



LISA FEINBERG

Facebook: Beyond Friends

Why CIPPIC lodged a privacy complaint to the Privacy Commissioner of Canada

There appear to be no strangers on Facebook. Every relationship that Facebook facilitates is purportedly based on a “real life” connection (Kirkpatrick, 2006). Facebook users communicate with “Friends”¹ with whom they have lived, dated, worked, and studied. This is why seven million Canadians have chosen to trust Facebook with a lot of personal information, including our name, birthday, sexual orientation, contact information, school, job, pictures, personal messages, and so forth. Youth in particular choose sites like Facebook to “hang out” with Friends (Boyd, 2007). But how well does Facebook model “real life” connections? And how well does Facebook protect the privacy of its users? This is what we, a team of law students, sought to find out as part of our internship with the Canadian Internet Policy and Public Interest Clinic (CIPPIC).²

As a commercial operation with a huge Canadian user base, Facebook has a responsibility to comply with Canadian privacy law. Our research exposed what we believe are twenty-two separate violations by Facebook of the *Personal Information Protection and Electronic Documents Act (PIPEDA)*. We lodged a complaint detailing these violations with the Privacy Commissioner of Canada.³ At the core of our complaint are three principles:

OUR SCHOOLS/OUR SELVES

- Facebook should be open with its users about its use of their personal information;
- Facebook should obtain express permission to share its users' personal information; and
- Facebook should limit the personal information that it shares to what is necessary.

I will examine these briefly and then discuss their broader implications.

Facebook should be more open about its uses of personal information to allow users to make informed decisions. On its welcome page, Facebook presents itself as “a social utility that connects you with the people around you.” However, Facebook is also connecting users to third party advertisers and application developers. Facebook generates huge revenues by allowing advertisers to search users by sex, location, age, relationship status, political views, education status, workplace, and keywords to serve them precisely targeted ads. Facebook only mentions its advertising activities briefly in its Privacy Policy. This is not sufficient notice to users. I doubt that most users expect that advertisers will have this much access to their information.

Facebook must also live up to its promise of giving a high level of control to users. On its welcome page, Facebook advertises itself as a tool “to control privacy online.” But how much control are users really given? When users first register for Facebook, they are not directed to adjust their privacy settings. Instead, Facebook makes default choices for their users — the default being to share their personal information with their Friends and Networks. This means that a thirteen year old who joins the Toronto Network will automatically be broadcasting their intimate details to all others in the Network. To opt out of these default settings, users must take action themselves to find the settings and change them. Further, Facebook takes away some choices from users completely. For example, users cannot opt out of sharing their information with advertisers who deliver targeted ads to their Profiles. Facebook also makes it very difficult for users to delete their accounts. Under Facebook's account settings, users may choose to “deactivate” their accounts, but not to delete them. Facebook is retaining the information of users who have deactivated their accounts for an undisclosed period of

time. To delete accounts completely, users must email Facebook. It should be much easier to delete an account.

Further, Facebook is not limiting the personal information that it shares to that which is necessary to operate its service. The most extreme instance of this occurs with third party application developers. Users can add applications, like horoscopes or slideshows, developed by third parties to their Facebook Profile. To add these applications, users must agree to allow

Facebook is not limiting the personal information that it shares to that which is necessary to operate its service.

the application “to know who I am and access my information.” There is no limitation on the personal information that is disclosed to applications. Furthermore, these application developers also have access to all the personal information of users’ Friends. This excess sharing is noted only briefly in the Facebook Privacy Policy. This means that a user’s choice not to add applications is irrelevant if his or her Friends have added applications. What makes this more concerning is that Facebook has stated in its Terms of Use that “Third Party Applications 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 [...] privacy practices or other policies.” Rogue third party application developers could easily exploit personal information for fraudulent purposes (Williams, 2007).

So what are the implications of these practices? Do we not appreciate that our social networking Profiles are open to the public? I would argue that we do not. We join Facebook, because our Friends — not strangers — are there. Facebook encourages this behaviour by representing itself as a safe place to meet Friends. When I joined Facebook, I gave it permission to share my personal information within certain parameters. For example, I certainly did not give permission for Facebook to share my information with third party applications that my Friends had added. We should be able to have social Profiles that are only accessible by our Friends. Social networking sites like Facebook have the technology to create protected communities in cyber-

OUR SCHOOLS/OUR SELVES

space. Canadians, including young Canadians, should be able to develop relationships in cyberspace.

There is no protected community yet. Facebook is sharing our information expansively, beyond our Friends. When we communicate with Friends on Facebook, we leave behind an evidentiary record. Unless we manually delete our information off Facebook, it remains on there indefinitely. Facebook and other social networking sites have become a resource for cyberstalkers (Poulsen, 2007) and identity thieves (Michaels, 2007; York, 2006). They have also rendered our reputations more vulnerable. Our intimate information can be unwittingly leaked to our detriment — to our employers (CBS, 2006) and teachers (Brown, 2008).

Social networking sites know a lot about us, but we know very little about them. We should incorporate the issues around social networking websites into our education system. Educators should teach us about privacy protection. Privacy is integral to maturity — we need a safe space to grow into ourselves. It is important for us to be able to recognize when a space is not safe — when there are unwanted listeners. It is also important for us know that we have rights: we cannot be bound by illegal terms of service. We should be taught to challenge the questionable practices of these online social networking sites. As customers of these commercial websites, we have a voice. We can complain to the privacy officers of sites like Facebook or to the Privacy Commissioner of Canada.⁴

CIPPIC's complaint about Facebook has caught the attention of the media, academics, and most importantly, Facebook users. Canadians are talking about the implications of online social networking. The Privacy Commissioner will report her findings and recommendations within one year. We hope that Facebook will comply. Regardless, this conversation is not over. We are moving towards a larger discourse on the privacy concerns with social networking sites.

* * *

Lisa Feinberg is in her second year of a joint Bachelor of Law and Masters in the International Affairs Program held by the University of Ottawa and the Norman Paterson School of International Affairs. She is interning at the Canadian Internet Policy and Public Interest Clinic (CIPPIC) in Ottawa.

ENDNOTES

¹ The capitalization of words like Friends, Profile, Terms of Use, and Privacy Policy reflect the use and meaning of these terms in the Facebook context.

² The Canadian Internet Policy and Public Interest Clinic (CIPPIC) was established in fall of 2003 at the University of Ottawa, Faculty of Law, Common Law Section. CIPPIC seeks to ensure balance in policy and law-making processes on issues that arise as a result of new technologies. Law students work with clinic counsel on projects and cases involving the intersection of law, technology and the public interest. (www.cippic.ca)

³ To view the entire complaint, please visit http://www.cippic.ca/uploads/CIPPICFacebookComplaint_29May08.pdf

⁴ For more information on how to file a privacy complaint, see Instructions on the website of the Privacy Commissioner of Canada: http://www.privcom.gc.ca/i_i/index_e.asp.

REFERENCES

Boyd, Danah. (2007). Why Youth (Heart) Social Network Sites: The Role of Networked Publics in Teenage Social Life. *MacArthur Foundation Series on Digital Learning — Youth, Identity, and Digital Media Volume* (ed. David Buckingham). Cambridge, MA: MIT Press. Retrieved June 7, 2008, from <http://www.danah.org/papers/WhyYouthHeart.pdf>

Brown, Louise. (March 6, 2008). "Student faces Facebook consequences: Freshman hit with 147 academic charges for online study network at Ryerson University." *The Toronto Star*. Retrieved on June 7, 2008, from <http://www.thestar.com/News/GTA/article/309855>.

CBS (June 20, 2006). "Employers look At Facebook too: Companies turn to online profiles to see what applicants are really like." Retrieved on June 8, 2008, from <http://www.cbsnews.com/stories/2006/06/20/eveningnews/main1734920.shtml>

Kirkpatrick, David. (October 6, 2006). "Why Facebook matters." *Fortune Magazine*. Retrieved June 7, 2008, from http://money.cnn.com/2006/10/06/magazines/fortune/fastforward_facebook.fortune/index.htm.

Michaels, Scott. (December 3, 2007). "No charges in MySpace suicide." *ABC NEWS*. Retrieved June 5, 2008, from <http://abcnews.go.com/TheLaw/story?id=3946124&page=1>.

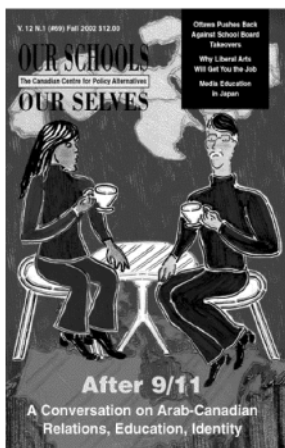
Poulsen, Kevin. (June 14, 2007). "MySpace database search starts yielding sex offender busts." *Wired Blog*. Retrieved June 7, 2008, from http://blog.wired.com/27bstroke6/2007/06/myspace_databas.html.

Williams, Chris. (September 12, 2007). "Facebook application hawks your personal opinions for cash." *The Register*. Retrieved June 13, 2008, from http://www.theregister.co.uk/2007/09/12/facebook_compare_people/.

OUR SCHOOLS/OUR SELVES

York, Will. (February 2, 2006). "Student arrested on identity theft charges." *The Pacer*, 78:19. Retrieved on June 7, 2008, from <http://pacer.utm.edu/2946.htm>.

Knowledge is a powerful tool.



OUR SCHOOLS Canadian Centre for Policy Alternatives OUR SELVES

*"...an excellent general-interest journal...
Engagingly written, it bridges the gap
between theory and practice."*

—The Utne Reader

Our Schools / Our Selves is the Canadian Centre for Policy Alternatives' quarterly education publication. Since 1988 it has been a forum for debates and commentary on issues such as environmental activism; commercialism in schools; young women in trades; labour, education and the arts; schools and social justice, and teaching for democratic citizenship.

Subscriptions (4 issues/year) are \$51.36 (including shipping, handling and GST). Make cheque payable to Canadian Centre for Policy Alternatives, 410-75 Albert Street, Ottawa, ON, K1P 5E7. Phone: 613-563-1341. Fax: 613-233-1458. Email: ccpa@policyalternatives.ca. Visit our web site for more information.

<http://www.policyalternatives.ca>

I'd like to subscribe to **Our Schools/Our Selves**

Please find enclosed my cheque in the amount of \$ _____

Please charge my VISA or MasterCard for the amount of \$ _____

Card# _____ Expiry Date: _____

Signature: _____

Name: _____

Address: _____

Phone: _____
