REPORT OF FINDINGS
INTO THE COMPLAINT FILED BY THE CANADIAN INTERNET POLICY AND PUBLIC INTEREST CLINIC (CIPPIC)
against
FACEBOOK INC.
UNDER THE
PERSONAL INFORMATION PROTECTION AND ELECTRONIC DOCUMENTS ACT

BY

ELIZABETH DENHAM

ASSISTANT PRIVACY COMMISSIONER

of CANADA

July 16, 2009

TABLE OF CONTENTS

EXECUTIVE SUMMARY 3

COMPLAINT 5

INTRODUCTION 6

SECTION 1 – Collection of Date and Birth..... **10**

SECTION 2 – Default Privacy Settings **18**

SECTION 3 – Facebook Advertising **28**

SECTION 4 – Third-Party Applications..... **37**

SECTION 5 – New Uses of Personal Information..... **55**

SECTION 6 – Collection of Personal Information from Sources Other than Facebook..... **57**

SECTION 7(a) – Account Deactivation and Deletion..... **58**

SECTION 7(b) – Accounts of Deceased Users **65**

SECTION 8 – Personal Information of Non-Users..... **70**

SECTION 9 – Facebook Mobile and Safeguards **78**

SECTION 10 – Monitoring for Anomalous Activity..... **84**

SECTION 11 – Deception and Misrepresentation **88**

SUMMARY OF CONCLUSIONS..... 89

APPENDIX A 91

APPENDIX B 104

Executive Summary

The Complaint

The complaint against Facebook by the Canadian Internet Policy and Public Interest Clinic (CIPPIC) comprised 24 allegations ranging over 11 distinct subjects. These included default privacy settings, collection and use of users' personal information for advertising purposes, disclosure of users' personal information to third-party application developers, and collection and use of non-users' personal information.

The Issues

The central issue in CIPPIC's allegations was **knowledge and consent**. Our Office focused its investigation on whether Facebook was providing a sufficient knowledge basis for meaningful consent by documenting purposes for collecting, using, or disclosing personal information and bringing such purposes to individuals' attention in a reasonably direct and transparent way. **Retention** of personal information was an issue that surfaced specifically in the allegations relating to account deactivation and deletion and non-users' personal information. **Security safeguards** figured prominently in the allegations about third-party applications and Facebook Mobile.

Findings and Conclusions

On four subjects (e.g., deception and misrepresentation, Facebook Mobile), the Assistant Commissioner found no evidence of any contravention of the *Personal Information Protection and Electronic Documents Act* (the Act) and concluded that the allegations were **not well-founded**. On another four subjects (e.g., default privacy settings, advertising), the Assistant Commissioner found Facebook to be in contravention of the Act, but concluded that the allegations were **well-founded and resolved** on the basis of corrective measures proposed by Facebook in response to her recommendations.

On the remaining subjects of third-party applications, account deactivation and deletion, accounts of deceased users, and non-users' personal information, the Assistant Commissioner likewise found Facebook to be in contravention of the Act and concluded that the allegations were **well-founded**. In these four cases, there remain unresolved issues where Facebook has not yet agreed to adopt her recommendations. Most notably, regarding third-party applications, the Assistant Commissioner determined that Facebook did not have adequate safeguards in place to prevent unauthorized access by application developers to users' personal information, and furthermore was not doing enough to ensure that meaningful consent was obtained from individuals for the disclosure of their personal information to application developers.

Follow-up

Where well-founded allegations were deemed to be resolved, the Assistant Commissioner notified Facebook that her Office would follow up after 30 days to verify implementation of the proposed corrective measures. Where well-founded allegations remained unresolved, the Assistant Commissioner asked Facebook to reconsider the recommendations in question and gave notice that her Office, in following up on other matters after 30 days, would also check for evidence of acceptance and implementation of those outstanding recommendations or acceptable alternatives.

Report of Findings

Complaint under the *Personal Information Protection and Electronic Documents Act* (the Act)

1. In a letter dated May 30, 2008, representatives of the Canadian Internet Policy and Public Interest Clinic (CIPPIC) filed a multi-faceted complaint against Facebook Inc. on topics ranging from the collection of date of birth at registration to the sharing of users' personal information with third-party application developers. Because of the complexity of the complaint, this report has been structured as a series of mini-reports addressing the various allegations, which have been grouped by subject. We notified Facebook of the complaint on June 3, 2008.

2. On June 20, 2008, CIPPIC provided additional information on the allegations relating to third-party applications, specifically the trend for third-party application developers to commercialize their products through advertising.

3. Facebook provided representations on July 14, 2008, and gave a technical presentation to staff of the Office of the Privacy Commissioner of Canada on August 21, 2008.

4. Our Office issued a preliminary report to both parties on March 27, 2009. In our report to Facebook, we highlighted numerous concerns and made 20 recommendations.

5. We subsequently met twice with Facebook officials, on April 15 and May 8, 2009, to discuss our preliminary report and the concerns expressed in it. After each meeting, Facebook submitted written representations in response to our recommendations in the preliminary report. The present report of findings is the culmination of our investigation and consultations with Facebook.

Introduction

6. Social networking sites are a cultural phenomenon. In the last five years, the popularity of these sites has exploded, with millions of people around the world joining them to keep in touch with their friends and family and to meet new people. They represent a dramatic shift in the way people communicate, and their use raises interesting questions about long-held views on what it means to have a private life or a sense of "privacy".

7. In an age where it appears almost everyone is leaving their digital footprints everywhere, including their views, pictures, beliefs and sometimes romantic foibles, our notions of controlling one's personal information – the foundation on which the *Personal Information Protection and Electronic Documents Act* (the Act) is built – are being significantly challenged.

8. Facebook is the most popular social networking site in the world – with over 200 million users worldwide and nearly 12 million users in Canada alone. It describes itself as a "social utility that helps people communicate more efficiently with their friends, family and coworkers." Its tag line is "Facebook is a social utility that connects you with the people around you."

9. Our role as a privacy educator and advocate is clear. Users and employers need some signposts to help them navigate this world in a way that balances the social benefits many receive from social networking with the knowledge that what is posted online is never completely private.

10. In terms of our regulatory role, social networking sites like Facebook present an interesting challenge. The purpose of the Act is to balance an organization's need to collect, use and disclose personal information for appropriate purposes with the individual's right to privacy vis-à-vis their personal information. In the off-line world, organizations may collect particular personal information, and use and disclose such personal information, in order to provide a specific service. On Facebook, users decide what information they provide in order to meet their own needs for social networking. In order for individuals to join Facebook, Facebook requires that users provide only four pieces of personal information: their name, email address, date of birth, and gender. All other information is uploaded voluntarily by the user for the express purpose of sharing it with others.

11. To be sure, individuals do post personal information for purely personal reasons. Nonetheless, personal information posted by individuals for purely personal

purposes that would otherwise be exempted under the Act does fall under the Act and imposes obligations on Facebook to the extent that Facebook uses such personal information in the course of commercial activities. There is no conflict between the same information being both for personal purposes and commercial purposes. Such scenarios are particularly clear in the parts of the report that deal with advertising and non-user personal information.

12. It is reasonable to assume that those features of the site that do not have an obvious link to its business model are included to enhance the user's experience on Facebook. Enhancing the experience likely encourages existing members to continue to use the site and presumably encourages others to join as well – thereby indirectly contributing to the success of Facebook as a commercial enterprise. In that sense, collection, use and disclosure of personal information in relation to a feature without an apparent direct commercial link can still be characterized as occurring "in the course of commercial activity" in the sense required under the Act.

13. One of the key concepts of the Act is that of one's control of their personal information. As well, the cornerstone of the legislation is knowledge and consent. Many of the complaints made to his Office are essentially matters of consent, and my focus has been on whether consent in any given case is meaningful. This Office has previously considered consent to be meaningful if the individual in question is informed in a clear and understandable manner of the purposes for collecting, using and disclosing personal information, prior to any such collection, use or disclosure of personal information. It is relatively straightforward to describe how Facebook meets this requirement in terms of how it informs users of its purposes via the privacy policy, terms of service and other documents. We have made several recommendations to Facebook – many of which have been accepted or some other acceptable alternative proposed – that seek to ensure that users have the information they need to make meaningful decisions about how open they wish to be in sharing their personal information. Although we are proponents of "real-time" notification, we are mindful of and appreciate that Facebook wants to provide its users with a seamless experience.

14. However, as in all investigation complaints, each case must be considered on the evidence presented and this is a business that presents a model that is different from those considered in past cases. Our views with respect to advertising have adapted to the social networking site business model. We have accepted that a certain amount of advertising is something users have to agree to since use of the site is free and the company needs to generate revenue. However, we do draw distinctions (as does Facebook) between various types of advertising and consent. As for third parties, in a traditional

model, an organization may subcontract parts of its business to third parties (thus transferring personal information to another entity), or it may disclose personal information to another company that is purchasing customer lists for marketing, for example. In this investigation, we find that the company is in effect providing third-party application developers with the ability to retrieve the personal information of users (and their friends) who sign up for the applications. We have concerns around the safeguards Facebook has in place and are of the view that these could be better. We also believe that Facebook should be doing much more to ensure that meaningful consent is duly obtained from users when developers access their personal information.

15. A few other comments about the investigation and findings: the scope of the investigation was limited to users over the age of 18. Our comments and findings do not therefore reflect the experience of under-aged users.

16. Moreover, Facebook is a dynamic environment that has undergone many changes, primarily in terms of appearance and documentation since CIPPIC filed its complaint on May 30, 2008. For example, Facebook introduced a new user interface in the fall of 2008 and the Statement of Rights and Responsibilities recently replaced the Terms of Use. My findings are largely based on the site as it appeared when the complaint was filed. However, site and documentation changes are taken into account in the discussion of complaint allegations and findings.

17. Facebook users, I note, are well-known for expressing their views to the company if they do not like (or if they do like) a particular feature of the site. In its response to our recommendations, Facebook noted that it would have to consult its users about any changes to site documentation it intended to make in response our requests. While we understand the importance Facebook places on user feedback, the legislative requirements and obligations imposed by the Act are not contingent on user approval.

18. That said, Facebook is to be commended for offering granular privacy control settings to its users. It frequently contains the kinds of information users need to make reasonable decisions, though the information is scattered about the site. Many of the recommendations made to Facebook ask it to consolidate this information into one spot for the ease of the user. We think that doing so does not unduly affect the user experience, and that users would reasonably expect this.

19. We – social networking sites, users, employers, data protection authorities – are only beginning to develop the appropriate rules of engagement in this new world. This report is our contribution to the development of these rules. We

gratefully acknowledge Facebook's cooperation in the course of this investigation, and we appreciate its stated commitment to allow users to control their personal information while offering the opportunity to connect with others.

Section 1
Collection of Date of Birth

Allegations

20. In its complaint, CIPPIC alleged that Facebook

    (1) was unnecessarily requiring users to provide their dates of birth as a condition of registration, in contravention of Principle 4.3.3[1]; and

    (2) was not adequately explaining to users why they had to provide their dates of birth and how these would be used, in contravention of Principle 4.3.2.

Summary of Investigation

21. At the time of the complaint, a user had to provide his or her name, email address, and date of birth (DOB) in registering for a Facebook account. Below the space where a user inputs his or her DOB, there is a clickable link that reads, "Why do I need to provide this?" An accompanying pop-up, entitled "Why do I need to provide my birthday?", states in part as follows:

    "*Facebook requires users to provide their real date of birth as both a safety precaution and as a means of preserving the integrity of the site*. *You will be able to hide this information from your profile if you wish."*

    With reference to the last sentence, it should be noted that users have the option of hiding all or part of the DOB in their profiles.

22. In its written representations to our Office, Facebook stated that it uses DOB to calculate age in order to both enforce the age minimum of 13 years and to allow special rules to apply to adult viewing of profiles of minors.

23. According to Facebook, its limiting of registration to persons aged 13 and over was driven by a legal requirement in the U.S. *Children's Online Privacy Protection Act* (COPPA). Specifically, COPPA prohibits internet sites from collecting personally identifiable information from children under 13 without verifiable parental consent. In requesting specific DOB rather than simply asking the question whether the user is over or under age 13, Facebook says that it is following a recommended best practice of the U.S. Federal Trade Commission (FTC), the body responsible for enforcing COPPA. In its Report to Congress entitled *Implementing the Children's Online Privacy Protection Act*, the FTC states its views on online age verification as follows:

[1] All of the Principles referred to into this report appear in Schedule 1 of the *Personal Information Protection and Electronic Documents Act*, S.C. 2000, c.5.

"A site that has a log-in registration page that only permits a visitor to enter a birth year starting with age 13, or that flags for visitors the fact that children under 13 are not permitted to participate on the site, may invite age falsification. By contrast, a site that allows visitors to enter any date of birth, and does not indicate why it is seeking such information, may be able to more effectively screen out children under age 13."

24. The FTC also encourages sites to use a tracking mechanism to prevent children from back-clicking to change their DOBs once they have been blocked from a site.

25. In its response to CIPPIC's allegations, Facebook referred to an agreement it had entered into in May 2008 with 49 U.S. attorneys general. Aimed at making the Facebook site safer for underage users, this agreement includes provisions for the design and implementation of technologies and features that will:

    - prevent underage users from accessing the site;
    - protect minors from inappropriate contact;
    - protect minors from inappropriate content; and
    - provide safety tools for all social networking site users.

    For example, Facebook agreed to implement and enforce the feature of "age locking", whereby the site will monitor and review the profile of any user who initiates an age change indicating that he or she is over or under 18.

26. Also as part of this initiative, Facebook agreed to participate in the Internet Safety Technical Task Force, headed by Harvard University's Berkman Center for Internet and Society. Created as a result of an agreement between the U.S. attorneys general and MySpace, this task force addressed the subject of implementing age and identity verification software. In its December 2008 final report, entitled *Enhancing Child Safety and Online Technologies*, the task force identifies, evaluates, and proposes solutions for online risks for children and youth.

27. In its representations to our Office, Facebook noted that the task force's dialogue had taken place in public, and submitted that it was therefore disingenuous of CIPPIC to suggest that Facebook had not been open about why it was collecting DOB.

28. In February 2009, Facebook was one of 17 social networking services (SNSs) that signed on to an agreement brokered by the European Commission to make SNSs safer for European youth. In conjunction with the agreement, the European Commission issued a document entitled *Safer Social Networking*

Principles for the EU, which advocates various safety measures according to the user's age.

29. The second of Facebook's two stated reasons for collecting DOB as a condition of service is to help verify the identity of adults. At the time of the complaint, types of behaviour prohibited on the site were listed under Facebook's Terms of Use and Code of Conduct. Notably, in accepting the Terms and the Code, users agreed not to use the service to impersonate any person or entity or falsely state or otherwise misrepresent themselves, their ages, and their affiliations with any person or entity. As of May 1, 2009, the Terms and the Code were replaced by a Statement of Rights and Responsibilities, which performs much the same function.

30. Facebook encourages individuals to use their real identities because it believes that doing so promotes a safe online environment by inspiring individuals to be responsible for their actions. As part of its monitoring for anomalous behaviour, it takes into account a user's age and the actions that a user takes on the site, such as what networks the individual joins and the age of his or her friends. Any discrepancies would trigger a flag.

31. In its representations to our Office, Facebook stated as follows:

"Responsibility for comments and other actions through Facebook is the norm; this has avoided – not eliminated, but reduced the likelihood – of substantial misuse."

32. The fact that Facebook is restricted to users 13 years of age and over is mentioned in the Privacy Policy and the new Statement of Rights and Responsibilities and on the site in the "Help" section under the heading "Safety". In order to register, users have to acknowledge that they have read and agreed to the Privacy Policy and Terms of Use (now replaced by the Statement of Rights and Responsibilities). However, neither of these texts specifically mentions the collection of DOBs.

33. In fact, the Facebook site contains no specific references to the collection of DOB except in the above-mentioned pop-up. When asked to comment on this matter, Facebook stated as follows:

"[A] time-of-collection notice is widely recognized as an industry best practice. … [T]he Privacy Policy addresses the birthdate requirement with explicit discussion of users under 13 and those 13-18; without the collection of birthdate, such a section would lack any relevance. In addition, the regular provision of birthday updates on the site, through the home page and the available email service, provides users with a regular reminder that birthdate

has been collected, and may be used in conjunction with the site's operation."

34. Facebook also confirmed that a user's age may be used for advertising purposes. Specifically, the company stated as follows:

    "[A user's age] may be used only in non-personally identifiable form for advertising purposes in accordance with the revelation of the targeting of profile data in the Privacy Policy through the following language: Facebook may use information in your profile without identifying you as an individual to third parties."

35. From Facebook's representations and site literature, our Office initially formed the impression that, if users chose not to have their DOBs appear in their profiles, then their DOBs would not be used for advertising purposes. However, it came to our attention that a Facebook user who had chosen, in the words of Facebook, "to hide" her DOB from her profile had nevertheless received a Facebook ad targeted to persons of her age.

36. From further representations by Facebook about this matter, we have determined the following:

    - In offering users the option to "hide" DOBs from their profiles, Facebook is in effect offering only to keep the DOBs from "public display", not to exempt them from use for purposes of advertising or third-party applications.
    - Facebook considers a DOB thus "hidden" from a profile to be nonetheless "profile" information that could be used for advertising purposes.
    - By "profile" information, Facebook does not necessarily mean the information that appears on the "Profile" tab of a user's account.

37. This new information sheds light on an earlier comment made by Facebook:

    "*We do not think there would be a legal distinction drawn between registration and profile information since the same data is provided by the same person to the same entity, for the general purposes articulated in the Privacy Policy and shown to the user by the operation of the service*."

38. It should be noted, however, that nowhere in its Privacy Policy or elsewhere on the site does Facebook make it clear to users that it does not distinguish between registration information and profile information or that hiding a DOB from a profile does not mean preventing its use for purposes of targeted advertising. Indeed, nowhere does Facebook even clearly define what it means by profile information.

Application

39. In making our determinations, we applied Principles 4.1.4(d), 4.2.1, 4.2.3, 4.3, 4.3.2, 4.3.3, and 4.8 and subsection 5(3).

40. Principle 4.1.4(d) states in part that organizations shall implement policies and practices to give effect to the principles, including developing information to explain the organization's policies and procedures.

41. Principle 4.2.1 states that an organization shall document the purposes for which personal information is collected in order to comply with Principle 4.8 (Openness) and Principle 4.9 (Individual Access).

42. Principle 4.2.3 states in part that the identified purposes should be specified at or before the time of collection to the individual from whom the personal information is collected.

43. Principle 4.3 states in part that the knowledge and consent of the individual are required for the collection, use, and disclosure of personal information, except where inappropriate.

44. Principle 4.3.2, noting that Principle 4.3 requires both knowledge and consent, states that organizations shall make a reasonable effort to ensure that the individual is advised of the purposes for which the information will be used. It goes on to say that, to make the consent meaningful, the purposes must be stated in such a manner that the individual can reasonably understand how the information will be used or disclosed.

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

46. Principle 4.8 states that an organization shall make readily available to individuals specific information about its policies and practices relating to the management of personal information.

47. Subsection 5(3) states that an organization may collect, use, or disclose personal information only for purposes that a reasonable person would consider appropriate in the circumstances.

Findings

48. In practice, Facebook requires users to provide DOBs for purposes of (1) enforcing the site's age minimum so as to protect the safety of minors and

(2) ensuring that users use their real identities on the site so as to lessen the incidence of inappropriate content and behaviour and promote a safe and respectful environment for all users.

49. In my view, these are appropriate and legitimate purposes in keeping with subsection 5(3), the collection of DOB is necessary to the fulfilment of them, and it is therefore reasonable for Facebook to require provision of DOB as a condition of the supply of its service.

50. Nevertheless, since the Act makes it clear that consent depends on knowledge of purposes, and given the heightened need for transparency with users about the collection and use of a piece of personal information so coveted by identity thieves, I am concerned that in some respects Facebook is not making a reasonable enough effort, in accordance with Principle 4.3.2, to document, specify, and explain the purposes for which it collects users' DOBs.

51. I find the purpose statement as explained in the pop-up phrase "preserving the integrity of the site" to be vague. Principle 4.3.3 stipulates that purposes must be not only legitimate, but also "explicitly specified". I doubt whether the phrase in question would be reasonably understandable to the average Facebook user. Since I consider real-time notification to be the best way of informing individuals about the uses of their personal information in an online environment, I commend Facebook for having provided a real-time notification in a pop-up to explain its collection of DOB. However, it strikes me as counterproductive to pose so clear a question and then provide so vague an answer to it. In my view, the phrase is not clear or specific enough to ensure that users have the knowledge for making an informed choice about consent under Principle 4.3.

52. I note that the pop-up in question addresses the purposes for which Facebook *requires* DOB, but does not specify other purposes for which DOB will be used – notably, the targeting of ads according to age. In my view, 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.

53. The pop-up in question is the only place on the site where DOB is specifically mentioned in a context of purposes for collection and use. Although the Privacy Policy does discuss in general terms the purposes for which "profile" information may be used, including purposes of targeting ads, it does not refer to DOB specifically in that context. Given that DOB is required information used for both essential and significant other purposes, I believe that it should be distinguished and its uses specifically explained in the Privacy Policy.

54. By failing to provide clear definitions and explanations in its site literature, Facebook makes it easy for users to form the impression that they can opt out of receiving ads targeted according to age. Facebook tells users that it may use their profile information for purposes of targeting ads or third-party applications, but also tells them that they may "hide" their DOBs from their profiles. In my view, it would be quite reasonable for users to assume that profile information means information that appears in a profile and that a DOB hidden from a profile would not be considered profile information and would therefore not be used for advertising purposes. It appears, however, that what Facebook actually means by "hiding" the DOB is simply making it unviewable to Facebook users. Facebook does not consider a hidden DOB to be any less an item of profile information or any less accessible for purposes of targeted advertising. Facebook needs to explain what it means by profile information and clarify that hiding one's DOB from one's profile does not exempt it from use in advertising. The issue of advertising is discussed more fully in section 3 of this report.

55. In sum, with respect to its collection of DOB, I find Facebook to be in contravention of the above-cited principles, most notably Principles 4.2.3 and 4.3.2.

Recommendations and Response

56. In my preliminary report, I recommended that Facebook

    (1) revise the pop-up phrase "a means of preserving the integrity of the site" so as to more clearly capture the true purpose intended and make it more understandable to users;

    (2) amend its Privacy Policy so as to explain the purposes for which DOB specifically is collected and used;

    (3) revise its site literature wherever appropriate, including pop-ups on the registration page, so as to clearly define what it means by profile information and to clearly dispel the notion that "hiding" DOBs from a profile means exempting them from use in targeted advertising; and

    (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. Facebook should likewise specify any other purposes for which it intends to use or disclose users' DOBs.

57. In response, Facebook has agreed to amend the language of the pop-up in question as follows:

"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 if you wish, and its use is governed by the Facebook Privacy Policy."

58. Facebook has also agreed to make changes to the language of its Privacy Policy with respect to its use of personal information for advertising and has stated that it is dedicated to "full disclosure as to the collection and use of information for advertising purposes."

59. Facebook has stated that any language changes in its Privacy Policy will need to go through a "notice and comment period" with users. However, regardless of user acceptance, our Office expects Facebook to honour its commitment to meet these recommendations.

Conclusion

60. I am satisfied that, once implemented, Facebook's proposed corrective measures as set out above will meet our recommendations and bring it into compliance with the Act. Accordingly, I conclude that the allegations in this regard are well-founded and resolved.

61. We will be following up with Facebook on the status of its implementation of these measures within 30 days of the issuance of this report.

Section 2
Default Privacy Settings

Allegations

62. CIPPIC alleged that Facebook, by preselecting default privacy settings, was in effect using opt-out consent for the use and disclosure of personal information without meeting the requirements for opt-out consent as articulated in previous findings of our Office. Specifically, CIPPIC contended that much of the personal information being shared by users, including photographs, marital status, age, and hobbies, is sensitive and therefore requires express consent.

63. CIPPIC also alleged that Facebook does not, in the context of its privacy settings, make a reasonable effort to advise users of the purposes for which and the extent to which their personal information is used and disclosed. Specifically, CIPPIC contended that:

    - Facebook does not inform users of the extent to which their personal information may be shared through the default settings and so does not have meaningful consent.
    - Facebook does not direct users to the privacy settings when they complete registration, when they upload photos, or when Facebook makes changes to the settings.
    - Facebook does not inform users that failure to alter the default settings constitutes consent to those settings.
    - Facebook fails to provide adequate notice to users posting photo albums that the default privacy settings for photo albums enable sharing with everyone, with the result that a user's non-friends can view his or her photographs and associated comments, even if the user's profile is searchable only by his or her friends.
    - When users sign up for a network, their default privacy settings enable the sharing of their personal information, including sensitive information, with everyone on the network.

Summary of Investigation

64. Facebook preselects the privacy settings that control how much of a user's personal information can be accessed by others and whether a user's personal information is accessible to search engines. However, the settings can be customized by users to reflect individual preferences. It should be noted that all settings discussed in this section pertain to users aged 18 and over.

65. According to Facebook, CIPPIC has mischaracterized Facebook's privacy controls by implying that they are limited to the privacy settings, when in fact they include the friend and network architecture. In its representations to our Office, Facebook stated its case as follows:

"Contrary to common public reports, full profile data on Facebook is not available to everyone on the Internet. In fact, it is not even available to most users on Facebook. … Facebook's privacy settings have played a central part in giving users control over who has access to their personal information by allowing them to choose the friends they accept and networks they join. … In addition to the default access restrictions that are part of Facebook's core friend and network architecture, users are given extensive and precise controls that allow them to choose who sees what among their networks and friends, as well as tools that give them the choice to make a limited set of information available to search engines and other outside entities."

For example, information sharing is different for different networks. In regional networks, contact information is not considered to be part of the profile and so is not shared among network users. In university networks, contact information can be shared among users who have a university email address. Moreover, as part of the friend architecture, users can create friend lists that have varying access to profile information.

66. Facebook estimates that 20% to 30% of users change their privacy settings. Facebook selected the default privacy settings to reflect what they thought users want. In its representations to our Office, Facebook stated, "We believe that users should be empowered to make their own choices about sharing personal information. We facilitate this choice by setting powerful defaults that reflect common sense views about availability and allowing users to change the settings if they wish." According to Facebook, 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.

67. In response to CIPPIC's contention that users are not directed to the privacy settings, Facebook states that the privacy settings are available from a link that appears on every page of the site. Although this was true at the time the complaint was filed, the direct link disappeared when the new Facebook interface was introduced in the fall of 2008. Currently, there is a "Settings" link, which scrolls down to indicate a number of sublinks, including one for privacy settings.

68. Facebook states:

"A 'lock' icon appears throughout the site to denote the presence of the privacy settings. 'Friends lists', paired with privacy settings, allow users to configure subsets of confirmed friends as to who can see specific content. …Users generally have no problem finding the privacy settings and CIPPIC has not presented any evidence to the contrary."

69. This lock icon is present, for example, when users complete their contact information in their profiles. The icon appears off to the right-hand side beside each entry in the contact information section. When a user clicks on the icon, a pop-up box titled "Who can see this?" appears, showing the default setting and allowing the user to use the dropdown menu to change the setting if so desired. Facebook also allows users to see their profiles through the eyes of other users, which illustrates in real time what information is visible to others.

70. With respect to photo albums, Facebook's practice is to automatically present users who upload photos with a screen in which the question "Who can see this?" is answered. If the default setting remains unchanged, the answer is "Everyone". The screen also presents an easy means of scrolling down and changing the privacy setting.

71. Users are also made aware of privacy settings in the Facebook Privacy Policy, which opens with the following statement:

"We built Facebook to make it easy to share information with your friends and people around you. We understand you may not want everyone in the world to have the information you share on Facebook; that is why we give you control of your information. Our default privacy settings limit the information displayed in your profile to your networks and other reasonable community limitations that we tell you about.

"Facebook has two core principles:

a. *You should have control over your personal information.*
   Facebook helps you share information with your friends and people around you. You choose what information you put in your profile, including contact and personal information, pictures, interests and groups you join. And you control the users with whom you share that information through the privacy settings on the Privacy page.

b. *You should have access to the information others want to share.*
   There is an increasing amount of information available out there, and you may want to know why it relates to you, your friends, and people around you. We want to help you easily get that information.

"Sharing information should be easy. And we want to provide you with the privacy tools necessary to control how and with whom you share that

information. If you have questions or ideas, please send them to privacy@facebook.com."

72. Under the heading "Use of Information Obtained by Facebook", the policy states:

"Profile information is used by Facebook primarily to be presented back to and edited by you when you access the service and to be presented to others permitted to view that information by your privacy settings. In some cases where your privacy settings permit it (e.g., posting to your wall), other Facebook users may be able to supplement your profile.

"Profile information you submit to Facebook will be available to users of Facebook who belong to at least one of the networks you allow to access the information through your privacy settings (e.g., school, geography, friends of friends). Your name, network names, and profile picture thumbnail will be available in search results across the Facebook network and those limited pieces of information may be made available to third party search engines. This is primarily so your friends can find you and send a friend request. People who see your name in searches, however, will not be able to access your profile information unless they have a relationship to you (friend, friend of friend, member of your networks, etc.) that allows such access based on your privacy settings.

73. Under "Sharing your Information with Third Parties", the policy states:

"Facebook is about sharing information with others — friends and people in your networks — while providing you with privacy settings that restrict other users from accessing your information. We allow you to choose the information you provide to friends and networks through Facebook. Our network architecture and your privacy settings allow you to make informed choices about who has access to your information."

74. At the time of the complaint, users were required to indicate at registration that they had read and accepted the Privacy Policy, as well as the Terms of Use. The Terms of Use have since been replaced by a Statement of Rights and Responsibilities, to which users must agree at registration.

75. For purposes of our discussion of privacy settings, the default settings at the time of the complaint do not differ significantly from the current version. All profile fields are set at "My Networks and Friends" for users who have joined networks and "Only Friends" for those who have not. All contact information fields are set at "Only Friends" ("All Friends" in the earlier version). The photo albums field is set at "Everyone", meaning everyone on Facebook. (It should

be noted that, on June 2, 2009, Facebook announced on its blog that it is taking steps to remove regional networks. Once the process is complete, regional networks will no longer appear in the privacy settings.)

76. The setting for the field "Public Search Listing" is especially noteworthy. This field determines whether or not a limited amount of a given user's information (i.e., name, networks, thumbnail picture, and friends) will be made available to search engines such as Google. The entry consists of a check box beside a single option, as follows: "Create a public search listing for me and submit it for search engine indexing." Facebook's default setting in this instance is the box checked. "Public Search Listing" field and its default setting do not apply to minors.

77. During registration, users are brought to a three-step process that allows them to "Find Friends already on Facebook". At the third step of the process, entitled "Join a Network", users are asked to type in their city, workplace, school, or region to find their networks. Just below the join box, Facebook states, "Once you join, you will be able to see the profiles of other people in your network, and they will be able to see yours. You can change your privacy settings on the Privacy page."

78. It should be noted that a user can skip through all these steps and not join a network. According to Facebook, more than half of its users are not members of any network.

79. If a user does not join a network, his or her privacy settings will be defaulted to sharing with "Only Friends". However, if that user subsequently joins a network for the first time, his or her default privacy settings will automatically change to include sharing with network members. Although the Privacy Policy contains notification about information sharing among network members, the user is not told in real time upon joining a network after registration that other people in the network will be able to see his or her profile and is not advised that the original privacy settings have been changed.

80. To address the consent allegation, Facebook again bases its argument on the voluntary nature of data uploading, as follows:

"Facebook users are not forced or required to provide any information beyond [name, email, DOB & gender]. When they make the opt-in choice to provide such information, they are doing it with the intention of sharing it with others. They have come explicitly to the Facebook site and made choices to upload information. In fact, many users have seen the false reports in the mainstream press, repeated in the CIPPIC complaint, that sharing information through

Facebook means it is available to everyone on the Internet, and nonetheless gone ahead and made the affirmative choice to provide this information."

81. In Facebook's view, users are providing express consent by virtue of voluntarily using the site for the purpose of sharing information with others. This purpose is reflected in Facebook's motto, which appears on its home page. At the time the complaint was filed, the motto was "*Facebook is a social utility that connects you with the people around you*." The current motto is "*Facebook helps you connect and share with the people in your life*," which has the same underlying philosophy.

Application

82. In making our determinations, we have applied Principles 4.2.3, 4.3, 4.3.2, and 4.3.5.

83. Principle 4.2.3 states in part that the identified purposes should be specified at or before the time of collection to the individual from whom the personal information is collected.

84. Principle 4.3 states that the knowledge and consent of the individual are required for the collection, use, and disclosure of personal information, except where inappropriate.

85. Principle 4.3.2, noting that Principle 4.3 requires both knowledge and consent, states that organizations shall make a reasonable effort to ensure that the individual is advised of the purposes for which the information will be used. It goes on to say that, to make the consent meaningful, the purposes must be stated in such a manner that the individual can reasonably understand how the information will be used or disclosed.

86. Principle 4.3.5 states in part that the reasonable expectations of the individual are relevant in obtaining consent.

Findings

87. I commend Facebook for providing its users with extensive privacy settings. I consider the settings to give effect to the principles of the Act by allowing users to control how they share their information. That said, Facebook can fine tune some of these settings, as discussed below.

88. With reference to CIPPIC's main allegation, I emphasize that the circumstances of this case are vastly different from those of the past cases in which this Office

developed and articulated its positions on matters of consent. Most notably, unlike individuals in earlier cases, Facebook users proactively and voluntarily upload their personal information to the Facebook site for the express purpose of sharing it with others.

89. In these circumstances, the distinction between opt-in and opt-out consent as it relates to default privacy settings is not the real issue. Ideally, I would prefer that users be required to make their own selections at registration instead of having them preselected. I acknowledge however that, given the sheer number of settings involved, the task of selecting each one at registration could make the registration process complicated and time-consuming and could discourage potential users from interacting with the site. Given the nature of the site, I have no serious objection to Facebook's preselection of the settings, provided that the default settings are reasonable and the users properly informed of them. In my view, the more serious and compelling privacy issues here are whether the default privacy settings meet the reasonable expectations of Facebook users, in keeping with Principle 4.3.5, and whether Facebook is making a reasonable effort, in keeping with Principles 4.2.3 and 4.3.2, to inform them how their information will be shared according to the various settings.

90. On the question of reasonable expectations, I note that most of the default privacy settings – and notably all those relating to profile fields – indicate information sharing with "My Networks and Friends." It is quite reasonable for Facebook to have preselected the settings in this way. 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", as well as with those networks they have joined, especially if they receive adequate notification

91. On the whole, then, I am satisfied that Facebook has preselected privacy settings in accordance with users' reasonable expectations, except in two instances.

92. Firstly, with regard to the setting for photo albums, I commend Facebook for its privacy-sensitive practice of automatically presenting users uploading photos with notification of who can see the photos and with an easy means of changing the privacy setting if they wish. This seems at odds, however, with making the default privacy setting "Everyone".

93. Facebook contends that many users do wish to share their photos with everyone. I find it difficult to accept then that the same users who reasonably expect to share their information only with friends and fellow network members in most other cases somehow have widely broadened expectations in the case

of photo albums. In sum, I find the setting of "Everyone" in respect of photo albums to be inconsistent with other default settings.

94. Secondly, I note that the default privacy setting for "Search" provides that users (with the exception of minors) be searchable by search engines. I consider this, too, to be out of line with users' reasonable expectations. As in the case of photo albums, Facebook contends that many users do wish to be searchable, but did not provide any evidence of this. As Facebook has suggested, its users see themselves as a community. In my view, it should be left up to the individual user to decide for himself or herself whether to make information available outside the community.

95. In sum, I find that Facebook's default settings in respect of photo albums and search engines do not meet users' reasonable expectations as envisaged in Principle 4.3.5.

96. Finally, I would suggest that Facebook is not doing as much as it should to inform users about privacy settings at registration. On the registration pages, there is no direct link to the privacy settings and no upfront message about these settings and the fact that they have been preselected by Facebook and can be changed. There is a direct link to the Privacy Policy, and I am satisfied with the explanation provided there. I also find it commendable that Facebook uses lock icons and "Who can see this?" pop-ups for profile information. However, given that Facebook has preselected privacy settings, and given that many of Facebook's new users at registration may be unfamiliar with the notion of privacy settings and unaware of their power to control the sharing of their personal information on Facebook, I do not consider these measures in themselves to be sufficient notification in the circumstances.

97. As for whether Facebook is making a reasonable effort to inform users how their information will be shared according to the various settings, there is a notification discrepancy between users who join a network at registration and ones who join at a later time. Users who join at registration automatically receive a message to the effect that their profile information can be seen by other members of the network. I commend Facebook for providing this message – it is exactly the sort of notification that the circumstances warrant. However, users who do not join a network until some time after registration receive no such message. In my view, Facebook should treat all network joiners equally with respect to notification, regardless of when they choose to join.

98. To conclude, I find that Facebook's notification efforts relating to privacy settings fail to meet a reasonable standard in the circumstances, as envisaged

in Principles 4.2.3 and 4.3.2. In particular, Facebook needs to do more to ensure that new users can make informed decisions about controlling access to their personal information when registering. Facebook has given its users tools to control their personal information; it needs to ensure that users better understand these tools.

Recommendations and Response

99. In my preliminary report, I recommended that Facebook

    (1) make user profiles inaccessible to search engines by default;

    (2) change the default setting for photo albums to "Your Networks and Friends";

    (3) provide a link to the privacy settings at registration, accompanied by a means whereby users can inquire and be informed specifically about the meaning of the term "privacy settings" and can be notified that Facebook has preselected the settings and that the settings can be changed according to the users' preferences; and

    (4) provide users who join networks *after* registration with the same notification as received by users who join networks *at* registration.

100. In response, Facebook has taken a holistic approach to meeting our Office's concerns relating to privacy settings. The company intends to implement the following two significant changes in the near future:

    (1) It will introduce a "Privacy Wizard", whereby users will be able to select a low, medium, or high privacy setting. This selection will dictate more granular default settings. Notably, users who choose the "high" setting will not be included in public search listings. Facebook maintains that its new Privacy Wizard and emphasis on per-object privacy (see below) will meet the purpose of assuring that users have made a fully informed choice about whether their information is made available in any way to search engines.

    (2) It will also implement a per-object privacy tool, whereby users will be given "an easily configurable setting on every piece of content that they will be able to configure at the time of uploading or other sharing. In a matter of weeks, the changes that are in testing will allow users to choose privacy settings on individual photos and pieces of content such as status updates." Our Office infers from this that Facebook intends to extend its notification practice in respect of photo albums to other types of information.

101. Facebook has also stated that it is conducting preliminary testing on a revised registration flow that will provide more information on privacy settings.

102. As for our fourth recommendation, Facebook has agreed to implement the appropriate measure.

Conclusion

103. I am satisfied that, once implemented, Facebook's proposed corrective measures as set out above will meet our recommendations and bring it into compliance with the Act. Accordingly, I conclude that the allegations in this regard are well-founded and resolved.

104. We will be following up with Facebook on the status of its implementation of these measures within 30 days.

Section 3
Facebook Advertising

Allegations

105. CIPPIC alleged that Facebook

(1) was not making a reasonable effort to notify users clearly that it used their personal information for advertising purposes, in violation of Principle 4.3.2;

(2) for Social Ads in particular, was improperly using opt-out rather than opt-in consent in accordance with Principle 4.3.6, given the sensitivity of users' personal information;

(3) was not allowing users to opt out of Facebook Ads, in contravention of Principle 4.3.8; and

(4) since users were not allowed to opt out of Facebook Ads, was unnecessarily requiring users to agree to such ads as a condition of service, in violation of Principle 4.3.3.

106. With regard to the first allegation, CIPPIC noted that, although Facebook's Privacy Policy did state that personal information may be used for Social Ads, the notification was insufficient because, given the demographics, many users would not be able to comprehend the "legal jargon and complicated wording in the Privacy Policy." In CIPPIC's view, if opt-out consent was to apply, notification should be particularly clear.

Summary of Investigation

107. Facebook Ads are targeted to demographic profiles or key words in a user's profile. For example, a woman in her 40s might see an ad entitled "Get your young face back."

108. Social Ads are triggered not by individual words in a profile, but rather by social "actions", such as the action of becoming a fan of a page, joining a group, or doing something else that would appear in the feature "News Feed". For example, if a user announced himself to be a fan of a certain restaurant, this action would be posted to his friends' News Feeds, and if the restaurant has purchased advertising from Facebook, an ad containing the user's name and a thumbnail picture (if the user has chosen to include this in the profile) would accompany the action.

109. Facebook readily admits that the revenue generated by advertising allows it to offer its service for free to users. In its written representations to our Office,

Facebook stated as follows:

"*Facebook aims to be transparent about the fact that advertising is an important source of our revenue and to explain to them fully the uses of their personal data they are authorizing by using Facebook in order to deliver advertising that is relevant and personal. … The Privacy Policy and, more importantly, users' experiences inform them of how advertising on the service works – advertising that enables Facebook to provide the service to users for free is targeted to the expressed attributes of a profile and presented in the space on the page allocated for advertising. This is done without granting an advertiser access to any individual user's profile.*"

110. Facebook's Privacy Policy states as follows:

"Facebook may use information in your profile without identifying you as an individual to third parties. We do this for purposes such as aggregating how many people in a network like a band or movie and personalizing advertisements and promotions so that we can provide you Facebook. We believe this benefits you. You can know more about the world around you and, where there are advertisements, they're more likely to be interesting to you. For example, if you put a favourite movie in your profile, we might serve you an advertisement highlighting a screening of a similar one in your town. But we don't tell the movie company who you are."

111. Facebook has confirmed that the above-described model of not providing personally identifiable information to advertisers applies to Social Ads as well as to Facebook Ads. In either case, advertisers who purchase ads do not receive personal information about the users. What the advertiser receives is confirmation from Facebook that an ad was served on a certain number of occasions and that a certain number of users clicked on the ad.

Facebook Ads

112. With regard to Facebook Ads in particular, Facebook summarized its position as follows:

"We do not believe the serving of an advertisement to a user, where the advertiser has had access only to the number of aggregate people associated with a keyword based on aggregated data, associated with no personal information, could reasonably be construed as a use of personal information in violation of PIPEDA. Users are explicitly told in the Privacy Policy that their personal information will be used in exactly this fashion, complete with simple examples that dispel any potential confusion. With that knowledge, they continue to use the site and see ads on every page. At any time, a user can

deactivate or delete their account, bringing an end to any potential use of their information."

113. Facebook has also confirmed that it does not authorize access by advertisers to the personally identifiable information uploaded by users. According to the company, in the case of Facebook Ads, unless a user willingly decides to share his or her information with an advertiser (for example, in a contest), "advertisers may only target advertisements against non-personally identifiable attributes about a user of Facebook derived from profile data." Facebook's Help section explains as follows in the context of Facebook Ads:

"These attributes are based on interests, activities, and favorite books, TV shows, movies, or job titles that users list in their Facebook profiles. For example, if you choose to target the keyword 'Dave Matthews Band', then your ad will only display on users' accounts that have listed Dave Matthews Band in the 'Favorite Music' section of their profile."

114. All users receive Facebook Ads, and there is no way to opt out.

115. Facebook explained that advertisers who purchase Facebook Ads specify the characteristics of the users to whom they want their ads served. Facebook guarantees that the ads will run to people with those characteristics, and provides the advertisers with statistics such as numbers of ads served and numbers of people who clicked on the ad.

116. Most ads are served by Facebook, but there are also third parties that serve ads on Facebook as part of their ad network. In Canada, Microsoft is Facebook's exclusive third-party ad serving partner. In its Privacy Policy, Facebook addresses the serving of ads by third-party ad networks as follows:

"*Advertisements that appear on Facebook are sometimes delivered (or 'served') directly to users by third-party advertisers. They automatically receive your IP address when this happens. These third-party advertisers may also download cookies to your computer, or use other technologies such as JavaScript and "web beacons" (also known as '1x1 gifs') to measure the effectiveness of their ads and to personalize advertising content."*

Social Ads

117. With regard to Social Ads, Facebook noted that advertisers "pay for promotion of certain interactions users take online to those users' friends." Furthermore, "No social ad is generated unless a user has taken a specific action such as becoming a supporter of a political figure…". Social Ads are served only to confirmed friends. According to Facebook, "An advertiser is not purchasing and does not have access to users' personal data – they are only told that a certain number of users have taken relevant actions and the number of ads generated by those actions."

118. By means of the privacy settings, users can control which of their actions will appear in their friends' News Feeds and consequently what personal information will be used for the purpose of Social Ads. Users can also opt out of Social Ads altogether via the privacy settings.

119. At the time of the complaint, the features in question were called "News Feed" and "Mini-Feed", and the default setting for these was "Only My Friends." In the newer version of Facebook, the features are called "News Feed" and "Wall", with the default still being "Only My Friends."

120. In its Help section, Facebook explains Social Ads as follows:

"What's the deal with ads in News Feed?

"The advertisements that you see in your News Feed are called Social Ads. Social ads can be just an ad or a combination of an ad and any actions your friends have taken that are related to that ad. Social actions move down your News Feed just like any other story. Facebook is committed to maintaining a clean, uncluttered environment for you to connect with your friends. Our goal is to only present ads that are useful and non-intrusive, and we are continually working to increase their relevance. Social Ads provide related information about your friends alongside advertisements that should help tailor the ads you see to what you and your friends find interesting.

"Why is an action I took appearing with an ad?

"We believe that ads can be meaningful to you and actually improve your Facebook experience. Social Ads, which can appear either in News Feed or in the left-hand column ad space, now provide advertisements alongside related information about your friends. If you took an action related to a Page or Application that an advertiser owns, that is considered a social action that may be placed alongside an advertisement. Social Ads will only ever include actions that you allow News Feed to publish according to your News Feed privacy settings. And don't worry, advertisers won't be able to see the actions that are

published alongside any of the ads they create. The related information simply allows ads to be tailored to what you and your friends find interesting, so that you see ads that are useful and more informative."

121. On the subject of consent, Facebook stated that no Social Ad would be generated unless a user took a specific action that was published in a friend's News Feed. In Facebook's view, this constitutes a real-time consent on the part of the user.

122. Facebook's new Statement of Rights and Responsibilities, which recently replaced the Terms of Use, contains two sections on advertising – one aimed at users and the other at advertisers. The section for users is titled, "About Advertisements on Facebook", and reads as follows:

"Our goal is to deliver ads that are not only valuable to advertisers, but also valuable to you. In order to do that, you agree to the following:

1. *You can use your privacy settings to limit how your name and profile picture may be associated with commercial or sponsored content. You give us permission to use your name and profile picture in connection with that content, subject to the limits you place.*
2. *We do not give your content to advertisers.*
3. *You understand that we may not always identify paid services and communications as such."*

Application

123. In making our determinations, we have applied Principles 4.1.4(d), 4.2.1, 4.2.3, 4.3.3, 4.3.2, and 4.8.

124. Principle 4.1.4(d) states in part that organizations shall implement policies and practices to give effect to the principles, including developing information to explain the organization's policies and procedures.

125. Principle 4.2.1 states that an organization shall document the purposes for which personal information is collected in order to comply with Principle 4.8 (Openness) and Principle 4.9 (Individual Access).

126. Principle 4.2.3 states in part that the identified purposes should be specified at or before the time of collection to the individual from whom the personal information is collected.

127. Principle 4.3.2, noting that Principle 4.3 requires both knowledge and consent, states that organizations shall make a reasonable effort to ensure that the

individual is advised of the purposes for which the information will be used. It goes on to say that, to make the consent meaningful, the purposes must be stated in such a manner that the individual can reasonably understand how the information will be used or disclosed.

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

129. Principle 4.8 states that an organization shall make readily available to individuals specific information about its policies and practices relating to the management of personal information.

Findings

130. In the past, when discussing marketing, the Office always drew a distinction between primary and secondary purposes. A primary purpose is that which is essential to the service. A secondary purpose is additional to that for which the information was needed in the first place. In our earlier cases regarding advertising, it was often considered to be a secondary purpose – one that users can opt out of in certain circumstances.

131. Facebook has a different business model from organizations we have looked at to date. The site is free to users but not to Facebook, which needs the revenues from advertising in order to provide the service. From that perspective, advertising is essential to the provision of the service, and persons who wish to use the service must be willing to receive a certain amount of advertising.

132. This complaint concerns two types of advertising that involve the use of personal information – one which the user must consent to in order to use the site (Facebook Ads) and one which a user can opt out of (Social Ads). As far as Facebook Ads are concerned, I am satisfied that the information Facebook gives to advertisers is in aggregate form and therefore Facebook does not *disclose* users' personal information to advertisers. Nevertheless, there is no doubt that accessing users' attributes from their profiles, rendering the data into aggregate form, and serving ads to users constitute *uses* of personal information under the Act.

133. Of the two types of targeted advertising at issue, I view Social Ads to be the more problematic because of their inherently intrusive nature. A Social Ad uses the individual's actions, thumbnail photo and name to promote a certain product or service. The ad then becomes part of the news feed and intertwines

itself in the regular interactions of the user and his or her friends. In effect, the Social Ad takes on the appearance of an endorsement of the product by the user. For this reason, users would not reasonably expect their information to be used in such a manner and they should, as is the current situation, be able to opt out of such an active use of their personal information.

134. In contrast, Facebook Ads are far less invasive. Only the user can see the ads delivered to him or her and the user is not being co-opted into endorsing a product. We acknowledge that Facebook needs to have a means of generating revenue and most Facebook users reasonably expect to receive advertisements. In the circumstances of Facebook's ostensibly "free" social networking service, I find it reasonable that users are required to consent to Facebook Ads as a condition of service.

135. The problem lies in determining whether the advertising purposes are "explicitly specified" as required under Principle 4.3.3 and whether Facebook is making a reasonable enough effort, as required under Principle 4.2.3, to notify users of those purposes.

136. Firstly, in consideration of Principles 4.1.4(d), 4.2.1, 4.3.2, and 4.8, I am concerned that, given the prominent and essential role that advertising plays in its business, Facebook is not making a reasonable enough effort to document and explain in its Privacy Policy its use of advertising, its use of users' information for purposes of targeted advertising, and the extent of users' ability to opt out of Social Ads. Unlike CIPPIC, I do not find Facebook's Privacy Policy to be full of "legal jargon and complicated wording". I do, however, find its discussion of advertising to lack sufficient detail. Notably, it mentions targeted advertising only in very general terms and does not explain the differences between Facebook Ads and Social Ads. Nor does it indicate that users may opt out of Social Ads, but not Facebook Ads.

137. I acknowledge that Facebook's Help section does contain a more detailed and helpful discussion of advertising and the new Statement of Rights and Responsibilities informs users that they can use privacy settings to limit the use of their personal information in Social Ads. However, I am of the view that, for ease of reference, privacy-related information, especially information related to purposes for collection and use of personal information, should be gathered and explained fully in an organization's privacy policy.

138. In sum, in respect of documenting and explaining purposes related to advertising, I find that Facebook has failed to meet a reasonable standard in the circumstances, as envisaged by Principles 4.1.4(d), 4.2.1, 4.3.2, and 4.8.

139. Secondly, in consideration of Principles 4.2.3 and 4.3.2, I am concerned that at the time of the complaint, Facebook was not providing users with sufficient time-of-collection notification of its use of advertising. In my preliminary report, I indicated that Facebook needed to better ensure that new users at the time of filling out their profiles or otherwise uploading information to the site could begin immediately to understand the implications of doing so and to make informed decisions. Given the prominent and essential role of advertising in Facebook's operations, and given that Facebook Ads are a condition of service, I consider it important for Facebook to be more transparent with users about its advertising practices.

Recommendations and Response

140. In my preliminary report, I recommended that Facebook

(1) expand the advertising section of the Privacy Policy so as to

(i) explain more fully the role of advertising in the Facebook environment and the differences between Facebook Ads and Social Ads, particularly with respect to users' ability to opt out; and

(ii) inform users of the use of their profile information for targeted advertising purposes, the impossibility of opting out of Facebook Ads and the ability and means to opt out of Social Ads; and

(2) provide at the Profile tab, as well as at other locations where the uploading of information may trigger either a Facebook Ad or a Social Ad,

(i) a reminder to users that the personal information they are uploading is collected, used, and disclosed in accordance with Facebook's Privacy Policy; and

(ii) a link that brings users directly to the expanded advertising section of the Privacy Policy, as recommended above.

141. In response, Facebook has agreed in principle to describe advertising more clearly in its Privacy Policy. Specifically, the company stated as follows:

"Further description of the Facebook Ads system overall is still under development, as there are evolutions in the ways that Facebook is serving ads. We are dedicated to describing the difference between Social Ads and other Facebook Ads and full disclosure as to the collection and use of information for advertising purposes."

142. Facebook objected in principle to recommendation 2 above on grounds that it was opposed to interruptive notices that disrupt the user experience. Nevertheless, the company agreed to configure its systems so as to "allow

users who are particularly privacy sensitive to discover more information easily about site operations and to provide feedback on their concerns to Facebook."

143. Facebook has stated that any language changes in its Privacy Policy will need to go through a "notice and comment period" with users. However, regardless of user acceptance, our Office expects Facebook to honour its commitment to meet these recommendations.

Conclusion

144. I am satisfied that, once implemented, Facebook's proposed corrective measures as set out above will meet our recommendations and bring it into compliance with the Act. Accordingly, I conclude that the allegations in this regard are well-founded and resolved.

145. We will be following up with Facebook on the status of its implementation of these measures within 30 days.

Section 4
Third-Party Applications

Allegations

146. CIPPIC alleged that Facebook

(1) was not informing users of the purpose for disclosing personal information to third-party application developers, in contravention of Principles 4.2.2 and 4.2.5;

(2) was providing third-party application developers with access to personal information beyond what was necessary for the purposes of the application, in contravention of Principle 4.4.1;

(3) was requiring users to consent to the disclosure of personal information beyond what was necessary to run an application, in contravention of Principle 4.3.3;

(4) was not notifying users of the implications of withdrawing consent to sharing personal information with third-party application developers, in contravention of Principle 4.3.8;

(5) was allowing third-party application developers to retain a user's personal information after the user deleted the application, in contravention of Principle 4.5.3;

(6) was allowing third-party developers access to the personal information of users when their friends or fellow network members added applications without adequate notice, in contravention of Principle 4.3.2;

(7) was not adequately safeguarding personal information in that it was not monitoring the quality or legitimacy of third-party applications or taking adequate steps against inherent vulnerabilities in many programs on the Facebook Platform, in contravention of Principle 4.7;

(8) was not effectively notifying users of the extent of personal information that is disclosed to third-party application developers and was providing users with misleading and unclear information about sharing with third-party application developers, in contravention of Principles 4.3.and 4.8;

(9) was not taking responsibility for the personal information transferred to third-party developers for processing, in contravention of Principle 4.1.3; and

(10) was not permitting users to opt out of sharing their name, networks, and friend lists when their friends add applications, in contravention of Principle 4.3 and subsection 5(3).

Summary of Investigation

147. Since May 2007, Facebook has provided third parties with a platform (Facebook Platform) that enables them to create within Facebook applications that users can add to their accounts. These applications, which include such items as games, quizzes, horoscopes, and classified ads, access Facebook's database, but reside on the developers' servers.

148. According to Facebook's developer blog (June 4, 2009):

"The growth we have seen on Platform has been tremendous. Today there are over 350,000 active applications on Platform from over 950,000 developers living in more than 180 countries. These range from simple applications created by single users to share with their friends to impressive businesses employing hundreds of people and reaching tens of millions of users every month and generating tens of millions of dollars of revenue. For example, close to 10,000 applications have 10,000 or more monthly active users, and more than 100 applications have more than 1 million monthly active users."

149. When users add an application, they must consent to allow the third-party application developer to have access to their personal information, as well as that of their friends. Moreover, as CIPPIC has correctly pointed out, unless users completely opt out of all applications and block specific applications, they are not given the option of refusing to share their names, networks, or lists of friends when friends add applications.

150. Since CIPPIC filed its complaint on May 30, 2008, Facebook has changed the screens that appear when a user adds an application.

151. At the time of the complaint, users adding an application were presented with a screen on which they were required to allow the third-party application developer to "know who I am and access my information." In the present version of the screen in question, users are told: "Allowing [*application name*] access will let it pull your profile information, photos, your friends' info, and other content that it requires to work …. By proceeding, you are allowing [*application name*] to access your information…." In the older version, users were informed that they were agreeing to the Facebook Platform User Terms of Service, with a link provided. In the present version, users are told that they are agreeing to the Facebook Terms of Use, likewise with a link provided.

152. The Facebook Terms of Use and the above-mentioned Facebook Platform User Terms of Service have been replaced by the new Statement of Rights and

Responsibilities (SRR). Although the SRR does contain a section relating to third-party applications, it is addressed not to users, but rather specifically to application developers and operators. Unlike the former Terms of Use, and despite the fact that users are required to agree to it in the context of third-party applications, the SRR itself contains no applications-related information directed specifically to users who are not application developers. At the end of the SRR, there are links to several documents, one of which, "Understanding Platform", leads to the document "Platform Applications Terms of Use".

153. There are default privacy settings that apply specifically to Facebook Platform. The default privacy settings for both the most recent and the earlier version of Facebook Platform are the same. The preselected general option permits the sharing of a user's name, networks, and list of friends, as well as a further series of optional items. The items preselected are profile picture, basic info, personal info (activities, interests, etc.), current location (city), education history, work history, profile status, Wall, notes, groups the user belongs to, events the user is invited to, photos taken by the user, photos taken of the user, relationship status, and online presence. Items not preselected are what type of relationship the user is looking for, what gender the user is interested in, whom the user is in a relationship with, and religious views.

154. The general option not preselected reads as follows: "Do not share any information about me through the Facebook API." It is not possible for users to download applications if they select this option, or to select this option if they have already downloaded applications.

155. Facebook has also added to the privacy settings pages for Platform an explanatory section regarding the collection and use of personal information by third-party applications. CIPPIC alleged that the language of both the settings page and the overview page was confusing as to whether the applications privacy settings relate only to applications that users add themselves or to applications added by users' friends.

156. Facebook explained that, when a user requests an application, the user gives permission to the developer to request the user's information from Facebook. Facebook then gives the developer a key that allows the developer access to the user's personal information (except contact information) as well as the user's friends' information in accordance with their privacy settings. If the user has joined a network, the platform application may also be able to access some personal information about members of the network.

157. On the subject of information access by platform applications, Facebook stated as follows in its representations:

"*Generally speaking, a platform application can access only the data that an individual could otherwise access through the Facebook service. In other words, the application provider is effectively authorized to stand in the shoes of the individual user on behalf of whom the data is requested. It is not given complete access to all Facebook data by virtue of having its application added*."

158. Facebook also pointed out the following in its representations:

- An application cannot randomly go in and access data, but rather may call on the user profile only when the application is engaged.
- When a third-party application interacts with users, it must respect their privacy settings. For example, it cannot allow other users to access information that a user has restricted.
- The developer has to agree to the Developer Terms of Service (now covered in the SRR) and the Facebook Platform Application Guidelines (now called "Platform Guidelines"), which stipulate that all data the developer accesses has to be destroyed 24 hours after it is accessed and that data can only be used for the purposes of the application.

159. On the last point, the new SRR in fact contains no mention of data destruction after 24 hours. The Platform Guidelines, which replace the former Facebook Platform Application Guidelines, state:

"Due to privacy and other considerations, you cannot store data you receive from Facebook, except certain Storable Data. However, for performance purposes, you can cache data you receive from us for up to 24 hours after you obtained it.

Additional clarification is provided to developers in the policy on storable data, "Platform Guidelines 11-15: Storable Data", which state that developers must delete most user data within 24 hours if the user has deleted the application.

160. In order to develop and provide applications on Facebook, developers must themselves be Facebook members with profiles set up. As indicated in paragraph 151 above, Facebook members must acknowledge at registration that they agree to the Facebook Terms of Use (now the SRR), for which a link is provided. On creating a new application, the developer must again acknowledge agreement to what the screen in question refers to as the "Facebook Terms", for which a link is provided to the SRR.

161. Section 9 of the SRR, titled "Special Provisions Applicable to Developers/Operators of Applications and Websites", includes the following provisions:

"If you are a developer or operator of a Platform application or a website using Connect ("application") or otherwise use Platform, the following additional terms apply to you:

1. *You are responsible for your application and its content and all uses you make of Platform. This includes ensuring your application or use of Platform meets our **Platform Guidelines**.*
2. *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:*
    1. *You will only use the data you receive for your application, and will only use it in connection with Facebook.*
    2. *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.*
    3. *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.*
    4. *You will delete all data you received from us relating to any user who removes or disconnects from your application unless otherwise permitted in our **Platform Guidelines**.*
    5. *You will delete all data you received from Facebook if we disable your application or ask you to do so.*
    6. *We can require you to update any data you have received from us.*
    7. *We can limit your access to data.*
    8. *You will not transfer the data you receive from us without our prior consent."*

162. At the time of the complaint, Facebook did not require application developers to make it clear to users what specific user data was going to be used and how it would be used, displayed, or shared, as now stipulated in subsection 9.2.2 of the SRR (see preceding paragraph).

163. With reference to subsection 9.2 of the SRR in general, Facebook has not provided any evidence of technological barriers to a developer's use, display, or sharing of a user's data in a manner prohibited under that subsection.

164. The Platform Guidelines contain a section titled "Enforcement", which reads as follows:

"If Facebook determines (in its sole judgment) that you or your Application violates Facebook Platform Terms and Policies, Facebook can take enforcement action against the violating Application and/or any or all of your other applications. Such enforcement action can include temporarily or

permanently disabling your Application(s), terminating Facebook's agreement(s) with you, temporarily or permanently restricting you or your application's access to some or all Facebook Platform functionality, or other action as Facebook (in its sole discretion) deems appropriate."

165. In this regard, Facebook has provided no evidence that it systematically screens or audits the activities of application developers. Rather, it relies primarily on users themselves to identify developers that may be violating the SRR and Platform Guidelines. In Facebook's opinion, it is in the developers' best interest to "play nice" because it is the developers who have the most to lose if they do not respect the rules, given that many applications are commercial in nature and aim to generate traffic and serve ads.

166. In its site literature, Facebook has represented itself as taking little or no responsibility for the activities of third-party application developers. Notably, at the time of the complaint, Facebook's Terms of Use stated as follows:

"… Third Party Sites and Third Party Applications, Software or Content are not investigated, monitored or checked for accuracy, appropriateness, or completeness by us, and we are not responsible for any Third Party Sites accessed through the Site or any Third Party Applications, Software or Content posted on, available through or installed from the Site, including the content, accuracy, offensiveness, opinions, reliability, privacy practices or other policies of or contained in the Third Party Sites or the Third Party Applications, Software or Content. Inclusion of, linking to or permitting the use or installation of any Third Party Site or any Third Party Applications, Software or Content does not imply approval or endorsement thereof by us. If you decide to leave the Site and access the Third Party Sites or to use or install any Third Party Applications, Software or Content, you do so at your own risk and you should be aware that our terms and policies no longer govern. You should review the applicable terms and policies, including privacy and data gathering practices, of any site to which you navigate from the Site or relating to any applications you use or install from the site.

167. The new SRR does not contain the language quoted immediately above. However, similar language remains in the Privacy Policy:

"Before allowing any Platform Developer to make any Platform Application available to you, Facebook requires the Platform Developer to enter into an agreement which, among other things, requires them to respect your privacy settings and strictly limits their collection, use, and storage of your information. While we have undertaken contractual and technical steps to restrict possible misuse of such information by such Platform Developers, we of course cannot and do not guarantee that all Platform Developers will abide by such

agreements. Please note that Facebook does not screen or approve Platform Developers and cannot control how such Platform Developers use any personal information that they may obtain in connection with Platform Applications. In addition, Platform Developers may require you to sign up to their own terms of service, privacy policies or other policies, which may give them additional rights or impose additional obligations on you, so please make sure to review these terms and policies carefully before using any Platform Application. You can report any suspected misuse of information through the Facebook Platform and we will investigate any such claim and take appropriate action against the Platform Developer up to and including terminating their participation in the Facebook Platform and/or other formal legal action."

168. Facebook maintains that the architecture of the application platform plays a critical security role:

"*Applications require the establishment of application keys, which make data requests trackable and drive more responsible behavior by the applications. While the complete removal of risk of misuse from the system is of course impossible, this structural decision to require individual requests and tie them to responsible accounts allows for easy accountability*."

169. In November 2008, Facebook introduced the "Application Verification Program", whereby it reviews and monitors developers to ensure that they have verified that they meet Facebook standards. For a fee of $375, Facebook will review an application to ensure that it follows the company's guiding principles. One of the elements reviewed by Facebook is the application developer's collection and use of personal information. In its description of program requirements, Facebook states as follows:

"*Data privacy is something we take seriously at Facebook. We will require an explanation for all of the data that your application calls, and use cases for that data. We will verify this information and ensure to users that you are pulling the data that you need to create the best experience possible, and no more*."

Approved applications get a Facebook-verified badge as well as increased distribution on the site. The program is strictly voluntary on the part of developers.

170. On the issue of users' consent to developers' collection and use of their personal information when friends add applications, Facebook stated as follows:

"Users have an extensive ability to choose whether or not they will interact with any particular Facebook application, and additionally have the ability to block any particular application and opt-out of all Facebook applications in a simple

way."

171. With regard to withdrawing consent, CIPPIC alleged that, when a user withdraws consent to sharing information with developers, the user automatically loses all applications without any notice. Facebook contended that this has never been the case since, in reality, users cannot withdraw consent if they have added applications. In the new Facebook interface, this is explained via a pop-up, which says that, in order to withdraw consent, users first need to delete any applications they have added and remove permissions to all external applications they may have used. CIPPIC did not provide any screen captures in support of its allegation, and subsequently acknowledged that Facebook had adequately addressed its concern in this regard.

172. CIPPIC alleged that Facebook does not effectively inform users why their personal information is disclosed to third-party application developers and the extent of the disclosure. In addition to the information in the screen captures as described above, Facebook's Privacy Policy discusses third-party applications as follows:

"If you, your friends, or members of your network use any third-party applications developed using the Facebook Platform ("Platform Applications"), those Platform Applications may access and share certain information about you with others in accordance with your privacy settings. You may opt-out of any sharing of certain or all information through Platform Applications on the ***Privacy Settings*** *page. In addition, third party developers who have created and operate Platform Applications ("Platform Developers"), may also have access to your personal information (excluding your contact information) if you permit Platform Applications to access your data."*

173. This excerpt from the Privacy Policy mentions access to users' information by developers when *members of their network* use third-party applications. However, the privacy setting screens for applications make no mention of network members, but rather refer only to friends. The same applies to the "Allow Access" screen that appears when users add an application. Our Office asked Facebook to indicate where, apart from the Privacy Policy, users are made aware that their information may be shared with developers when someone in their network uses an application, and to indicate whether the application privacy settings can be used to restrict information sharing when a fellow network member uses an application.

174. Facebook responded as follows:

"*Privacy settings apply to all applications on Facebook Platform; if I were to block an application for instance, the privacy settings would then prevent that*

application from getting any of my data; regardless of whether it was called on behalf of a friend or network member who would otherwise be able to see the data."

175. Facebook's Platform Application Terms of Use is more specific about the type of personal information that may be provided to developers:

> ***"PLEASE NOTE: The Facebook Platform does not give Developers access to your e-mail address, personal website, instant messenger ID, telephone number or street address ("Contact Information"). Facebook will only disclose your Contact Information to third parties in accordance with the* Facebook Privacy Policy*.***
> *II. Consent Regarding Use of Facebook Site Information*
> *(a)* ***Information That May Be Provided to Developers.*** *In order to allow you to use and participate in Platform Applications created by Developers ("Developer Applications"), Facebook may from time to time provide Developers access to the following information (collectively, the "Facebook Site Information"):*
> *(i) any information provided by you and visible to you on the Facebook Site, excluding any of your Contact Information, and*
> *(ii) the user ID associated with your Facebook Site profile.*
> *(b)* ***Examples of Facebook Site Information.*** *The Facebook Site Information may include, without limitation, the following information, to the extent visible on the Facebook Site: your name, your profile picture, your gender, your birthday, your hometown location (city/state/country), your current location (city/state/country), your political views, your activities, your interests, your musical preferences, television shows in which you are interested, movies in which you are interested, books in which you are interested, your favorite quotes, the text of your "About Me" section, your relationship status, your dating interests, your relationship interests, your summer plans, your Facebook user network affiliations, your education history, your work history, your course information, copies of photos in your Facebook Site photo albums, metadata associated with your Facebook Site photo albums (e.g., time of upload, album name, comments on your photos, etc.), the total number of messages sent and/or received by you, the total number of unread messages in your Facebook in-box, the total number of "pokes" you have sent and/or received, the total number of wall posts on your Wall™, a list of user IDs mapped to your Facebook friends, your social timeline, and events associated with your Facebook profile.*
> *(c)* ***Privacy Settings****: You may revoke or modify your permission for Facebook to provide Facebook Site Information to Developers at any time through the means provided in your* ***privacy settings****."*

176. CIPPIC contended that the above information in Facebook's Platform Application Terms of Use is not easily accessible by the user since he or she would have to follow a link in the Facebook Terms of Use in order to find it. In its original complaint, CIPPIC also contended that the document was not accessible from the main Facebook page, but rather only from the developer's site. However, CIPPIC subsequently acknowledged that the link to the Platform Application Terms of Use was to be found in the Facebook Terms of Use under the heading "Facebook Platform Applications". Facebook has remarked that, in general, links to the Platform Application Terms of Use are available at "key interaction points between individuals and the service."

177. Our Office has been unable to find more than one current link to the Platform Application Terms of Use. That link appears among several others at the end of the new SRR. Though the link in question leads to the document titled "Platform Application Terms of Use", the link itself is called "Understanding Platform".

178. At the time of the complaint, the Facebook Terms of Use stated that users who installed third-party applications had to agree to the terms and conditions set forth in the Platform Application Terms of Use. However, when users added an application, they were advised that they were agreeing to the Facebook User Terms of Service, and no mention was made of the Platform Application Terms of Use. Currently, as indicated above, there is no stated requirement that users agree with the Platform Application Terms of Use.

179. Generally, the sources of information about third-party applications are not clearly set out or titled.

180. CIPPIC alleged that Facebook did not provide a complete description of the purposes for which it would permit application developers to collect, use, and disclose personal information through the Facebook platform. When adding applications and when at the applications overview screen, users are advised that the application developer's access to their personal information will be limited to what is required to work. However, the former Developers Terms of Service and Developers Guidelines appeared to permit developers to collect, use, and disclose personal information for marketing purposes. CIPPIC alleged that users were not informed of that purpose.

181. CIPPIC pointed out that the Platform Application Terms of Use state, "You may revoke or modify your permission for Facebook to provide Facebook Site Information to Developers at any time through the means provided in your **privacy settings**." In CIPPIC's opinion, users reading that statement could be left with the impression that they will have a greater degree of control than they

actually have over what information is provided to any application that either they themselves or their friends and fellow network members add.

182. Since third-party application developers can conceivably be granted access to large amounts of personal information, the question arises whether applications generally require personal information in order to run and, if so, how much. In October 2007, two researchers at the University of Virginia published a survey of the information needs of the top 150 Facebook applications. The researcher reported general results as follows:

*"We found that 8.7% didn't need any information; 82% used public data (name, network, list of friends); and only 9.3% needed private information (e.g., birthday). Since all of the applications are given full access to private data, this means that **90.7% of applications are being given more privileges than they need**."* [Original emphasis.]

183. Facebook questioned the researchers' methodology and commented as follows:

"[The survey] *took what we would characterize as an unnecessarily limited view as to the legitimate, pro-social use of information, and actively avoided any discussion of the significant limits we have put in place on actual as opposed to potential access of data, as well as ignoring the limits on use and retention and the enforcement mechanisms that have made Facebook Platform a success*."

Application

184. In making our determinations, we applied Principles 4.2, 4.2.3, 4.3, 4.3.2, 4.3.4, 4.3.5, 4.3.6, 4.7, 4.7.1, and 4.7.3 and subsection 5(3).

185. Principle 4.2 states that the purposes for which personal information is collected shall be identified by the organization at or before the time the information is collected.

186. Principle 4.2.3 states in part that the identified purposes should be specified at or before the time of collection to the individual from whom the personal information is collected.

187. Principle 4.3 states in part that the knowledge and consent of the individual are required for the collection, use, and disclosure of personal information, except where inappropriate.

188. Principle 4.3.2, noting that Principle 4.3 requires both knowledge and consent, states that organizations shall make a reasonable effort to ensure that the

individual is advised of the purposes for which the information will be used. It goes on to say that, to make the consent meaningful, the purposes must be stated in such a manner that the individual can reasonably understand how the information will be used or disclosed.

189. Principle 4.3.4 states in part that, in determining the form of consent to use, organizations shall take into account the sensitivity of the information and that any information can be sensitive depending on the context. Principle 4.3.5 states in part that, in obtaining consent, the reasonable expectations of the individual are also relevant. Principle 4.3.6 states in part that an organization should generally seek express consent when the information is considered sensitive.

190. Principle 4.7 states that personal information shall be protected by security safeguards appropriate to the sensitivity of the information. Principle 4.7.1 states in part that the security safeguards shall protect personal information against unauthorized access, disclosure, copying, use, or modification. Principle 4.7.3 states in part that methods of protection should include technological measures.

191. Subsection 5(3) states that an organization may collect, use, or disclose personal information only for purposes that a reasonable person would consider appropriate in the circumstances.

Findings

192. In my preliminary report, I stated as follows:

193. *"In our investigation, we have identified the following matters of concern with regard to third-party applications in the Facebook environment:*

(1) In consideration of Principles 4.7 and 4.7.1 and subsection 5(3), I am concerned that Facebook gives third-party application developers potentially unlimited access to users' information, but does not monitor the developers to ensure that they

(i) obtain only the information they need for the purpose of providing applications;

(ii) retain the information only for as long as necessary for the purpose of providing applications; and

(iii) otherwise comply with privacy principles in the handling of the personal information.

In my view, to make all of a user's personal information accessible to a third

party is in effect to disclose it to that party. I do not believe that any reasonable person would consider such disclosure appropriate in such circumstances, especially given that the third party would typically need very little of the information for its own purposes. Moreover, given the vast potential for unauthorized access, use, and disclosure in such circumstances, I am not satisfied that contractual arrangements in themselves with the developers constitute adequate safeguards for the users' personal information in the Facebook context.

(2) In consideration of Principles 4.2, 4.2.3, 4.3, and 4.3.2, I am concerned that users are not informed of what personal information developers are accessing and are not adequately informed of the purposes for which their personal information is to be used or disclosed. In this regard, I should add that I do not consider Facebook's current consent language to be a significant improvement over the original, nor do I consider it to be a reasonable basis for consent.

(3) In consideration of Principles 4.3 and 4.3.4, I am concerned that Facebook is not using the appropriate form of consent for its disclosure of users' personal information to third-party application developers. In my view, given the potential sensitivity of users' information, express opt-in consent should be sought in each case.

(4) In consideration of Principle 4.3, I am concerned that users lack control of their personal information insofar as no consent is sought from them for the disclosure of their personal information to applications when their friends and fellow network members add applications.

194. Facebook objected strenuously to our preliminary treatment of the allegations relating to third-party applications. However, after considering Facebook's objections, I remain concerned about the issues I raised in my preliminary report.

195. There are two main issues raised in the allegations: safeguards and consent.

196. On the first, I would note that, according to Principles 4.7 and 4.7.1, organizations must institute safeguards to protect personal information against unauthorized access, use, and disclosure. Also, Principle 4.7.3 states that methods of protection should include technological measures. It was primarily with these principles in mind that I made my recommendation that Facebook "limit" application developers access to user information not required to run a specific application.

197. In my preliminary report,I noted that the seemingly unlimited and unmonitored access to Facebook users' personal information by third-party application

developers was the subject of much criticism by privacy advocates. Facebook objected as follows:

"The phrase "seemingly unlimited and unmonitored access" offers an apparent endorsement of the view that there are no limits and no monitoring. This has been repeatedly shown to be completely false in presentations, and is shown to be false by other information presented throughout the Preliminary Report. There appears to be some confusion within the description of the problem here about the legal disclaimer of responsibility for monitoring – a standard term in web contracts – and the fact that we have a well-designed structure that allows identification and removal of potentially problematic applications."

198. Facebook also objected to my suggestion that the company gave third-party application developers potentially unlimited access to personal information and made all of a user's personal information accessible to third parties. Facebook maintains rather that "the granting of an application key gives a developer a limited ability to query for data defined in the application program interface ("API") after a user interacts with that application, and a limited license to use that data solely in accordance with Facebook's Developer Guidelines."

199. In the absence of any evidence of technological safeguards, I can only assume that, when Facebook speaks of limits on access to users' information, it speaks of contractual limits. In other words, as means of limiting access, it is relying mainly upon certain prohibitions stated in policy documents, and upon trust in the application developers' acknowledged agreement to abide by those prohibitions. Most notably, in its Statement of Rights and Responsibilities, to which all Facebook users including developers are supposed to agree, Facebook instructs developers as follows:

"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:

1. *You will only use the data you receive for your application, and only use it in connection with Facebook.*
2. *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.*
3. *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. …"*

Facebook appears to regard such statements as its most effective safeguard against unauthorized access.

200. When I speak of limits to access, and especially when I consider the vast amounts of Facebook users' personal information potentially available to large

numbers of application developers, I believe something much more substantial in the way of safeguards is required. Specifically, I mean technological safeguards that will not simply forbid, but effectively prevent, developers' unauthorized access to personal information that they do not need.

201. In making my final determinations on this matter, I have considered the following:

- With the exception of contact information, applications technically can access virtually any personal information in a given user's account, including the list of friends, some information about the friends, and information that could be considered sensitive outside the circle of friends. Even though Facebook contractually requires developers to respect users' privacy settings, I have not been presented with any evidence of any technological barrier to a developer's access to information precluded by the settings.
- I question how much user personal information an application typically needs to run. Therefore, it seems that Facebook is, in a technical sense, making available to developers far more information than they require.
- In its Privacy Policy, Facebook tells users that it "does not screen or approve Platform Developers."
- Facebook's new Application Verification Program is strictly voluntary and is not a real-time monitoring system. Aside from this program, in which developers are not required to participate, there is no evidence that Facebook makes any significant sustained effort to ensure that the information accessed by developers is only that which is truly needed to run their applications.
- Since developers can in effect copy users' personal information from the Facebook site to their own servers, there would appear to be no way for Facebook to effectively monitor the developers' subsequent use and disposal of the information. Facebook admits as much to users in its Privacy Policy when it tells them that it "cannot control how …Platform Developers use any personal information that they may obtain in connection with Platform Applications." Moreover, in the same paragraph, Facebook in effect puts the onus on the users to detect and report problems. The inability to monitor developers' usage after the fact is all the more reason for Facebook to take effective preventative measures.
- Facebook maintains that it has a well-designed structure that allows identification and removal of potentially problematic applications. However, Facebook has provided no evidence that it actually applies such a structure in any thorough, systematic way to *prevent* problems – and specifically the

problem of unauthorized access. Indeed, such evidence as Facebook has provided suggests to the contrary that any monitoring that Facebook conducts is largely reactive, rather than preventive.

202. I find that Facebook does not have adequate safeguards in place to prevent unauthorized access to users' personal information by application developers and is thus in contravention of Principles 4.7, 4.7.1, and 4.7.3.

203. On the question of consent, I find Facebook's manner of seeking consent to be problematic in two ways.

204. First, the consent language that Facebook uses is excessively broad. In past cases, our Office has often expressed disapproval of much less broad consent language and has determined that such language was not a sufficient basis for consent. In this case, there is no specificity in Facebook's consent language. Facebook is in effect telling users that whenever they add an application, they must consent to allowing access to almost anything and everything that the developer asks for. In my view, consent obtained on such a basis is meaningless. In the circumstances, the user's meaningful consent to the collection and use of specified information should be sought at each instance of a user's adding an application.

205. Second, technically, application developers' receipt of users' personal information through the Facebook API may be considered not only a collection by the developer, but also a disclosure by Facebook. Accordingly, Facebook has an obligation to ensure that users consent to such disclosure of their personal information. However, given Facebook's platform as it relates to third-party applications, Facebook can meet this obligation by taking reasonable measures to ensure and verify that application developers are obtaining meaningful consent on behalf of Facebook.

206. In its SRR, Facebook takes a big step towards ensuring that users have the necessary knowledge to give meaningful consent regarding the disclosure and collection of their personal information. The SRR includes among its instructions for application developers the requirement that they make it clear to users what information will be used and how it will be used, displayed, or shared. When a user, on being presented with such clear notification, proceeds to add the particular application, the developer can be deemed to have obtained that user's meaningful consent both to its own collection and to Facebook's disclosure of the information in question.

207. But in my view, Facebook's responsibility does not end with simply stating the requirement in the SRR. In order to rely on developers to obtain the users'

consent, Facebook should take further steps to ensure that developers are well aware of the requirement to do so and that they comply with it. For one thing, Facebook should feature the requirement prominently in the Platform Guidelines and other instructions to developers, as well as in the SRR. For another, the company should develop a means of monitoring applications to ensure that developers are complying with the requirement to obtain consent. The company might even consider providing developers with a means of explaining to users what information they need and why (possibly by adjusting the current template so as to provide space for such an explanation).

208. Another consent-related concern that I have is the fact that no specific consent is sought from users for the disclosure of their personal information to applications when their friends and fellow network members add applications. Facebook maintains that, through its privacy settings, users have an extensive ability to choose whether or not they will interact with any particular Facebook application and to block any particular application and opt-out of all Facebook applications in a simple way. However true this statement may be in theory, I would note that users' "ability to choose" would depend on their being knowledgeable about developers' practice of accessing and using third-party information when friends add applications. I would also note that the only way users can control the exposure of their personal information to application developers when their friends and fellow network members add applications is either to opt out of all applications altogether or to block specific applications. Moreover, the latter option would effectively require them to guess which of the more than 350,000 applications their friends and fellow network members are likely to add.

209. I do not consider it appropriate for Facebook to put on users the onus of informing themselves and opting out of the disclosure of their personal information when friends and fellow network members add applications. Nor do I believe that the practice meets the reasonable expectations of users.

210. In sum, with reference to Principles 4.2, 4.2.3, 4.3.2, 4.3.4, 4.3.5, and 4.3.6 and subsection 5(3), I find that Facebook is in contravention of Principle 4.3 in that it does not provide for users' meaningful consent to the disclosure of their personal information to application developers when either the users themselves or their friends and networks add applications.

Recommendations and Response

211. In my preliminary report, I recommended that Facebook consider and implement measures

    (1) to limit application developers' access to user information not required to

run a specific application;

(2) whereby users would in each instance be informed of the specific information that an application requires and for what purpose;

(3) whereby users' express consent to the developer's access to the specific information would be sought in each instance; and

(4) to prohibit all disclosures of personal information of users who are not themselves adding an application.

212. In response, Facebook raised objections as noted in my findings above and in effect declined to implement the recommendations.

Conclusion

213. Accordingly, I conclude that the allegations as they relate to consent and safeguards are well-founded.

214. I would ask that Facebook reconsider my recommendations in the light of my findings above. In our follow-up on other matters in 30 days, we will also check for evidence of acceptance and implementation of these recommendations or acceptable alternatives. Should we find no such evidence, we will then consider how best to address these and other unresolved issues in accordance with our authorities.

Section 5
New Uses of Personal Information

Allegation

215. CIPPIC alleged that Facebook was not notifying users of new purposes for which their personal information would be collected, used, or disclosed, in violation of Principle 4.2.4.

216. In CIPPIC's view, Facebook must both provide notice to users about any new purposes and obtain users' consent before using or disclosing their personal information for those new purposes. However, CIPPIC did not identify any instances where Facebook has introduced a new purpose without giving notice and obtaining consent.

Summary of Investigation

217. Any changes to the purposes for which personal information is collected, used, or disclosed by Facebook would need to be reflected in the Facebook Privacy Policy. In response to CIPPIC's allegation, as outlined above, Facebook cited the following section of its Privacy Policy:

"We reserve the right to change our Privacy Policy and our Terms of Use at any time. Non-material changes and clarifications will take effect immediately, and material changes will take effect within 30 days of their posting on this site. If we make changes, we will post them and will indicate at the top of this page the policy's new effective date. If we make material changes to this policy, we will notify you here, by email, or through notice on our home page. We encourage you to refer to this policy on an ongoing basis so that you understand our current Privacy Policy."

218. Facebook stated, "We have not instituted any material change since this policy has been in effect; all new features have been designed to respect the existing privacy infrastructure."

219. At the time of the complaint, Facebook also stated as follows in its Terms of Use:

"We reserve the right, at our sole discretion, to change, modify, add or delete portions of these Terms of Use at any time without further notice. If we do this, we will post the changes to these Terms of Use on this page and will indicate at the top of this page the date these terms were last revised. Your continued use of the Service or Site after any such changes constitutes your acceptance of the new Terms of Use. If you do not agree to abide by these or any future

Terms of Use, do not use or access (or continue to access) the Service or this Site. It is your responsibility to regularly check the Site to determine if there have been changes to these Terms of Use and to review such changes."

220. It should be noted that the Terms of Use have recently been replaced by the new Statement of Rights and Responsibilities (SRR). The SRR contains a section titled "Amendments", which reads as follows:

    1. *We can change this Statement so long as we provide you notice through Facebook (unless you opt out of such notice) and an opportunity to comment.*
    2. *For changes to sections 7, 8, 9 and 11 (sections relating to payments, applications developers, website operators, and advertisers), we will give you a minimum of three days notice. For all other changes we will give you seven days notice.*
    3. *If more than 7,000 users comment on the proposed change, we will also give you the opportunity to participate in a vote in which you will be provided alternatives. The vote shall be binding on us if more than 30% of all active registered users as of the date of the notice vote.*
    4. *We can make changes for legal or administrative reasons upon notice without opportunity to comment.*

Findings

221. In the absence of any evidence that Facebook has failed to inform its users of new uses of their personal information, I am at present unable to find Facebook to be in contravention of the Act in this regard.

Conclusion

222. Accordingly, I conclude that the allegation relating to new uses of personal information is not well-founded.

Section 6
Collection of Personal Information from Sources Other than Facebook

Allegations

223. CIPPIC alleged that Facebook

(1) was failing to provide users with specific information relating to the purposes and method of collecting personal information from sources outside Facebook, the sources of the information, and the use and disclosure of the information; and

(2) having failed to inform users of these specifics, was therefore not obtaining their meaningful consent.

Summary of Investigation

224. In its Privacy Policy, Facebook states:

> *Facebook may also collect information about you from other sources, such as newspapers, blogs, instant messaging services, and other users of the Facebook service through the operation of the service (e.g., photo tags) in order to provide you with more useful information and a more personalized experience.*

225. In its representations to our Office, Facebook stated that it does not collect personal information from outside sources, but may do so in future and has therefore included the above-cited passage in its Privacy Policy.

Findings

226. In the absence of evidence that Facebook was collecting personal information from outside sources at the time the complaint was filed, I am unable at present to find the company to be in contravention of the *Act* in this regard.

Conclusion

227. Accordingly, I conclude that the allegations relating to collection of personal information from sources other than Facebook are not well-founded.

Section 7(a)
Account Deactivation and Deletion

Allegations

228. CIPPIC alleged that Facebook was in effect offering only an account deactivation option as distinct from an account deletion option and was therefore inappropriately depriving users of a means whereby they could delete all their personal information from the site.

229. CIPPIC stated its general allegation as follows:

> *"[W]e are concerned that Facebook's current practice of effectively offering only the deactivation option to Users leads to confusion as to the nature of the deactivation option and separate availability of a deletion option. … [The deletion] option is inaccessible and users are not notified of it when deactivating their account. Facebook should give users who decide to terminate their accounts a clear option between [temporary] account deactivation and [permanent] account deletion*."

230. CIPPIC specified its concerns as follows:

- Facebook should make equally available to users an account deletion option whereby they can delete their entire accounts so that there is no retention of information by Facebook.
- The account deactivation option should be clearly distinguished from the account deletion option and users should be informed of both.
- The account deactivation option should clearly state that user profiles will be retained by Facebook for future reactivation.
- The account deactivation option should include a specified retention period, preferably set by the user, after which period the information will be deleted from Facebook's records, in accordance with Principles 4.5.2 and 4.5.3.
- User information kept by Facebook during account deactivations should be stored in a secure manner.

Summary of Investigation

231. Since Facebook was made available to the public, users have been able to deactivate their accounts. In the past, users were able to manually delete information in their profile, but not to delete their account all at once. In February 2008, as a result of public criticism and an inquiry by the United

Kingdom's Information Commissioner's Office, Facebook began to allow users to permanently delete their accounts.

232. Querying "delete account" in Facebook's Help section brings users to a page on which both account deletion and account deactivation are distinguished and explained. A request for account deletion can be made from this screen, but a request for account deactivation must be made from the Account Settings page (also titled "My Account"), which users may reach through the Settings link. The Account Settings page includes an option for account deactivation, but not for account deletion. Thus the account deactivation and account deletion options are in effect offered on different screens.

233. Account deletion means that all personal information of a user is removed from active databases, including photo tags. In the Help section, under the rubric "I want to permanently delete my account", Facebook explains account deletion as follows:

"If you deactivate your account from the "Deactivate Account" section on the Account page, your profile and all information associated with it are immediately made inaccessible to other Facebook users. What this means is that you effectively disappear from the Facebook service. However, if you want to reactivate at some point, we do save your profile information (friends, photos, interests, etc.), and your account will look just the way it did when you deactivated if you decide to reactivate it. Many users deactivate their accounts for temporary reasons and expect their information to be there when they return to the service.

"If you do not think you will use Facebook again and would like your account deleted, we can take care of this for you, but keep in mind that you will not be able to reactivate your account or retrieve any of the content or information you have added. If you would like your account permanently deleted with no option for recovery, please submit your request here."

234. However, Facebook has stressed to our Office that deletion of data is technically challenging and that it is impossible to completely delete all information from the site. At the September 2007 meeting of the International Working Group on Data Protection in Telecommunications, Facebook stated that the average retention period for deleted data was 10 to 15 days, but could be even longer in some parts of the system.

235. Account deactivation means that a user profile and all associated content "disappear" from the website itself, but remain on Facebook servers until the user requests deletion or reactivation of the account. In the Help section, under the rubric "How do I deactivate my account?", Facebook explains

account deactivation as follows:

"If you are worried about who can see you and what they can see, you have complete control over this and can edit your settings as you see fit from the Privacy page. If you still want to leave Facebook, you can deactivate your account from the "Settings" tab on the Account page. Deactivation will completely remove your profile and all associated content on your account from Facebook. In addition, users will not be able to search for you or view any of your information. If you reactivate your account, your profile will be restored in its entirety (friends, photos, interests, etc.)."

236. In its representations to our Office, Facebook stated as follows:

"We offer deactivation for those users who wish to disappear for a time; approximately 50% of users who deactivate their accounts come back within the next month following their deactivation, and a smaller number reactivate after that period. User account information for these users is retained to allow people to have a consistent experience if they wish to return. In the time that users are deactivated, they are not present in any way on the site. … Many users are not sure whether or not they wish to return and should have the option to reactivate their account easily."

237. On the subject of retention, Facebook acknowledged that what users upload stays on the site until it is removed by the user or at the request of the user. According to Facebook, this practice reflects user expectations since users treat their Facebook account as a repository of information. For example, as of October 2008, there were 10 billion photos on Facebook. Facebook does not consider it appropriate and in the users' best interests to limit the time that they can store information.

238. The only reference to retention on the Facebook site was found in the Privacy Policy, which states as follows:

"When you use Facebook, you may set up your personal profile, form relationships, send messages, perform searches and queries, form groups, set up events, add applications, and transmit information through various channels. We collect this information so that we can provide you the service and offer personalized features. In most cases, we retain it so that, for instance, you can return to view prior messages you have sent or easily see your friend list. When you update information, we usually keep a backup copy of the prior version for a reasonable period of time to enable reversion to the prior version of that information…

"You understand and acknowledge that, even after removal, copies of User Content may remain viewable in cached and archived pages or if other Users have copied or stored your User Content. …

"Removed information may persist in backup copies for a reasonable period of time but will not be generally available to members of Facebook.

"Where you make use of the communication features of the service to share information with other individuals on Facebook, however, (e.g., sending a personal message to another Facebook user) you generally cannot remove such communications."

Application

239. In making our determinations, we applied Principles 4.1.4(d), 4.5, 4.5.2, 4.5.3, 4.3.8, and 4.8.

240. Principle 4.1.4(d) states in part that organizations shall implement policies and practices to give effect to the principles, including developing information to explain the organization's policies and procedures.

241. Principle 4.5 states in part that personal information shall be retained only as long as necessary for the fulfilment of the purposes for which it was collected. Principle 4.5.2 states in part that organizations should develop guidelines and implement procedures with respect to the retention of personal information and that these guidelines should include minimum and maximum retention periods. Principle 4.5.3 states in part that personal information no longer required to fulfil the identified purposes should be destroyed, erased, or made anonymous.

242. Principle 4.3.8 states that an individual may withdraw consent at any time, subject to legal or contractual restrictions and reasonable notice, and that the organization shall inform the individual of the implications of such withdrawal.

243. Principle 4.8 states that an organization shall make readily available to individuals specific information about its policies and practices relating to the management of personal information.

Findings

244. On the whole, I am satisfied that Facebook is in compliance with Principle 4.3.8 by virtue of offering users an account deletion option, which is in effect a consent withdrawal mechanism. I am also satisfied that Facebook's Help section provides a good explanation of this option vis-à-vis the account

deactivation option. However, I do have some concerns relating to both options.

245. To clarify, I am not suggesting that Facebook establish a retention policy regarding active accounts. Rather, my concerns relate to deactivated accounts. Under Facebook's current account deactivation policy, the personal information of users who have deactivated their accounts is retained indefinitely. Indefinite retention is a contravention of Principle 4.5 and 4.5.3. In my view, a reasonable person would not consider it appropriate for Facebook to continue to retain indefinitely the personal information of a user who has deactivated his or her account and not reactivated it for a long time. While I acknowledge that by deactivating their accounts users are in effect choosing to have Facebook temporarily retain unused personal information, I would note that, the longer an account remains deactivated and the information in it unused, the more difficult it is to argue that retention of the user's personal information is reasonable for the social networking purposes for which it was collected. I am also not suggesting any specific retention period for a deactivated account. Rather, Facebook should set a retention cutoff that a reasonable person would consider appropriate in the circumstances and based on its experiences with user reactivation patterns. It should also inform users of this period when they deactivate their accounts.

246. In sum, with respect to its indefinite retention of users' personal information in deactivated accounts, I find that Facebook is in contravention of Principles 4.5 and 4.5.3.

247. Secondly, although I am generally satisfied that Facebook does provide in its Help section a good explanation of the two options, I am concerned that, as CIPPIC has suggested, by offering only the account deactivation option on users' Account Settings pages, Facebook may cause some users to assume that account deactivation is the only option available to them. I see no reason why Facebook should not and could not easily put an account deletion option, as well as an account deactivation option, on users' Account Settings pages so as to give equal exposure to the two options and make it clear to users that they can choose between the two.

248. Finally, I am also concerned that Facebook does not explain the account deletion and account deactivation options in its Privacy Policy. As I say elsewhere in this report, I am of the view that, for ease of reference by interested users, privacy-related matters should be explained in the organization's privacy policy, regardless of where else they may be explained.

Recommendations and Response

249. In my preliminary report, I recommended that Facebook develop, institute, and inform users of a retention policy whereby the personal information of users who have deactivated their accounts will be deleted from Facebook's servers after a reasonable length of time.

250. I also suggested, as best practice in the interest of clarity for users, that Facebook

    (1) include an account deletion option, as well as an explanation thereof as distinct from account deactivation, on its users' Account Settings pages; and

    (2) include in its Privacy Policy an explanation of the difference between account deletion and account deactivation.

251. In response to my recommendation, Facebook objected on the following grounds:

    "… [A] majority of deactivating users reactivate within weeks, and those who reactivate on a longer timeframe are generally expecting their social connections to be intact when they return. Because the option to delete data is present for users, and because of interdependencies on certain data, setting a firm date for erasing a user's information without clear direction from them in this context would be inappropriate."

252. The Act is clear that organizations must retain personal information only for as long as necessary to fulfil the organization's purposes, that organizations should develop guidelines and implement procedures with respect to the retention of personal information, and that such guidelines should include minimum and maximum retention periods. While I acknowledge that the length of time an organization may retain personal information may vary depending on the circumstances, I do not consider it either necessary or reasonable in the present circumstances for Facebook to retain personal information indefinitely in deactivated accounts.

253. I am also disappointed that Facebook has chosen not to adopt the first of my suggested best practices. I continue to believe that adding an account deletion option on the user's Account Settings would be a simple and effective way of promoting greater transparency for the user.

254. On a more positive note, however, I am pleased to acknowledge that Facebook has agreed to implement my second suggested best practice. Specifically, the

organization has proposed to add the following wording to its Privacy Policy:

"Individuals who wish to deactivate their Facebook account may do so on the My Account page. Removed information may persist in backup copies for a reasonable period, but will not be generally available to members of Facebook. Individuals who wish to delete their accounts may use the attached form to submit their account for the deletion process, which may take several weeks to complete processing."

Conclusion

255. Accordingly, I conclude that the allegation is well-founded insofar as it pertains to Principles 4.5 and 4.5.3.

256. I would ask that Facebook reconsider my recommendation. In our follow-up on other matters in 30 days, we will also check for evidence of acceptance and implementation of this recommendation or an acceptable alternative. Should we find no such evidence, we will then consider how best to address this and other unresolved issues in accordance with our authorities.

Section 7(b)
Accounts of Deceased Users

Allegations

257. CIPPIC alleged that Facebook

(1) by including only in its Terms of Use and not in its Privacy Policy a notice of its intention to keep deceased users' profiles active for memorial purposes, was not obtaining users' meaningful consent for such use of their personal information; and

(2) was obligating users, in contravention of Principle 4.3.3, to consent to this purpose as a condition of service even though memorializing a profile is not necessary to Facebook's primary purpose of providing a social networking venue.

258. CIPPIC specified its concerns as follows:

- Facebook should, in its Privacy Policy as well as its Terms of Use, inform users of the practice of keeping deceased users' profiles active for memorial purposes, in keeping with Principle 4.8.1.
- Facebook should give users a clear opportunity to opt out of posthumous displays of their profiles, in keeping with Principle 4.3.8.
- Facebook should provide a procedure whereby relatives of a deceased user can request the removal of a user's profile, in keeping with subsection 5(3). CIPPIC suggested that "a reasonable person would not expect Facebook to continue to display a user's profile posthumously despite the user's family's wishes to the contrary."

Summary of Investigation

259. At the time of the complaint, users were informed in the Terms of Use, to which they were required to agree when they registered, that Facebook retained the right to keep a deceased user's profile active for memorial purposes:

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

260. Currently, the new Statement of Rights and Responsibilities (SRR), which replaces the Terms of Use, does not mention Facebook's practice of keeping accounts active for memorial purposes. However, the practice itself continues,

as evidenced by the following Help Centre search entry:

"I'd like to report a deceased user or an account that needs to be memorialized.
*" Please **report this information here** so that we can memorialize this person's account. Memorializing the account removes certain more sensitive information like status updates and restricts profile access to confirmed friends only. Please note that in order to protect the privacy of the deceased user, we cannot provide login information for the account to anyone. We do honor requests from close family members to close the account completely."*

261. The "report this information here" link leads to a form that requests the deceased's name, date of birth, account email addresses, networks, and the reporter's relationship to the deceased. This form begins with the following statement:

"IMPORTANT: This form is solely for the reporting of a deceased person to memorialize the person's account. Please note that unrelated inquiries through this form may not receive a response."

262. Facebook does not view memorializing a site as a new purpose under the *Act*. In its representations to our Office, Facebook stated as follows:

"Our policy leaves the choice of whether or not a profile is 'memorialized' or retained indefinitely, to the next of kin. … Friends of users who were killed …have enjoyed using a user's Facebook page as a memorial and…we concluded that the legal next of kin is the proper person to make a decision as to whether the deceased would have wanted the site to stay up for their friends."

Application

263. In making our determinations, we applied Principles 4.1.4(d), 4.2.1, 4.2.3, 4.3.2, 4.3.3, 4.3.5, 4.3.6, 4.3.8, and 4.8.

264. Principle 4.1.4(d) states that organizations shall implement policies and practices to give effect to the principles, including developing information to explain the organization's policies and procedures.

265. Principle 4.2.1 states that the organization shall document the purposes for which personal information is collected in order to comply with Principle 4.8 (Openness) and Principle 4.9 (Individual Access).

266. Principle 4.2.3 states in part that the identified purposes should be specified at

or before the time of collection to the individual from whom the personal information is collected.

267. Principle 4.3.2 states in part that organizations shall make a reasonable effort to ensure that the individual is advised of the purposes for which the information will be used.

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

269. Principle 4.3.5 states in part that in obtaining consent the reasonable expectations of the individual are also relevant.

270. Principle 4.3.6 states in part that the way an organization seeks consent (express or implied) may vary, depending on the circumstances and the type of information collected.

271. Principle 4.3.8 states that an individual may withdraw consent at any time, subject to legal and contractual restrictions and reasonable notice and that the organization shall inform the individual of the implications of such withdrawal.

272. Principle 4.8 states that an organization shall make readily available to individuals specific information about its policies and practices relating to the management of personal information.

Findings

273. In my preliminary report, I stated as follows:

274. *"In our investigation, we have identified the following matters of concern with regard to Facebook's practice of memorializing the accounts of deceased users:*

(1) In consideration of Principles 4.2.1, 4.2.3, 4.3.2, and 4.8, I am concerned that, by limiting its description of this practice to its Terms of Use only, Facebook is failing to make a reasonable enough effort in the circumstances to ensure that its users are advised of this intended use of their personal information. I consider the description in the Terms of Use to be a good one. However, in deference to its users and for ease of reference, Facebook should also include an explanation of the practice in its Privacy Policy.

(2) In consideration of Principles 4.3.3 and 4.3.8, I am concerned that, by omitting to allow users to opt out of Facebook's future use of their personal information for purpose of memorializing their accounts, Facebook is in effect requiring them to consent to an unnecessary purpose as condition of service.

275. With regard to my first concern above, I would note that, along with its Terms of Use, Facebook also appears to have recently discontinued any adequate description of its practice of memorializing accounts. There is no mention of the practice in the new SRR, and I do not consider the Help section material on how to report "an account that needs to be memorialized" to be an adequate description of the practice itself or adequate notification to users generally. In my view, Facebook's keeping a deceased user's account active under special status for memorial purposes constitutes an intended use of the user's personal information. As such it should be both well-documented and well-communicated to users. The fact that Facebook no longer provides a good description of the practice in its Terms of Use is all the more cause for my concern that such a description be included in Facebook's Privacy Policy.

276. I find therefore that, with respect to informing individuals of its practice of account memorialization, Facebook is in contravention of 4.2.1, 4.2.3, 4.3.2, and 4.8.

277. As for my second concern, after reconsidering the position I took in my preliminary report, I have altered my position on user consent to the memorialization of accounts.

278. On the basis that Facebook's practice of keeping the accounts of deceased users active under special memorialized status constituted use of personal information for an unnecessary purpose, I was initially inclined to conclude that CIPPIC's allegations in this regard were well-founded with reference to Principles 4.3.3 and 4.3.8. However, I have since come to consider the question in the light of Principle 4.3.5.

279. This principle stresses the relevance of individuals' reasonable expectations in matters of consent. In my view, most typical Facebook users would welcome the prospect of being posthumously remembered and honoured by their friends on the site. Likewise, I am sure that users generally would regard the freedom to pay their respects to deceased friends and fellow users as an important part of the Facebook experience. I am also mindful that in memorializing an account Facebook takes care to remove information such as status updates and to restrict profile access to confirmed friends.

280. I am satisfied therefore that the practice of account memorialization meets the reasonable expectations of users and that Facebook may thus rely upon their continuing implied consent to the practice. In the circumstances, I do not believe that an opt-out mechanism is warranted. However, as I indicated above, Facebook should at least provide a basis for users' meaningful consent to the practice by describing it in the Privacy Policy.

Recommendations and Response

281. In my preliminary report, I recommended that Facebook

    (1) include in its Privacy Policy, in the context of all intended uses of personal information, an explanation of the intended use of personal information for the purpose of memorializing the accounts of deceased users; and

    (2) provide, and notify users of, a means whereby they may opt out of Facebook's intended use of their personal information for the purpose of memorializing accounts.

282. In response, Facebook has in effect declined to implement either recommendation, on the following grounds:

    "We still do not believe that retaining data for the purpose of allowing users to remember their friends constitutes another use under PIPEDA, and in any event users are perfectly capable of using other means to express their wishes in this area. We also believe that it would be inappropriate to create a standard for handling information in this case that would be at variance with existing legal norms for the disposition of estate property."

    Facebook also noted that services around access to digital assets in the event of death are carried out by private vendors.

Conclusion

283. I conclude that the allegations are well-founded as they relate to the requirement of consent, and well-founded as they relate to documentation and notification.

284. I will not insist upon Facebook's implementation of my second recommendation. My first, however, remains. I would strongly urge Facebook to reconsider it.

285. In our follow-up on other matters in 30 days, we will also check for evidence of acceptance and implementation of my first recommendation above. Should we find no such evidence, we will consider how best to address this and other

unresolved issues in accordance with our authorities.

Section 8
Personal Information of Non-users

Allegations

286. CIPPIC alleged that Facebook was not obtaining consent from non-users for the uploading of their personal information to the site, in contravention of Principle 4.3.

287. In this regard, the CIPPIC complaint deals with Facebook's collection and use of the personal information of non-users in the following situations:

(1) Users can post the personal information of non-users in their own profiles, as well as the profiles of other users through features such as "News Feed" and "Wall". Also, users can tag images of non-users with their names in photos or videos.

(2) Users can provide Facebook with the email addresses of non-users for the purpose of inviting them to join the site.

288. CIPPIC specified its concerns as follows:

- In the case of tags in photos and videos, the personal information is disseminated through the Facebook site. Non-users are not notified that their personal information has been provided to Facebook to be viewed by others. Non-users cannot untag themselves unless they join Facebook. Since some personal information in photographs and videos may be sensitive in that it may portray non-users in situations that could tarnish their reputation and prevent them from obtaining potential employment, Facebook should be obtaining express consent from non-users, in accordance with Principle 4.3.5.
- In order to send non-users invitations to join the site, Facebook collects from users the email addresses of non-users, retains these email addresses indefinitely unless it receives a deletion request from the non-user, and does not inform the non-users that their email addresses are being retained or that they can request deletion. Facebook can, in CIPPIC's view, generate an email invitation without storing the non-user's email address. For Facebook to retain non-users' email addresses for any extended period of time without their knowledge or consent is a violation of Principle 4.3.

- Facebook should prohibit users from posting non-users' information without consent and should impose on users a penalty of unilateral removal of unauthorized material. In some circumstances, such as persistent non-consensual posting of non-users' information, Facebook should impose a more extreme penalty such as account termination.
- Facebook should provide non-users with an efficient way of finding their personal information and removing it from the site. In CIPPIC's view, Facebook's neglecting to provide non-users with any opportunity to seek out and remove their personal information stored on the site is unacceptable in the circumstances and a violation of subsection 5(3) of the Act.

289. CIPPIC also alleged that non-users who are tagged in photos and videos are searchable on the site. Facebook denied that this was the case, and our Office has found no evidence to support CIPPIC's allegation.

Summary of Investigation

290. Facebook's Privacy Policy mentions non-user personal information only in the context of its invitation service:

"If you choose to use our invitation service to tell a friend about our site, we will ask you for information needed to send the invitation, such as your friend's email address. We will automatically send your friend a one-time email or instant message inviting him or her to visit the site. Facebook stores this information to send this one-time invitation, to register a friend connection if your invitation is accepted, and to track the success of our referral program. Your friend may contact us at info@facebook.com to request that we remove this information from our database."

The Privacy Policy does not raise the subject of non-users' consent.

291. At the time of the complaint, both the Terms of Use and the Code of Conduct prohibited the posting of information that would violate or infringe the privacy rights of third parties, including contact information, social security numbers, and credit card numbers. However, the wording used did not specifically mention any requirement for obtaining consent before posting non-user personal information.

292. The new Statement of Rights and Responsibilities (SRR), which replaces the Terms of Use and the Code of Conduct, contains the following section titled "Protecting Other People's Rights":

"We respect other people's rights, and expect you to do the same.

1. *You will not post content or take any action on Facebook that infringes someone else's rights or otherwise violates the law.*
2. *We can remove any content you post on Facebook if we believe that it violates this Statement.*
3. *We will provide you with tools to help you protect your intellectual property rights. To learn more, visit our* ***How to Report Claims of Intellectual Property Infringement*** *page.*
4. *If we removed your content for infringing someone else's copyright, and you believe we removed it by mistake, we will provide you with an* ***opportunity to appeal****.*
5. *If you repeatedly infringe other people's intellectual property rights, we will disable your account when appropriate.*
6. *You will not use our copyrights or trademarks (including Facebook, the Facebook and F logos, FB, Face, Poke, Wall and 32665) without our written permission.*
7. *If you collect information from users, you will: obtain their consent, make it clear you (and not Facebook) are the one collecting their information, and post a privacy policy explaining what information you collect and how you will use it.*
8. *You will not post anyone's identification documents or sensitive financial information on Facebook."*

293. The SRR does not specifically address obtaining consent to upload the personal information of third parties. Moreover, unlike the former Terms of Use and Code of Conduct, it does not specify that the privacy rights of third parties are among the rights that users must not infringe.

294. On the issue of photographs, Facebook stated in its representations to our Office that "users make their own choices about what they put up" and that, under copyright law, "the reproduction rights for a photograph or video generally belong to the person who took it." From this, our Office inferred that Facebook believes that the responsibility for obtaining the consent of non-users rests not with Facebook, but rather with the users who upload non-users' personal information.

295. Facebook makes it possible for users to "tag" – that is, identify by name in a photo – any persons appearing in a posted photo. When a user posts a photo, Facebook asks the user whether he or she wishes to add tags. Facebook permits non-users to be tagged, but permits only users to have tags removed. Facebook offers a feature that allows the user to enter the email address of the tagged person. With the provision of the email address, Facebook can

determine whether the tagged person is a non-user. Facebook then sends a message to the non-user notifying the person of the tagging, providing a link to the photo and extending an invitation to join Facebook. Non-users who wish to have their tags removed from photos cannot do so without first joining Facebook.

296. Apart from the context of photo tagging, Facebook runs an invitation program whereby it asks users for the email addresses of non-users in order to send them invitations to join Facebook. The "Invite Your Friends" page allows for users to provide Facebook either with single addresses or with access to the address books of their Webmail accounts or email applications. The page makes no reference to a requirement for non-users' consent.

297. The invitation that Facebook sends to non-users permits the invitee to opt out of "any future commercial mailings from Facebook". If an invitee opts out of joining Facebook, the next user who attempts to send the same non-user an invitation receives a message to the effect that the person cannot be invited. The non-user is not informed that Facebook retains the email address even if the invitation is not accepted.

298. In its representations to our Office, Facebook stated its position as follows:

"Facebook does retain the email address an invitation is sent to and a record of the account from which it was sent, in order to make the friend connection between the two individuals if and when the invitation is accepted. Previous invitations are kept as well so that users can make connections with all individuals who have invited them. This is primarily to serve the interests of the person who uploaded the contact information, to allow them to know when their friend (notably, the person whose email address they already had in their address book) joins the service."

299. Facebook also confirmed that the email addresses are used solely for the purpose of the invitation service and are not available to any user of the service other than the one who provided it. Facebook acknowledged that it retains these email addresses indefinitely unless it receives a request from the non-user to remove it.

300. On the "Invite Your Friends" page, there is an "Invite History" function whereby users may view the entire history of their invitations, including members who have joined because of them. When non-users register for Facebook, any friend requests they have received will appear on their home page.

Application

301. In making our determinations, we applied Principles 4.3 and 4.5.

302. Principle 4.3 states that the knowledge and consent of the individual are required for the collection, use, or disclosure of personal information, except where inappropriate.

303. Principle 4.5 states in part that personal information shall be retained only as long as necessary for the fulfilment of the purposes for which it was collected.

Findings

304. In my preliminary report to Facebook, I stated the following:

305. *"In our investigation, we have identified the following matters of concern with regard to Facebook's treatment of information of non-users:*

(1) In consideration of Principle 4.3, I am concerned that Facebook does not have non-users' informed consent to their being tagged in photos. In my view, given that the company makes such tagging possible and uses the occasion of tagging to invite non-users to become members, it is incumbent on Facebook to seek the non-users' consent.

(2) Likewise in consideration of Principle 4.3, I am also concerned that Facebook does not obtain the consent of non-users in respect of its invitation feature, whereby it actively encourages users to provide non-users' email addresses, uses these addresses to send invitations to the non-users, retains the addresses indefinitely, and further uses the addresses to provide users with an invitation history and track the success of its referral program.

(3) In consideration of Principle 4.5, I am concerned that, in cases where a non-user does not accept the invitation to join Facebook, the company nevertheless retains the non-user's email address indefinitely for purposes of providing the user with an invitation history and tracking the success of its referral program."

306. In conveying these concerns, I was mindful of a clear distinction between activities conducted by Facebook users for strictly personal reasons and activities in which Facebook itself is involved. When users post information about non-users to their profiles, Walls, or News Feeds, such postings are made for personal purposes and as such fall outside the purview of the Act. The Act would apply only where Facebook uses non-users' personal information for purposes of its own.

307. One such activity is the email notification of non-users who have been tagged in photographs. When a user tags a non-user, the user has the option of uploading the non-user's email address. Facebook then uses the address to send the non-user a notification of the photo tagging and an invitation to join Facebook. Obviously, non-users greatly benefit from being notified that they have been tagged. However, Facebook's purposes are also being served through the invitation that is extended to the tagged non-user, since Facebook's ability to generate revenue is closely tied to its membership numbers.

308. The "Invite New Friends" email invitation feature is also an activity by Facebook. Facebook maintains that it provides this service for the use of its users, but clearly the service also helps Facebook gain new members and thereby increase its ability to generate revenue.

309. In my view, therefore, Facebook should assume some responsibility for seeking consent in these contexts. The question is, what kind of responsibility?

310. I was initially of the view that Facebook should take responsibility for directly *obtaining* from non-users their consent to being tagged in photos and to the collection and use of their email addresses for invitation purposes. Indeed, I said that it was "incumbent on Facebook to seek the non-users' consent." Upon further reflection, however, I have come to see the question of responsibility in a different light.

311. In my view, tagging constitutes personal use by Facebook users. The fact that Facebook makes photo tagging possible is not in itself sufficient to necessitate responsibility for consent, no more than the fact that it makes possible other features such as Wall and News Feed. Nevertheless, I continue to believe that responsibility for consent should begin to apply at the point in the tagging process where Facebook actively solicits non-users' email addresses from users with the intention of using them for purposes of its own.

312. Furthermore, Principle 4.3 states that the knowledge and consent of the individual are required. For situations where one party collects from a second party the personal information of a third, our Office has determined in previous cases that, depending on the circumstances, it may be deemed incumbent on the second party (in this case, the Facebook user) to directly obtain the consent from the third (in this case, the non-user). We have also determined in such cases that the first party (in this case, Facebook), though not responsible for directly obtaining consent, must nevertheless take reasonable measures to ensure that consent is obtained by the second party. In other words, the first party must exercise due diligence to ensure that the requirement for consent is met.

313. Accordingly, I am satisfied that Facebook may reasonably rely on users to obtain non-users' consent, provided that the company itself exercises reasonable due diligence. Moreover, I believe that reasonable due diligence in the circumstances would consist in taking appropriate steps to ensure that users are well aware that they must obtain non-users' consent before disclosing their email addresses to Facebook. This would mean not only informing users clearly of the consent requirement in the Privacy Policy, but also notifying them of the requirement at each instance of disclosing non-users' email addresses to Facebook. It would also mean enforcing punitive measures to deal with users who are found to be in violation of the consent requirement.

314. Regrettably, Facebook does not at present exercise, nor has it exercised in the past, such due diligence with respect to non-users' consent. I find therefore that Facebook is in contravention of Principle 4.3 in this regard.

315. Facebook's *retention* of non-users' email addresses beyond the initial use is a different matter, warranting a much higher degree of responsibility on the company's part. In its direct invitation to non-users, Facebook has, but does not use, the opportunity to inform them of its further intention, and give them a means to opt out, of retaining their email addresses for purposes of providing an invitation history and tracking the success of its referral program. Facebook is thus retaining and using the personal information of non-users for these purposes without their knowledge and consent. I find therefore that the company is in contravention of Principle 4.3 also in this regard.

316. I also find that, by retaining non-users' email addresses indefinitely beyond the initial purpose for which they have been collected, Facebook is in contravention of Principle 4.5.

Recommendations and Response

317. In my preliminary report, I recommended that Facebook

(1) consider and implement measures to address our concerns about non-users' lack of knowledge of, and consent to, their being tagged in photographs;

(2) consider and implement measures to improve its invitation feature so as to address our Office's concerns about non-users' lack of knowledge and consent to Facebook's collection, use, and retention of their email addresses; and

(3) set a reasonable time limit on the retention of non-users' email addresses

for purposes of tracking invitation history and the success of the referral program.

318. In response to my first and second recommendations, Facebook declined to implement on the following grounds:

"… Facebook believes we continue to provide significantly greater notice to nonusers as to the presence of any information about them on our site than does any other site on the web. If a nonuser wishes to block further notifications, we honor that request, and data is otherwise retained at the direction of the user who uploaded it initially, making action Facebook would take to delete the data inappropriate without an intervening action by the person who uploaded it in the first place."

319. As to the practice of tagging non-users, Facebook commented as follows:

"With regard to photographs in particular, Facebook's tagging infrastructure offers users more notice than they get on other websites as to the presence of a photograph they may want to review. While on most sites a picture of an individual can be uploaded and they may have no idea of its presence, Facebook provides a means for them to be notified and to get in touch with the person who uploaded the photo if they have an objection. For non-users, this can be done by adding an e-mail address to a tag. Furthermore, we have designed the tagging infrastructure to allow removal of tags by the individual tagged, and for blocking of further emails if the recipient so desires."

320. Over all, Facebook has argued that non-user data is the responsibility of the user who uploads it, that the photo tagging and invitation features constitute personal uses by users themselves, and Facebook provides non-users with better notice than any other website about the presence of their data on the site.

321. As was also the case with my other recommendation relating to retention, Facebook made no direct response to my third recommendation above.

Conclusion

322. I conclude that the allegations as they relate to consent and retention in the context of invitations are well-founded. I would ask that Facebook reconsider recommendations 2 and 3 in light of my findings above. In following up on other matters in 30 days, we will also check for evidence of acceptance and implementation of these recommendations or acceptable alternatives to them. If we find no such evidence, I will then consider how best to pursue these and other unresolved issues in accordance with our authorities.

Section 9
Facebook Mobile and Safeguards

Allegation

323. With respect to users of the mobile version of the Facebook website (Mobile Facebook), CIPPIC alleged that, by providing such users with a persistent cookie having no apparent expiration date, Facebook was failing to properly safeguard their personal information, in contravention of Principles 4.7, 4.7.1, and 4.7.3.

324. Specifically, CIPPIC cited the following security concerns:

    (1) If a user logs onto his or her Facebook account by means of another person's mobile device and forgets to log off, the other person will have access to the user's Facebook account indefinitely, even if the user changes the password.

    (2) If a user gives his or her Facebook password to another person, that person can log in as the user on a mobile device and have access indefinitely, even if the user changes the password.

325. In CIPPIC's view, Facebook should have a cookie that expires within an appropriate period of time and whenever users change their passwords online.

326. Because special research was required, our Office investigated this allegation separately and under a different file number from CIPPIC's other allegations in its complaint against Facebook. This allegation was not covered in our preliminary report.

Summary of Investigation

327. Cookies are small text files embedded in HTTP requests and responses and sent between a web browser and a web server. They are issued by the web server when a user first visits a website. They are stored on a web browser on the user's computer or device. A persistent cookie continues to be stored on the user's machine even after the session ends, until a given expiry date.

328. In the context of Facebook Mobile, the purpose of the persistent cookie is to obviate the necessity for users to log in every time they access Facebook from a mobile device.

329. From a mobile device such as a Blackberry or iPhone, the Facebook website

can be accessed by several different methods. The one specifically mentioned in the CIPPIC allegation is that of entering http://m.facebook.com in the web browser of the mobile device. This alternative to the www.facebook.com URL uses a visual layout more suited to the small screens of mobile devices and is recommended for the Blackberry browser and Internet Explorer Mobile.

330. Our Office used the services of a software engineering firm to perform tests on how various mobile devices interact with m.facebook.com.

Overview of the testing

331. We tested session management with m.facebook.com on four platforms:

1. Blackberry;
2. iPhone;
3. Windows Mobile; and
4. desktop computer.

The mobile devices selected represent the majority of mobile devices having web browsers.

332. The following tests were completed on each platform:

1. Loading the m.facebook.com website from the browser on the mobile device by providing username and password.
2. Verifying the cookie expiration by waiting the amount of time specified in the cookie and then attempting to perform an action on the Facebook personal status message.
3. Modifying personal data on m.facebook.com before changing the password on a desktop machine.
4. Modifying personal data on m.facebook.com after changing the password on a desktop machine.

333. The test results were essentially the same for all platforms. This was expected since the behaviour of m.facebook.com is driven by the server and not the mobile device.

Cookie expiry date (Tests 1 and 2)

334. When a user first logs onto the m.facebook.com website, an HTTP Post message is sent to host m.facebook.com providing the username and password. Facebook responds with a 302 HTTP response accepting the request and essentially redirecting the web browser to the Facebook home

page.

335. Within the response are several “Set-Cookie” headers asking the web browser to save specific cookies identifying the session. Five cookies are sent to the web browser from Facebook in this response.

336. The testing revealed that one of these is the persistent cookie that m.facebook.com uses to identify and remember a user’s session for up to 14 days. Further testing confirmed that, after 14 days, the user is prompted to re-authenticate. It should be noted, however, that each time the user visits the m.facebook.com site, the cookie timeout is extended for another 14 days.

337. Facebook has acknowledged its use of a 14-day persistent cookie on m.facebook.com. According to Facebook, “a persistent cookie is used to provide users with convenient access to their information.”

338. In its representations to our Office, Facebook responded to CIPPIC’s allegations as follows:

“Facebook’s practices with regard to mobile access do not differ from the mainstream of any service that allows connections from mobile devices. It is standard to allow repeated sign-ins once a device is authenticated. For example, the default setting on the Blackberry service is not to require a complex authentication scheme with every use. Some users may choose to put a password on their Blackberry for enhanced security, just as users may choose to sign out of Facebook on their mobile device such that they must explicitly sign-in again the next time. That is not required under any reasonable interpretation of PIPEDA, nor should it be.”

339. Users can log out of their Facebook account by scrolling down to the bottom LOGOUT button. With m.Facebook.com, as with the www.facebook.com URL, another persistent cookie is used to remember users’ id names, but not their passwords. In other words, when users log back onto their Facebook accounts, their email addresses are remembered, but they must re-enter their passwords.

340. Facebook mentions its use of cookies in its Privacy Policy:

“When you enter Facebook, we collect your browser type and IP address. This information is gathered for all Facebook visitors. In addition, we store certain information from your browser using "cookies." A cookie is a piece of data stored on the user's computer tied to information about the user. We use session ID cookies to confirm that users are logged in. These cookies terminate once the user closes the browser. By default, we use a persistent

cookie that stores your login ID (but not your password) to make it easier for you to login when you come back to Facebook. You can remove or block this cookie using the settings in your browser if you want to disable this convenience feature."

341. The Privacy Policy makes no specific reference to the 14-day persistent cookie used on the m.facebook.com URL. When asked whether the use of persistent cookies was mentioned elsewhere on the Facebook site, Facebook replied:

"Cookies are mentioned in the privacy policy at the appropriate level of generality, and any necessary linguistic clarifications will be made in the upcoming revision to the privacy policy."

Results after password change (Tests 3 and 4)

342. After logging onto the m.facebook.com site from a mobile device, we used another platform to change the password to a Facebook account. We then returned to the mobile device and attempted to perform an action on the Facebook account. The attempt was unsuccessful. Instead, we were redirected to the login screen and forced to re-authenticate.

Summary of testing on m.Facebook.com

343. The testing revealed the following with respect to all four platforms:

- When users log onto m.facebook.com, whether from a mobile device or a desktop machine, the Facebook website sends back a persistent cookie with a valid expiration date of 14 days.
- When a cookie expires, any action taken on the website requires users to re-authenticate.
- Contrary to CIPPIC's allegation, when a password change is performed on another platform, any subsequent request from a mobile device already logged on to m.facebook.com is denied by Facebook and the mobile user is prompted to re-authenticate.

Industry review

344. On review, our Office found that there are no official industry specifications or standards that websites must follow with regard to session management. However, we learned that an organization known as the Open Web Application Security Project (OWASP) promotes the development of secure applications and has created several guidelines addressing issues of session management. Among many other things, OWASP recommends to website creators that

sessions should timeout after 5 minutes for high-value applications, 10 minutes for medium-value applications, and 20 minutes for low-value applications. Although OWASP has not provided actual definitions for high-, medium-, or low-value data, it does cite accounting, high-value banking and electronic trading systems, health records, and government records as examples of high-value data and blogs and forums as examples of low-value data.

345. However, our Office's review of how various websites manage sessions indicates that the OWASP guidelines are not widely used in the industry. Most websites seem reluctant to re-prompt a user to re-authenticate after a relatively short period of inactivity because it may detract from the usability of the site. Some banking websites offering online banking do prompt users to re-authenticate after relatively short periods of inactivity (e.g., 30 minutes in one case and 10 minutes in another).

346. Over all, it appears that in the industry user convenience takes precedence over security concerns in the context of session management for applications on mobile devices. However, it should be noted that users always have the option of password-protecting the entire device, just as they have with a desktop or laptop computer.

Application

347. In making our determinations, we applied Principles 4.1.4, 4.7, 4.7.1, 4.7.3, and 4.8.

348. Principle 4.1.4 states in part that organizations shall implement policies and practices to give effect to the principles, including, among other things, developing information to explain the organization's policies and procedures. Principle 4.8 states that an organization shall make readily available to individuals specific information about its policies and practices relating to the management of personal information.

349. Principle 4.7 states that personal information shall be protected by security safeguards appropriate to the sensitivity of the information. Principle 4.7.1 states in part that the security safeguards shall protect personal information against loss or theft, as well as unauthorized access, disclosure, copying, use, or modification. Principle 4.7.3 states in part that the methods of protection should include technological measures.

Findings

350. CIPPIC specified that it was concerned about two scenarios of potential

unauthorized access and use of Facebook users' personal information via mobile devices. I am satisfied that Facebook provides users both with a simple method of logging out of sessions on m.Facebook.com and, contrary to CIPPIC's allegations, with the additional security safeguard of an ability to effectively cease Facebook sessions initiated on mobile devices by changing their passwords on other platforms. Users themselves should assume the burden of responsibility for safeguarding their personal information in their Facebook accounts by ensuring that their mobile devices are password-protected and by not sharing their Facebook passwords or otherwise lending or giving their mobile devices to other people. (I should note here that, in its new Statement of Rights and Responsibilities, Facebook prohibits sharing passwords and giving others access to one's account.)

351. In sum, I find that Facebook is not in contravention of Principles 4.7, 4.7.1, and 4.7.3 in the circumstances.

Conclusion

352. Accordingly, I conclude that the allegation is not well-founded.

353. Nevertheless, with reference to Principles 4.1.4 and 4.8, I would strongly suggest as a best practice that Facebook expand its treatment of cookies in its Privacy Policy so as to fully explain the use of all cookies on the site and the effect of such use on sessions, including sessions initiated via Facebook Mobile.

Section 10

Monitoring for Anomalous Activity

Allegation

354. CIPPIC alleged that Facebook was not informing users that it monitors the site for anomalous behaviour and, in particular, failed to mention this practice in its Privacy Policy, in violation of Principle 4.8.

Summary of Investigation

355. As evidence that such monitoring takes place, CIPPIC cited an interview with a Facebook executive in which he had acknowledged that Facebook used technology to actively search for anomalous behaviour.

356. In arguing that users are well aware that their activities are monitored, Facebook pointed to the fact that its "Mini-Feed" and "News Feed" features were based on monitoring of user activity. (Mini-Feed is no longer a Facebook feature.)

357. Furthermore, in its representations to our Office, Facebook acknowledged its monitoring activities as follows:

"[We use] certain algorithms to protect users on Facebook by monitoring anomalous behaviour and…are quite open with how this activity works, especially with those it directly affects on the site. Where users cross the tripwires set by our anomalous activity monitoring algorithms, they are given a real-time notice that they have exceeded the relevant limits. For instance, sending too many friend requests – especially if those requests have been reported by other users as harassing conduct – will result in the suspension of a user's ability to send friend requests. We use this infrastructure broadly to prevent abuse of the site by spammers and scammers, and to keep users safer more broadly by quickly showing anyone who might attempt to take advantage of our younger users that their misbehaviour will result in consequences."

358. At the time of the complaint, the Facebook Terms of Use contained a section entitled "User Conduct", which listed and described 15 types of activities prohibited on the site – for example, harvesting or collecting email addresses or other contact information of other users from the site by electronic or other means for the purposes of sending unsolicited emails or other unsolicited communications. Further down in the Terms of Use, under "User Content Posted on the Site", Facebook went on to state as follows:

"You understand and agree that the Company may, but is not obligated to, review the Site and may delete or remove (without notice) any Site Content or User Content in its sole discretion, for any reason or no reason, including User Content that in the sole judgment of the Company violates this Agreement or the Facebook Code of Conduct, or which might be offensive, illegal, or that might violate the rights, harm or threaten the safety of users or others".

359. The new Statement of Rights and Responsibilities (SRR), which replaces the Terms of Use, lists several types of prohibited activities and also advises as follows in a section titled "Termination":

    "If you violate the letter or spirit of this statement, or otherwise create possible legal exposure for us, we can stop providing all or part of Facebook to you. We will generally try to notify you, but have no obligation to do so. …"

    However, the new SRR does not explicitly indicate that Facebook will review or monitor for anomalous activity.

360. The first paragraph of the Facebook's Safety section states as follows:

    "… [W]e are constantly improving our systems for identifying and removing inappropriate content and people from the site."

361. Facebook also noted that its monitoring for anomalous activity was publicly described in its May 2008 agreement with the U.S. Attorneys General, which is aimed at making Facebook safer for underage users. In part, Facebook agreed to "continue to use technological tools that identify potentially inappropriate approaches to minors" and take "appropriate action as necessary to limit or forbid site access to users based on their inappropriate activity."

Application

362. In making our determinations, we applied Principles 4.1.4, 4.2.1, 4.3.2, and 4.8.

363. Principle 4.1.4 states in part that organizations shall implement policies and practices to give effect to the principles, including developing information to explain the organization's policies and procedures.

364. Principle 4.2.1 states that the organization shall document the purposes for which personal information is collected in order to comply with Principle 4.8 (Openness) and Principle 4.9 (Individual Access).

365. Principle 4.3.2 states in part that organizations shall make a reasonable effort to ensure that the individual is advised of the purposes for which the information

will be used.

366. Principle 4.8 states that an organization shall make readily available to individuals specific information about its policies and practices relating to the management of personal information.

Findings

367. Facebook openly acknowledges that it monitors the site for anomalous behaviours. However, whereas the former Terms of Use both set out types of prohibited behaviours and informed users that it monitored the site for these behaviours, the new SRR is silent about the practice of monitoring. Moreover, the Privacy Policy contains no mention of the practice. Indeed, at present only a single sentence in the site's Safety section implies, but does not explicitly state, that Facebook monitors users' activities.

368. While I do not find the practice to be unreasonable or inappropriate in itself, in consideration of the Principles cited above I am concerned that Facebook is not making a reasonable effort to document it and inform users of it. I must reiterate my view that, where an organization posts a formal Privacy Policy for reference by individuals, that document should be reasonably comprehensive. It should, in other words, endeavour to explain all the organization's privacy-related practices, even if they are explained in whole or part elsewhere.

369. In sum, with respect to notifying users that it monitors the site for anomalous activity, I find Facebook to be in contravention of Principles 4.1.4, 4.2.1, 4.3.2, and 4.8.

Recommendation and Response

370. In my preliminary report, I recommended that Facebook include in its Privacy Policy an explanation of its practice of monitoring its site for anomalous activity.

371. In response, Facebook has proposed to include the following wording in its Privacy Policy:

"To improve the security of the site, Facebook uses a variety of technological systems to detect and address anomalous activity that may be undertaken by users. This may on occasion result in a temporary or permanent suspension of some functions for some users on the Facebook service."

372. Facebook has stated that any language changes in its Privacy Policy will need to go through a "notice and comment period" with users. However, regardless of user acceptance, our Office expects Facebook to honour its commitment to

meet these recommendations.

Conclusion

373. I am satisfied that, once implemented, Facebook's proposed corrective measure as set out above will meet our recommendation and bring the organization into compliance with the Act. Accordingly, I conclude that the allegation in this regard is well-founded and resolved.

374. We will be following up with Facebook on the status of its implementation of this measure within 30 days.

Section 11
Deception and Misrepresentation

Allegations

375. CIPPIC alleged that Facebook

(1) was misrepresenting itself by claiming to be purely a social networking site when in fact it was engaged in other activities not clearly explained, such as advertising and third-party applications, in contravention of Principles 4.3.2 and 4.4.2; and

(2) was misrepresenting users' level of control over their personal information, in contravention of Principles 4.3.2 and 4.4.2.

Summary of Investigation

376. We found no evidence that Facebook is willfully misleading or deceiving users about the purposes for which it collects information or is obtaining consent through deception.

Findings

377. In my view, allegations of deception are serious and require at least some evidence of an intent to deceive. As we have found no such evidence, I am unable to find Facebook to be in contravention of the *Act*.

Conclusion

378. Accordingly, I conclude that the allegation of misrepresentation is not well-founded.

Summary of Conclusions

Allegations Not Well-Founded

379. With regard to New Uses of Personal Information, Collection of Personal Information from Sources Other than Facebook, Facebook Mobile and Safeguards, and Deception and Misrepresentation, I have concluded that CIPPIC's allegations are not well-founded.

Allegations Well-Founded and Resolved

380. With regard to Collection of Date of Birth, Default Privacy Settings, Advertising, and Monitoring for Anomalous Activity, I have concluded that CIPPIC's allegations are well-founded and resolved on the basis of corrective measures proposed by Facebook in response to my recommendations.

381. I have indicated to Facebook that our Office will follow up after 30 days to verify that the proposed measures have been implemented.

Allegations Well-founded with Issues Unresolved

382. With regard to Third-Party Applications, Account Deactivation and Deletion**,** Accounts of Deceased Users, and Personal Information of Non-Users, I have concluded that CIPPIC's allegations are well-founded. In these cases, however, there remain unresolved issues where Facebook has not yet agreed to adopt certain of my recommendations or acceptable alternatives.

383. The recommendations remaining at issue are as follows:

(Third-Party Applications)

- That Facebook consider and implement measures
    1. to limit application developers' access to user information not required to run a specific application;
    2. whereby users would in each instance be informed of the specific information that an application requires and for what purpose;
    3. whereby users' express consent to the developer's access to the specific information would be sought in each instance; and
    4. to prohibit all disclosures of personal information of users who are not themselves adding an application.

(Account Deactivation and Deletion)

- That Facebook develop, institute, and inform users of, a retention policy whereby the personal information of users who have deactivated their accounts will be deleted from Facebook's servers after a reasonable length of time.

(Accounts of Deceased Users)

- That Facebook include in its Privacy Policy, in the context of all intended uses of personal information, an explanation of the intended use of personal information for the purpose of memorializing the accounts of deceased users.

(Personal Information of Non-Users)

- That Facebook consider and implement measures to improve its invitation feature so as to address our Office's concerns about non-users' lack of knowledge and consent to Facebook's collection, use, and retention of their email addresses;
- That Facebook set a reasonable time limit on the retention of non-users' email addresses for purposes of tracking invitation history and the success of the referral program.

384. I have asked Facebook to reconsider these remaining recommendations in the light of my findings. I have also indicated that, in our follow-up on other matters after 30 days, our Office will check for evidence of acceptance and implementation of these recommendations or acceptable alternatives to them. Should we find no such evidence, we will then consider how best to address any unresolved issues in accordance with our authorities.

385. I look forward to reviewing Facebook's progress in implementing my recommendations and to its continuing cooperation in resolving the issues involved in this complaint.

APPENDIX A

Allegations	Findings
Section 1 – Collection of Date of Birth 1) That Facebook was unnecessarily requiring users to provide their dates of birth as a condition of registration, in contravention of Principle 4.3.3. 2) That Facebook was not adequately explaining to users why they had to provide their dates of birth and how these would be used, in contravention of Principle 4.3.2.	Findings: 1) Date of birth is acceptable as a condition of service since purposes for its use are appropriate. 2) However, Facebook was not clearly explaining these purposes. Recommendation(s): • Facebook was asked to clearly tell users, when registering, why birth dates are required. • It was also asked to clarify in its site documentation the reasons for collecting date of birth and how it may be used. Response: Facebook agreed to all recommendations. Conclusion: Well-founded and resolved
Section 2 – Default Privacy Settings 1) That Facebook, by preselecting default privacy settings, was in effect using opt-out consent for the	Findings: 1) Users voluntarily upload their

use and disclosure of personal information without meeting the requirements for opt-out consent as articulated in previous findings of our Office. Specifically, it was contended that much of the personal information being shared by users, including photographs, marital status, age, and hobbies, is sensitive and therefore requires express consent.

2) That Facebook does not, in the context of its privacy settings, make a reasonable effort to advise users of the purposes for which and the extent to which their personal information is used and disclosed. Specifically,

   - Facebook does not inform users of the extent to which their personal information may be shared through the default settings and so does not have meaningful consent.
   - Facebook does not direct users to the privacy settings when they complete registration, when they upload photos, or when Facebook makes changes to the settings.
   - Facebook does not inform users that failure to alter the default settings constitutes consent to those settings.
   - Facebook fails to provide adequate notice to users posting photo albums that the default privacy settings for photo albums enable sharing with everyone, with the result that a user's non-friends personal information for the purpose of sharing it with others.

   2) Default privacy settings are acceptable as long as they meet users' reasonable expectations. They do not in two instances: photo albums (set to "Everyone") and search (consent to being searchable by search engines).

   3) Sufficient information was not provided to users with regard to how privacy settings are defaulted and the implications of not modifying the defaulted settings.

Recommendations:

Facebook was asked to:

- make user profiles inaccessible to search engines by default;
- change the default setting for photo albums to "Your Networks and Friends," and
- provide a link to the privacy settings at registration, accompanied by a statement of what the settings are for, that Facebook has preselected settings, and that settings can be changed according to preferences.

Response:

Facebook is making changes to its

can view his or her photographs and associated comments, even if the user's profile is searchable only by his or her friends.

- When users sign up for a network, their default privacy settings enable the sharing of their personal information, including sensitive information, with everyone on the network.

privacy settings a) by allowing users to choose a high, medium, low setting and b) introducing a per-object privacy that allows users to choose privacy settings on individual photos and pieces of content such as status updates.

Conclusion: Well-founded and resolved

Section 3 – Facebook Advertising

1) That Facebook was not making a reasonable effort to notify users clearly that it used their personal information for advertising purposes, in violation of Principle 4.3.2.
2) That Facebook, for Social Ads in particular, was improperly using opt-out rather than opt-in consent in accordance with Principle 4.3.6, given the sensitivity of users' personal information.
3) That Facebook was not allowing users to opt out of Facebook Ads, in contravention of Principle 4.3.8.
4) Since users were not allowed to opt out of Facebook Ads, Facebook was unnecessarily requiring users to agree to such ads as a condition of service, in violation of Principle 4.3.3.

Findings:

1) Users cannot opt out of all advertising as advertising revenues are required to run site (which is free to users).
2) Users can opt out of Social Ads - this type of advertising is more intrusive (the individual is used to promote products, services, etc.) and therefore users should not be required to consent to Social Ads.
3) Requiring users to consent to Facebook Ads is acceptable as they are not being co-opted into endorsing a product.
4) However, Facebook is not informing users of advertising purposes.

Recommendations:

- Facebook was asked to expand the advertising section of the Privacy Policy to more fully explain advertising and to inform users that their profile information is used for targeted advertising.

Response:

Facebook agreed to describe advertising more clearly and to configure its systems to allow users to more easily find information about advertising.

Conclusion: Well-founded and resolved

Section 4 – Third-Party Applications

1) That Facebook was not informing users of the purpose for disclosing personal information to third-party application developers, in contravention of Principles 4.2.2 and 4.2.5.
2) That Facebook was providing third-party application developers with access to personal information beyond what was necessary for the purposes of the application, in contravention of Principle 4.4.1.
3) That Facebook was requiring users to consent to the disclosure of personal information beyond what was necessary to run an application, in contravention of Principle 4.3.3.
4) That Facebook was not notifying

Findings:

1) Facebook had inadequate safeguards to effectively restrict these outside developers from accessing users' profile information, along with information about their online friends.

2) Facebook was not obtaining users' meaningful consent to the disclosure of their personal information to application developers when either they or their friends add applications.

users of the implications of withdrawing consent to sharing personal information with third-party application developers, in contravention of Principle 4.3.8.

5) That Facebook was allowing third-party application developers to retain a user's personal information after the user deleted the application, in contravention of Principle 4.5.3.

6) That Facebook was allowing third-party developers access to the personal information of users when their friends or fellow network members added applications without adequate notice, in contravention of Principle 4.3.2.

7) That Facebook was not adequately safeguarding personal information in that it was not monitoring the quality or legitimacy of third-party applications or taking adequate steps against inherent vulnerabilities in many programs on the Facebook Platform, in contravention of Principle 4.7.

8) That Facebook was not effectively notifying users of the extent of personal information that is disclosed to third-party application developers and was providing users with misleading and unclear information about sharing with third-party application developers, in contravention of Principles 4.3.and 4.8.

9) That Facebook was not taking responsibility for the personal information transferred to third-party

Recommendations:

- Facebook was asked to implement technological measures to limit application developers' access to user information that is not required to run a specific application.
- The site should also ensure that users are informed of the specific information that an application requires and for what purpose. In addition, users' express consent for the developer's access to the specific information must be sought each time someone signs up for an application.
- Finally, measures are needed to prohibit all disclosure of the personal information of users who are not themselves adding an application.

Response:

Facebook has not agreed to implement the recommendations.

Conclusion: Well-founded

developers for processing, in contravention of Principle 4.1.3. 10) That Facebook was not permitting users to opt out of sharing their name, networks, and friend lists when their friends add applications, in contravention of Principle 4.3 and subsection 5(3).	
Section 5 – New Uses of Personal Information	
1) That Facebook was not notifying users of new purposes for which their personal information would be collected, used, or disclosed, in violation of Principle 4.2.4.	Findings: There was no evidence that Facebook had failed to inform its users of new uses. Conclusion: Not well-founded
Section 6 – Collection of Personal Information from Sources Other than Facebook	
1) That Facebook was failing to provide users with specific information relating to the purposes and method of collecting personal information from sources outside Facebook, the sources of the information, and the use and disclosure of the information. 2) Having failed to inform users of these specifics, Facebook was therefore not obtaining their	Findings: Although Facebook's privacy policy contains language about collecting personal information from outside sources, in fact, it does not do so at the present time. Conclusion: Not well-founded

meaningful consent.

Section 7(a) – Account Deactivation and Deletion

1) That Facebook was offering only an account deactivation option as distinct from an account deletion option and was therefore inappropriately depriving users of a means whereby they could delete all their personal information from the site.

Findings:

1) Account deactivation and deletion are explained on the site, but not in the same part of the site. It may cause some users to believe that deactivation is their only option.

2) It is retaining personal information from deactivated accounts indefinitely.

Recommendations:

- Facebook was asked to develop, institute and inform users about a retention policy under which the personal information of users who have deactivated their accounts will be deleted from Facebook's servers after a reasonable length of time.

- As a best practice, the Assistant Commissioner also suggested that Facebook make the account deletion option more prominent for users.

Response:

Facebook agreed to add information about account deletion to its privacy

	policy, but declined to develop a retention policy for deactivated accounts. Conclusion: Well-founded
Section 7(b) – Accounts of Deceased Users	
1) By including only in its Terms of Use and not in its Privacy Policy a notice of its intention to keep deceased users' profiles active for memorial purposes, Facebook was not obtaining users' meaningful consent for such use of their personal information. 2) That Facebook was obligating users, in contravention of Principle 4.3.3, to consent to this purpose as a condition of service even though memorializing a profile is not necessary to Facebook's primary purpose of providing a social networking venue.	Findings: 1) Memorialization can be considered a primary purpose since most users would reasonably expect it. 2) However, users are not informed of the practice, whereby they would effectively provide their consent to it. Recommendation: • Facebook was asked to include in its Privacy Policy an explanation about the practice of using the personal information to memorialize the accounts of deceased users. Response: Facebook did not agree to implement the recommendation, considering it unnecessary under the law. Conclusion: Well-founded
Section 8 – Personal Information of	

Non-users

1) That Facebook was not obtaining consent from non-users for the uploading of their personal information to the site, in contravention of Principle 4.3, in the following situations:

   - Users can post the personal information of non-users in their own profiles, as well as the profiles of other users through features such as “News Feed” and “Wall”. Also, users can tag images of non-users with their names in photos or videos.
   - Users can provide Facebook with the email addresses of non-users for the purpose of inviting them to join the site.

Findings:

1) When users post personal information about non-users on walls, profiles, or the News Feed, such postings are made for personal purposes only and fall outside the scope of the Act.

2) In the cases of tagging of and invitations to non-users, the Act only applies where Facebook uses non-users personal information for purposes of its own, namely, informing non-users when they have been tagged or inviting them to join Facebook.

3) Facebook may rely on users to obtain the consent of non-users for these two purposes, provided that the company exercises reasonable due diligence. This could simply mean taking steps to ensure that users know that they must obtain non-users’ consent before disclosing their email addresses to Facebook, and punishing users who violate the consent requirement.

4) However, such information is currently missing from the Privacy Policy.

Recommendations:

- It was asked to implement measures to improve the invitation feature so as to address our concerns about non-users' lack of knowledge and consent to Facebook's collection, use, and retention of their email addresses; and
- It was asked to set a reasonable time limit on the retention of non-users' email addresses after they have been invited to join Facebook.

Response:

Facebook declined to implement the first and second recommendations above on grounds that the site already provides "significantly greater notice to non-users as to the presence of any information about them on our site than does any other site on the web."

Facebook also noted that it could not realistically delete the personal information of non-users when it is uploaded by users, because that information is in the user's possession and control. As such, non-user data is the responsibility of the user who uploads it.

Facebook made no direct response to the third recommendation.

Conclusion: Well-founded

Section 9 – Facebook Mobile and Safeguards

1) With respect to users of the mobile version of the Facebook website (Mobile Facebook), it was alleged that, by providing such users with a persistent cookie having no apparent expiration date, Facebook was failing to properly safeguard their personal information, in contravention of Principles 4.7, 4.7.1, and 4.7.3.

2) Specifically, CIPPIC cited the following security concerns:
    (1) If a user logs onto his or her Facebook account by means of another person's mobile device and forgets to log off, the other person will have access to the user's Facebook account indefinitely, even if the user changes the password.
    (2) If a user gives his or her Facebook password to another person, that person can log in as the user on a mobile device and have access indefinitely, even if

Findings:

1) Facebook uses a persistent cookie with a 14-day expiration date. A password change on another platform causes a session open on Facebook Mobile to close and require re-authentication for a user to log back on.

2) Therefore, Facebook provides users with a simple method of logging out of sessions on Facebook Mobile, as well as the ability to effectively cease Facebook sessions initiated on mobile devices by changing their passwords on other platforms.

3) As such, Facebook provides users of Facebook Mobile with adequate safeguards to protect their sessions from unauthorized access.

Conclusion: Not well-founded

the user changes the password.

3) In CIPPIC's view, Facebook should have a cookie that expires within an appropriate period of time and whenever users change their passwords online.

Section 10 – Monitoring for Anomalous Activity

1) That Facebook was not informing users that it monitors the site for anomalous behaviour and, in particular, failed to mention this practice in its Privacy Policy, in violation of Principle 4.8.

Findings:

1) The practice of monitoring the site for anomalous behaviour was appropriate, but Facebook was not making a reasonable effort to inform users of it.

Recommendation:

- Facebook was asked to explain the practice in its Privacy Policy

Response:

Facebook agreed to the recommendation.

Conclusion: Well-founded and resolved

Section 11 – Deception and Misrepresentation

1) That Facebook was misrepresenting itself by claiming to be purely a

Findings:

social networking site when in fact it was engaged in other activities not clearly explained, such as advertising and third-party applications, in contravention of Principles 4.3.2 and 4.4.2.	There was no evidence of intent to deceive or misrepresent. Conclusion: Not well-founded
2) That Facebook was misrepresenting users' level of control over their personal information, in contravention of Principles 4.3.2 and 4.4.2.	

APPENDIX B

Personal Information Protection and Electronic Documents Act

Division 1

5. (1) Subject to sections 6 to 9, every organization shall comply with the obligations set out in Schedule1.

(2) The word “should”, when used in Schedule 1, indicates a recommendation and does not impose an obligation.

(3) An organization may collect, use, or disclose personal information only for purposes that a reasonable person would consider appropriate in the circumstances.

Schedule 1 - Principles set out in the National Standard of Canada entitled *Model Code for the Protection of Personal Information, CAN/CSA-Q830-96*

4.1 Principle 1 — Accountability

An organization is responsible for personal information under its control and shall designate an individual or individuals who are accountable for the organization’s compliance with the following principles.

4.1.1
Accountability for the organization’s compliance with the principles rests with the designated individual(s), even though other individuals within the organization may be responsible for the day-to-day collection and processing of personal information. In addition, other individuals within the organization may be delegated to act on behalf of the designated individual(s).

4.1.2
The identity of the individual(s) designated by the organization to oversee the organization’s compliance with the principles shall be made known upon request.

4.1.3
An organization is responsible for personal information in its possession or custody, including information that has been transferred to a third party for processing. The organization shall use contractual or other means to provide a comparable level of protection while the information is being processed by a third party.

4.1.4

Organizations shall implement policies and practices to give effect to the principles, including

(*a*) implementing procedures to protect personal information;

(*b*) establishing procedures to receive and respond to complaints and inquiries;

(*c*) training staff and communicating to staff information about the organization's policies and

practices; and

(*d*) developing information to explain the organization's policies and procedures.

4.2 Principle 2 — Identifying Purposes

The purposes for which personal information is collected shall be identified by the organization at or before the time the information is collected.

4.2.1

An organization shall document the purposes for which personal information is collected in order to comply with Principle 4.8 (Openness) and Principle 4.9 (Individual Access).

4.2.2

Identifying the purposes for which personal information is collected at or before the time of collection allows organizations to determine the information they need to collect to fulfil these purposes. Principle 4.4 (Limiting Collection) requires an organization to collect only that information necessary for the purposes that have been identified.

4.2.3

The identified purposes should be specified at or before the time of collection to the individual from whom the personal information is collected. Depending upon the way in which the information is collected, this can be done orally or in writing. An application form, for example, may give notice of the purposes.

4.2.4

When personal information that has been collected is to be used for a purpose not previously identified, the new purpose shall be identified prior to use. Unless the new purpose is required by law, the consent of the individual is required before information can be used for that purpose. For an elaboration on consent, please refer to Principle 4.3 (Consent).

4.2.5

Persons collecting personal information should be able to explain to individuals the purposes for which the information is being collected.

4.2.6

This principle is linked closely to Principle 4.4 (Limiting Collection) and Principle 4.5 (Limiting Use, Disclosure, and Retention).

4.3 Principle 3 — Consent

The knowledge and consent of the individual are required for the collection, use, or disclosure of personal information, except where inappropriate.

> Note: In certain circumstances personal information can be collected, used, or disclosed without the knowledge and consent of the individual. For example, legal, medical, or security reasons may make it impossible or impractical to seek consent. When information is being collected for the detection and prevention of fraud or for law enforcement, seeking the consent of the individual might defeat the purpose of collecting the information. Seeking consent may be impossible or inappropriate when the individual is a minor, seriously ill, or mentally incapacitated. In addition, organizations that do not have a direct relationship with the individual may not always be able to seek consent. For example, seeking consent may be impractical for a charity or a direct-marketing firm that wishes to acquire a mailing list from another organization. In such cases, the organization providing the list would be expected to obtain consent before disclosing personal information.

4.3.1

Consent is required for the collection of personal information and the subsequent use or disclosure of this information. Typically, an organization will seek consent for the use or disclosure of the information at the time of collection. In certain circumstances, consent with respect to use or disclosure may be sought after the information has been collected but before use (for example, when an organization wants to use information for a purpose not previously identified).

4.3.2

The principle requires “knowledge and consent”. Organizations shall make a reasonable effort to ensure that the individual is advised of the purposes for which the information will be used. To make the consent meaningful, the purposes must be stated in such a manner that the individual can reasonably understand how the information will be used or disclosed.

4.3.3

An organization shall not, as a condition of the supply of a product or service, require an individual to consent to the collection, use, or disclosure of information beyond that required to fulfil the explicitly specified, and legitimate purposes.

4.3.4

The form of the consent sought by the organization may vary, depending upon the circumstances and the type of information. In determining the form of consent to use, organizations shall take into account the sensitivity of the information. Although some information (for example, medical records and income records) is almost always considered to be sensitive, any information can be sensitive, depending on the context. For example, the names and addresses of subscribers to a newsmagazine would generally not be considered sensitive information. However, the names and addresses of subscribers to some special-interest magazines might be considered sensitive.

4.3.5

In obtaining consent, the reasonable expectations of the individual are also relevant. For example, an individual buying a subscription to a magazine should reasonably expect that the organization, in addition to using the individual's name and address for mailing and billing purposes, would also contact the person to solicit the renewal of the subscription. In this case, the organization can assume that the individual's request constitutes consent for specific purposes. On the other hand, an individual would not reasonably expect that personal information given to a health-care professional would be given to a company selling health-care products, unless consent were obtained. Consent shall not be obtained through deception.

4.3.6

The way in which an organization seeks consent may vary, depending on the circumstances and the type of information collected. An organization should generally seek express consent when the information is likely to be considered sensitive. Implied consent would generally be appropriate when the information is less sensitive. Consent can also be given by an authorized representative (such as a legal guardian or a person having power of attorney).

4.3.7

Individuals can give consent in many ways. For example:

(*a*) an application form may be used to seek consent, collect information, and inform the individual

of the use that will be made of the information. By completing and signing the form, the individual

is giving consent to the collection and the specified uses;

(*b*) a checkoff box may be used to allow individuals to request that their names and

addresses not
be given to other organizations. Individuals who do not check the box are assumed to consent to
the transfer of this information to third parties;
(*c*) consent may be given orally when information is collected over the telephone; or
(*d*) consent may be given at the time that individuals use a product or service.

4.3.8
An individual may withdraw consent at any time, subject to legal or contractual restrictions and reasonable notice. The organization shall inform the individual of the implications of such withdrawal.

4.4 Principle 4 — Limiting Collection

The collection of personal information shall be limited to that which is necessary for the purposes identified by the organization. Information shall be collected by fair and lawful means.

4.4.1
Organizations shall not collect personal information indiscriminately. Both the amount and the type of information collected shall be limited to that which is necessary to fulfil the purposes identified. Organizations shall specify the type of information collected as part of their information-handling policies and practices, in accordance with the Openness principle (Clause 4.8).

4.4.2
The requirement that personal information be collected by fair and lawful means is intended to prevent organizations from collecting information by misleading or deceiving individuals about the purpose for which information is being collected. This requirement implies that consent with respect to collection must not be obtained through deception.

4.4.3
This principle is linked closely to Principle 4.2 (Identifying Purposes) and Principle 4.3 (Consent).

4.5 Principle 5 — Limiting Use, Disclosure, and Retention

Personal information shall not be used or disclosed for purposes other than those for which it was collected, except with the consent of the individual or as required by law. Personal information shall be retained only as long as necessary for the fulfilment of those purposes.

4.5.1
Organizations using personal information for a new purpose shall document this purpose (see Principle 4.2.1).

4.5.2
Organizations should develop guidelines and implement procedures with respect to the retention of personal information. These guidelines should include minimum and maximum retention periods. Personal information that has been used to make a decision about an individual shall be retained long enough to allow the individual access to the information after the decision has been made. An organization may be subject to legislative requirements with respect to retention periods.

4.5.3
Personal information that is no longer required to fulfil the identified purposes should be destroyed, erased, or made anonymous. Organizations shall develop guidelines and implement procedures to govern the destruction of personal information.

4.5.4
This principle is closely linked to Principle 4.3 (Consent), Principle 4.2 (Identifying Purposes), and Principle 4.9 (Individual Access).

4.6 Principle 6 — Accuracy

Personal information shall be as accurate, complete, and up-to-date as is necessary for the purposes for which it is to be used.

4.6.1
The extent to which personal information shall be accurate, complete, and up-to-date will depend upon the use of the information, taking into account the interests of the individual. Information shall be sufficiently accurate, complete, and up-to-date to minimize the possibility that inappropriate information may be used to make a decision about the individual.

4.6.2
An organization shall not routinely update personal information, unless such a process is necessary to fulfil the purposes for which the information was collected.

4.6.3
Personal information that is used on an ongoing basis, including information that is disclosed to third parties, should generally be accurate and up-to-date, unless limits to the requirement for accuracy are clearly set out.

4.7 Principle 7 — Safeguards

Personal information shall be protected by security safeguards appropriate to the sensitivity of the information.

4.7.1
The security safeguards shall protect personal information against loss or theft, as well as unauthorized access, disclosure, copying, use, or modification. Organizations shall protect personal information regardless of the format in which it is held.

4.7.2
The nature of the safeguards will vary depending on the sensitivity of the information that has been collected, the amount, distribution, and format of the information, and the method of storage. More sensitive information should be safeguarded by a higher level of protection. The concept of sensitivity is discussed in Principle 4.3.4.

4.7.3
The methods of protection should include

(*a*) physical measures, for example, locked filing cabinets and restricted access to offices;

(*b*) organizational measures, for example, security clearances and limiting access on a “need-to-know” basis; and

(*c*) technological measures, for example, the use of passwords and encryption.

4.7.4
Organizations shall make their employees aware of the importance of maintaining the confidentiality of personal information.

4.7.5
Care shall be used in the disposal or destruction of personal information, to prevent unauthorized parties from gaining access to the information (see Clause 4.5.3).

4.8 Principle 8 — Openness

An organization shall make readily available to individuals specific information about its policies and practices relating to the management of personal information.

4.8.1

Organizations shall be open about their policies and practices with respect to the management of personal information. Individuals shall be able to acquire information about an organization's policies and practices without unreasonable effort. This information shall be made available in a form that is generally understandable.

4.8.2

The information made available shall include

(*a*) the name or title, and the address, of the person who is accountable for the organization's

policies and practices and to whom complaints or inquiries can be forwarded;

(*b*) the means of gaining access to personal information held by the organization;

(*c*) a description of the type of personal information held by the organization, including a general
account of its use;

(*d*) a copy of any brochures or other information that explain the organization's policies, standards,
or codes; and

(*e*) what personal information is made available to related organizations (e.g., subsidiaries).

Principle 4.8.3 states that an organization may make information on its policies and practices available in a variety of ways. The method chosen depends on the nature of its business and other considerations. For example, an organization may choose to make brochures available in its place of business, mail information to its customers, provide online access, or establish a toll-free telephone number.

4.9 Principle 9 — Individual Access

Upon request, an individual shall be informed of the existence, use, and disclosure of his or her personal information and shall be given access to that information. An individual shall be able to challenge the accuracy and completeness of the information and have it amended as appropriate.

> Note: In certain situations, an organization may not be able to provide access to all the personal information it holds about an individual. Exceptions to the access requirement should be limited and specific. The reasons for denying access

should be provided to the individual upon request. Exceptions may include information that is prohibitively costly to provide, information that contains references to other individuals, information that cannot be disclosed for legal, security, or commercial proprietary reasons, and information that is subject to solicitor-client or litigation privilege.

4.9.1

Upon request, an organization shall inform an individual whether or not the organization holds personal information about the individual. Organizations are encouraged to indicate the source of this information. The organization shall allow the individual access to this information. However, the organization may choose to make sensitive medical information available through a medical practitioner. In addition, the organization shall provide an account of the use that has been made or is being made of this information and an account of the third parties to which it has been disclosed.

4.9.2

An individual may be required to provide sufficient information to permit an organization to provide an account of the existence, use, and disclosure of personal information. The information provided shall only be used for this purpose.

4.9.3

In providing an account of third parties to which it has disclosed personal information about an individual, an organization should attempt to be as specific as possible. When it is not possible to provide a list of the organizations to which it has actually disclosed information about an individual, the organization shall provide a list of organizations to which it may have disclosed information about the individual.

4.9.4

An organization shall respond to an individual's request within a reasonable time and at minimal or no cost to the individual. The requested information shall be provided or made available in a form that is generally understandable. For example, if the organization uses abbreviations or codes to record information, an explanation shall be provided.

4.9.5

When an individual successfully demonstrates the inaccuracy or incompleteness of personal information, the organization shall amend the information as required. Depending upon the nature of the information challenged, amendment involves the correction, deletion, or addition of information. Where appropriate, the amended information shall be transmitted to third parties having access to the information in question.

4.9.6

When a challenge is not resolved to the satisfaction of the individual, the substance of the unresolved challenge shall be recorded by the organization. When appropriate, the existence of the unresolved challenge shall be transmitted to third parties having access to the information in question.

4.10 Principle 10 — Challenging Compliance

An individual shall be able to address a challenge concerning compliance with the above principles to the designated individual or individuals accountable for the organization's compliance.

4.10.1

The individual accountable for an organization's compliance is discussed in Clause 4.1.1.

4.10.2

Organizations shall put procedures in place to receive and respond to complaints or inquiries about their policies and practices relating to the handling of personal information. The complaint procedures should be easily accessible and simple to use.

4.10.3

Organizations shall inform individuals who make inquiries or lodge complaints of the existence of relevant complaint procedures. A range of these procedures may exist. For example, some regulatory bodies accept complaints about the personal-information handling practices of the companies they regulate.

4.10.4

An organization shall investigate all complaints. If a complaint is found to be justified, the organization shall take appropriate measures, including, if necessary, amending its policies and practices.