Stoddart found that Facebook contravenes Canada's five-year-old Personal Information Protection and Electronic Documents Act because the site keeps users' personal information indefinitely, regardless of whether they close their accounts.

She also criticized Facebook sharing users' files with nearly one million third-party software developers around the world, who create applications for the site, such as "Finish the Lyrics" music quizzes and virtual pillow fight games.

Stoddart made several recommendations designed to protect the privacy of those using the website in Canada.

They include:

Clarifying Facebook's privacy policies

Making it easier for users to remove their profiles

Curbing the amount of personal information the site collects from its members

==========

Facebook tracks your every move, employee claims

by Ian Paul, PC World

Editor’s Note: The following article is reprinted from the Today @ PC World blog at PCWorld.com.

Facebook is tracking your every move on the site—or so says one purported Facebook employee, according to an anonymous interview with the Rumpus online magazine. In the interview, the Facebook employee, whose identity was protected so she wouldn’t lose her job for talking to the media, also said that Facebook employees have relatively easy access to user accounts.

Comments posted on the site have accused the Rumpus of posting a fake interview. In response, Jeremy Hatch, the site’s editor, said he “determined to [his] satisfaction that this interview really took place...[and]...would not have included it if there were even the slightest suspicion of a hoax.”

Facebook fired back, saying that the interview contained “the kind of inaccuracies and misrepresentations you would expect from something sourced

‘anonymously,’ and we’ll leave it at that,” according to several reports.

So what exactly was so interesting about the Rumpus’ interview? Here are the highlights:

Facebook tracks you

Every time you view a profile, look at a picture, send a message or take any other action on Facebook, the company records that action, according to the Facebook employee. At first glance, that sounds like a scary prospect, but the engineer argues that the company does this to deliver a better product. As a result of this tracking, for example, you can get suggestions to reconnect with a Facebook friend.

The employee also claimed that as a result of Facebook’s tracking, when you search for a friend on Facebook the auto complete function lists your friends by the people you interact with the most. However, in my tests this claim turned out to be false, as I was never able to see my friends list in anything but an alphabetized list when using the search function.

Universal access

There used to be a universal password that Facebook employees could use to view any Facebook account, the anonymous employee claims. But the password has since been discontinued, and now Facebook uses a different system where employees must provide a reason in writing for logging into a user’s account. If the employee cannot back up the reason they had for accessing someone’s account, the employee can be fired.

I have no doubt that Facebook has a mechanism for accessing a user’s account, and it wouldn’t surprise me if that access has been abused on occasion. The Facebook employee said that she knew of two people who were fired for unauthorized account snooping. But remember, it’s not just Facebook that has had to deal with this problem. In 2008, several government employees and contractors were caught snooping around in electronic passport records.

Facebook can read your messages

The employee claims that Facebook has all of your messages, deleted or not, stored in a database that any Facebook employee can access. The notion that your Facebook messages are stored in a database is about as stunning a discovery as finding out my laptop has a keyboard.

Then again, if any Facebook employee can just query that database to read your personal messages any time they like, well, that’s a problem. I certainly hope Facebook has better safeguards for personal messages than that.

So what do we make of all this? Personally, I don't think these issues are too concerning. The bigger issue around Facebook and security isn't with Facebook itself, but all those third-party services that have access to your data whenever you authorize a Facebook application.

======