The devil is in the defaults

If Facebook were truly committed to protecting privacy, it would start with the assumption that people want less access to their information, not more

Ian Kerr
Citizen Special

Saturday, May 29, 2010

A couple of weeks ago, Facebook CEO Mark Zuckerberg celebrated his 26th birthday. Well, sort of.

While he did indeed turn 26, it is reported that he was forced to cancel his Caribbean celebration to lead a series of emergency meetings on one of his least favourite topics: privacy.

These meetings resulted in significant alterations to the website's platform and user interface and a major media event that took place on Wednesday. Although numerous trusted media outlets, privacy advocates and politicians around the globe reported this event as "a privacy U-turn" (The Sun in Britain), an "about face" change (Economist), "a major step forward for privacy" (American Civil Liberties Association) and a "significant first step that Facebook deserves credit for," (Senator Charles Schumer), I am not so sure.

CREDIT: Gabriel Bouys, Agence France-Presse, Getty Images

Facebook founder Mark Zuckerberg introduces new privacy measures Wednesday in the face of unrest among users.

Facebook claims it will make the following four privacy revisions.

First, Facebook says its user interface will soon provide a single simplified control panel where you can choose who gets to see the content you post.

Second, Facebook says it will reduce the amount of personal information that must be visible to everyone. (Although Facebook users previously had no choice but to expose their friends and the pages they like, these fields are no longer required to be in public view.)

Third, Facebook says it will be easier for users to control whether its third-party applications and partner websites can access your information.

Fourth, Facebook has promised that this will be the last revision to its privacy settings for a long time. As Zuckerberg put it, "Believe me, we're probably happier about this than you are."

For those who deem these changes a positive global development in online privacy, Canada has at least some bragging rights. In May 2008, a complaint was made to the Privacy Commissioner of Canada by students and some of my colleagues at the Canadian Internet Policy and Public Interest Clinic (CIPPIC) at the University of Ottawa, Faculty of Law. The

original complaint comprised 24 allegations on a range of issues surrounding Facebook's 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 three central issues in the complaint concerned whether:

(i) Facebook's collection, use and disclosure of its users' personal information was in accord with Canadian privacy law's requirement of "knowledge and consent,"

(ii) Facebook's data retention policy relating to account deactivation and deletion was reasonable, and

(iii) Facebook and its third-party application providers offered sufficient security safeguards.

In June 2008, the Privacy Commissioner of Canada commenced an investigation that resulted in a report issued in July 2009. The report indicated that a number of CIPPIC's complaints were well-founded, while others were not.

On this basis, the commissioner worked with Facebook, resolving some of the well-founded complaints by way of corrective measures proposed by Facebook. Other complaints not resolved at the time led the privacy commissioner to set out a number of recommendations with a view to following up, once Facebook had been given an adequate opportunity to consider them and comply. As Facebook is well aware, the commissioner does not have the power to order that those recommendations be carried out, but she can seek a binding order from the courts.

So far as I know, none of these Canadian events of 2009 caused Zuckerberg to miss his 25th birthday.

By December 2009, things briefly seemed to be looking up. Zuckerberg posted an open letter on the Facebook Blog announcing a series of changes to its privacy settings. Users were promised more granular control and could decide whether they wanted to share any given piece of information with "friends," "friends of friends" or "everyone." They were also offered a "transition tool" that provided recommended privacy settings based on users' current settings.

But what Facebook gave with one hand, it took away with the other.

The so-called increase in privacy control came alongside requirements that name, profile picture, current city, gender, networks and the pages that you are a "fan" of would all become publicly available. Facebook wanted more "Google hits" and was willing to expose its users to the web's wide world in order to get them. (Recall that Facebook started out as exclusive to college students for precisely the opposite reason; Zuckerberg is no longer a 19-year-old college student.) Shortly after this, new complaints emerged and on Jan. 27, 2010, the privacy commissioner of Canada launched another investigation of Facebook, having commenced a public consultation on social network sites, including Facebook, just a few weeks earlier.

Things started to get even more interesting when, on April 21, 2010, Facebook announced two new applications: "instant personalization" and "open graph."

Instant personalization shares a veritable sea of Facebook users' personal information with third-party websites automatically, without seeking users' consent. Its aim is to personalize users' experience on other websites, taking into account their likes and dislikes, interests, hobbies, political affiliations, religious views, socio-economic status and mountains of other personal information they share with their friends on Facebook. For some people, instant personalization is a desirable new feature because it automates the process of stroking their preferences when they visit a new website. For others, who don't want to unknowingly share their information with marketers and other corporate strangers, it's not a feature, but a serious privacy bug.

Facebook has characterized its second new application, Open Graph, as "transformative" -- allowing all participating websites and marketers to build a web that is "smarter, more social, more personalized and more semantically aware." These applications comport well with Facebook's stated goal: to build "a web where the default is social."

Much to the chagrin of my friends who work at Google, I think of Open Graph as Facebook's answer to Google Streetview -- just as the relationship between physical objects on the street can be mapped by way of special cameras and software that can stitch the pieces together in a seamless whole, so too can the data points of people's personal information and preferences on Facebook be connected in ways that create a larger graphical understanding of their social landscape. Powerful stuff.

The problem is that Open Graph lacks any of the privacy safeguards that Google Streetview had carefully put in place. With it, Facebook is charting the maps of our social lives.

Perhaps even more troubling is the fact that Facebook snuck these new applications in the back door through a process that presumes people are fine with all of this, though allowing users to opt-out as a reward for successfully navigating an extremely convoluted and cumbersome series of clicking links and un-clicking checked boxes. When they did this they must have known full well that the vast majority of people will never figure out how to opt-out.

Within a week of the roll-out of these new applications, four U.S. Senators responded with a letter and news conference expressing their concerns about Facebook's confusing and unfair practices. In the weeks since, we have seen a leaked 2003 instant message from Zuckerberg to a friend in which Zuckerberg apparently mocked all Facebook users at the time for trusting him with their personal information. "Dumb f*#ks," he called them.

No doubt, these recent events in the U.S. played a role in Zuckerberg's cancelled 26th birthday party and the expedited roll-out of the new privacy settings on Wednesday. They have also spurred the development of a potential competitor for Facebook called Diaspora and the emergence of Quit Facebook Day, coming up on May 31.

Interesting though all of this may be, my main contention is this. In the two years since the original CIPPIC complaint, Facebook has done nothing to improve privacy in its default settings.

The fix is really simple. Start with the presumption that people only want to share with their friends, build that in as the default across the board and give everyone who wants to share beyond that a clear and user-friendly interface for managing their settings.

On Wednesday, Facebook offered up the user-interface only, leaving the default settings tuned in favour of exposure rather than privacy. To me, ignoring the default settings for more than two years demonstrates Facebook's lack of true commitment to privacy.

With all due respect, I don't buy Zuckerberg's self-aggrandizing and disingenuous rhetoric about "trying to make the world a more open place by helping people connect and share."

The devil is in the defaults. As Canada's government continues to contemplate improvements to Canadian privacy law, I think it is time to enact a set of legal provisions that prescribes what others and I call "privacy by default."

Ian Kerr holds the Canada Research Chair in Ethics, Law and Technology and is a member of the University of Ottawa's Centre for Law, Technology and Society.