.[196] Again, this appears to now include all 'publicly available' and 'Everyone' data and there is no indication that a public search opt-out is accounted for.

Data acquired in this manner is subject to Facebook's "Storable Data" policy – meaning much of it may only be kept for 24 hours at a time.[197] Of course, since session-less (null) display data can be re-requested any time anyone views a website (including a search engine), this is, once again, a fairly meaningless restriction. More to the point, however, the storable data policy appears to apply only to "data…receive[d] from Facebook".[198] This appears limited to data 'requested' from Facebook through API, FQL or FBML – that is, to data provided by Facebook in response to automated data request commands. Post-Transition, however, developers no longer need to 'receive' data from Facebook to find out more about their users. They can merely visit the user's profile pages directly to gain their 'publicly available' and 'Everyone' data, as long as they can find it. As noted above (page 39), there are countless ways to access user data now on Facebook.

All a developer needs to do so is, really, to know who its users are, or their profile URLs. CIPPIC notes to this effect that the sessionless Users.getInfo API command referred to above provides developers with Facebook users ID (UID), first name, last name and, particularly, *user profile URLs*.[199] CIPPIC can find nothing to prevent a developer from accessing Facebook, taking profile URLs of users who have visited its site within the last 24 hours, for example, and collecting publicly available and 'Everyone' data directly from the user profile itself. Indeed, there is apparently *nothing* to stop developers from crawling *all* Facebook public profiles, creating their own *internal* database of now publicly available data (as one researcher has already done),[200] and

---

[194] Facebook Help Center, What Can I Make Public?, *supra* note 169.
[195] Facebook Developers, Users.getInfo, *supra* note 55.
[196] Facebook Developers, Connect/Access Data, *supra* note 166, emphasis in original.
[197] Facebook Developers, Storable Data, *supra* note 57.
[198] *Ibid.*, and see also Facebook, Principles and Policies, *supra* note 145, s. III.1.
[199] Facebook Developers, Users.getInfo, *supra* note 55.
[200] Kirkpatrick, Facebook's Soul, *supra* note 62.

merely matching incoming users against this. CIPPIC can find no limitation against then further displaying all this data in association with whatever actions the user has taken on its site. Information acquired by such means would not be subject to the storage restrictions, or any restrictions, really. But, disclosed in new contexts in this way, it can be extremely damaging and might, if harvested directly from within Facebook, effectively bypass user controls such as the public search opt-out.

CIPPIC's concern is that, if a website chooses to collect and disclose data in this manner, it is not prevented from doing so by Facebook's terms of use or piecemeal protections. In such circumstances, the disclosure Facebook is facilitating – not just by making data 'publicly available' to 'Everyone' on its site, but by doing so on other external sites, in different contexts and potentially associated with other actions on those sites, and without express or even opt-out user consent – is truly 'without limitation' and in violation of Principles 4.3, 4.3.2, 4.3.3, 4.3.4, 4.3.5 and 4.3.6. CIPPIC does not believe users are currently aware that any developer they interact with is potentially capable of gaining such data and disclosing it in association with their actions on its site. While the site remains subject to its own privacy policy and to PIPEDA generally, CIPPIC is not certain that these will be sufficient in and of themselves to prevent the types of collections, uses and disclosures contemplated here.

iii. Quality and Clarity of Consent – what must developers tell users?

Regardless of whether Facebook mandates the appropriate form of consent (opt-out/in for unnecessary data and purposes), it must still ensure that developers meaningfully inform users of their data practices if it is to meet its own disclosure consent obligations. To this effect, Facebook now requires developers to "make it clear to users what user data [they] are going to use and how you will use, display, or share that data."[201] This requirement will not, as it currently stands, lead to sufficiently informed consent, in CIPPIC's view. Nowhere does the SRR specify the level of precision with which developers must make this 'clear' and, further, it appears that Facebook deems privacy policies to be an appropriate medium for such notification as opposed to time-of-collection notification. Second, as noted above, Facebook putatively limits developers to requesting data 'required to operate their services'.[202] Nowhere, however, does it define the term 'require' to its developers, and it appears to take an expansive view of this term in its developer materials. Third, it is not clear the extent to notification requirements apply to data collected manually, directly from Facebook profiles (as opposed to data 'requested' from Facebook), in the manner described above. None of this is conducive to meaningful notification, especially with respect to 'publicly available' and 'Everyone' information. These issues are especially problematic in the context of connect website developers, as illustrated in the Digg.com example below.

To begin with, it has been CIPPIC's experience that, in crafting privacy policies, service providers will opt for broad imprecise language in order to provide themselves with maximum flexibility. Typically, this might be sufficient, particularly where the user is providing data to these service providers directly. A policy may state, for example, "we will collect demographic data such as gender and date of birth from you and use it only for internal analytical purposes". What makes this acceptable in many cases is that the user will be aware of what information she provides the

[201] SRR, *supra* note 71, s. 9.2.2.
[202] *Ibid*.

organization – she will be the primary source of that data and will therefore know precisely what it is collecting. Here, though, it is Facebook making the disclosures. Often the user will not even be expressly aware of what data is being provided and when. For this reason, it is necessary to ensure that developers, and especially connect website developers, itemize each item of data they intend to request from each Facebook user connecting to them and why. It is the only way users will know precisely what Facebook will disclose.

Second, it is not enough to place such notification in a privacy policy. Adding applications and connecting to websites is a quick and simple process, involving minimal flow screens and far less form filling than a typical sign up. This streamlined process is, indeed, one of the primary purposes of Facebook Connect – to provide users with a quick way to set up accounts, as Facebook informs potential developers:

> **What are the benefits of implementing Facebook Connect?**
>
> […]**Registration**
> Every website wants registration to be easy. We have 300 million users, simple registration, and robust data. By increasing traffic, user engagement, and registrations, you can grow your revenue and increase monetization opportunities.[203]

Lengthy privacy agreements are not conducive to such expedited processes. Users should be informed expressly, within the Connect or 'add application' flow screens, what items of their data a developer will request from Facebook and, perhaps, for what general purposes. At the very least, users should be provided with a list itemizing each category of their data a developer intends to request. This should not be difficult to do – Facebook could provide a form for developers to fill with data they wish to request and display it automatically to users. That is the only way to provide user knowledge of collection practices as required by Principle 4.3, under these circumstances.

Facebook's apparent misclassification of what is 'required to operate a service' will also impact on the capacity of privacy policies to properly inform users what will be requested upon connecting. As illustrated in the example in the next section, 'need' is a shifting target that, to begin with, is ambiguous in common usage.[204] Without guidance on what qualifies as 'required to operate', developers may inform users in their policies that data is required, even where doing so would not meet PIPEDA principles of legitimacy. Indeed, as noted above (pages 54-56), what guidance Facebook provides on the issue is not helpful, as it in itself supports overly broad definitions of 'need'. Disclosure of such information to developers, where not needed in the strictest sense of the term, cannot be required as a condition of service, and must be opt-out at least and preferably opt-in. But that is not in itself sufficient. As explained in our analysis of the Transition (see pages 22-23 above), providing misleading explanations of what is 'necessary' is not a solid basis for meaningful consent under Principle 4.3.2, regardless of whether it is opt-out or opt-in. Where Facebook's unclear definition of 'need' leads to developers refusing to deal with users unless certain information is provided, this constitutes a violation of Principles 4.3.2, 4.3.3, and 4.3.4.

---

[203] Facebook Developers, "Build and Grow with Facebook Connect", developers.facebook.com, online at: <http://developers.facebook.com/connect.php>, (last accessed February 12, 2010).
[204] See also, specifically: Finding, *supra* note 1 at paras. 182-183.

Third, Facebook must make it clear that its consent requirements, which will be more precise than typically required of general websites, apply to *all* information developers intend to acquire from its users. It must include 'publicly available' and 'Everyone' data. It is not clear that it currently does, as developers may believe they already *have* consent to access such data 'without privacy limitation' and without the need to 'request user permission'.[205] CIPPIC would not be surprised to find descriptions such as 'we will request any publicly available data we require to provide you with our services'. This might in fact meet Facebook's currently imposed SRR obligations to 'make things clear' to users given its limitless releases with respect to such data. It would not, in CIPPIC's view, exonerate Facebook's PIPEDA obligations to gain meaningful consent for disclosures of such data made to developers.

In addition, Facebook must ensure developers are aware that users must be provided with precise, per-item descriptions of what 'publicly available' and 'Everyone' data will be collected through direct profile access, as opposed to merely through API 'requests'. Again, developers, and even Facebook, may not feel additional notification is required for collection of this nature, as Facebook's Privacy Policy clearly states that such data may be imported and exported at will without privacy limitation.

The problem with Connect Websites – Connecting to Digg.com

Connect website developers raise distinct challenges to Facebook's existing notification requirements. CIPPIC is concerned that many connect websites will rely on their own internal privacy policies to meet these requirements instead of providing the granular, time-of-collection, per-item of information notice that is required.

An examination of a typical Facebook Connect website may illustrate our potential concerns, and we use Digg.com as a relatively innocuous example of these. Currently, the Digg connect dialogue simply informs users that 'connecting' means you "[b]ring your friends and info" to the new website. Its privacy policy supplements this information with the following:

> **Information You Provide to Us:**
> We receive and store any information you enter on our website or provide to us in any other way. You can choose not to provide us with certain information, but then you may not be able to take advantage of many of our special features.
>
> Registration: In order for you to use Digg services, such as submitting new links to the website, you must complete a registration form. As part of this registration form, we require select personal information (including your full name, city, state and e-mail address).
>
> User Profile: To allow you to express yourself beyond just the information collected during registration, we enable you to provide additional information, such as a bio, favorite URLs, and instant messaging IDs. In addition, you may choose to include photos of yourself in your profile. As indicated below, in the section titled "Sharing Your Information", you can control how your information is displayed and used.
>
> **Automatic Information:**
> We receive and store certain types of information whenever you interact with us. Digg and its authorized agents automatically receive and record certain "traffic data" on their server logs

[205] Privacy Policy, *supra* note 12, definition of 'Everyone' and Applications>Learn More, *supra* note 51, respectively.

> from your browser including your IP address, Digg cookie information, and the page you requested. Digg uses this traffic data to help diagnose problems with its servers, analyze trends and administer the website. Digg may collect and, on any page, display the total counts that page has been viewed. This includes User Profile pages.
>
> Many companies offer programs that help you to visit websites anonymously. While Digg will not be able to provide you with a personalized experience if we cannot recognize you, we want you to be aware that these programs are available.[206]

The problem with this and similar Facebook Connect notifications is that the sites in question gain personal information from their users through a number of mediums. Such policies lack a Facebook-specific section. But there is a core difference between average Digg.com users and Facebook Connect users – the former provide Digg.com with all their information directly while with the latter it is Facebook that discloses the information. This causes a great deal of confusion as to what precise items of data Digg.com and other similar websites are receiving from Facebook when a user connects.

The Digg policy quoted above refers to three categories of information – mandatory information collected as a condition of registration; additional information users provide such as "bio, favourite URLs, and instant messaging IDs"; and 'automatic information' (traffic data).

Mandatory information includes full name, city, state and Email address. Digg.com's non-Facebook Connect signup process states that it requires date of birth as well ["required for legal reasons"]. While it appears Facebook will provide some of this mandatory information upon connecting, it is not clear how much of it. For example, Facebook clearly states that it will not provide Email addresses, which Digg uses to manage user accounts:

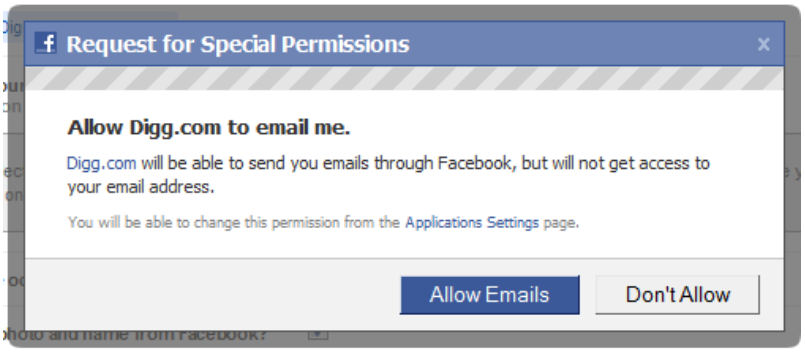


Figure 15 – Special Permissions popup

What is not clear is how Digg.com expects to manage user accounts without the capacity to contact those users. Indeed, it is impossible to either communicate with Digg.com or to delete a Facebook Connected account if one does not provide Digg.com with an Email or 'Allow Emails' through Facebook:

[206] Digg, "Privacy Policy", Digg.com, last updated September 19, 2007, online at: <http://about.digg.com/privacy>, (last accessed Jan 20, 2010).

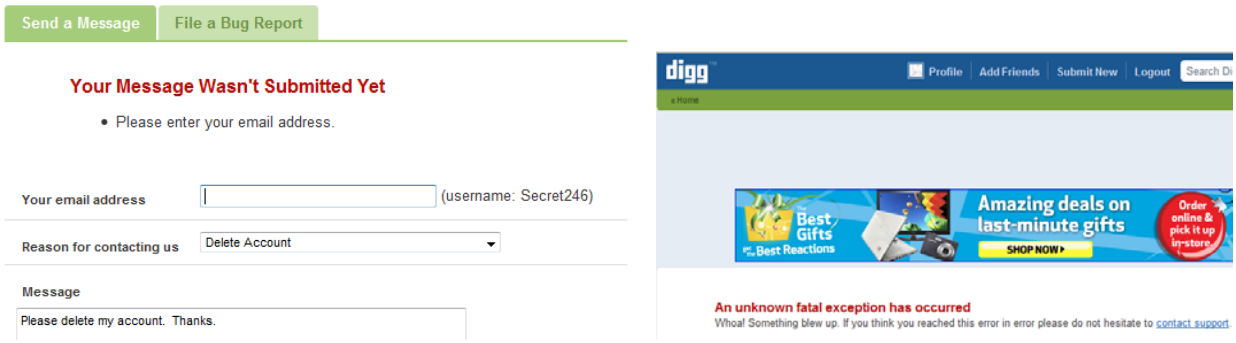


Figure 16 – Attempting to delete connected Digg account – no Email

With respect to the second category of information, optional information provided to "allow you to express yourself", much of this information *will* be contained in Facebook accounts. Much of it will be designated "Everyone" information, whether by default or otherwise, meaning Facebook purports to have user consent to disclose it to Connected websites (see below). But, since Digg's privacy policy is tailored towards specific users explicitly providing it with 'additional information', and with Facebook Connect it is Facebook that is disclosing the information in place of the users, this privacy policy does not help a user determine what information will be disclosed. In sum, while it is clear that Facebook will not provide Digg with all of the *mandatory* information it requires, it will provide some, and it is not clear how much.

While a detailed examination of a post-Connect Digg account demonstrates that not a lot of additional information is provided it by Facebook and disclosed further, this is by no means clear until *after* the connection is complete and Facebook has already disclosed the information in question. Nor is it at all clear what disclosures occur on other Facebook Connect sites.

Further, even some of what little information is collected in the Digg connect process itself is demonstrably unnecessary, as it requests user's profile names and pictures from Facebook, but allows users to opt-out of sharing these for the service itself:

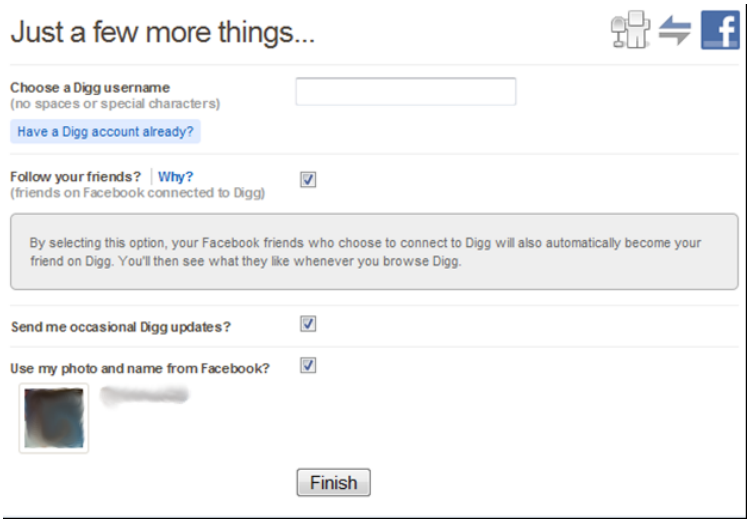


Figure 17 – Digg Connect flow screens – name and image blurred

Finally, it is not at all clear to what extent Digg.com considers the detailed profile information Facebook provides its developers for 'internal analytics' (see page 55 above) as falling within the scope of its 'Automatic Information' definition.

In conclusion, a user connecting to an external site, even one with a working privacy policy, will in many cases have no clear idea of what information is being passed along during the connect process (or thereafter). The 'publicly available' and 'Everyone' information categories serve to confound this lack of clarity, as it becomes increasingly difficult to ascertain what a developer is even authorized to collect. In CIPPIC's view, Facebook cannot base informed meaningful consent to disclose on this model without violating Principles 4.2, 4.2.3, 4.3, 4.3.2, and particularly 4.3.1 of PIPEDA.

If Facebook is to abrogate its notification and consent obligations under PIPEDA. It can either notify users directly precisely what items of information it will disclose to websites as part of the Connect dialogue, or it can require Connect websites to do so. As the Connect dialogue appears to allow for some measure of customization by the connecting website, this should not be difficult to do. In addition, the more granular controls Facebook has undertaken to provide with respect to information disclosed to application developers should be applied even more rigidly to Connect developers, as the data Facebook discloses to these may be dispersed beyond Facebook itself and to the broader web.

Potential Violation	**Requested Fix**
Facebook is not meaningfully notifying users what information it will disclose to developers upon connecting in violation of Principles 4.2, 4.2.3, 4.3, 4.3.1 and 4.3.2.	Facebook should require developers to list what items of data they intend to collect from it directly at time of collection – as part of the connect or add application flow screens;
Facebook now provides a great deal of information publicly, to 'Everyone', through its user profiles but does not make it clear that restrictions placed on information provided to developers through its API apply equally to the collection, use, disclosure and retention of data harvested	Clarify that all data protection restrictions limiting developer collection, use, disclosure and retention of user data apply equally to data acquired through direct harvesting from sources such as user profile URL;

directly from user profiles; without such clarification, developers appear authorized to access all 'publicly available' and 'Everyone' data 'without privacy limitation'; such authorization is extremely broad and in violation of Principles 4.2 and 4.3.4.	
Facebook will disclose user information to developers who 'require it to operate their service' but does not adequately prevent excessively broad definitions of 'need', resulting in refusal to deal requests for unnecessary information, which violate Principles 4.3.2, 4.3.3 and 4.3.4.	▪ Facebook should better define in its terms of use what user information its developers are able to require as a condition of service; ▪ Specifically, Facebook should clarify that 'advertising' and 'internal analytics' are not 'necessary' to operate a service; ▪ Alternatively, if Facebook wishes to permit developers to collect 'unnecessary' user data, it must require them to gain express consent before doing so, such as through its Independent data policies;
Facebook currently contractually limits developers from *collecting* user information they do not require, but fails to limit them from *using* otherwise collected information for purposes not strictly necessary to the operation of their service, in violation of Principles 4.3.2, 4.3.3, 4.3.4, 4.3.5, 4.3.6, 4.5 and 4.5.1.	▪ Facebook should clarify its SRR so as to ensure developers are limited to *using* information they collect only for the purposes for which it is collected; ▪ Alternatively, Facebook should ensure developers gain opt-out or opt-in consent for secondary uses, using Facebook's promised granular control tool;
It is not clear the extent to which Facebook authorizes connect website developers to disclose personal information of users in new contexts on their external websites and to public search engines, potentially in violation of Principles 4.3, 4.3.3, 4.3.4, 4.3.5, 4.3.6, 4.5 and 4.5.1	Facebook should clarify that connect website developers cannot disclose information gained from it on their websites and to public search without express user consent to such disclosures;

B. Can Facebook still meet its Resolution obligations?

CIPPIC has strong doubts that post-Transition Facebook is capable of meeting these requirements. In the Resolution, Facebook specifically undertook to "improve[e] consent and safeguards around third party application developers' access to users' personal information".[238] This involved clarifying Facebook's consent process to, as detailed in the Finding, better inform users as to which items of their data will be disclosed when they add an application.[239] It additionally involved "implementing significant changes to its site (namely, retrofitting its API) in order to give its users granular control over what personal information developers may access and for what purposes."[240] Finally, it involved "adopt[ing] [technical] measures" to ensure that third party developers will only be able to access information they are authorized to access.[241]

These commitments were made in response to concerns, voiced more fully in the Finding, that Facebook was providing application developers effectively unrestricted access to far more

[238] Resoultion, *supra* note 107.
[239] Finding, *supra* note 1 at para. 207.
[240] Resolution, *surpa* note 107.
[241] *Ibid*.

personal information then required to operate their applications.[242] As noted in Facebook's developer materials:

> Facebook users create rich profiles with Facebook in order to share information with their friends. We offer rich privacy settings that allow people to feel secure sharing highly personal information including interests, thoughts, and contact information. Given this rich set of control, a significant number of Facebook users have filled out information on their profile. […]
>
> Once a user connects to your site or application, you are able to access and use information that the user has shared on their profile to provide a richer experience. In addition, you can access information about the user's friends and others on behalf of the user of your app – basically any information that is available to that user on Facebook can be used through the lens of your site or application.[243]

CIPPIC's concern is that, given potential holes in Facebook's new approach to privacy highlighted in the previous section, user's "highly personal information" will be leveraged to applications and websites that do not provide the same feelings of security that prompted users to share their information with Facebook in the first place.

i. Improving quality of consent – will users be better informed post-Transition?

In response to this requirement, Facebook has included a term in its SRR requiring developers to 'make it clear' to users what data will be used and how it will be used, displayed or shared.[244] As noted in section A.iii above, CIPPIC does not view this as sufficient, particularly in light of the challenges raised by Connect websites and the new limitless 'Everyone' and 'publicly available' information categories.

At the time of the Finding, users adding an application were notified its developer could 'pull their profile information, photos, friends' info, and other content it required to work'.[245] Given the current breadth of 'Everyone' and 'publicly available' information definitions, which can be imported and exported from Facebook without privacy limitation, CIPPIC would not be surprised if developers attempting to meet their obligations to 'make it clear' to users what information the intend to request will merely state:

- We will request any publicly available information we require to better provide you our service'; and
- We will acquire your permission before requesting any additional information from Facebook.

This approach would, indeed, track Facebook's own, which informs users that developers will only need to ask their permission before collecting non-'publicly available' or 'Everyone' data.[246]

---

[242] Finding, *supra* note 1 at para. 200.
[243] Facebook Developers, Understanding Privacy, *supra* note 31.
[244] SRR, *supra* note 71, at s.9.2.2.
[245] Finding, *supra* note 1 at para. 151.
[246] "Applications>Learn More", *supra* note 51.

Given the lack of clarity surrounding what developers can legitimately 'require' to work in Facebook's current SRR and surrounding documents, CIPPIC does not believe such results will add sufficient clarity to meet Facebook's resolution obligations in this sense, as well as the Finding and Principles 4.3, 4.3.2 and 4.3.4 of PIPEDA.[247] What is necessary, particularly in the case of connect website developers, is an itemized list of every piece of data an application intends to collect and an explanation of why it requires these. In addition, as noted in our discussion of the Transition, any consent based on inaccurate descriptions of 'necessity' or purpose is not meaningful. Facebook should clarify what a developer may 'require' to operate its services. This is, as far as PIPEDA is concerned, a fairly narrow amount of data for most websites. It should not in all cases include real name, birthday, gender, locale, and especially profile URL which, essentially, is now a potential window to any and all 'publicly available' and 'Everyone' data (see pages 54-56 above). Nor does it include collection for marketing purposes. Facebook must additionally clarify that this notification requirement applies to any information collected directly from a user's profile URL as well as to data 'requested' from Facebook's API. Where a developer wishes to collect user data that is *not* strictly necessary for operating its service, Facebook should require it to indicate as such in its user notifications.

Finally, given the streamlined add application and particularly the connect process, it is not enough to merely notify users in a privacy policy of data practices, as currently required in s. 9.2.2 of the SRR.[248] Some time-of-collection notice is, in CIPPIC's view, required by Principle 4.3.4 as part of the add application and especially the website connect flow screens – at the very least an itemized list of data categories the developer intends to collect. The Digg.com connect process referenced above is a good example for how this can be done, as it provides users with the option, upon connecting, of whether to display their real names and profile pictures on Digg or not.[249] Ideally, it would be modified so that it is presented to users *before* the developer is given any data, not after, and to utilize opt-in instead of opt-out consent. This should be the case for every and any item of data a developer wishes to collect from Facebook but does not require in the strictest sense to operate its service.

ii. Granular User control – will it protect publicly available data?

It is also not clear how Facebook envisions its obligation to "give its users granular control over what personal information developers may access and for what purposes" to manifest in light of the above.[250] As noted above, it appears to CIPPIC that Facebook currently authorizes developers to access *all* 'publicly available' and 'Everyone' data at any time without the need for user permission. If Facebook's promised granular control is to meet its obligations under the resolution it must, in CIPPIC's view, apply to any and all user data disclosed to developers. The only legitimate exception can be for data without which the developer could not provide the service in question to its users. A granular control that simply does not apply to 'publicly available' or 'Everyone' data would be insufficient. CIPPIC found a number of indications suggesting that this will indeed be the case with Facebook's promised tool.

[247] Finding, *supra* note 1 at para. 207. See also para. 193.3.
[248] SRR, *supra* note 71.
[249] See Figure 17 at p. 67 above.
[250] Resolution, *supra* note 107.

First, the newly added Applications>Learn More page expressly informs users that developers will not need to ask user permission before requesting 'Everyone' or 'publicly available' data.[251] Facebook developer documentation further appears to reinforce this notion when informing connect developers that, while they must respect user privacy settings, if they wish to display information 'without condition', requests should be limited to 'public' and 'Everyone' data.[252] Indeed, as explained above in detail, it is not at all clear that Facebook does not intentionally authorize developer collection of such data 'without privacy limitation'.[253]

Second, Facebook's Sessionless API requests appear to provide developers with profile URLs for their users. Such URLs may only be stored for 24 hours at a time, however since developers can request such URLs at any time, without any direct user interaction, this is no serious roadblock. Once a developer has this URL, it can access any user's profile directly and collect whatever 'publicly available' and 'Everyone' data it wants, whenever it wants it.[254]

Third, Facebook permits its newly implemented granular wall Publisher tool to be undermined by the same publicly available designation or 'Everyone' setting in other contexts. An item, such as a Wall photo, posted to the Wall under increased granular privacy ('only friends') will still be visible to 'Everyone' if a user has not changed her 'Wall Photo album' defaults from 'Everyone' to 'Only Friends'.[255]

Finally, an 'Everyone' privacy designation completely undermines express user decisions to opt categories of data out of developer access. Facebook provides users opt-out controls intended to remove items of data from developer access in situations where a user's friend has interacted with the developer, but the user has not. Above these controls, however, is a clear statement that Facebook will allow developers access to 'publicly available' and 'Everyone' data regardless of the item-specific express opt-outs provided on that page (see Figure 18, below).[256]

In addition, Facebook's commitment was to provide more granular control over "what personal information developers may access *and for what purpose*."[257] As noted above (pages 56-62), while Facebook purports to contractually limit developer data collection to 'what is required', it does not even attempt to limit subsequent uses to the legitimate purposes for which information is initially acquired.

---

[251] Applications>Learn More, *supra* note 153.

[252] Facebook Developers, Understanding Privacy, *supra* note 31: "Users may choose to make some of this data public, which you can then use to display publicly as well"; and "You may not display any of this data outside the user's specified privacy settings which control exactly what other users can see a piece of information. This setting ranges from everyone, to all friends, or even just a selected group of friends. The APIs have ways to help you determine this – see the implementation details below. If you do not want to display information conditionally, you should only use information available to everyone."

[253] See section IV.A.ii and specifically pages 54-56 above.

[254] See section IV.A.ii, above and particularly at page 61.

[255] The Wall photos album is automatically created the first time a user posts a photo to her wall. In CIPPIC testing, the wall photos album reflects the default for wall postings. Photos posted to it under more granular protection (Only Friends) using the new Publisher tool will still be visible to 'Everyone' through the album.

[256] Facebook, Privacy Settings>Applications and Websites>What your friends can share about you ["Facebook, What your friends can share"], (accessed January 11, 2010) [see Figure 18 below].

[257] Resolution, *supra* note 107.

If developers wish to collect data for purposes other than those strictly required to operate their services, they can do so. But in such cases, granular controls must at the least (Principle 4.3.3) permit users to opt-out of such data. Opt-in is by far preferable given the breadth and sensitivity of the information involved, and in CIPPIC's view required by Principles 4.3.4, 4.3.4 and 4.3.6. As noted in the Finding:

> Facebook is not using the appropriate form of consent for its disclosure of users' personal information to third-party application developers…given the potential sensitivity of users' information, express opt-in consent should be sought in each case.[258]

Designating certain information categories as 'publicly available to everyone' does not abrogate Facebook's obligation to get the appropriate granular form of consent for such secondary purposes. These granular opt-out/opt-in controls must additionally apply to any subsequent use or disclosure a developer wishes to make of otherwise legitimately collected data for secondary purposes such as marketing or internal analytics. If Facebook is to live up to its Resolution obligations, the Finding and PIPEDA, its promised granular controls must extend at least this far, in CIPPIC's opinion.[259]

iii. Technical measures must cover all data

CIPPIC is concerned that whatever technical measures Facebook is preparing in response to its obligations under the Resolution, these will not be sufficient if it reflects the misperceptions highlighted above – particularly if such safeguards will not protect 'publicly available' and 'Everyone' data with the same diligence as other data.

Facebook has not provided any public details as to how it intends to address the effectively "unlimited" access it currently provides all developers to the data of users, their friends, and even friends of friends.[260] Its roadmap refers to forthcoming "enhancements" to the extended data permissions model it currently operates. It makes no mention, however, of any upcoming technical safeguards. To date, Facebook has used the extended permissions model to prevent API access to certain types of data such as information in a user's stream, access to her inbox, or offline access to user data. Developers are blocked from accessing such data until and unless they acquire express extended permissions for doing so.[261] It appears, from its description in the Applications>Learn More page as though Facebook may address the technical safeguards issues by making 'publicly available' and 'Everyone' data available to all developers while placing all other data behind extended permission walls which require 'express consent'.[262] This will not be

---

[258] Finding, *supra* note 1, at para. 193.3.

[259] See Resolution, *supra* note 107 and Finding, *supra* note1, at para. 193.3.

[260] Finding, *supra* note 1 at para. 198. Facebook explains to its developers how they may gain 'friends of friends' data in its Help Center FAQ:

> **Is it possible to run an FQL query that will return the friends of a friend?**
> There is currently no means to do this, but there is a way to find mutual friends.
> Try using: SELECT uid1 FROM friend WHERE uid1 IN (SELECT uid2 FROM friend WHERE uid1=A) AND uid2=B

Facebook, "Privacy: Update to settings – Is it possible to run an FQL query that will return the friends of a friend?", ["Facebook Help Center, Getting Friends of Friends"] Help Center, online at: <http://www.facebook.com/help/?page=888#!/help/?faq=15224>, (last accessed February 12, 2010).

[261] Facebook Developers, "Extended Permissions", wiki.developers.facebook.com, last modified January 29, 2010, online at: <http://wiki.developers.facebook.com/index.php/Extended_permissions>, (last accessed February 7, 2010).

[262] Applications>Learn More, *supra* note 153.

sufficient to meet Facebook's requirements under the Resolution and the Finding. While this is speculative, as CIPPIC has seen no clear indication from Facebook how it intends to address its safeguards obligations in light of the new privacy settings. CIPPIC would like to point out that, in its opinion, this will not be an adequate solution and requests clarification from Facebook that any technical solution it provides will cover any and all information a user has not expressly authorized a developer to access. If Facebook does not intend to apply such safeguards to 'publicly available' or 'Everyone' information, it will remain in violation of Principles 4.7, 4.7.1 and 4.7.3, as developers will still have "unauthorized access to personal information that they do not need."[263]

In addition, Facebook documentation suggests that developers can potentially access other types of data as well. Its explanation of its platform includes the following description of data developers may access:

> Examples of the types of information that applications and websites may have access to include the following information, to the extent visible on Facebook: 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, your relationship status, your dating interests, your relationship interests, your network affiliations, your education history, your work history, your course information, copies of photos in your photo albums, metadata associated with your 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 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 friends, your social timeline, notifications that you have received from other applications, and events associated with your profile.[264]

Further, its Developers Principles and Policies stats that developers "must not track visits to a user's profile, or estimate the number of such visits, whether aggregated anonymously or identified individually",[265] implying developers have access to such data. It appears from this document and from a recent article that Facebook may be collecting and retaining such data and further that developers could potentially access or collect similar data.[266] If developers do, indeed, have access to data such as your 'social timeline' or a list of visitors to a user's profile, CIPPIC believes granular controls as well as technical safeguards should apply to these types of data as well.

Potential Violation	**Requested Fix**
Facebook's new notification requirements do not appear to meet its obligation, undertaken in the Resolution, to improve clarity of consent gained by developers for	Require developers to inform users, at time of collection (during the connect or add application flow screens), each category of data (including

[263] Finding, *supra* note 1, at para. 200.

[264] Facebook Developers, "Facebook Platform", last modified August 28, 2009, online at: <http://developers.facebook.com/about_platform.php>, (last accessed February 12, 2010).

[265] Facebook Developers, Principles and Policies, *supra* note 145 at s.II.5 b.

[266] P. Wong, "Conversations About the Internet #5: Anonymous Facebook Employee", The Rumpus, January 11, 2010, available online at: <http://therumpus.net/2010/01/conversations-about-the-internet-5-anonymous-facebook-employee/>, (last accessed January 20, 2010). CIPPIC cannot confirm the authenticity of claims made in this article, but merely asks that Facebook confirm or deny whether this is indeed its practice to retain such data and whether and on what grounds it is made available to developers.

information it discloses to them;	'publicly available' data) they intend to collect directly from Facebook and why;
It is no longer clear that Facebook intends its promised granular control tool to apply to *all* user data disclosed, including 'publicly available' and 'Everyone' data, as required by the Resolution;	Clarify that the granular control tool will allow users to opt-out/in of each item of data disclosed to a developer that is not required for the service that developer is offering;
It is no longer clear that Facebook intends its promised granular control tool to apply to *purposes* for which the information is collected, as stated in the Resolution;	Clarify that the granular control tool will permit users to opt-out/in of any secondary uses a developer intends to make of collected data;
It is not clear that the technical safeguards Facebook intends to provide to meet its Resolution obligations reflect a proper understanding of what developers can and cannot legitimately access;	Ensure that the promised technical safeguards apply to *all* personal information, including publicly available and 'Everyone' data and user activity data, as well as means of accessing such data;

C. What developers get before you interact with them

In CIPPIC's view, Facebook discloses far too much information to developers that a user has never interacted with, or interacted with only minimally. Developers appear under some circumstances to have carte blanche access to all 'publicly available' and 'Everyone' data of all users at any time, regardless of whether a user has ever interacted with their services. Facebook appears to provide developers with 'Everyone' and 'publicly available' information in situations where minimal interaction has occurred, such as when a user does no more than visits their site. Finally, Facebook will disclose even more information when a user's friend, but not the user herself, has interacted with an application or website. In none of these cases, in CIPPIC's view, is there adequate knowledge or consent on the part of the users.

i. Users who have not interacted with a developer at all

Post-Transition, it appears that any and all developers are given access to 'publicly available' and 'Everyone' data of all users, regardless of whether they or their friends have ever interacted with a particular developer. There are a number of reasons to believe this is so. To begin with, 'Everyone' and 'publicly available' data is defined in a manner that leaves little room for any limitations.

> by default, every application and website, including those you have not connected with, can access "everyone" and other publicly available content.[267]

Facebooks 'learn more' about developer information access asks users to "[p]lease note that applications will *always* be able to access your publicly available information…and information that is visible to Everyone".[268]

Facebook will release some information only when it is being requested in the context of an active session – that is, where the data request is accompanied by a session key, which Facebook will only provide while the user is actively interacting with the developer's service or website.[269] In addition, Facebook permits developers to access some data without a session key. As long as a

[267] Privacy policy, *supra* note xii.
[268] Applications>What Friends Can Share, *supra* note 256, my emphasis. See also Figure 18 on p. 81 below.
[269] Facebook Developers, Authorizing Applications, *surpa* note 54.

developer has access to a user's ID (UID), it can, at any time, get the following information on the user:

- uid
- first_name
- last_name
- name
- locale
- current_location
- affiliations (regional type only)
- pic_square
- profile_url
- sex[270]

In addition, a developer can acquire a user's Fan pages,[271] profile pictures,[272] or any other sessionless information Facebook chooses to make available in the future.[273] This information, it seems, can be requested of any user by anyone with access to the API at any time. All that is needed is the User's UID.

In addition, once a developer has a user's profile URL, it can access the user's profile directly and manually collect all 'publicly available' and 'Everyone' information. While all this data is subject to Facebook's Storable Data policies (meaning only UID can be stored for longer than 24 hours), as noted above (see page 55), this policy can be bypassed with ease – the information can be renewed every 24 hours, or re-obtained directly from the user's profile URL. UID is easily acquired in many situations, such as when a friend of a friend 'interacts' with an application or connect website.[274]

As all this data is now considered 'publicly available' and, frankly, can be accessed by anyone anyways, in and of itself it is no more troubling than in general that developers can access it as well. Nonetheless, developers should not be authorized to do so if they do not require the information. Users should be able to prevent such access through opt-out/opt-in mechanisms (as described above, at pp. 37-45). Principles 4.3, 4.3.3, and 4.3.4 demand no less. Facebook's materials and API calls serve to legitimize and facilitate such collection. CIPPIC's greatest concerns, however, are raised by situations wherein some interaction, no matter how tenuous, has occurred between a user and a developer.

ii. Users who have only minimally interacted with a developer

Facebook will permit developers to access publicly available user information in contexts that reveal a great deal about the individuals in question. In particular, Facebook notes that merely

[270] Facebook Developers, Users.getInfo, *supra* note 55
[271] Facebook Developers, "Pages.getInfo", ["Facebook Developers, Pages.getInfo"], wiki.developers.facebook.com, last modified on January 23, 2010, online at: <http://wiki.developers.facebook.com/index.php/Pages.getInfo>, (last accessed February 12, 2010).
[272] Facebook Developers, "Fb:profile-pic", wiki.developers.facebook.com, last modified November 20, 2009, online at: <http://wiki.developers.facebook.com/index.php/Fb:profile-pic>, (last accessed February 12, 2010).
[273] CIPPIC would like confirmation that Facebook does not plan to extend sessionless calls to include all 'publicly available' and 'Everyone' data.
[274] Facebook Help Center, Getting Friends of Friends, *supra* note 260.

visiting a developer is sufficiently strong an interaction to justify providing that developer with user information:

> To help those applications and [connect websites] operate, they receive publicly available information automatically when you visit them, and additional information when you formally authorize or connect your Facebook account with them.[275]

Additionally, Facebook's description of 'Everyone' data informs users that such information "may be associated with you outside of Facebook (such as when you visit other sites on the internet)".[276] In addition, Facebook's developer documentation states the following:

> **What you Get Before a User Authorizes Your Application**
>
> When a user who hasn't authorized your application visits your application's canvas page, Facebook sends you some user data and lets your application take a number of actions. The following occurs:
>
> - Facebook passes the viewing user's ID to your application.
> - Facebook passes the viewing user's friend UIDs.
> - You can call any API method that doesn't require a session.
> - You can get user information that's publicly available via search (except for any users who have chosen to not display a public search listing).
> - You can use FBML tags to show a user's profile pic and name based on the UIDs passed.
> - You can publish Feed stories by the user via Feed forms.
> - You can send requests on behalf of the user via request forms.[277]

At least with respect to application developers, it is clear that Facebook indeed intents to identify any user visiting the application's page. A process Facebook refers to as "Automatic Authentication" automatically provides developers UIDs for each and every user who visits the developer's canvas page. Facebook considers UID 'Storable Data', meaning it is not subject to 24 hour storage restrictions placed on other data.[278] As noted above, a broad range of data can be accessed, directly or indirectly, once the UID parameter is provided. Indeed, through Automatic Authentication, Facebook provides direct (as opposed to indirect) methods of accessing more information, such as friends' lists (which includes the UID of each friend).[279] Users should be able to browse applications without being identified. Identification aside, rich demographic information is being provided to developers a user may never intend to interact with. This hardly appears necessary.

---

[275] Privacy Policy, *supra* note xii.

[276] *Ibid*.

[277] Facebook Developers, Authorizing Applications, *supra* note 54. Note this document has been updated (February 4, 2010) and currently states:

> When a user who hasn't authorized your application visits your application's canvas page, Facebook sends you some user data (known as automatic authentication) and lets your application take a number of actions.

[278] Facebook Developers, Storable Data, *supra* note 57.

[279] Facebook Developers, "Automatic Authentication", wiki.developers.facebook.com, last modified February 4, 2010, online at: <http://wiki.developers.facebook.com/index.php/Automatic_Authentication>, (last accessed February 12, 2010).

Most concerning to CIPPIC, however, is the potential application of this practice to external websites. In keeping with Facebook's new approach to privacy, it asks users to authorize it to disclose information to applications *and* websites "when you visit them":

> To help those applications and [connect websites] operate, they receive publicly available information automatically when you visit them, and additional information when you formally authorize or connect your Facebook account with them.[280]

It does so in the same terms. While, currently, Facebook does not appear to provide external connect websites with UID "when you visit",[281] this portion of its privacy policy appears to authorize it to do so – without providing users with any additional notice. Needless to say, were Facebook to facilitate identification of otherwise anonymous visitors to external websites in this manner, it would be an egregious violation of PIPEDA, in CIPPIC's opinion. Such an unexpected result of browsing while on Facebook would need to be clearly and unequivocally spelt out, brought to the direct attention of users, and an opt out/opt in mechanism would need to be utilized with respect to this practice.

Even without this development, Facebook already provides external connect websites with too much user information. Specifically, Facebook provides a mechanism by which a connect developer can detect whether a user visiting its site is logged in to Facebook while doing so or not.[282] Connect websites are permitted to store this information in a cookie on the visiting user's browser, and to use that information to tailor the user experience. That is, Facebook will allow third party websites to identify which of their visitors are Facebook users who are logged in while visiting their site and to use this information to promote the connect service to those users.[283]

The current form of consent relied upon by Facebook to disclose such information is, in CIPPIC's view, inadequate. Aside from visiting a website, users have not agreed to interact with these developers in any way. The Privacy Policy disclaimers – that developers 'receive publicly available information when you visit them' – are insufficient.[284] They lack precision as they appear to cover the nearly limitless disclosures made to an application developer when a user visits its canvas page as well as the more limited disclosures made to a connect developer when a user visits its external website, all in one phrase. In order to meet meaningful consent requirements under Principle 4.3.2 and express consent requirements under Principle 4.3.3, more details are

---

[280] Privacy Policy, *supra* note xii.

[281] Facebook connect utilized a process it refers to as "Cross Domain Communication" to facilitate information exchanges. During such exchanges, all communications between a connect website and Facebook are conducted through the user's browser. This means that Facebook is able to process user-specific requests sent from external sites without providing those sites with the user's UID or giving it access to the user's Facebook cookies, or any other identifying data before a user connects to the site. See Facebook Developers, "Cross Domain Communications", wiki.developers.facebook.com, last modified January 13, 2010, online at: <http://wiki.developers.facebook.com/index.php/Cross_Domain_Communication>, (last accessed February 12, 2010). See also Facebook Developers, "How Connect Authentication Works", wiki.developers.facebook.com, last modified July 23, 2009, online at: <http://wiki.developers.facebook.com/index.php/How_Connect_Authentication_Works>, (last accessed on February 12, 2010):

> All communication is mediated by the browser. A Facebook user ID is not given unless the user sitting at the computer has authenticated to Facebook.

[282] Facebook Developers, "Detecting Connect Status", ["Facebook Developers, Connect Status"], wiki.developers.facebook.com, last modified January 29, 2010, online at: <http://wiki.developers.facebook.com/index.php/Detecting_Connect_Status>, (last accessed February 12, 2010).

[283] *Ibid*.

[284] Privacy Policy, *supra* note xii.

required. In addition, CIPPIC doubts that much or any of these disclosures can be classified as 'necessary' to providing the services in question. Indeed, upon the mere visit of an application canvas page, no service has yet been requested at all. Similarly, a visit to an external third party website does not entail a need for any Facebook connect tailored services. Not only are such disclosures unnecessary, but CIPPIC does not believe a user would reasonably expect them to be occurring. As such, Facebook must gain either opt-out or opt-in consent for its practices in this respect, further to Principles 4.3, 4.3.3 and 4.3.4. In addition, were it to begin identifying otherwise anonymous users to external connect websites, this would be a violation of section 5(3) of PIPEDA.

iii. Users whose friends have interacted with a developer

Facebook discloses too much of a user's information when a friend of that user adds an application or connects to a website. This was the case before the Transition, and it is CIPPIC's opinion that Facebook's commitments on this issue in the Resolution were insufficient to meet the requirements of PIPEDA and, indeed, those articulated in the initial Finding. This has only been aggravated by the recent changes Facebook has made, as increasing amounts of information now become available to developers through the API and otherwise in such situations. Regardless of the changes, however, it is unclear to CIPPIC how disclosing the personal information of users without consent can be justified under PIPEDA.

As much information as developers are able to gain on users in general, they are able to gain much more when a user's friend authorizes them:

> Unless you change your privacy settings, an application or website that you connect with can generally access the same information that you can see about yourself and your friends, and an application or website that your friend connects with can access the same information about you that the friend can see.[285]

Whereas an application or website added by Alice must currently 'request her permission' before accessing data set to 'friends of friends' or 'only friends',[286] this still does not appear to be the case for Alice's *friends*. Once Alice adds an application or connects to a website, there appears to be no obligation on developers to 'request permission' before accessing anything 'Alice can see about her friends'.

As stated above, CIPPIC does not believe developers or anyone else can be given carte blanche access to 'publicly available' and 'Everyone' data. This is no less the case, in its opinion, with respect to data belonging to Alice's friends who have never interacted with a given application or website. There is no basis for consent to such broad and unspecified disclosures under PIPEDA. This applies *a fortiori* to 'friends of friends' and 'only friends' data of users who have never interacted with a developer's services. Nor, from a practical perspective, does it appear defensible to offer more protection to users who *have* explicitly authorized an application than is offered to those who have *not*.

---

[285] Facebook Developers, Facebook Platform, *supra* note 264. Essentially, when a user authorizes a developer's website or application, that developer is given a session key that is linked to the user's account. This session key allows the developer to request, not only the user's data, but also any friends' or friends' of friends' data the user can see. The developer will be provided a list of User IDs (UIDs) corresponding to the user's friends, and can call those friends' data on behalf of the user. See Facebook Developers, Users.getInfo, *supra* note 55 and Facebook Developers, Authorizing Applications, *supra* note 54.

[286] Applications>Learn more, *supra* note 51.

Facebook's justifications for these disclosures were summarized in the Resolution as such:

> As for friend's data, a user can now choose if they want to share their friends' data with a particular application…Friends can limit the information they share with their friends, de-friend someone, block all applications, block specific applications or block certain information through their application privacy settings.[287]

In addition, Facebook could attempt to rely on broad statements in its privacy policy for user consent to such disclosures. CIPPIC finds none of these sufficient.

To begin with, the Privacy Policy does not currently do an adequate job of informing users developers can access their information through their friends. It provides the following description of data provided to developers:

> **Facebook Platform.** …To help those applications and sites operate, they receive publicly available information automatically when you visit them, and additional information when you formally authorize or connect your Facebook account with them. You can learn more details about which information the operators of those applications and websites can access on our About Platform page.[288]

Nowhere does this description mention the information Facebook will provide a developer when a *friend* authorizes or connects its service. This information is contained solely in a bullet further down, which explains to users that:

> You can use your application settings to limit which of your information your friends can make available to applications and websites.[289]

This is misleading as a user is never asked to provide specific items of friends' data to developers. Rather, Facebook makes such data available by default. A user currently has no option to restrict developer access to her friends' data. More details are provided in the "About Platform" page, but, in CIPPIC's opinion, this is not enough. Few reasonable users would expect Facebook to provide so much data to developers whose services they have never even interacted with. In the circumstances, notification for such broad and uncontrolled disclosure should be, at the least, extremely prominent if meaningful consent under Principle 4.3.2 is to be achieved.

Regardless of clarity, however, Facebook will not be able to provide users with sufficiently precise notification in its Privacy Policy on this issue. At best, it can prominently inform users that any time a friend interacts with a developers website, application, or even canvas page, all data visible to that individual will be made accessible to that developer. Users will still have no indication of which developer is accessing what of their data when. Such broad, unspecified disclosure can hardly meet the most rudimentary consent requirements under Principle 4.3,[290] let alone more demanding meaningful and explicit consent requirements under Principles 4.2, 4.2.3, 4.3.2 and 4.3.3.

---

[287] Resolution, *supra* note 107.
[288] Privacy Policy, *supra* note 12.
[289] *Ibid*.
[290] Finding, *supra* note 1 at para. 193.3-193.4.

Facebook's other justifications, that users can limit exposure to developers:

- through controlling friend access to data by:
  - limiting what is shared with a specific, or with all friends; or
  - de-friending friends altogether;
- through global controls permitting users to:
  - opt all data out of developer access;
  - blocking specific applications; or
  - expressly inform it not to provide certain items of data to friend's applications and websites; and
- that users consent on behalf of their friends to these data disclosures

are all without merit, as explained below.

Forcing users who wish to prevent Alice's applications and websites from accessing their data to withhold that data from Alice herself is no solution. Indeed, to ensure lack of developer access, a user would have to stop sharing with *all* of her friends. People join Facebook to share information with the people in their lives, not with developers. When deciding what information to share with a friend, the context in which that decision is made, the calculation, is whether they wish that friend to access the data, not the developers of that friend's applications. More to the point, they have no knowledge or control over the latter, only over what information they permit Facebook to disclose to that friend. De-friending someone is equally no solution. Again, when a user adds a friend, that friend's application usage practices are hardly at the forefront her consideration process. Indeed, she would have little idea of those practices. Even after adding that friend, few closely monitor application usage practices, nor is it practical for particular users to do so for all of their hundreds of Facebook friends. In neither case does the user have any meaningful idea of how her information is being disclosed and to whom, nor would a reasonable person find it acceptable in the circumstances to penalize a user by forcing them to withdraw friendship merely to avoid exposure to a friend's application developers. This is not a reasonable basis for any form of consent.

The option of blocking all applications and connect websites does not appear to be available any longer, although Facebook's privacy policy still states that users can completely remove their personal information from the API.[291] Even if available, it would be insufficient – forcing users to agree to vast uncontrolled disclosures as a condition of application/connect service does not appear legitimate within the context of Principle 4.3.3. Neither is the option of blocking specific applications sufficient. Users will simply have no idea which of the hundreds of thousands of applications and websites their friends have added in order to assess whether to block them or not. Nor would they have the time to assess every single application added by the multitude of their friends and block each individually were they aware. Additionally, there does not appear to be any readily available mechanism for blocking website developers a friend has connected to.[292] Finally

[291] Privacy Policy, supra note 12: "You can choose to opt-out of Facebook Platform and Facebook Connect altogether through your privacy settings."

[292] The Privacy Settings>Applications>Blocked Applications screen, which lists all blocked applications, only refers to applications and is triggered from the home page of the application itself. CIPPIC could not find an analogous 'block connect website' button.

Facebook allows users to prevent friends from sharing some specific items of data. But, first, this control utilized opt-out consent which is insufficient given the sensitivity of the data and user expectations.[293] Second, there is no opt-out capacity for 'publicly available' information.[294] More concerning, even if users expressly opt specific categories of information out, an 'Everyone' privacy default setting overrides that explicit opt-out, as noted on the opt-out page itself:

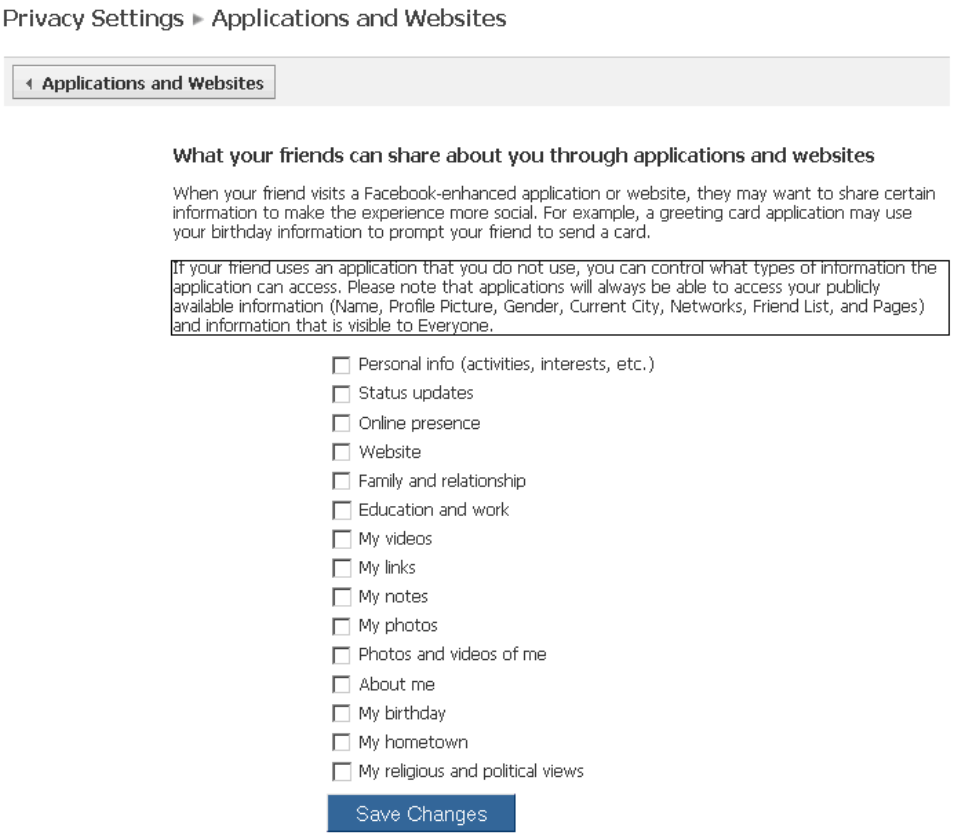


Figure 18 – Privacy Settings>Applications and Websites>Edit Settings – "Please note that applications will always be able to access your publicly available information…and information that is visible to Everyone"[295] *– emphasis added*

Finally, it appears that Facebook considers it acceptable to rely on Alice's consent to authorize its disclosure of her friend's information to applications and websites she interacts with – the Resolution notes its reliance on such consent as such: ."a user can now choose if they want to share their friend's data with a particular application".[296] Facebook's explanation of its Platform additionally states a user "can share [her] information and [her] friends' information to add a social layer to [her] experience."[297] To begin with, CIPPIC was not able to find any such optional control in the privacy settings, the application settings or within the 'add application' or website connect process. Facebook does notify users upon adding an application that developers will "pull…your

[293] See Principles 4.3, 4.3.4, 4.3.5 and 4.3.6 in particular.
[294] Privacy Policy, *supra* note 12: "by default, every application and website, including those you have not connected with, can access "everyone" and other publicly available content".
[295] Applications>What your friends can share, *supra* note 256.
[296] Resolution, *supra* note 107.
[297] Facebook Platform, *supra* note 12.

friends' info", but there does not appear to be an option to refuse or limit this. Regardless, this is no substitute for gaining the consent of the user herself.

The core of PIPEDA is that commercial organizations such as Facebook must gain the meaningful consent of individuals as to the collection, use and disclosure of their own personal information. This is to provide users with knowledge and control over their personal information in commercial settings. Gaining consent from user's friends under these circumstances provides the user with neither knowledge, nor control and cannot stand as a reasonable basis for consent. As it does not fall under any of the exceptions found in s.7(3) of PIPEDA, and as the information is collected and placed on the API in the course of Facebook's general commercial activities, Principle 4.3 applies and Facebook must gain meaningful consent directly from its users before disclosing that information to developers whose services a friend has added.

The Privacy Commissioner has consistently held that data held by a third party that is identifiable information of another is the personal information of both. In an early case, for example, it held that incoming telephone numbers in a debtor's phone account are the personal information of *both* the debtor *and* the caller.[298] In a more recent case, the Assistant Privacy Commissioner affirmed this approach, stating that an IP address used to access an Email account was the personal information of both the owner of that account and the hypothetical operator of the computer that generated the IP address.[299] In such cases, it does not appear to matter that the personal information in question is part of another's account. It remains "information about an identifiable individual."[300]

In some past cases of third party disclosure, the Privacy Commissioner has held that an organization can indirectly rely on the third party disclosing the information to gain informed, meaningful consent of the first party on its behalf. Regardless of the general acceptability of this interpretation of PIPEDA, it has been employed only in exceptional circumstances that raised specific concerns, none of which are applicable to this scenario.

In a number of early findings, for example, the Privacy Commissioner has found that credit agencies may rely on an organization requesting a credit check to gain the informed, meaningful consent of its customer – the object of the credit check – for any disclosures made by the agency in response to the request. This is less an exception to consent requirements and more a means to imply consent via the intermediary organization. The agencies were required, therefore, to exercise due diligence in order to ensure (through contractual measures) that the intermediary organization in fact gained consent from the customer.[301] It should be noted that due diligence is just that – a means to implying consent. An organization cannot rely on measures such as those adopted by the credit agencies in situations where it would be unreasonable to assume the intermediary organization in fact gained the consent from, say, a specific customer.[302] In such cases, there would be no basis for consent whatsoever. Further, implicit consent is at best an

[298] PIPEDA Case Summary #2002-99, available online at: <http://www.priv.gc.ca/cf-dc/2002/cf-dc_021202_2_e.cfm>.
[299] PIPEDA Case Summary #2005-315, available online at: <http://www.priv.gc.ca/cf-dc/2005/315_20050809_03_e.cfm>.
[300] Personal Information and Protection of Electronic Documents Act, S.C. 2000, c.5, s. 2(1), "Personal Information".
[301] See for example PIPEDA Case Summary #2003-194, available online at: <http://www.priv.gc.ca/cf-dc/2003/cf-dc_030716_e.cfm> and PIPEDA Case Summary #2003-182m available online at: <http://www.priv.gc.ca/cf-dc/2003/cf-dc_030710_06_e.cfm>.
[302] *Ibid*.

imperfect alternative to direct consent. The credit agency cases presented special challenges where it would have been wholly impractical to get consent directly from the individuals themselves, as noted by the Commissioner:

> It was reasonable for the credit agency to obtain the consumer's consent through its client businesses and not directly, given the large number of information requests it receives daily and the considerable amount of work this type of procedure could involve.[303]

In addition to this line of cases, the Commissioner has held that where a reasonable person would not find it appropriate in the circumstances to require direct consent, it is appropriate under s.5(3) of PIPEDA to permit an organization to rely on indirect consent gained through a third party. As with the credit agency cases, exceptional circumstances were required before such indirect consent was permitted. In this case, the Canadian Nuclear Safety Commission (CNSC) required nuclear power plant employees to consent to security checks on their own behalf as well as on behalf of their spouses.[304] The Commissioner held it appropriate that the onus for either gaining spousal consent to the security checks or withdrawing from employment falls upon the employee, not the spouse. The rationale in this finding again rested, even to a greater extent than in the credit agency cases, on the impracticality of achieving the eminently legitimate purpose of protecting national security without relying on third party consent in this manner. Notably, even in this case, it would not have been acceptable for the CNSC to conduct its investigation of the spouse where it could not reasonably infer that the spouse had provided meaningful, informed consent and where it did not fall under an exception in s.7(1) of PIPEDA.[305] In a circumstance where it was unreasonable for the CNSC to imply indirect spousal consent, or consent of a specific spouse, it would fall to it to dismiss the employee for failing to meet security requirements unless the employee voluntarily quit.

Turning to the situation at hand, it is difficult to see how this indirect approach, if legitimate at all, could apply to the disclosures Facebook seeks to make. To begin with, Facebook imposes no obligation (by contract or otherwise) on users to gain the informed, meaningful consent of their friends to such disclosures prior to adding an application or connecting to a website. As such, even the semblance of diligence is currently lacking in its approach to disclosures of this nature. More to the point, any such obligations it imposed on users would be a fiction at best. It would be nigh impossible for a user to gain meaningful consent from all of her friends prior to adding any application and Facebook could hardly reasonably infer that this was the case. No amount of due diligence can cure this deficiency in consent.

Nor are the practical limitations that animated indirect consent methods in previous cases present here. Indeed, it is actually *more* impractical for Alice to gain all of her friends' consent each time she wishes to add an application or connect to a website than it is for Facebook to do so directly. Under such circumstances, it is difficult to see how it could be acceptable for Facebook to shirk its consent obligations in favour of indirect implied consent.

---

[303] PIPEDA Case Summary #2003-188, available online at: <http://www.priv.gc.ca/cf-dc/2003/cf-dc_030710_08_e.cfm>.

[304] PIPEDA Case Summary #2003-232, available online at: <http://www.priv.gc.ca/cf-dc/2003/cf-dc_031001_03_e.cfm>.

[305] B. McIsaac, R. Shields and C. Klein, "The Privacy Law in Canada", vol. 1, looseleaf, 2006 (Toronto: Thomson Canada Limited, 2000-), at pp. 4-44 to 4-45. CIPPIC notes that, whereas other cases involved implied consent with respect to collection of personal information, this particularly case involves disclosure, meaning s.7(3) of PIPEDA applies, which states (my emphasis):

> For the purpose of clause 4.3 of Schedule 1, and despite the note that accompanies that clause, an organization may disclose personal information without the knowledge or consent of the individual only if the disclosure is […]

The reason Facebook is better placed than anyone to get direct consent here is that it is, in fact, the one making the disclosure. The information being disclosed has been collected by it for commercial purposes and is stored on its servers. While Alice, who is connecting to a website, may have access to her friend's information, she does not have control of it (she cannot remove it from Facebook's servers, she cannot change its privacy settings, etc.). Alice's *friends*, who *do* have control over the information, have no idea when it is being disclosed and to whom or, really, for what purpose. They are not aware that Alice has connected to a website, unless she decides to inform them. Facebook, however, is aware of all these interactions as they occur since it is the one enabling the disclosure.

Nor is it clear to CIPPIC that Facebook's purpose in making such disclosures is legitimate, except perhaps in very limited circumstances. Alice's friend, Bob, should not be forced to interact with a website or application merely because Alice has connected with it, except, perhaps, to the extent necessary to assess whether he wishes to do so (i.e. through an invitation). Even for such invitations, the developer need never know who Bob is, let alone gain access to all his data. An invitation can be sent at Alice's behest and through Facebook's architecture. The developer need never know who Bob is for him to get such an invitation. The only legitimate purpose to disclose Alice's friends to facilitate her interactions with other friends of hers who have added the application as well. This, too, can be achieved without disclosing all of Alice's friends to the developer – through a mechanism analogous to the friends.getAppUsers API method.[306] This method allows a developer to send Facebook a connected user's (Alice's) ID. Facebook will then send back IDs only for Alice's friends who have connected with that developer's particular website as opposed to all of her friends. CIPPIC does not see any need to disclose anything beyond this limited set of data to developers.

The only time a developer need know who a user's friends are is, perhaps, to match that user with friends who have also added the developer's service. But again, this matching process can be completed by Facebook itself, in a process similar to that currently employed when connect developers user the Linking Friends mechanism.[307] Given that there does not appear to be any legitimate need to provide developer access to Alice's friend's data in the first place, nor is there any practical reason why Facebook cannot directly get her friends' consent to such disclosures, nor is there any reasonable basis to imply that Alice has gotten her users informed consent to such disclosures, CIPPIC finds such disclosures a clear violation of the most basic PIPEDA consent requirements.

In CIPPIC's view, Facebook should not provide developers access to any data of users who have not directly authorized such access. It sees no justification for doing so. Users can invite their friends to participate in applications and connect websites they have added, if they so wish. Friends can then decide whether to do so or not. Without such consent, there is no justifiable reason to do so.

---

[306] Facebook Developers, "Friends.getAppUsers", wiki.developers.facebook.com, last modified November 4, 2009, online at: <http://wiki.developers.facebook.com/index.php/Friends.getAppUsers>, (last accessed February 7, 2010).

[307] Facebook Developers, "Linking Accounts and Finding Friends", wiki.developers.facebook.com, last modified October 7, 2009, online at: <http://wiki.developers.facebook.com/index.php/Linking_Accounts_and_Finding_Friends>, (last accessed January 20, 2010).

An imperfect solution for providing such functionality may be through a method similar to Facebook's current Applications>What your friends can share opt-out (Figure 18 above).[308] Such a method *must*, however, be opt-in and must additionally apply to *all* user information, regardless of whether it is currently designated 'publicly available to Everyone' or not. Nothing less is acceptable in the circumstances, and so section 5(3) of PIPEDA requires no less.

Potential Violation	**Requested Fix**
Facebook's Privacy Policy reserves it the right to provide external websites with "publicly available information automatically when you visit them"; while it does not appear to do so at this time, any such disclosures would violate section 5(3) of PIPEDA;	Facebook should clarify in its Privacy Policy that it does not, will not and can not identify otherwise anonymous users to external websites "when you visit them";
Facebook appears to authorize and facilitate developer collection of some user data for users when neither they, nor even their friends have interacted with the developer's services in any way, in violation of Principles 4.3, 4.3.3, and 4.3.4 of PIPEDA;	▪ Facebook should prevent developers from accessing user data unless a user has specifically interacted with their services, and then only with express user consent; ▪ Alternatively, if Facebook is to rely on global controls for consent, these must be opt-in, and must apply to *all* user data;
Facebook appears to disclose user data to applications and external website developers upon the mere visitation of such sites by a user, without any authorization or substantial interaction with those services and without opt-out or express user consent, in violation of Principles 4.3, 4.3.3, and 4.3.4 of PIPEDA;	▪ Facebook should not provide developers with user information simply because a user has viewed their website or canvas screen; ▪ Facebook should ensure its otherwise anonymous users cannot be identified by developers upon visiting their external websites or canvas screens;
Facebook fails to get user consent before disclosing personal information to developers when a friend of that user adds an application or connects to a website, in violation of Principle 4.3 and section 5(3) of PIPEDA;	Facebook should gain opt-in express user consent before disclosing *any* information to applications a user's *friends* have interacted with, but with which a user has not.

D. Facebook and the open web

CIPPIC has some additional concerns regarding what the increasingly blurry line between Facebook Fan Pages, connect websites, and external websites in general. To begin with, Facebook's description of what data fan pages can access on their 'fans' is inaccurate or at best incomplete, post-Transition. Second, in order to provide external website functionality such as Fan Box Widgets and Facebook connect functions, Facebook receives a great deal of the browsing history of its users. CIPPIC would like its assurances that such data is not tracked, and that it will not be tracked, except perhaps in anonymized and aggregated format, in the future.

Third, CIPPIC is concerned regarding future implementations Facebook has proposed. Recently, Facebook announced in its RoadMap a proposed Open Graph API,[309] which will allow third party websites to interact with Facebook users as if the site were actually on Facebook. Information on this new development is scarce as the API has not yet been introduced; however CIPPIC is

[308] Applications>What your friends can share, *supra* note 256.
[309] Facebook Developers, "Roadmap Open Graph API", ["Facebook Developers, Open Graph API"], last modified October 29, 2009, online at: <http://wiki.developers.facebook.com/index.php/Roadmap_Open_Graph_API>, (last accessed January 20, 2010).

concerned about many potential privacy issues related to having external web sites using information gleaned from Facebook – especially once such sites are divorced of the 'connect' feature.

i. Fan Pages – what information can they currently get?

Fan Page accessibility to user data is not addressed in Facebook's current Privacy Policy.[310] Facebook's 'help' page provides a little more guidance, informing users that fan:

> Pages cannot see the profiles of their fans. They can only see the profile photo and name of each of their fans. In addition, Pages do not receive a News Feed with information about what their fans are doing. Pages can communicate with their fans through updates in your Inbox, but they have no additional access to your personal information.[311]

This, of course, is no longer a reality in Post-Transition Facebook, as a Fan Page developer need only click on the links of its fans to access all their 'publicly available' and 'Everyone' data. In addition, CIPPIC notes that Fan Page developers are provided an API key when first creating their page. This means they are capable of requesting any Sessionless API call, as long as they have access to a user ID.

ii. Facebook functionality on external websites

Many external sites now have Facebook elements this requires data interactions between it and these sites. Facebook connect sites, for example, can request and are provided logged in status of all random visitors to their sites. Facebook estimates that 40% of visitors to external websites are logged in while visiting, and uses this as a promotional tool for its connect services.[312]

In addition, Facebook provides any website that has a Fan Page the option to add a 'Fan Box Widget' to its site.[313] A visitor to such a site who is not logged into Facebook will see a box listing random Facebook Globe fans with links to their profiles. Fans that have opted out of public search engine indexing will have only their first name displayed to the visitor, with no link and no profile picture. A visitor to such a site who *is* logged in to Facebook, however, will be presented with names, profile pictures, and profile links for all Facebook 'fans' of the website, regardless of whether those 'fans' are searchable on Facebook, on Google, or at all. Facebook will additionally tailor the Fan Box Widget to display more of a user's friends among the otherwise random fans displayed.[314]

It is possible, and indeed likely, that Facebook employs the same Cross Domain Communication technique it uses to provide connect websites with data in order to furnish external sites with such Fan Boxes.[315] If this is the case, external websites with Fan Boxes, but no connect button, are likely given access to, at least, the fact that a user is logged into Facebook while visiting their

---

[310] Privacy Policy, *supra* note 12.

[311] Facebook, "Facebook Pages: Finding, Viewing and Interacting with Pages", Facebook Help Center, online at: <http://www.facebook.com/help/?ref=pf#/help/?faq=12277>, (last accessed January 20, 2010).

[312] Facebook Developers, Connect Status, *supra* note 282. See also pages 75-78 above for more details.

[313] Facebook Developers, "Fan Box", wiki.developers.facebook.com, last modified on January 26, 2010, online at: <http://wiki.developers.facebook.com/index.php/Fan_Box>, (last accessed February 12, 2010).

[314] *Ibid*.

[315] See Facebook Developers, Cross Domain Communication, *supra* note 281 and comments in that note for more details.

external website (see pages 75-78 above for more details). CIPPIC would be concerned if such pages were getting any user identifying information.

Regardless, each time a Facebook user visits an external page that has connect capability or Facebook widgets, information is passed to Facebook, not directly from the site, but from the user herself. Utilizing Facebook's Cross Domain Communication technique, a connect website will prompt a visiting user to access her Facebook cookies, located on Facebook's servers, identifying whether the user is logged in, and whether the user has, in the past, connected to the website in question.[316] This means that Facebook receives both the user's ID (in the form of the user's login and user name [labelled c_user in the cookie the user sends to Facebook]) as well as an identifier for the website being visited (its API key as well as the host URL, contained in the referrer header field).[317] Information sent to Facebook from the user computer includes the following:

> GET /connect.php/en_US/js/Api/CanvasUtil/Connect/XFBML HTTP/1.1\r\n
> **Host**: static.ak.connect.facebook.com\r\n
> **Connection**: keep-alive\r\n
> **Referer**: http://www.huffingtonpost.com/\r\n
> **Cookie**: s_vsn_facebookpoc_1=9156991271302; locale=en_US; lsd=7iOhD;
> c_user=100000545321947;
> datr=1265503963-d2ef5a8725b3389227bf5b788d46313b19cf1b3723f9688e82666;
> h_user=AAAAAQAQ9CN9VBfXK1AjxU44g3Q24QAAABXUc93eADreK8GfoAG-1k7EB
> E6rMqNQUHS.; lxe=privacy.fella%40gmail.com; lxs=1;
> xs=62ecacc40afdd390f1a17395a1f49291;
> x-referer=http%3A%2F%2Fwww.facebook.com%2Fhome.php%3Fref%3Dhome%23%2Fho
> me.php%3Fref%3Dhome; […][318]

Similarly, when Facebook delivers a widget box to an external website *without* connect functionality, but whose owner has opened a Fan Page, it must know the user's identity (to customize the box) and it must be aware of the destination website.

Facebook's Privacy Policy provides the following description of its use of cookies:

> **Cookie Information**. We use "cookies" (small pieces of data we store for an extended period of time on your computer, mobile phone, or other device) to make Facebook easier to use, to make our advertising better, and to protect both you and Facebook…We also use them to confirm that you are logged into Facebook, and to know when you are interacting with Facebook Platform applications and websites, our widgets and Share buttons, and our advertisements. You can remove or block cookies using the settings in your browser, but in some cases that may impact your ability to use Facebook.[319]

The Privacy Policy additionally states:

---

[316] Facebook Developers, Connect Status, *supra* note 282.
[317] *Ibid*.
[318] HTTP packets sent from user computer to Facebook as user opened www.huffingtonpost.com while logged in to Facebook account with user name: privacy.fella@gmail.com, user profile URL: http://www.facebook.com/profile.php?ref=profile&**id=100000545321947** (user ID: **100000545321947**). Captured using Wire Shark, underline mine.
[319] Privacy Policy, *supra* note 12.

> Whenever you authorize a Facebook-enhanced application or website, we will receive information from them, including information about actions you take. In some cases, in order to personalize the process of connecting, we may receive a limited amount of information even before you authorize the application or website.
>
> **Information from other websites.** We may institute programs with advertising partners and other websites in which they share information with us:
>
> - We may ask advertisers to tell us how our users responded to the ads we showed them (and for comparison purposes, how other users who didn't see the ads acted on their site). This data sharing, commonly known as "conversion tracking," helps us measure our advertising effectiveness and improve the quality of the advertisements you see.
>
> - We may receive information about whether or not you've seen or interacted with certain ads on other sites in order to measure the effectiveness of those ads.
>
> If in any of these cases we receive data that we do not already have, we will "anonymize" it within 180 days, meaning we will stop associating the information with any particular user. If we institute these programs, we will only use the information in the ways we explain in the "How We Use Your Information" section below.[320]

It is not clear to CIPPIC that Facebook collects and stores external URLs in this manner. It does, however, appear to encourage developers to read referrer header fields to identify users who have, for example, been directed to their site from links posted on Facebook[321].

If URL history *is* collected, it is equally unclear whether Facebook stores or uses browsing information from users who have never authorized the sites they are visiting. If Facebook is doing so, it must, in CIPPIC's view, gain opt-in consent. Tracking browsing history is problematic in other contexts, but much more so on Facebook. The potential merging of personally identifiable information hosted on Facebook with the browsing history of a user creates enormous and highly problematic potential for data mining. With the two sets of information, Facebook would now be able to create a highly accurate picture of a person and her life – an invasion of the user's privacy if done without her informed and explicit consent.

This is made worse by layout changes Facebook has recently made to its interface. There is no longer a 'logout' button, but rather a less accessible logout option from a dropdown menu. Accessibility with respect to logout buttons is important, as users closing their browser or browser tab will remain logged in until this button has been pressed. Facebook recognizes the importance of having a prominent and visible logout button in its own materials, where it requires connect website developers to provide users with an "explicit 'Log Out' option".[322] An inaccessible logout option is, in CIPPIC's view, a violation of PIPEDA principle 4.7, which calls on organizations to put in place appropriate safeguards.

Typically, online tracking of browsing activity of this type would require at least opt-out consent and more likely opt-in, even when only connected to a pseudonym. With the potential to connect browsing history to the rich profiles already contained on Facebook, such tracking should in

---

[320] *Ibid*.
[321] Facebook Developers, Connect Status, *supra* note 282.
[322] Facebook Developers, Principles and Policies, *supra* note 145 at s. XI.3.

CIPPIC's view be unconditionally opt-in. Principle 4.3.6 demands opt-in consent in such situations. If Facebook is not collecting, retaining or using this type of browsing activity, CIPPIC asks that it makes this explicit in its Privacy Policy in order to comply with Principle 4.8.

iii. Open Graph API

Facebook has consistently modified its API to allow for new and innovative uses. CIPPIC recognizes that engaging in this activity is consistent with Facebook's business model, however it is concerned that potential new developments may not be fully explained to users and privacy concerns are not being adequately addressed.

Facebook recently announced on its developer's Road Map a proposed Open Graph API. This API appears to provide external pages with Facebook functionalities: Facebook describes it at "allow[ing] any page on the Web to have all the features of a Facebook Page."[323]

In CIPPIC's view, this raises potential privacy concerns surrounding precisely the extent to which these new functionalities will include information sharing. Potential concerns are numerous – will a website with Open Graph functionality be capable of identifying Facebook users as they visit? Will they be able to associate that information with additional information from the user's Facebook account? Will the external site be able to publish Facebook user information on its site, publicly and searchably? Will these external sites be able to publish Facebook user activities taken on their sites in association with Facebook IDs? Will Facebook have access to off-Facebook user activity (i.e. Open Graph API websites visited) if those users are logged into their accounts when they visit?

Many of these concerns are troubling to CIPPIC, and we would like Facebook to clarify its vision with respect to this new upcoming feature, either in its documentation, or to the Privacy Commissioner.

Potential Violation	**Requested Fix**
Facebook's Privacy Policy does not clearly articulate what information it provides owners of Fan Pages; specifically, such owners now have access, at the least, to all 'publicly available' and 'Everyone' information; Principle 4.3.2 requires clearer articulation of what users provide such individuals;	Clarify what information Fan Page owners have access to in the Privacy Policy and 'Help' FAQs;
Facebook's new logout button is no longer readily accessible, and this is problematic as users are more likely to close their Facebook tab/browser without logging out, potentially exposing their accounts to other passers by; this constitutes a violation of Principle 4.7	Return the logout button to a prominent location on Facebook pages;
Facebook has access to significant browsing activity of its users but does not clarify whether such activity is collected, stored or used, and if so, how and for what purposes; collection, retention and use of such data without opt-in user consent would constitute a violation of Principles 4.3 and 4.3.6 of PIPEDA; Principle 4.8 further requires Facebook to explicitly specify in its Privacy Policy what its data practices	▪ Facebook should clarify its policies around collection, retention and use of external browsing activity; ▪ If Facebook wishes to retain or use such data, it must gain informed, meaningful opt-in consent;

[323] Facebook Developers, Open Graph API, *supra* note 309.

are with respect to such information;	

V. Data Retention

Facebook's data retention policy is in violation of PIPEDA as it does not clearly state what types of information will be stored, nor does it provide for deletion of data after a reasonable amount of time. First, Facebook's general retention policy does not meet the requirements of PIPEDA. Secondly, Facebook does not adequately provide a 'deletion' option to users nor explain what data is being retained despite deletion. Finally, Facebook does not conform to the standards laid out in PIPEDA or the Resolution with respect to retention of third party information provided by users.

A. Retention of user data manually deleted from active accounts

CIPPIC is troubled by reports that Facebook is retaining information about its users even after a user removes that information from her profile. In a recent article, an anonymous employee of Facebook seemed to indicate that any information once provided by the user, even if later removed, is stored by Facebook indefinitely.[324] Such limitless and unjustified retention is in violation of PIPEDA.

Facebook discloses to its users that many of the interactions that a user has with Facebook are logged and stored. The Facebook Policy states:

> We keep track of the actions you take on Facebook, such as adding a friend, becoming a fan of a Facebook Page, joining a group or an event, creating a photo album, sending a gift, poking another user, indicating you "like" a post, attending an event, or authorizing an application. In some cases you are also taking an action when you provide information or content to us. For example, if you share a video, in addition to storing the actual content you uploaded, we might log the fact you shared it.[325]

In addition to this, Facebook appears to collect information such as visits to a user's profile, both in aggregate and individually identified.[326] The Policy, however, fails to note whether or not Facebook stores this information indefinitely, and whether a user can have the information deleted.

Facebook does not, however, mention whether it retains data, such as 'Interests', comments made, photos posted, etc., previously added by the user but later manually removed. The 'anonymous employee' cited in the report above indicated that this information is stored along with the information Facebook mentions in its privacy policy. If this information is being retained, Facebook must disclose this fact to the user. Alarmingly, the anonymous employee suggested that even personal messages deleted by the user are stored indefinitely.[327] CIPPIC cannot confirm these claims but, if true, they raise issues under PIPEDA.

In this scenario, not only would Facebook fail to adequately disclose its data collection policies to its users, it would additionally fail to provide its users with a method of permanently removing

[324] Wong, *supra* note 266. CIPPIC cannot confirm the information contained in this article. However the possibility that such activity is occurring is a concern for CIPPIC, and it wishes confirmation that it is not.
[325] Privacy Policy, *supra* note 12.
[326] Facebook Developers, Principles and Policies, *supra* note 145, s. 5(b) states that developers are capable of collecting such data, implying that Facebook has such data for them to access and collect.
[327] Wong, *supra* note 266.

information from Facebook or anonymizing it. Once a user deletes her information from Facebook, the initial purpose for which it was provided by the user is no longer applicable. The users who have provided Facebook with this information have deleted it, can no longer access it, and are not clearly aware it still exists. Such indefinite and unjustified retention, if occurring, is a violation of Principle 4.5, and the lack of notification surrounding it would be a violation of Principle 4.8. If Facebook is retaining this data and using it for some unknown legitimate purposes, it has not informed users of such uses and so would not have their consent to do so as required by Principle 4.3.

CIPPIC asks that Facebook clarify whether it does indeed store information even after a user manually removes it. If so, it must fix its policies and practices to be in compliance with PIPEDA

Potential Violation	**Requested Fix**
If Facebook is retaining personal information that users have manually removed from its site, it must notify them gain their informed consent for doing so, as required by Principles 4.8 and 4.3.	If Facebook retains manually deleted information, it should notify its users precisely what will be retained, under what conditions and for how long; If it is retaining such information for a legitimate purpose, it should gain its users informed consent for doing so.
If Facebook is retaining personal information that users have manually removed from the site, this is a violation of Principle 4.5 as the initial purpose for which it was provided is no longer applicable.	If Facebook is retaining personal information manually deleted by its users, it should cease doing so within a reasonable period of time.

B. Deletion and deactivation

Facebook allows users to both deactivate and delete accounts. Though CIPPIC commends Facebook for providing users with both these options, CIPPIC finds the manner in which the user is presented with these options remains problematic. First, the user is not clearly informed that she has the choice of deletion over deactivation. Second, Facebook utilized an improper form of consent upon deactivating an account by relying on opt-out instead of opt-in consent for further communication during the deactivation period. Finally, Facebook retains data indefinitely, regardless of how long an account remains deactivated and even upon deletion.

i. Facebook does not clearly present the 'deletion' option to users

If a user wishes to deactivate her account, she finds this option under 'Account Settings'. However, if a user wishes to delete her account, she must either go to the privacy policy and find the required link or search the Help pages. As held in the Finding,[328] by prominently presenting only the 'deactivation' option, users are led to incorrectly believe that this is their *only* option when in fact deletion remains an option.

In the Resolution, Facebook committed to better explaining to users the difference between deactivation and deletion in the privacy policy as well as to increasing the prominence of the 'deletion' option, specifically by including it in the 'deactivation flow' screens.[329] If Facebook is to continue to rely on the availability of the deletion option in meeting its obligations under Principle 4.3.8 to provide an effective consent withdrawal mechanism, it must at the very least

[328] Finding, *supra* note 1 at para. 247.
[329] Resolution, *supra* note 107.

comply with these undertakings. Facebook should provide both options from the same, easily accessible interface so that users can make a meaningful choice between the two options. In addition, Facebook should add information and access to the deletion option as part of the deactivation flow screens to ensure it has meaningful authorization to retain data in deactivated accounts. Without such meaningful consent, it will have no legitimate purpose to retain this data.

ii. Facebook utilizes an improper form of consent for continued post-deactivation communications

When a user deactivates her account, she is now told that:

> 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.[330]

This option is presented as *opt out*, rather than *opt in*. Unlike the situation where a user has consented to Facebook using her data, here the user is explicitly stating her preference to suspend her interactions with Facebook. As a result, Facebook can no longer reasonably rely on the presumption that a user would prefer to receive these emails from Facebook.

Indeed, failing to opt-out of this feature effectively undermines the entire deactivation process. A deactivated user invited to an Event, for example, is sent an Email notification with a link to the Event, but cannot accept or decline without logging in which entails, of course, re-activation.

More to the point, if Alice invites deactivated Bob to an event, she is able to access Bob's full profile (although she will not be able to post on his wall). Hardly deactivated, in CIPPIC's view. Instead of opt-out, a user should be presented with the option to opt in to receiving emails from Facebook. Principles 4.3.4, 4.3.6 and especially 4.3.5 requires this opt-in form of consent, as users would not reasonably expect such continued uses of their email and other personal information while 'deactivated'.

iii. Facebook retains certain user information indefinitely when a user 'deactivates' or 'deletes' her account

When a user deactivates her account, Facebook retains all her data indefinitely.[331] Even if a user deletes her account, Facebook states that, "we may retain certain information to prevent identity theft and other misconduct even if deletion has been requested."[332] Both of these activities violate PIPEDA.

With respect to deactivation, Facebook must delete all of a user's information after a reasonable period of time. Facebook claims that approximately 50% of users reactivate their accounts within one month of deactivation, and a smaller number does so later.[333] It is apparent from these statements that Facebook has data regarding the number of users that have deactivated and if and when these users typically return. As a result, Facebook should be able to determine when it is reasonably certain a user is no longer likely to return to Facebook and reactivate her account. In

[330] Facebook deactivation page, Accessed January 20, 2010.
[331] Privacy Policy, *supra* note 12 at s. 6.
[332] *Ibid*.
[333] Finding, *supra* note 12 at para. 236

addition, the current deactivation process does *not* remove the user's profile from Facebook. That profile remains accessible through links (such as that generated when an existing user invites the deactivated user to an event) or by directly inputing the deactivated user's URL into the address bar. CIPPIC submits that under Principle 4.5 and 4.5.3 of PIPEDA, Facebook must delete the user's information after this time, as the initial purpose for which it was collected is no longer applicable. Furthermore, Facebook should inform the user of the length of this retention time so the user will be well aware that her data will only be retained for a reasonable period of time. Indefinite retention is not justifiable under PIPEDA, nor would a reasonable person consider it appropriate under these particular circumstances.

With respect to deletion, Facebook retains 'certain information' to protect the user from 'identity theft'. CIPPIC is doubtful that retention of *any* information protects the user from identity theft. Regardless, Facebook neither informs the user of what, exactly, it is retaining, nor does it allow the user to opt-out of this 'service'. Furthermore, when the user deletes her account, she is not informed that Facebook is retaining any information *at all*. No notification is given at time of deletion. A user may reasonably assume Facebook is retaining no personal information, however she would be mistaken. The only way she would be aware of this is if she had found the particular provision in the privacy policy. However given the opacity of the statement, which neither informs what information is being stored nor how to remove it from Facebook, the user is not making a meaningful choice to allow Facebook to retain this information, as required by Principle 4.3. Additionally, CIPPIC is suspect of the legitimacy of indefinite retention as a measure against identity theft. Prohibitions against such retention of information are, rather, typically put in place to *prevent* identity theft through data breach. CIPPIC does not believe a reasonable person would find this to be an acceptable purpose to indefinitely retain data, under the circumstances, nor that it is legitimate to require consent to such retention as a condition of service under Principle 4.3.3.

Facebook's indefinite retention of user data from deactivated or deleted accounts is in violation of Principles 4.5 and 4.5.3.[334] In addition, Facebook does not adequately explain its identity theft prevention program, and thus lacks the informed consent required by Principle 4.3.2 to do so and is additionally in violation of the openness principle (4.8).

Potential Violation	**Requested Fix**
Facebook relies on the deletion option as a mechanism for facilitating user withdrawal of consent, but this option remains obscured, placing Facebook in violation of Principle 4.3.8 as well as its undertakings in the Resolution.	▪ The deletion option should be displayed beside the deactivation option on the account settings page; ▪ An explanation of and a link to the deletion option should be included in the deactivation flow screens, as Facebook undertook to do in the Resolution.
Facebook is employing an improper form of consent by requiring users to opt-out of ongoing Facebook activity such as communications while deactivated, in violation of both their reasonable expectations and Principles 4.3.4, 4.3.6 and especially 4.3.5.	Gain opt-in consent for any specific uses of personal information from deactivated accounts Facebook wishes to make.
Facebook indefinitely retains user data from deactivated accounts and continues to make such information available to others long after it can be	▪ Facebook must set a reasonable retention period for deactivated account information; ▪ Facebook should notify users upon deactivation

[334] *Ibid*. at para 245.

reasonably implied that the initial purposes for its provision remain, in violation of Principles 4.5 and 4.5.3.	that their data will only be retained for x period of time.
Facebook retains personal information of users who have deleted their accounts for the stated purpose of 'preventing identity theft', but fails to explain what information it will keep, why it is required for preventing identity theft, and why it should be retained indefinitely, in violation of Principles 4.3.2, 4.5, 4.5.3 and 4.8. Facebook additionally requires users to consent to such retention as a condition of service, in violation of Principle 4.3.3.	▪ Facebook should explain to users what information it retains after an account is deleted, why it feels this is necessary to prevent identity theft, and why it feels it should be retained for an explicitly stated period of time; ▪ Facebook should provide users with the opportunity to refuse retention of their deleted information for the purpose of protecting them from identity theft.

C. Retaining Personal Information of Non-users

Facebook collects and retains Email addresses of non-users from its users. It does so in a number of situations, such as when a user sends a non-user a Facebook invitation, when a user tags a non-user in a photo and is prompted to enter an Email address for the latter in order to notify her she has been tagged, or when a user imports her contacts from a pre-existing Email account, either upon signup or at any other time.

The initial purpose for which Facebook collects these Email addresses is, as with all activity on Facebook, dual. From the user's perspective, it is to invite her friend to Facebook or perhaps to get her consent for tagging her in a photo. For Facebook, it is a means of promoting its own service. When a user sends an invitation to a non-user friend, either through the contact importer or through the 'find a friend' mechanism, it is an opportunity for Facebook to gain one more user. Similarly, when a user tags a non-user in a photo, Facebook sends the non-user an 'invitation' to join Facebook and, indeed, if that non-user wishes to untag herself from the photo, she still must first join Facebook to do so.

The purpose for retaining these Email addresses is even less personal and more commercial in character. This is especially the case with respect to Email invitations where, as described below, there is a strong indication that either the user or the third party does *not* wish for the Email to be kept. But also in other cases.

CIPPIC sees Facebook's collection and retention processes with respect to non-user Emails to be flawed. In the Resolution, Facebook is noted to have stated that "it does not keep a specific list of such addresses for its own use."[335] CIPPIC is not satisfied that this is the case, nor is it satisfied that Facebook is exercising sufficiently due diligence to ensure that its users gain non-user consent before disclosing personal information of others to it. Even in cases where due diligence has been exercised, indefinite retention in the absence of use is not, in CIPPIC's view, a legitimate policy. Finally, in cases where it is relatively clear that users do *not* wish their Emails to be kept, Facebook should delete them immediately.

[335] Resolution, *supra* note 107.

i. PIPEDA and information of non-users

Under PIPEDA, data such as Email addresses relating to a third party and held by an individual is the personal information of both the individual and the third party.[336] An organization collecting such third-parties data of an individual must ensure it has the consent of both parties. In some limited cases, the Commissioner has held that an organization may rely on the individual it is colleting the data from to gain informed consent from the third party on its behalf. These circumstances are limited, however, and even in such cases before implying third party consent the organization must act with due diligence to ensure this is in fact the case, and cannot rely on such consent where it is unreasonable to imply the individual in question has in fact consented.[337]

Facebook has agreed to add language in its SRR obligating users to gain third-party consent before providing it with Email addresses of others, and has done so. This is not the end of its obligation, however, as it must exercise due diligence to ensure that such third party consent is acquired and, where it is unreasonable to infer that it has been given, it cannot rely on it at all. In either case, indefinite retention without ongoing periodic consent is not reasonable. Facebook has an obligation to set reasonable retention policies.

This obligation arises from Facebook's commercial use of such Emails, which are a mechanism for promoting its service. That the use is commercial is evident from Facebook's own Privacy Policy, which states:

> **To help your friends find you.** By default, we make certain information you have posted to your profile available in search results on Facebook to help your friends find you. However, you can control who has access to this information, as well as who can find you in searches, through your privacy settings. We also partner with email and instant messaging providers to help their users identify which of their contacts are Facebook users, **so that we can promote Facebook to those users.**[338]

but is perhaps most clearly demonstrated from Facebook's policy of retaining all Emails indefinitely regardless of user intention or action.

So, for example, where Alice imports her Email address book and opts out of sending Email invitations to a select and expressly chosen number of her contacts, suppose Bob is among these, Facebook still retains their Email addresses as well as the fact that Alice is somehow connected to them. If the owners of those de-selected Emails ever join Facebook, Alice will appear as a 'suggested contact' to them based solely on this action: that is, Alice expressly decides *not* to send Bob an invitation, but upon joining, Facebook will suggest Alice to Bob as a friend.

Also, if Alice *does* send an invitation to Bob and Bob decides to ignore it or reject it, upon joining Facebook (even a year later), Facebook will suggest Alice to Bob as a friend and will notify Alice that Bob has joined.

---

[336] PIPEDA Case Summary #2002-99, available at: <http://www.priv.gc.ca/cf-dc/2002/cf-dc_021202_2_e.cfm>

[337] See discussion above at pages 296-308.

[338] Privacy Policy, *supra* note 12, my emphasis.

Especially under such circumstances, CIPPIC does not see how Facebook is retaining Email addresses for any purposes other than its own, and these are demonstrably commercial.[339] Under such circumstances, Facebook must either gain consent from third parties or, if it is to imply it through the auspices of its users, it cannot do so indefinitely and must do so reasonably. In CIPPIC's view, it does neither of these.

ii. Due Diligence

Facebook is not exercising sufficiently due diligence before implying third-person consent of non-users. It needs to take greater steps to ensure both that its users are aware of their obligations in this respect, and that the non-user is aware her Email will be collected and kept by Facebook. In CIPPIC's view, this is both a collection and a retention issue, as Facebook need not collect the Email at all to generate an automatic Email invitation sent on behalf of the user to the non-user. The decision to keep that Email constitutes, in our opinion, collection for the purpose of promoting its product.

To begin with, it has, in CIPPIC's view, yet to adequately meet its undertaking under the Resolution to inform "users of their obligation to obtain the consent of non-users before providing their e-mail addresses to Facebook."[340] The SRR now includes the following provision under the heading 'Protecting Other People's Rights':

> You will not email invitations to non-users without their consent. [341]

This notification is in and of itself woefully inadequate, in CIPPIC's view. Nowhere does Facebook explain to users what they must gain non-user consent for. In fact, the SRR gives users the mistaken impression they must seek a non-user's consent to *invite* her to Facebook – patently non-sensible as the email is, in itself, the invitation. Under PIPEDA, users need not gain consent of non-users to the invitation itself, but rather to the resulting indefinite retention of non-user emails that accompanies the invitation. As stated in the Resolution, the concerns this SRR notification was intended to address revolved around:

> non-users' lack of knowledge and consent to Facebook's collection, use, and retention of their email addresses;[342]

The current notification does not do this at all. Moreover, its localization to the SRR largely diminishes its capacity to inform users of their obligations in this respect. Facebook's Privacy Policy, for example, currently states:

> **Friend Information.** We offer contact importer tools to help you upload your friends' addresses so that you can find your friends on Facebook, and invite your contacts who do not have Facebook accounts to join. If you do not want us to store this information, visit this help page. If you give us your password to retrieve those contacts, we will not store your password after you have uploaded your contacts' information.[343]

---

[339] Finding, *supra* note 1 at paras. 11-12.
[340] Resolution, *supra* note 107.
[341] SRR, *supra* note 71 at s. 5(9).
[342] Resolution, *supra* note 107.
[343] Privacy Policy, *supra* note 12.

It fails to mention, when describing this feature, that users must gain non-user consent. In CIPPIC's view, if Facebook wishes to imply consent of non-users, it must a.) ensure users are aware of what non-users must consent to, and b.) take greater steps to ensure users are aware of this obligation. It should do so by including such an explanation in its descriptions of friend finding mechanisms. In addition, it should do so within the flow screens by which users provide it with non-user Emails. The Contact importer a user is confronted with, for example, currently looks like this:

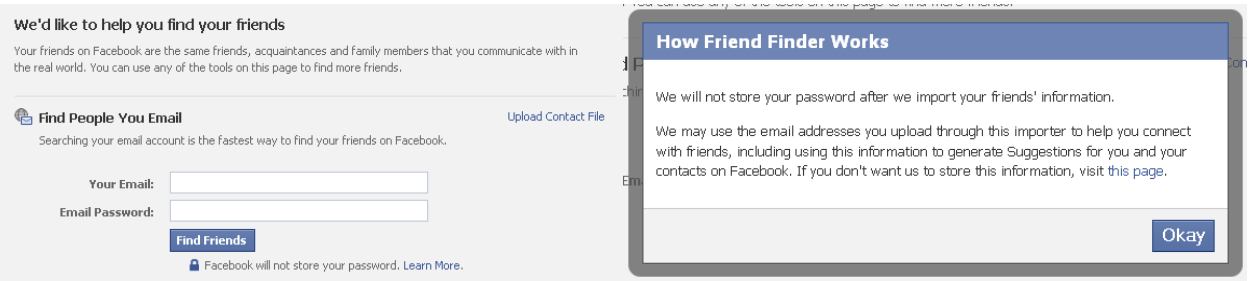


Figure 19 – Contact Importer (left) and 'Learn More' (right)

Facebook clearly notifies users it "will not store your password", but keeps the 'we will retain your imported contacts indefinitely and use them to make suggestions to those contacts' notification for the 'Learn More' pop-up. In neither place is a user notified she is obliged to gain non-user consent before uploading Email addresses. Indeed, it is not clear to CIPPIC whether many users will even be aware that their uploaded Email contact lists will be retained beyond the initial invitation stage. Instead (or in addition) of reassuring users their passwords will not be saved, Facebook should take greater steps to notify its users a.) that non-user emails provided will be kept indefinitely and b.) that they must gain non-user consent to such indefinite retention before disclosing their emails to Facebook.

Where there are practical limitations, it may be acceptable for an organization to rely on implied consent in this manner even where none of the exceptions under s. 7 of PIPEDA apply, but it must, in CIPPIC's view, take significant steps to ensure a reasonable basis for such consent if it is to fall within Principle 4.3 requirements. As matters currently stand, CIPPIC does not find it reasonable to imply that users are gaining non-user consent for Facebook email retention.

Further, as Facebook has direct access to the third party owner of the Email, it must exercise due diligence in its communications with that third party. The Emails Facebook sends to such third parties feature a prominent 'To sign up for Facebook, follow the link below' box. It also includes a 'if you do not wish to receive this type of email from Facebook in the future, please click here to unsubscribe' notification, but in small, light grey print at the bottom of the Email:

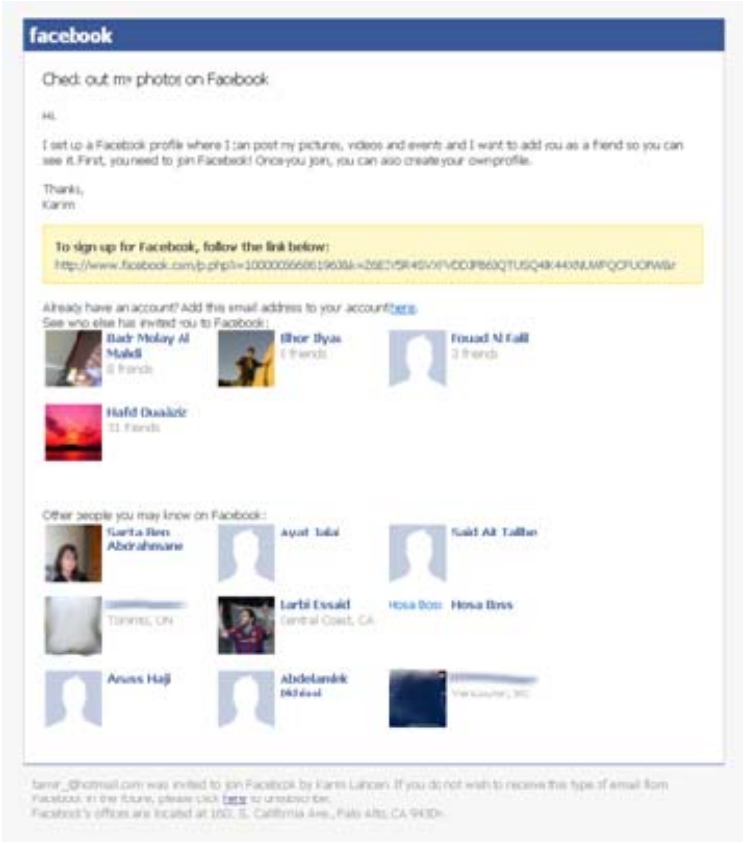


Figure 20 – Friend Invitation recovered from Email account – I note that, aside from the two blurred 'suggestions', the rest, including the person who sent the invitation, are unknown to the owner of the hotmail account to which this invitation was sent. I further note that the owner of the Email account never received an 'invitation' from the two blurred contacts above

There is no notification to the user that, barring his action, Facebook will retain his Email indefinitely and will additionally forever remember the fact that this Email is associated with the Facebook user who has sent the invitation. Non-users should be aware of this. The Facebook user initiating the Friend request (Alice) may be a spammer, or may be someone the non-user (Bob) would not like to be associated with. Yet it appears that by taking no action, Bob will continue to be associated with Alice on Facebook and this association will manifest if Bob eventually joins in the form of friend 'suggestions' or a notification to Alice that Bob has joined.

If Facebook wishes to rely on Bob's implied consent, it must take far greater steps to ensure that he is aware his Email will be retained. Any such opt-out should be far more prominent and provide more details. Indeed, it is not clear to CIPPIC that the current opt-out will erase the association between Bob's Email address and Alice – only that it will prevent Bob from receiving further Emails from Facebook. This may be sufficient to bring Facebook into compliance with CANSPAM, but not with Principle 4.3 of PIPEDA, as well as Principles 4.5 and 4.5.3. Implying indirect consent under current circumstances is not, in CIPPIC's view, acceptable in the context of s. 5(3). Indeed, as detailed below, CIPPIC believes consent to continued retention of Bob's Email address as well as to the association between Bob and Alice should be acquired by an opt-in hyperlink in the Email Facebook sends Bob: 'if you do not object to us retaining this Email, click here'.

iii. Indefinite Retention

Even if Facebook meets PIPEDA diligence requirements with respect to the initial collection, use and retention of non-user Emails, it is unreasonable to imply consent to retain Emails for an indefinite period of time without some ongoing input, whether implied or express. In CIPPIC's opinion, this is different from retention of user profile data, as such data is visible to the user, who can review it and edit it at any time. If retention is to be indefinite, Facebook needs some basis to imply ongoing consent at regular intervals.

With respect to Email addresses, it does not have this basis. While Facebook provides users with an option to delete any imported contact lists, this option is not among the privacy settings, but rather is only accessible through a link in the Privacy Policy to an obscure Help page which states:

> **Remove Contacts Imported using the Friend Finder**
>
> Facebook uses the email addresses you upload through the Friend Finder to help you connect with friends, including using this information to generate Suggestions for you and your contacts on Facebook. Please click the "Remove" button below if you want Facebook to remove these contacts. Note that it may take some time before your name will be completely removed from Suggestions.[344]

Further, CIPPIC was unable to find a location where a user can view which non-user Emails Facebook has collected from her and decide whether to continue to store these or not. Given the obscurity of this help page and the fact that, once provided, users are never confronted, and cannot even locate, their uploaded contact lists, it is unclear to CIPPIC how a user is able to gain continuing consent from her friends at reasonable intervals. Indeed, it is not clear to CIPPIC that users are even aware, under such circumstances, that Facebook continues to retain non-user Email addresses indefinitely.

In addition, as Facebook now has direct access to the non-user owners of those Email addresses, it should be gaining their consent for any form of ongoing retention directly. It is simply unreasonable, in CIPPIC's view, for Facebook to imply that a non-user has agreed to let it keep her Email indefinitely simply by sending her a one time Email months or even years previously. CIPPIC will not speculate as to what time period is appropriate, but in its view, after a certain lapse, it is no longer reasonable for Facebook to imply it has continued consent to retain non-user Email addresses. There is no basis for Facebook to assume that any user or non-user is making any meaningful use of an Email stored in its databanks years or even decades after it was first deposited there. Facebook should set a reasonable retention policy as required by Principles 4.5 and 4.5.3 and delete non-user Emails after a reasonable period of time has elapsed. Alternatively, Facebook can put in place a system for gaining continuing consent for retention from non-users, as it has their Email addresses. However, if repeated opt-out reminders are continuingly ignored, once again, CIPPIC does not see how retention can be justified indefinitely.

iv. Unreasonable implications of consent

There are, moreover, a number of situations where Facebook currently implies consent to retain Emails and other data under conditions where it is highly unreasonable to do so. It retains tagged

[344] Facebook, "Remove Contacts Imported using the Friend Finder", online at: <http://www.facebook.com/contact_importer/remove_uploads.php>, (last accessed February 12, 2010).

photos without explicit consent from non-users; it retains Email addresses from invitations a non-user has ignored, even repeatedly ignored; and it appears to retain Email addresses a user has imported through the Contact Importer even when the user has opted out of sending a particular user an invite.

To CIPPIC, it is difficult to understand how an ignored Email message can support an implication of consent to retention. When Alice tags Bob in a photo and enters his Email to notify him, no reply is not enough, especially in light of the fact that Facebook provides no easy mechanism for Bob to signal his discontent with respect to the photo. While Bob may view the tagged photo without joining Facebook, he is unable to untag himself or to ask Facebook to remove the photo without opening his own account. Given the steep barriers to signalling a lack of consent, Facebook cannot imply Bob's consent to his photo merely on the basis that he has not objected. This is easily fixed, in CIPPIC's view. Facebook need merely place a 'untag me' or 'report picture' button on the preview it now provides non-users of their tagged pictures. Without such a fix, Facebook remains in violation of Principles 4.5 and 4.5.3 as well as 4.3 as it is collecting and retaining non-user data where there is no reasonable grounds to imply informed consent.

Similar concerns apply when Facebook implies consent to retain Email addresses from ignored Facebook invitations. If Alice sends Bob an invitation and Bob ignores it, adequate notification notwithstanding, the reasonable inference under such circumstances is that Bob does *not* wish Facebook to retain his Email address and his connection to Alice. Alice may be a spammer, or someone Bob wishes to avoid. For this reason, CIPPIC believes Facebook should gain opt-in consent for retention of otherwise ignored Email invitations. It does not see how consent can be reasonably implied in the face of an ignored invitation, especially after a reasonable period of time has lapsed with no response, or in situations where a user ignores multiple invitations each listing Alice along with the new invitees.

With respect to imported contacts, retention becomes even less reasonable. In such cases, Facebook is retaining Bob's Email address even if Alice expressly opted out of sending Bob an invitation. She has chosen to deselect Bob from her list of imported contacts. CIPPIC cannot imagine a stronger signal to Facebook that Alice does not wish to be associated with Bob, and that she has no use for retaining Bob's Email in Facebook's databases. Yet it *does* retain these Emails and, when Bob finally joins Facebook, it suggests Alice as a potential friend to him. Under such circumstances, Facebook does not, in CIPPIC's view, have any reasonable basis to imply Bob's or Alice's consent to the retention of this Email, nor does it have any purpose for retaining such Emails aside from promoting its service by suggesting friends to Bob when he joins. If, as Facebook claims, it is not retaining such Email lists for its own use, CIPPIC is hard pressed to find a justification for why it is retaining them at all. It should delete them, as the initial purpose for which the user had provided them is no longer applicable.

Potential Violation	**Requested Fix**
Facebook does not adequately advise users they must gain non-user consent before permitting it to retain non-user Emails indefinitely, and as such cannot imply non-user consent to such retention and use and violates Principle 4.3.	▪ Facebook must explain in its SRR precisely what consent users must gain from non-users before providing it with their Emails; ▪ Facebook must add a similar notification to its Privacy Policy explanations of the friend finding process, as

	well as to the friend finding flow screens;
Facebook retains non-user Emails provided by users, as well as a 'friend' association between sending users and recipient non-users, indefinitely, but does not exercise due diligence before implying consent of non-users of such activities, despite having direct access to them, as required by Principle 4.3 and section 5(3) of PIPEDA.	▪ Emails sent at the behest of users must inform non-user recipients, prominently, that such Emails shall be retained by Facebook and associated with the sending user unless the non-user informs it otherwise; ▪ Preferably, neither Emails of non-users, nor accompanying associations to sending users, should be retained at all unless the non-user recipient provides express opt-in consent to such retention;
Regardless of how expressly and directly non-users are initially informed that their Email shall be retained by it, Facebook's indefinite retention policy for such data becomes unreasonable after a certain period of time and can no longer be justified under Principles 4.5 and 4.5.3 of PIPEDA.	Facebook should develop a reasonable period of time after which Emails of non-users as well as the association of those Emails to sending users will no longer, barring additional input, be retained and clearly notify non-users and users alike of that period;
Facebook implies non-user consent to collection, use and retention of Email address and its association to existing users in situations where it is unreasonable to do so, in violation of Principle 4.3, 4.5 and 4.5.3.	▪ Facebook should not retain Email addresses of non-users or their association with sending users in circumstances where it is clear either or both does *not* intend such connections to manifest; ▪ Specifically, it should not retain non-user Emails or associate them with users who have imported contact lists, but expressly decided *not* to send invitations to particular individuals; ▪ Additionally, it should not retain non-user Emails or associate them with sending users where these Emails have been ignored by recipient non-users, particularly where they have been repeatedly ignored.